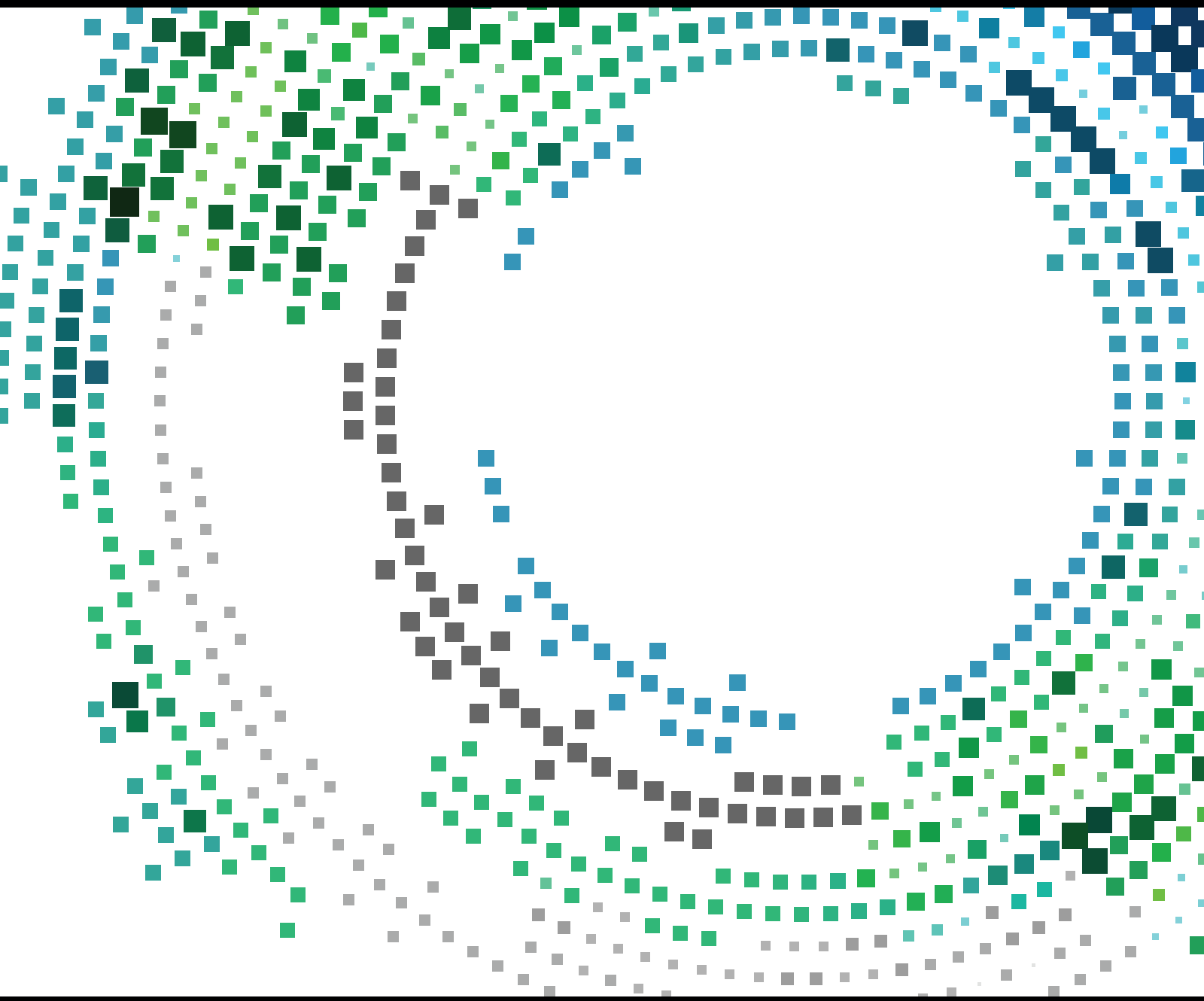
Mobile Information Systems

Research on Efficient Data Forwarding in Vehicular Networks

Lead Guest Editor: Syed H. Ahmed
Guest Editors: Ali K. Bashir, Mohamed Elhoseny, Wael Guibene, and Safdar H. Bouk



Research on Efficient Data Forwarding in Vehicular Networks

Mobile Information Systems

Research on Efficient Data Forwarding in Vehicular Networks

Lead Guest Editor: Syed H. Ahmed
Guest Editors: Ali K. Bashir, Mohamed Elhoseny, Wael Guibene, and Safdar H. Bouk

Editorial Board

Contents

Hindawi
Mobile Information Systems
Volume 2019, Article ID 2353478, 2 pages
https://doi.org/10.1155/2019/2353478

Editorial

Research on Efficient Data Forwarding in Vehicular Networks

Syed Hassan Ahmed,[1] **Ali K. Bashir**,[2] **Mohamed Elhoseny**,[3] **Wael Guibene**,[4] **and Safdar Hussain Bouk**[5]

[1]*Georgia Southern University, Statesboro, GA 30460, USA*
[2]*Manchester Metropolitan University, Manchester M15GD, UK*
[3]*Mansoura University, El Gomhouria St, Mansoura, Dakahlia 35516, Egypt*
[4]*Amazon Lab126, Sunnyvale, CA 94089, USA*
[5]*DGIST, Daegu 41566, Republic of Korea*

Correspondence should be addressed to Syed Hassan Ahmed; sh.ahmed@ieee.org

Received 16 April 2019; Accepted 17 April 2019; Published 2 May 2019

Recent advances in vehicular communications and intelligent transportation systems (ITS) intend to trim down the fuel expenditure by avoiding congested traffic, enhancement of traffic safety, and initiating new application, that is, mobile infotainment [1]. Commonly, we have three types of vehicle communication models, that is, vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-roadside (V2Rs) communications [2]. Due to the rapid growth in this field, many research constraints need to be addressed, for example, reliability and latency, appropriate scalable design of MAC and routing protocols, performance and adaptability to the changes in environment (node density and oscillation in network topology), and evaluation and validation of vehicular communication protocols under the umbrella of coherent assumptions using simulation methodologies.

This special issue aimed to emphasize the latest achievements to identify the robust and efficient data forwarding techniques in vehicular communications and similar networks. We believe that the high-quality accepted papers in this special issue will add new insight to the readers' knowledge.

The Internet of Vehicles (IoV) is a substrate for safe, efficient, and green ITS. Due to highly dynamic nature of the network, the reliable and timely dissemination of the safety and warning information, in basic safety messages (BSM), is a challenging task [3]. In the first paper entitled "A Local Information Sensing-Based Broadcast Scheme for Disseminating Emergency Safety Messages in IoV," the authors proposed the Local Topology Information Sensing technology-based broadcast (LISCast) protocol to address the slow response and local broadcast storm problem by employing the probability-based forwarding scheme. The results show that the proposed LISCast achieves low delay and alleviates broadcast redundancy in dynamic topology vehicular network. Furthermore, the authors in "A Heterogeneous IoV Architecture for Data Forwarding in Vehicle to Infrastructure Communication" proposed the architecture that ensures the reliable data transmission in IoV. As modern vehicles are equipped with multiple wireless interfaces, e.g., Wireless Access in Vehicular Environment (WAVE), Long-Term Evolution (LTE), Long-Range Wireless Fidelity (Wi-Fi), and so forth, the proposed architecture provides mechanism to select best wireless interface among the available ones to ensure data communication reliability and seamless connectivity, avoiding single point of failure. The next paper entitled "A Novel Method for Predicting Vehicle State in Internet of Vehicles" in the IoV domain of this special issue proposed the vehicle state prediction scheme. The authors used a decision tree method to recognize the driving behaviour and vehicle sate on different road segments.

In addition to the IoV related papers [4], there are some contributions by the authors that address communication problems in the specific vehicular communication scenarios, e.g., V2V, V2I, and V2X. For example, in the paper entitled "Integrated Packet Classification to Support Multiple Security Policies for Robust and Low Delay V2X Services," the authors proposed the memory efficient packet classification

algorithm for V2X scenario. The packet classification is necessary to avoid sophisticated cyber attacks that impact on the data delivery delay constraint. The authors in "Predicting the Route the Longest Lifetime and the Data Packet Delivery Time between Two Vehicles in VANET" proposed two schemes that predict packet delivery time by utilizing the vehicle density and vehicles' mobility information to determine the route lifetime for highway traffic scenarios. The performance and quality of data communication in vehicular network deteriorates due to intrinsic channel characteristics such as multipath fading and shadowing. Therefore, the authors in "Rate Adaptation Mechanism with Available Data Rate Trimming and Data Rate Information Provision for V2I Communications" proposed two data rate adaptation schemes, available data rate trimming and data rate information provision schemes, to increase communication performance of the network. The authors in the paper entitled "CMD: A Multichannel Coordination Scheme for Emergency Message Dissemination in IEEE 1609.4" proposed the safety message information disseminate scheme over multiple IEEE 1609.4 channels, control channel (CCH), and the service channels (SCHs).

In addition to the conventional networking technologies, authors have also investigated the future Internet architectures in vehicular networks. The authors in "Security & Privacy Issues in Vehicular Named Data Networks: An Overview" overviewed the security and privacy issues in Named-Data Networking (NDN) enabled vehicular networks. The NDN-based vehicular networks are at their earlier stage and require more detailed investigation. To this regard, authors in the work entitled "Cluster-Based Device Mobility Management in Named Data Networking for Vehicular Networks," proposed the cluster-based device mobility management (CB-DMM) system for NDN-based vehicular networks. Each cluster is managed by the cluster head, which maintains the route information for its cluster members. The content information is shared by the content producer, and this content location information is mapped and managed by the clusters. The content requesting Interest messages are forwarded based on that mapping information in the network. The results showed that the proposed CB-DMM has high content request satisfaction ratio.

Furthermore, in the paper entitled "Smartwatch-Based Legitimate User Identification for Cloud-Based Secure Services," the authors have proposed the smart watch-based activity recognition and gait-based legitimate user identification based on the time and frequency domain sensory information of user activity. In the next work, "A New Distance Vector-Hop Localization Algorithm Based on Half-Measure Weighted Centroid," a new distance vector-hop localization algorithm using the half-measure weighted centroid for wireless sensor networks. Using two-dimensional position distribution, the algorithm first constructs the approximate communication radius and network connectivity. The algorithm then corrects the distance between the beacon node and its neighbours to increase the jump distance accuracy to compute the optimized shortest path.

In the last paper of this special issue, the authors have proposed a Bloch chain-based incentive mechanism for data storing wireless sensor nodes in the paper entitled "Incentive Mechanism of Data Storage Based on Blockchain for Wireless Sensor Networks." More data-storing nodes receive more incentive because they offer their limited storage resource for other nodes in the network. The prime objective of the proposed scheme is to conserve the storage space of the wireless sensor nodes.

Conflicts of Interest

The guest editors declare that they have no conflicts of interest.

Acknowledgments

The guest editors would like to sincerely thank all the authors who submitted their contributions in our special issue. They would also like to thank all our reviewers and sincerely acknowledge their contribution that has been substrate to the success of this special issue.

Syed Hassan Ahmed
Ali K. Bashir
Mohamed Elhoseny
Wael Guibene
Safdar Hussain Bouk

References

[1] C. A. Kerrache, N. Lagraa, R. Hussain et al., "TACASHI: trust-aware communication architecture for social internet of vehicles," *IEEE Internet of Things Journal*, p. 1, 2018.

[2] S. H. Bouk, S. H. Ahmed, D. Kim, K.-J. Park, Y. Eun, and J. Lloret, "LAPEL: hop limit based adaptive PIT entry lifetime for vehicular named data networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 5546–5557, 2018.

[3] M. F. Majeed, S. H. Ahmed, and M. N. Dailey, "Enabling push-based critical data forwarding in vehicular named data networks," *IEEE Communications Letters*, vol. 21, no. 4, pp. 873–876, April 2017.

[4] J. Chen, G. Mao, C. Li, and D. Zhang, "A topological approach to secure message dissemination in vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–14, 2019.

Hindawi
Mobile Information Systems
Volume 2019, Article ID 3910127, 9 pages
https://doi.org/10.1155/2019/3910127

Research Article

Rate Adaptation Mechanism with Available Data Rate Trimming and Data Rate Information Provision for V2I Communications

Shigeru Kashihara,[1] **Takemi Sahara**,[1] **Shigeru Kaneda**,[2] **and Chikara Ohta**[3]

[1]*Nara Institute of Science and Technology, Ikoma, Nara 6300192, Japan*
[2]*Space-Time Engineering, LLC, Rolling Hills Estates, CA, USA*
[3]*Kobe University, Kobe, Hyogo 6578501, Japan*

Correspondence should be addressed to Shigeru Kashihara; shigeru@is.naist.jp

Received 5 October 2018; Accepted 26 March 2019; Published 15 April 2019

Guest Editor: Mohamed Elhoseny

We study a rate adaptation mechanism for improving communication performance between a connected vehicle and a roadside unit (RSU) using Wi-Fi during movement in a vehicle-to-infrastructure (V2I) environment. Wi-Fi communication provides various attractive services to connected vehicles during movement. However, as a connected vehicle is generally moving at high speed, the communication performance with an RSU that works as an access point is degraded because wireless link quality fluctuates abruptly and continuously. We then propose a rate adaptation mechanism employing the following two main features to mitigate such deterioration in communication performance: available data rate trimming and data rate information provision. To alleviate degradation of communication, the former avoids usage of excessively low data rates and the latter then provides data rate information suitable for channel quality from a dataset of adequate data rates based on the vehicle's location and speed. However, the data rate information provided from a dataset may not always be appropriate because of various indefinite factors such as multipath fading and shadowing. Thus, the proposed method also employs a measurement-based function to compensate for such a drawback of the dataset. Simulation experiments evaluate communication performance for 10, 60, and 100 km/h in single-vehicle and multiple-vehicles cases. Simulation results showed that the proposed method overall provides superior communication performance in situations involving more than one vehicle, in comparison with existing counter- and sample-based methods.

1. Introduction

With the goal of providing attractive services such as safety information, traffic efficiency management, and entertainment services for connected vehicles, intelligent transport systems (ITSs) are being developed at a fast pace [1]. A network component that connects a vehicle with other vehicles and with intelligent road infrastructures is essential for realizing an ITS. At present, vehicles have communication equipment, and advanced multimedia and infotainment services are about to start via the Internet [2].

As depicted in Figure 1, introducing edge computing [3] to vehicular networks is essential for providing attractive services such as data offloading [4] to connected vehicles. A connected vehicle creates data of various types and sizes and sends them to receive the services from an edge node or a server during movement. After receiving data, the edge node or server then provides appropriate services to the connected vehicle based on the situation analyzed from the data received. To provide such services, vehicle-to-infrastructure (V2I) communication is necessary for gathering a variety of information like the vehicle's position, speed, points of origin and destination, image data, and so on.

In V2I, the IEEE 802.11 series [5] is assumed to be employed for the communication media [6]. However, as a connected vehicle is moving at high speed, it may not have enough time to communicate with a roadside unit (RSU) that works as an access point (AP), because the coverage of an AP is relatively small. Also, in a high-mobility situation, it

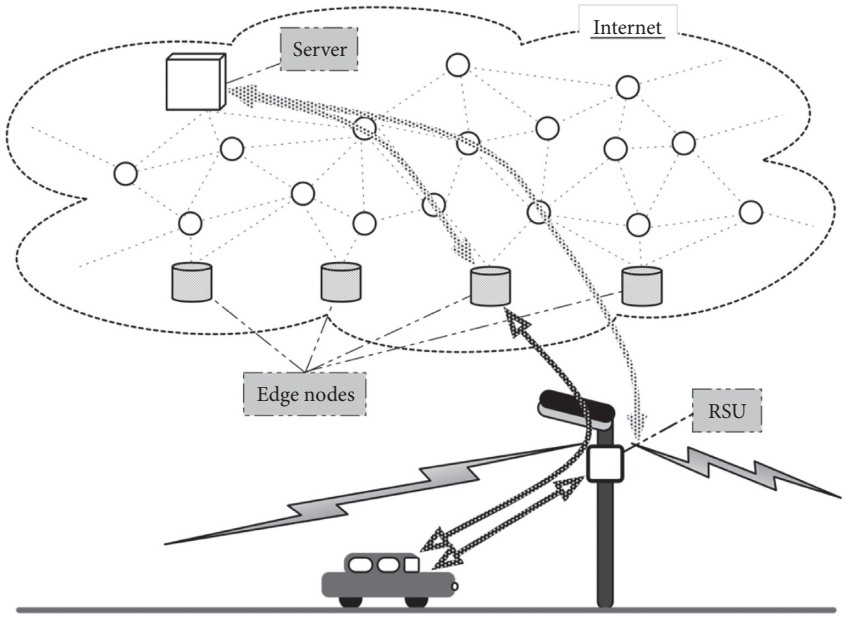


Figure 1: Communication between a connected vehicle and an RSU.

is difficult to enhance throughput due to sudden and continuous fluctuations in wireless channel quality. Therefore, improving the communication performance between a connected vehicle and an RSU is essential for providing various services.

In the above situation, as the connected vehicle communicates with single-hop RSUs or small-hops edge nodes, not with a remote server, it is essential to improve communication performance between a connected vehicle and an RSU. This paper, therefore, focuses on a rate adaptation mechanism as one approach to improving such communication performance in a high-mobility situation. Although a rate adaptation mechanism aims to set an appropriate data rate for wireless link conditions during movement, IEEE 802.11 [5] has not standardized a rate adaptation mechanism, and the mechanism, therefore, depends on implementation matters. Moreover, Wi-Fi communication generally employs multiple data rates (e.g., eight types of data rate on IEEE 802.11p) to provide better throughput for changes of channel quality, and each data rate is adjusted by channel quality measurement. However, as Wi-Fi communication was not designed to be employed in a high-mobility situation, it is difficult to follow rapidly fluctuating channel conditions at short intervals.

In this paper, to select an appropriate data rate for changes of channel quality, we propose a rate adaptation mechanism that has the following new two features: available data rate trimming and data rate information provision. Available data rate trimming alleviates the degradation of communication performance by reducing usage of excessively low data rates because a low data rate consumes more communication time than a high data rate. Also, the provision of data rate information from a dataset supplies adequate data rates for a vehicle's locations, without any measurement. However, the dataset may include erroneous data rate information for the situation. If the data rate provided from the dataset is not acceptable, the proposed method also utilizes a measurement-based function to mitigate the effects of such a problem. In summary, the significant contributions of our work to improve V2I communication performance in a high-mobility environment are as follows:

(i) Employing higher data rates by trimming regular data rates

(ii) Providing adequate data rate information from a dataset based on a vehicle's information

(iii) Cooperating dataset- and measurement-based functions

We also evaluate the communication performance of the proposed method through simulation experiments to show the effectiveness of the proposed method.

The remainder of the paper is organized as follows: Section 2 surveys existing research work on rate adaptation mechanisms. Section 3 discusses the communication performance of the existing rate adaptation mechanisms. Section 4 presents our proposed method, and Section 5 shows the results of the performance evaluation via simulations. Section 6 provides concluding remarks.

2. Related Work

As described in Section 1, rate adaptation mechanism has not been the objective in the standardization of IEEE 802.11 [5]. However, as a rate adaptation mechanism strongly influences communication performance over a wireless link, various rate adaptation mechanisms have been proposed to date [7–23]. In particular, communication performance is strictly dependent on the way channel quality is estimated. Thus, this section first classifies the mechanisms into counter-based and sample-based mechanisms, and we then consider other methods in a vehicular ad-hoc network (VANET) field for comparison.

Auto rate fallback (ARF) [7] and adaptive ARF (AARF) [8] are representative rate adaptation methods, and they are generally classified as counter-based mechanisms. ARF is the most straightforward mechanism, selecting the best data rate based on the numbers of continuous successful and failed transmissions. Concretely, when a sender successfully transmits a data frame ten consecutive times, it raises the current transmission rate to the next higher transmission rate. Conversely, when data frame transmission fails twice in succession, the current transmission rate is dropped to the next lower transmission rate. To achieve this, the sender counts the number of successful and failed data frame transmissions to estimate channel quality and changes the transmission rate when the count reaches the predetermined threshold.

Onoe [16, 17], SampleRate [16], and Minstrel [17, 18] are representative sample-based mechanisms. In the sample-based mechanism, to estimate channel quality, a sender employs statistical information such as retransmission rate, packet error rate, and throughput based on a sliding window process. For instance, in Onoe, the sender measures the number of data frame retransmissions within a window time (e.g., one second) and then compares the measurement result with a predetermined rate. If the result is 10% or less, a credit counter is increased by one. On the one hand, the credit counter is decreased by one if the result is 10% or more. When the credit counter reaches ten points, the sender moves the transmission rate up to the next higher one. If the sender experiences failed data frame transmission of over 50%, the transmission rate is moved down to the next lower one.

Also, in [19–21] a signal-to-noise ratio (SNR) is utilized, but it is difficult to obtain accurate SNR values in a practical environment. In [13] a threshold optimization algorithm for a rate adaptation mechanism that employs up/down threshold is proposed, and in [14] a rate adaptation algorithm that uses short-term loss ratio and an adaptive RTS filter is designed and implemented. The above approaches provide good communication performance for an environment where a sender and a receiver are stationary. However, if the sender moves at high speed like a vehicle, it is difficult to estimate changes of channel quality and set an appropriate transmission data rate based on the measurement result, because the measured channel quality may be outdated for the channel quality at the present location.

We describe rate adaptation methods focusing on a vehicular ad-hoc network (VANET). In [22] database for providing information of adequate data rate based on information of vehicle's location, i.e., location, velocity, and density, similar to with one of our approaches, is employed, but it may be difficult to obtain the density information of surrounding vehicles. The studies [9–12, 23] need parameter adjustments beforehand for particular environments, but such prior adjustments are difficult to apply in various situations. Besides, in [24] existing rate adaptation algorithms in vehicular networks with IEEE802.11p are evaluated, but it shows only that the communication performance of constant bit rate (CBR) for them via ns-3 simulations. As ITS including edge computing provides multiple services such as safety information, traffic efficiency management, and entertainment services to a connected vehicle, it is significant to improve the communication performance between a connected vehicle and an RSU. In this study, we, therefore, investigate a rate adaptation method that does not require such prior adjustments and consider the communication performance of UDP and TCP traffics for multiple services provided.

3. Communication Performance of Existing Rate Adaptation Mechanisms

This section presents the communication performance of existing rate adaptation mechanisms through simulation experiments. We use ARF and Onoe as representative counter-based and sample-based mechanisms, respectively, because they have been widely deployed in products. Section 3.1 describes the simulation model and parameters. Section 3.2 shows communication performance of file transfer protocol (FTP) and CBR applications for each mechanism at three speeds, i.e., 10, 60, and 100 km/h.

3.1. Simulation Model and Parameters. As depicted in Figure 2, in the simulation model, a connected vehicle passes by an RSU, an AP of a wireless communication infrastructure, in a straight line at three constant speeds of 10, 60, and 100 km/h. The simulation model also employs FTP and CBR applications to evaluate communication performance. The FTP application tries to send 2048 MByte data from the vehicle to the RSU, while the CBR application tries to send one 1500-byte packet per 222 μs from the vehicle to the RSU. The RSU is assumed to employ IEEE 802.11p, which provides eight data rates (3, 4, 5, 6, 9, 12, 18, 24, and 27 Mbit/s). The transmission powers of the RSU and the vehicle are set to 20 dBm, and the two-ray ground reflection model and Nakagami-m fading model are employed as propagation models. Table 1 summarizes the above parameters. Note that the simulation experiments work on Scenargie® Simulator (Space-Time Engineering, LLC, "Scenargie® Simulator," https://www.spacetime-eng.com/en/products), a commercial product for analyzing and evaluating wireless communications and networking systems.

3.2. Communication Performance during Movement. The simulation experiments investigate how much communication performance the existing rate adaptation mechanisms can obtain at the three movement speeds. Figure 3 shows the results of FTP and CBR applications for ARF and Onoe at the speed of 60 km/h, as an example. In these simulation results, the best value (Best) means the largest amount of data that the receiver could receive as data packets per 100 ms among 100 simulation experiments for each transmission rate. This is calculated as follows: we first have 100 simulation trials for eight data rates using the same model. The best performance per 100 ms is then extracted from 800 simulation results, that is, the best value is constructed from the best performance. In the results of ARF and Onoe, we employ the median value for 100 simulation experiments.

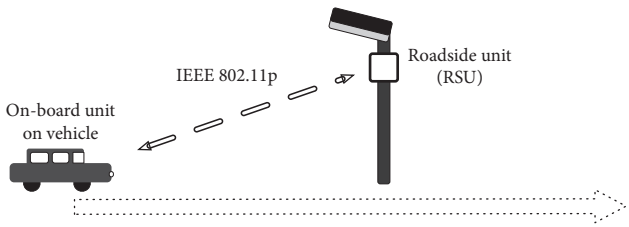


Figure 2: Simulation model.

Table 1: Simulation parameters.

Vehicle's speed	10, 60, 100 km/h	
Traffic model	FTP: sends a 2048-MByte file CBR: sends a 1500-byte packet at intervals of 222 μs	
Wireless medium	IEEE 802.11p (data rate: 3, 4.5, 6, 9, 12, 18, 24, and 27 Mbit/s)	
Rate adaptation mechanism	ARF (counter-based)	Onoe (sample-based)
Transmission power	20 dBm	
Propagation model	Two-ray ground reflection model Nakagami-m fading model	
Number of simulation trials	100	

Compared with the best value, we can see that ARF and Onoe cannot achieve a sufficient data rate at the beginning and the end of the communication. From these results, we infer that ARF is excessively downgrading the data rate used. As described in Section 2, the threshold in ARF for downgrading is very low, i.e., two consecutive failures, but that for upgrading is relatively high, i.e., ten consecutive successes. It can therefore be said that ARF sensitively reacts to lost frames. On the other hand, in Onoe, as the number of data frame retransmissions per second must be measured to estimate channel quality, the measurement period makes suitable channel estimation difficult.

From the above comparison between ARF and Onoe, we can say that ARF obtains the better performance when the vehicle is near the RSU, while Onoe cannot raise the performance to a higher level even if the vehicle is near the AP. This is because, since the change in data rate in ARF is based on the success or failure of frame transmission, ARF can change the data rate relatively fast. However, it does not always follow channel quality. On the other hand, since the changes in data rate in Onoe depend on measurement, Onoe needs more time to decide a change of data rate than ARF. Thus, it is difficult to make use of higher data rates by the conservative change policy of the rate adaptation mechanisms.

Table 2 presents the simulation results of FTP and CBR communications at three speeds of 10, 60, and 100 km/h. Note that room for improvement means the proportion of actual data received for the best value. From the results, we can see that although ARF provides better performance than Onoe for a moving vehicle, both mechanisms have more room for improvement for higher speed.

4. Rate Adaptation Mechanism

The previous section showed that the existing rate adaptation mechanisms have room for improvement in communication performance during movement. We now propose a rate adaptation mechanism employing the following two features to improve the performance: trimming the number of available data rates to four and using a dataset to provide data rate information based on a vehicle's location and speed. Section 4.1 outlines the design overview of our proposed method. Sections 4.2 and 4.3 then explain the above two features of the proposed rate adaptation mechanism. Sections 4.4 and 4.5 additionally describe two change policies for transmission data rate, with and without using information from the dataset.

4.1. Design Overview. As ARF and Onoe adapt the data rate depending only on past measurement information, it is difficult to use an appropriate data rate for the present channel quality during movement at high speed, that is, the measurement information for these existing methods may be stale when current channel quality is being estimated, especially at high speed. Besides, it is almost impossible to make an accurate estimation because the channel quality is changing continuously due to various indeterminate factors. To choose a data rate that is as appropriate as possible for the present channel quality, our proposed method therefore assumes the use of a dataset that provides data rate information based on a vehicle's speed and location.

Under this assumption, the dataset on an RSU collects three-tuple information of the vehicle's speed, location, and data rate used, and it determines an appropriate data rate based on the information collected. As a vehicle obtains RSU information via the Internet beforehand or through a local dynamic map (LDM) service [25], it can choose an appropriate data rate based on the dataset. However, as details of designing and analyzing the dataset constitute another research topic, they are beyond the scope of the present paper. Therefore, we assume here that the dataset has been created from measurement data collected in advance.

Figure 4 depicts the design overview of the proposed method. The existing rate adaptation mechanisms choose a transmission data rate based only on information that can be obtained within the MAC layer. On the other hand, as the proposed method utilizes a vehicle's speed and location information for selecting the data rate, the MAC layer needs to obtain context information (CI) from the Application layer. To access the CI on the Application layer from the MAC layer, a shared memory is employed. In this approach, the Application layer writes CI to the shared memory, while the MAC layer reads the CI from the shared memory and obtains an appropriate data rate based on the CI from the dataset.

However, it is too difficult to make a complete dataset because channel quality is affected by various invisible factors. In the proposed method, when a data rate selected based on the dataset is not appropriate for the channel

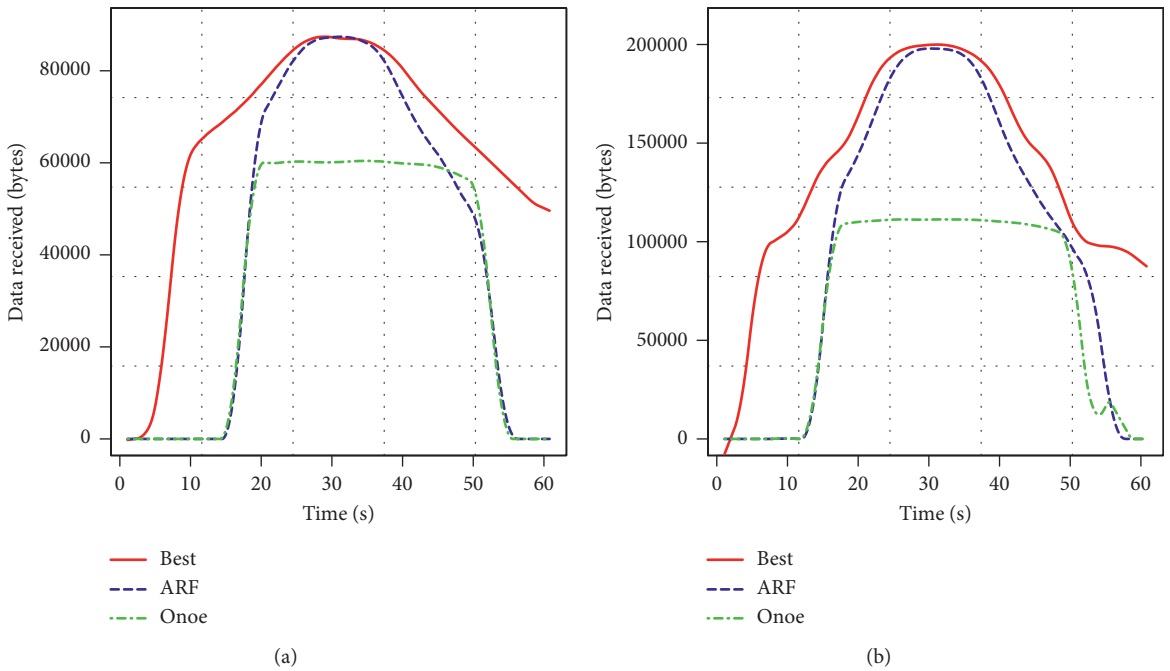


Figure 3: Communication performance of FTP and CBR for ARF and Onoe. (a) FTP. (b) CBR.

Table 2: Communication performance of FTP and CBR for ARF and Onoe.

	10 km/h		60 km/h		100 km/h	
	ARF	Onoe	ARF	Onoe	ARF	Onoe
FTP						
Best data received (MB)	222		37.2		21.9	
Data received (MB)	166	133	24.6	19.9	12.7	10.5
Room for improvement (%)	25.3	40.0	33.9	46.5	42.0	52.0
CBR						
Best data received (MB)	503		78.8		45.9	
Data received (MB)	374	259	57.2	38.9	31.2	21.7
Room for improvement (%)	25.6	48.5	27.4	50.6	32.0	52.7

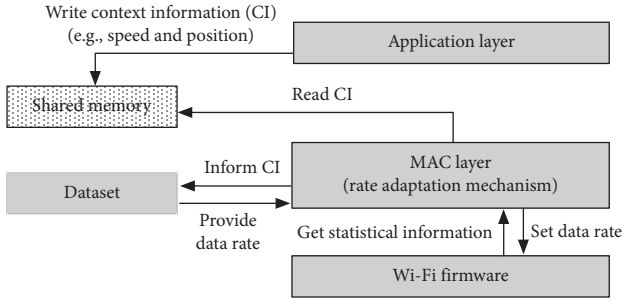


Figure 4: Design overview of the proposed method.

quality, the proposed method also employs data rate selection based on measurement information.

4.2. Dataset for Selecting a Data Rate. As mentioned in Section 2, the existing methods have several drawbacks for adapting a data rate for various situations. First, they raise and lower the data rate stepwise based on measurement information. In a movement environment where channel quality is fluctuating continuously and abruptly, as it is impossible to estimate channel quality without any delay, the estimated result may be obsolete. Hence, even if there were an opportunity to use a higher data rate, they might continue to use a lower data rate. Second, at the beginning of communication, since the channel quality is unknown, it takes time to evaluate the present channel quality and select a data rate. Besides, the data rate used begins with the lowest data rate. Thus, in Wi-Fi communication involving shared media, since the use of excessively low data rate causes the communication performance of the whole Wi-Fi system to degrade, an appropriate data rate must be selected promptly.

We therefore propose a rate adaptation mechanism based on a dataset. As described above, the dataset is assumed to consist of three-tuple information of the vehicle's location, speed, and data rate, that is, a vehicle can obtain data rate information suitable for its location and speed from the dataset. Employing the dataset, the proposed method contributes to reducing the use of an excessively low data rate, because it can select a suitable data rate without any delay of measurement. However, if inappropriate information is

provided, many frames may be frequently lost. To avoid such deterioration of communication performance, when a data rate selected is not suitable for the present channel quality, the proposed method switches to a data rate selection based on measurement. For this research, we employ a dataset that has collected and analyzed data beforehand.

4.3. Available Data Rate Trimming. Existing rate adaptation methods usually use all data rates, i.e., eight data rates for 802.11p. On the other hand, the proposed method reduces the available data rates. Thus, in the case of 802.11p, it employs only four data rates among eight data rates. Figure 5 shows the relationship between data received and data rate from an analysis of the results in Section 3. The figure plots data rate used for the best value in the CBR graph of Figure 2 and shows that data rates used are almost the top four data rates, i.e., 12, 18, 24, and 27 Mbit/s. Consequently, the proposed method employs only these four data rates.

Reducing the number of data rates leads to the following advantage. If all data rates are employed, it becomes more difficult to follow the present channel quality because of the time required to retransmit frames and the long occupancy of a channel when frame loss occurs in a low data rate. On the other hand, as shown in Figure 5, in the proposed method, as low data rates are not employed by trimming the number of available data rates, the opportunities for utilizing high data rates are increased, that is, the proposed method is expected to improve communication performance.

4.4. Inappropriate Data Rate Information from Dataset. The proposed method primarily provides suitable data rate information based on CI and a dataset. However, the data rate information does not always give an appropriate data rate due to various indefinite factors such as multipath fading and shadowing. Also, in the early phase of the system, the dataset itself may not be deployed at all locations.

The proposed method mainly utilizes data rate information suggested from the dataset to determine a suitable data rate. While employing this data rate, if a fixed number of consecutive frames are lost, the proposed method additionally prepares another data rate that is lower than the data rate provided by the dataset and then uses both of them alternately to transmit frames. This is because the method is designed to avoid unsuitable deterioration of the data rate due to burst lost frames. For instance, if a burst loss occurs during movement, the duration of the loss cannot be predicted. Also, if the data rate is immediately downgraded in reaction to the loss, this will cause unnecessary channel occupation due to the usage of a lower data rate, which might lead to the degradation of communication performance.

To alleviate the effect of such degradation, the proposed method uses two data rates and also brings a flexible data rate selection by utilizing the measurement result of channel quality. While it is employing two data rates, the proposed method records information regarding the success and failure of frames transmitted from each data rate and the elapsed time for transmission. This information is kept as an exponential moving average.

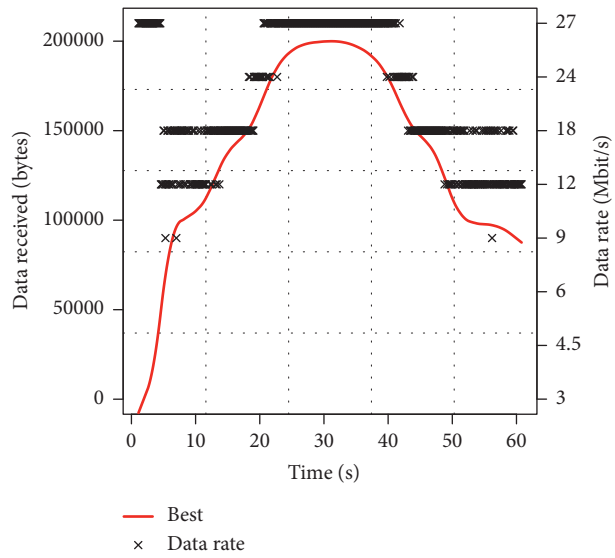


Figure 5: Relationship between data received and data rate in the best value result.

In communication for a certain period using two data rates, if only the higher data rate of two data rates experiences loss, the proposed method switches to using only the lower data rate for the communication. Besides, if both data rates experience loss, the data rates in use are downgraded to the next lower data rate. On the other hand, from a measurement result obtained during a certain period, if the number of frames lost at both data rates is lower than a predetermined threshold, the loss of consecutive frames is determined to be an accidental event, and the data rate in use is then switched to the higher data rate. Algorithm 1 illustrates the flexible data rate selection method described above.

4.5. Data Rate Selection with a Dataset and Measurement. A dataset may not always be able to provide adequate data rate information, and also the dataset may not be distributed in the early stage. To adequately work in such situations, the proposed method is equipped with a data rate selection based on measurement of channel quality, in addition to the dataset.

The proposed method employs statistical information about throughput as a measurement metric for channel quality. The throughput is calculated as follows:

$$\text{throughput} = \frac{\text{successfully transmitted bytes (TxBytes)}}{\text{occupation period for a channel by a data rate (airtime)}}, \quad (1)$$

```
(1) use data rate based on dataset
(2) IF a fixed number of consecutive frames are lost THEN
(3)    use two data rates (the current data rate and a data rate lower than the current data rate)
(4)    WHILE using two data rates
(5)       measure lost frames for each data rate
(6)       IF both data rates have no lost frames THEN
(7)          use the higher data rate
(8)       ELSE IF only the higher data rate has lost frames THEN
(9)          use the lower data rate
(10)      ELSE IF both data rates have lost more frames than a predetermined threshold THEN
(11)         use a third data rate lower than the lower data rate
(12)      ELSE IF both data rates have lost fewer frames than a predetermined threshold THEN
(13)         use the higher data rate
(14)      ENDIF
(15)   ENDWHILE
(16) ENDIF
```

Algorithm 1: Flexible data rate selection.

where TxBytes means the number of bytes for successfully transmitted frames within a certain period at a given data rate, while airtime denotes an accumulation time from sending a data frame to receiving an ACK frame for the data frame sent.

The proposed method keeps statistical throughput information for each data rate separately. After a certain period for a measurement, it selects the data rate that has the largest throughput as a data rate based on measurement information. Then, by comparing with a data rate based on the dataset and the measurement, if they both provide the same data rate or if the data rate based on the measurement is lower than that of the dataset, the proposed method switches back to the control based on the dataset.

5. Performance Evaluation

This section provides communication performance comparisons for the proposed method and the existing methods ARF and Onoe. Sections 5.1 and 5.2 show results of communication performance of both FTP and CBR applications for 10, 60, and 100 km/h in single- and multiple-vehicle cases, respectively.

5.1. Result for a Single Vehicle. The evaluation employs the same simulation model, with the parameters explained in Section 3. In the simulation experiments, in addition to ARF and Onoe, as the proposed method we employ two rate adaptation mechanisms: rate adaptation with dataset and measurement (RA-DM) and rate adaptation with dataset (RA-D). RA-DM utilizes both dataset and measurement functions, while RAD controls data selection by dataset information.

Table 3 shows the simulation results for the four methods. The evaluation shows room for improvement as the comparison metric; this means that a smaller value is approaching the best value. From the results, in the case of a single vehicle, we can see that RA-D shows the worst performance for FTP communication among the four, while it gives the best performance for CBR communication. This is because, since RA-D selects a data rate based only on the information from the dataset, it does not change the data rate in use to another data rate even if frame loss occurs. Consequently, consecutive frame loss leads to packet loss and delay, and then FTP performance degrades due to the retransmission control of transmission control protocol (TCP). On the other hand, in CBR communication, since user datagram protocol (UDP) employed for CBR continues to send packets without retransmission control even if packet loss occurs, the CBR performance is improved to become the best of the four methods.

Table 3: Room for improvement in a single-vehicle case.

Speed	10 km/h		60 km/h		100 km/h	
Application	FTP	CBR	FTP	CBR	FTP	CBR
ARF (%)	25.5	25.7	34.0	27.5	41.7	31.9
Onoe (%)	40.0	48.5	46.4	50.7	51.8	52.6
RA-D (%)	77.2	25.2	79.9	26.5	81.4	29.9
RA-DM (%)	32.1	31.4	39.1	33.8	46.2	43.4

In the result of RA-DM, the communication performances for both FTP and CBR are better than those of Onoe, but somewhat worse than those of ARF. The result indicates that RA-DM can follow the changes in channel quality more effectively for both FTP and CBR applications than Onoe and FTP of RA-D.

5.2. Result for Multiple Vehicles. The previous result showed that the performance of ARF is somewhat higher than RA-DM. However, in environments where multiple vehicles exist, ARF may not be able to sustain that excellent performance, because an increase in the number of vehicles prolongs the waiting time to send frames due to the characteristics of shared media. To evaluate the impact of such an effect, this section evaluates simulation models involving two and ten vehicles.

The simulation model and parameters are the same as those for the case of a single vehicle. From the initial evaluation, all vehicles are assumed to be driving at the same location, time, and speed.

Table 4: Improvement ratio of RA-DM to ARF, Onoe, and RA-D in two-vehicles case.

Speed	10 km/h		60 km/h		100 km/h	
Application	FTP	CBR	FTP	CBR	FTP	CBR
RA-DM/ARF	1.52	1.00	1.57	0.95	1.43	0.92
RA-DM/Onoe	1.11	1.42	1.15	1.27	1.06	1.26
RA-DM/RA-D	2.94	1.10	2.92	1.17	2.99	1.29

Table 5: Improvement ratio of RA-DM to ARF, Onoe, and RA-D in ten-vehicles case.

Speed	10 km/h		60 km/h		100 km/h	
Application	FTP	CBR	FTP	CBR	FTP	CBR
RA-DM/ARF	2.33	3.87	2.52	3.94	2.28	3.41
RA-DM/Onoe	1.06	3.12	1.00	1.58	0.98	1.34
RA-DM/RA-D	2.67	0.91	3.26	0.85	2.90	0.77

Tables 4 and 5 show the improvement ratio for the four methods in the two- and ten-vehicles cases, respectively. Here, as the comparison metric, we define the improvement ratio calculated as follows:

$$\text{the improvement ratio of RA-DM} = \frac{\text{the number of communication bytes on RA-DM}}{\text{the number of communication bytes on}\{\text{ARF} \mid \text{Onoe} \mid \text{RA-D}\}}. \quad (2)$$

The results demonstrate that the communication performances of RA-DM are overall improved in both cases. Moreover, the result for ARF is degrading with the increase of vehicles, while that for Onoe is improving. This is because, as the waiting time to send frames is prolonged as the number of vehicles increases, ARF is late in catching up with the changes in channel quality. The reason why the result for Onoe is improving is not that Onoe follows changes in channel quality but that the number of switches in data rates is small. That is, as ARF and Onoe necessarily transmit frames in order to change the data rate that starts with the lowest data rate, it is late to follow the changes.

On the other hand, the proposed method provides the following three features in order to improve communication performance. First, it employs higher data rates by trimming regular data rates, and it can then begin with an appropriate data rate based on a database. Lastly, it prepares the data rate selection based on measurement as a countermeasure against inappropriate data rate information from the dataset.

In the one-vehicle simulation result, RA-D has the best performance for the CBR traffic model, and it also has the worst performance for the FTP traffic model. However, to adapt to TCP and UDP traffics, a rate adaptation mechanism needs to improve the communication performance for both. On the other hand, the improvement of RA-DM is lower than that of the counter-based mechanism (ARF) but higher than that of the sample-based mechanism (Onoe).

On the other hand, in the case where multiple vehicles exist, RA-DM generally has a better communication performance than counter-based and sample-based mechanisms. On the other hand, in the case of CBR for ten vehicles, RA-D outperforms RA-DM if we can know the number of vehicles, but it is difficult to estimate it. Therefore, the proposed method (RA-DM) provides superior communication performance in situations involving more than one vehicle.

6. Conclusion

In this study, to improve communication performance between a connected vehicle and RSU using Wi-Fi during movement in a V2I environment, we proposed a rate adaptation mechanism introducing the following new two approaches: available data rate trimming and data rate information provision. In the available data rate timing, the proposed method selected four data rates among the standard eight data rates to avoid usages of excessively low data rates. Also, it utilizes data rate information provided from a dataset in order to select a suitable data rate without any delay of measurement. It does not, however, work well in every situation because of various indefinite factors such as multipath fading and shadowing. To compensate for the drawbacks of the dataset, the proposed method then also employed a data rate selection based on measurement. In the simulation experiments, we investigated the FTP and CBR communication performance in single- and multiple-vehicle cases. In a single-vehicle case, RA-D shows the worst performance for FTP communication among the four methods, while it gives the best performance for CBR communication. On the other hand, RA-DM provides better communication performance for both FTP and CBR next to ARF. In two- and ten-vehicles cases, communication performance of ARF is getting worse with increasing the number of vehicles, while RA-DM overall provides superior communication performance in

situations involving more than one vehicle, in comparison with other methods.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by JSPS KAKENHI (Grant number: 18H03232).

References

[1] E. Ndashimye, S. K. Ray, N. I. Sarkar, and J. A. Gutiérrez, "Vehicle-to-infrastructure communication over multi-tier heterogeneous networks: a survey," *Computer Networks*, vol. 112, pp. 144–166, 2017.

[2] R. Coppola and M. Morisio, "Connected car: technologies, issues, future trends," *ACM Computing Surveys*, vol. 49, no. 3, pp. 1–36, 2016.

[3] K. Kai, W. Cong, and L. Tao, "Fog computing for vehicular Ad-hoc networks: paradigms, scenarios, and issues," *Journal of China Universities of Posts and Telecommunications*, vol. 23, no. 2, pp. 56–96, 2016.

[4] N. Cheng, N. Lu, N. Zhang, X. Shen, and J. W. Mark, "Vehicular WiFi offloading: challenges and solutions," *Vehicular Communications*, vol. 1, no. 1, pp. 13–21, 2014.

[5] IEEE Computer Society, *Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standards Association, IEEE Computer Society, Washington, DC, USA, 2012.

[6] E. Ahmed and H. Gharavi, "Cooperative vehicular networking: a survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 3, pp. 996–1014, 2018.

[7] A. Kamerman and L. Monteban, "WaveLAN®-II: a high-performance wireless LAN for the unlicensed band," *Bell Labs Technical Journal*, vol. 2, no. 3, pp. 118–133, 2002.

[8] M. Lacage, M. H. Manshaei, and T. Turletti, "IEEE 802.11 rate adaptation: a practical approach," in *Proceedings of the 7th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, pp. 126–134, Venice, Italy, October 2004.

[9] Q. Xia, J. Pu, and M. Hamdi, "Model-tree-based rate adaptation scheme for vehicular networks," in *Proceedings of the 2009 IEEE International Conference on Communications*, pp. 1–5, Dresden, Germany, June 2009.

[10] C. Liu, S. Liu, and M. Hamdi, "GeRA: generic rate adaptation for vehicular networks," in *Proceedings of the 2012 IEEE International Conference on Communications (ICC)*, pp. 5311–5315, Ottawa, ON, Canada, June 2012.

[11] P. Shankar, T. Nadeem, J. Rosca, and L. Iftode, "CARS: context-aware rate selection for vehicular networks," in *Proceedings of the 2008 IEEE International Conference on Network Protocols (ICNP)*, pp. 1–12, Orlando, FL, USA, October 2008.

[12] J. He, H. Liu, P. Cui et al., "Design and experimental evaluation of context-aware link-level adaptation," in *Proceedings of the 2012 Proceedings IEEE INFOCOM*, pp. 2726–2730, Orlando, FL, USA, March 2012.

[13] Y. Song, X. Zhu, Y. Fang, and H. Zhang, "Threshold optimization for rate adaptation algorithms in IEEE 802.11 WLANs," *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 318–327, 2010.

[14] S. H. Y. Wong, H. Yang, S. Lu, and V. Bharghavan, "Robust rate adaptation for 802.11 wireless networks," in *Proceedings of the 12th Annual International Conference on Mobile Computing and Networking (MobiCom '06)*, pp. 146–157, Los Angeles, CA, USA, September 2006.

[15] S. Biaz and S. Wu, "Rate adaptation algorithms for IEEE 802.11 networks: a survey and comparison," in *Proceedings of the 2008 IEEE Symposium on Computers and Communications*, pp. 130–136, Marrakech, Morocco, July 2008.

[16] J. C. Bicket, *Bit-Rate Selection in Wireless Networks*, Massachusetts Institute of Technology, Cambridge, MA, USA, 2005.

[17] Linux Wireless, September 2018, https://wireless.wiki.kernel.org/en/developers/documentation/mac80211/ratecontrol/minstrel.

[18] D. Xia, J. Hart, and Q. Fu, "Evaluation of the minstrel rate adaptation algorithm in IEEE 802.11g WLANs," in *Proceedings of the 2013 IEEE International Conference on Communications (ICC)*, pp. 2223–2228, Budapest, Hungary, June 2013.

[19] J. Zhang, K. Tan, J. Zhao, H. Wu, and Y. Zhang, "A practical SNR-guided rate adaptation," in *Proceedings of the IEEE INFOCOM 2008—The 27th Conference on Computer Communications*, pp. 2083–2091, Phoenix, AZ, USA, April 2008.

[20] A. Vlavianos, L. K. Law, I. Broustis, S. V. Krishnamurthy, and M. Faloutsos, "Assessing link quality in IEEE 802.11 wireless networks: which is the right metric?," in *Proceedings of the 2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1–6, Cannes, France, September 2008.

[21] G. Judd, X. Wang, and P. Steenkiste, "Efficient channel-aware rate adaptation in dynamic environments," in *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services—MobiSys '08*, pp. 118–131, Breckenridge, CO, USA, June 2008.

[22] J. Xiong, C. Chen, X. Guan, C. Hua, and LRRA, "Location-related rate adaptation algorithm in IEEE 802.11p for DSRC technology in VANET," in *Proceedings of the 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, Montréal, Canada, September 2016.

[23] O. Puñal, H. Zhang, and J. Gross, "RFRA: random forests rate adaptation for vehicular networks," in *Proceedings of the 2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, pp. 1–10, Madrid, Spain, June 2013.

[24] A. Zekri and W. Jia, "Performance evaluation of rate adaptation algorithms in IEEE802.11p heterogeneous vehicular networks," in *Proceedings of the 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems, MASS*, vol. 2018, pp. 107–115, Chengdu, China, October 2018.

[25] ETSI, *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LSM)*, ETSI EN 302 895 V1.0.0 (2014-01), ETSI, Sophia Antipolis, France, 2014.

Hindawi
Mobile Information Systems
Volume 2019, Article ID 3101276, 12 pages
https://doi.org/10.1155/2019/3101276

Research Article

A Heterogeneous IoV Architecture for Data Forwarding in Vehicle to Infrastructure Communication

Hafiz Husnain Raza Sherazi,[1] **Zuhaib Ashfaq Khan**,[2] **Razi Iqbal**,[3] **Shahzad Rizwan**,[2] **Muhammad Ali Imran**,[4] **and Khalid Awan**[2]

[1]*Department of Electrical and Information Engineering, Politecnico di Bari, 70125 Bari, Italy*
[2]*COMSATS University Islamabad, Attock Campus, Kamra Road, Attock, Pakistan*
[3]*American University in the Emirate, Dubai International Academic City, Dubai, UAE*
[4]*School of Engineering, University of Glasgow, Glasgow, UK*

Correspondence should be addressed to Razi Iqbal; razi.iqbal@aue.ae

Received 4 October 2018; Accepted 15 November 2018; Published 3 February 2019

Guest Editor: Mohamed Elhoseny

The Internet of vehicles (IoV) is a newly emerged wave that converges Internet of things (IoT) into vehicular networks to benefit from ubiquitous Internet connectivity. Despite various research efforts, vehicular networks are still striving to achieve higher data rate, seamless connectivity, scalability, security, and improved quality of service, which are the key enablers for IoV. It becomes even more critical to investigate novel design architectures to accomplish efficient and reliable data forwarding when it comes to handling the emergency communication infrastructure in the presence of natural epidemics. The article proposes a heterogeneous network architecture incorporating multiple wireless interfaces (e.g., wireless access in vehicular environment (WAVE), long-range wireless fidelity (WiFi), and fourth generation/long-term evolution (4G/LTE)) installed on the on-board units, exploiting the radio over fiber approach to establish a context-aware network connectivity. This heterogeneous network architecture attempts to meet the requirements of pervasive connectivity for vehicular ad hoc networks (VANETs) to make them scalable and adaptable for IoV supporting a range of emergency services. The architecture employs the Best Interface Selection (BIS) algorithm to always ensure reliable communication through the best available wireless interface to support seamless connectivity required for efficient data forwarding in vehicle to infrastructure (V2I) communication successfully avoiding the single point of failure. Moreover, the simulation results clearly argue about the suitability of the proposed architecture in IoV environment coping with different types of applications against individual wireless technologies.

1. Introduction

Internet of Things (IoT) is paving a way forward for VANETs towards an evolution of Internet of vehicles (IoV) [1]. IoV paradigm not only benefits from pervasive vehicular connectivity for a bunch of services but also incorporates vehicular intelligence. To accomplish smart tasks, it also integrates vehicle to human (V2H) and vehicle to sensor (V2S) interactions in addition to conventional vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication modes. IoV is capable to process comprehensive information collected through the vehicles, roads, and surroundings to effectively supervise the drivers based on the integrated information. Thanks to the merger of industrial and Intelligent Transportation System (ITS) applications for IoV, it has successfully extended its support for several intelligent services (e.g., online vehicle status checking, intelligent root navigation and rescue, and avoiding illegal cyberspace operations).

ITS [2] is expected to be extensively deployed for the IoV paradigm to support a wide variety of applications ranging from low data rate traffic control services to high data rate and delay-critical multimedia services [3]. The ITS employs the coordination of sensors, on-board unit (OBU), and

trusted platform module (TPM) to share vital information of the vehicles with the road side unit (RSU). In the recent years, the number of vehicle users has immensely been increased which has turned the VANET [4] to be even more challenging. Moreover, the 24×7 demand for high speed internet access on-board and provision of multimedia services are inevitable for service providers to enable a robust, reliable, and secure data communication infrastructure [5].

Vehicular users demand ubiquitous communication with affordability while moving around in the urban, suburban, or even rural areas in countryside areas. Hence, moving vehicles are being designed keeping in view these demands, and a lot of work is being done in developing a range of ITS applications including road safety, traffic control, and numerous entertainment applications. The condition monitoring/warning systems, analytic systems, partner systems, location-based services, and different real-time applications are some of the examples that are expected to be installed on the modern vehicles being a part of IoV environment as shown in Figure 1.

In fact, VANETs still undergo some critical issues that cannot be tolerated towards the future IoV deployments. On the contrary, several quality of service (QoS) parameters are still compromised while data forwarding for multimedia (throughput intensive) applications that are anticipated to be an integral part of IoV to improve the driving experience through most updated multimedia contents [6]. The challenges of data forwarding in conventional VANETs environment vary as compared to the heterogeneous forwarding in IoV mainly due to the pervasive connectivity in V2V and V2I modes and frequent switching among the different operating modes. Moreover, the IoV infrastructures for persistent data forwarding in different scenarios (such as urban or highway) are still in their infancy and paving their way forward gradually. The IoV communication infrastructure is expected to improve the disaster and emergency situations in ITS through different applications (e.g., safety critical applications). Moreover, the IoV is expected to provide nonstop network connectivity and adaptiveness against network disconnections and long delays in emergency situations, even when the 4G/LTE [7] interface is connected. However, data forwarding based applications in the VANET infrastructure are limited in terms of modes of connectivity, switching, and bandwidth availability through the IEEE 802.11p WAVE [8] standard. The heterogeneous IoV framework applications require higher bandwidth and continuous network connectivity, but the challenge is unavailability of such networks, and increased user demand creates network resources hunt (such as safety, emergency videos, emergency audio and text messages dissemination, and reception) in such situations [9].

The IoV paradigm is a group of heterogeneous networks with increased number of different users in V2I and V2V under the centralized software-defined network (SDN) controller [10] using the desired applications in various environments. The problem of providing on-time and robust network interface-based connectivity is very crucial. The resilient multi-interfaced architecture for the Emergency Management Systems (EMS) [11] is a requirement of the modern era.

To circumvent these issues, a heterogeneous VANET architecture is proposed hereby keeping in view the requirements of IoV to make them more scalable and adaptable. The proposed architecture can exhibit several features to the network providers after successful deployment. First, it would be economical using inexpensive access units. Second, the heterogeneous architecture provides flexibility to the IoV paradigm by not only supporting current technology interfaces installed on Global ID (GID) but also being capable to implicitly support most of the future technologies (Section 3). Third, thanks to the presence of multiple interfaces available, it enables IoV nodes to avoid single point of failure. Forth, it can offer higher data rate support with reduced collisions by exploiting optical fiber at the backhaul. Fifth, the architecture is simple but robust to provide ease of management offering (i) fewer control stations, (ii) a centralized control for all the processing, and (iii) separating planes for client, connection, and cloud layers. Last, but not the least, it may reduce the extent carbon emission is polluting the environment due to Information and Communication Technology (ICT) infrastructures with fewer wireless links, hence, a step forward towards achieving "Green Networks" [12].

The rest of the paper is organized as follows. Section 2 provides the related work with discussion on major standards available in the state of the art for IoV. The proposed system model comprising the architecture, protocol design, and BIS algorithm for interface selection is described in Section 3. The simulation environment, results, and the discussion are presented in Section 4. Finally, the conclusions are given in Section 5.

2. Related Works

The industry and research community have proposed different wireless access technologies in the context of vehicular communications. They can broadly be seen into intravehicular, intervehicular, and vehicle to infrastructure communication in the context of an IoV environment. Although a rich variety of technologies is available in the literature for all the abovementioned categories, however, the point of focus for our domain would be the last category. Several access technologies have already been proposed and evaluated in the context of VANET (such as wireless local area network (WLAN) [13], Worldwide Interoperability for Microwave Access (WiMAX) [14], and cellular technologies such as 4G/LTE [7]). A quick overview of the state of the art of these access technologies for V2I communication is presented throughout this section.

The WLAN is foremost and widely accepted option available in the market. The most popular family in this category is IEEE 802.11. Several target groups have been working towards different variations of 802.11 family (e.g., 802.11 a/b/g/ah/n/p) All of them bear different characteristics and challenges associated with them that make them suitable for different environments. Overall, the standard supports short radio coverage with relatively higher data rate. A data rate of 600 Mbps is claimed to be supported by 802.11n which is based on 802.11a/b/g [6]. However, they

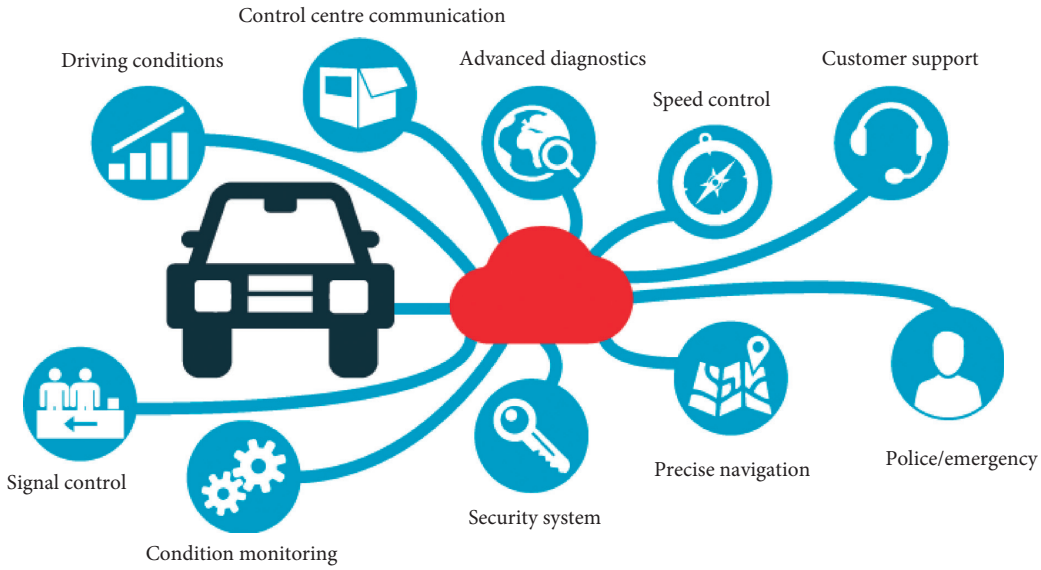


Figure 1: An ITS vehicle being a part of Internet of vehicles.

were not physically achievable in mobile environment. All these variations were not feasible for VANET environment with very high mobility and frequently changing topologies. Hence, a new variation of WAVE for 802.11p [8] was introduced for specific support in vehicular networks. WAVE is capable to support a range of applications and services belonging to ITS with a special focus on safety critical applications [15]. Several research efforts have been put in place to physically evaluate the performance of 802.11p with its predecessors [13, 16] on a highway environment. A recent addition to the same family is 802.11ah (that is, long-range WiFi) [17] which is also expected to be a decent option in vehicular environment. Long-range WiFi can provide a better radio coverage up to over 1 km as compared to other siblings which can improve the connection duration to provide sustainability with least number of handovers [18].

WiMAX [14] is another wide area network (WAN) access technology, belonging to WLANs, that has been considered for VANETs due to its large geographical coverage and capability to theoretically support a higher data rate up to 72 Mbps. The IEEE 802.16e was emerged as the mobile WiMAX standard that could support communication up to 160 km/h speed of moving vehicles with different QoS parameters, even for nonline of sight communication. A scheduling algorithm is employed in WiMAX as a channel access method where a mobile terminal needs to compete once initially, which could be more robust in collision scenarios [19]. The only problem with the WiMAX was nonconformance of a specific standard for high mobility environment; hence, the technology could not take off in VANETs as expected.

With the evolution of cellular infrastructures, 4G/LTE [7] has been a hot choice in vehicular environment. It can also support reasonable data rate with the smoother handover management mechanism as compared to WiMAX and WLAN. Several works throw light on various issues of 4G/LTE when employing into a very high mobility environment. The authors in [20] first presented an analytical framework to compare the performance of 4G/LTE with the WAVE in terms of beacon probability before the deadline expiry. Similarly, authors in [21] identified the potential use cases for operator-controlled device-to-device (D2D) [22] communication in VANET. Another article [23] discussed the suitability of LTE service with high bandwidth and long radio coverage in an urban environment. Satellite communication can be another access technology to be used in VANET [24]. Due to the huge costs involved, this access technology has not been employed widely except for some safety critical applications. However, it can still be considered a backup option in the absence/failure of other available technologies in case of an emergency.

In the recently conducted research discussed above, most of the roadside infrastructures use a single communication technology (single interface) to communicate with peer infrastructures and other entities of the network that inherits the limitations of that communication technology. Till date, no literature is available that proposes a system with multi-interface (heterogeneous) communication technology in VANETs. In this paper, the authors have proposed a heterogeneous VANET architecture to be used in IoV networks to enhance the overall performance and efficiency of data forwarding (data communication) in vehicular networks.

3. Proposed System Model

This section presents the generic system model for proposed heterogeneous solution leveraging multiple access technologies to enable ubiquitous communication in IoV targeting V2I communication. Three different access technologies have been considered in this work such as WAVE [8], long-range WiFi [17], and 4G/LTE [7]. The IEEE802.11p (WAVE) and IEEE802.11ah (long-range WiFi) are the members of WLAN family while 4G/LTE belonging to wireless cellular technologies. There are several reasons to

choose these three as access technologies among a bulk of options available in the market. First, they have already got equal acceptance by the academia and the industry. Second, the standards are already on the mature stage. Third, they have been individually deployed and tested and conform to the characteristics of vehicular environments. The system architecture, protocol stack, and BIS algorithm are presented in the rest of this section.

3.1. A Holistic View of Heterogeneous IoV Architecture. The multi-interfaced IoV system exploiting the radio over fiber (RoF) [15] paradigm is proposed where moving vehicles are equipped with the vehicular GID terminal with more than one wireless interfaces installed. These interfaces are capable to communicate with small radio access units (RAUs) installed along the roadside to relay the communication onto control station (CS) in the V2I mode. The optical fiber is employed to connect RAUs with the CS and for the onward backhaul connectivity with the network backbone as shown in Figure 2.

The architecture follows a three-layered approach in order to simplify the functionality of various components. The client layer at the bottom covers intravehicular and intervehicular communications (e.g., communication among various sensor nodes within a vehicle). It is also responsible for enabling IoV addressing and maintaining a trustworthy identity in the cyberspace. The connection layer deals with the interconnectivity of different network components within a network and integration of other available networks within vehicular environment. Similarly, the cloud layer is finally responsible for enabling all the IoV services and applications. It also offers many cloud-based services like mass storage, virtualization, and real-time interactions among different network entities. We now highlight the functionality of various components of this architecture.

3.1.1. Radio Access Unit. RAU is a radio antenna with very simple functionality that is capable to listen on a range of frequency bands irrespective of the underlying technology being used at the transmitter side. RAU moves all the other functionalities of a RSU onto CS. It only receives the signal and subsequently performs electrical to optical (E/O) conversion before relaying the packet onto fiber link. Similarly, it receives the reply back from the fiber link, the opto-electrical converter does its job, and the response is relayed back to the respective vehicle. Exploiting this kind of antenna structure brings several advantages, such as easier network planning and management due to very simple antenna structure and functionality, low interchannel interference, longer battery life, and very low capital expenditure (CAPEX) [25].

3.1.2. Control Station. The CS is another fundamental component that is responsible for controlling the rest of the operations of heterogeneous IoV architecture. The control functions of the system, such as frequency allocation, modulation/demodulation, and processing, are performed at the central site, simplifying the design of the RAU. Centralized architecture allows a dynamic configuration of radio resource and capacity allocation. The optical fiber is transparent to modulation, radio frequency, and bit rate; hence, multiple services on a single multimode fiber can be supported at the same time using RoF managed by the CS. The CS is further connected to cloud such as Public Switched Telephone Network (PSTN) or the Internet. Multimode optical fiber can dramatically play its role to achieve higher throughputs at the CS. In the context of VANETs, we argue that an RoF-based V2I architecture can provide reliable, secure, and cost-effective infrastructure if the fiber has already been deployed in an area. The proposed system is fully capable of exploiting the advantages of integrated wired (i.e., fiber) and wireless solutions for the throughput intensive infotainment applications as well as pervasive internet connectivity.

3.1.3. GID Terminal. The moving vehicles are equipped with GID terminals and are connected with RAUs using a radio link, and the front-end transmission takes place using the same radio link but irrespective of the fact which wireless interface at the vehicle side is currently active. Multi-interfaced GIDs are capable of providing continuous radio connectivity with different kind of wireless access options (such as WAVE, long-range WiFi, and 4G/LTE). Although different wireless interfaces possess different properties in terms of available bandwidth, data rates, communication range, and billing cost, however, the users demand continuous connectivity to fully utilize the set of communication services being always connected to the internet.

3.2. Protocol Design of Heterogeneous IoV Architecture. The protocol stack for the proposed multi-interfaced IoV architecture depicting the role of various communication layers is shown in Figure 3. There may be different kinds of throughput requirements for the apps running within different vehicles. All the radio signals irrespective of the technology are received by a nearby RAU and are further converted to optical signals through the electrooptical (E/O) conversion unit. Similarly, optoelectrical (O/E) conversion unit is present on the CS side which converts optical signals back into electrical ones for onward processing of the user request by the CS.

Let λ be the wavelength to represent a certain type of communication on the fiber link, and then different wavelength values ranging from λ_1, λ_2, λ_3 ... λ_n may be multiplexed to travel through multimode fiber to support multiple communications simultaneously. For example, the well-known IEEE 802.11p signal may be assigned as λ_1, IEEE 802.11ah is λ_2 and, similarly, the communication on the 4G/LTE interface can be assigned as λ_3. The optical fiber link is capable to carry these different lambdas employing multimode fiber. However, the data rates offered by multimode fiber may vary from 10 Gbps to 1 Gbps up to a distance of 550 m and 1000 m, respectively [26]. Different communication layers depicted in Figure 3 have certain type of roles.

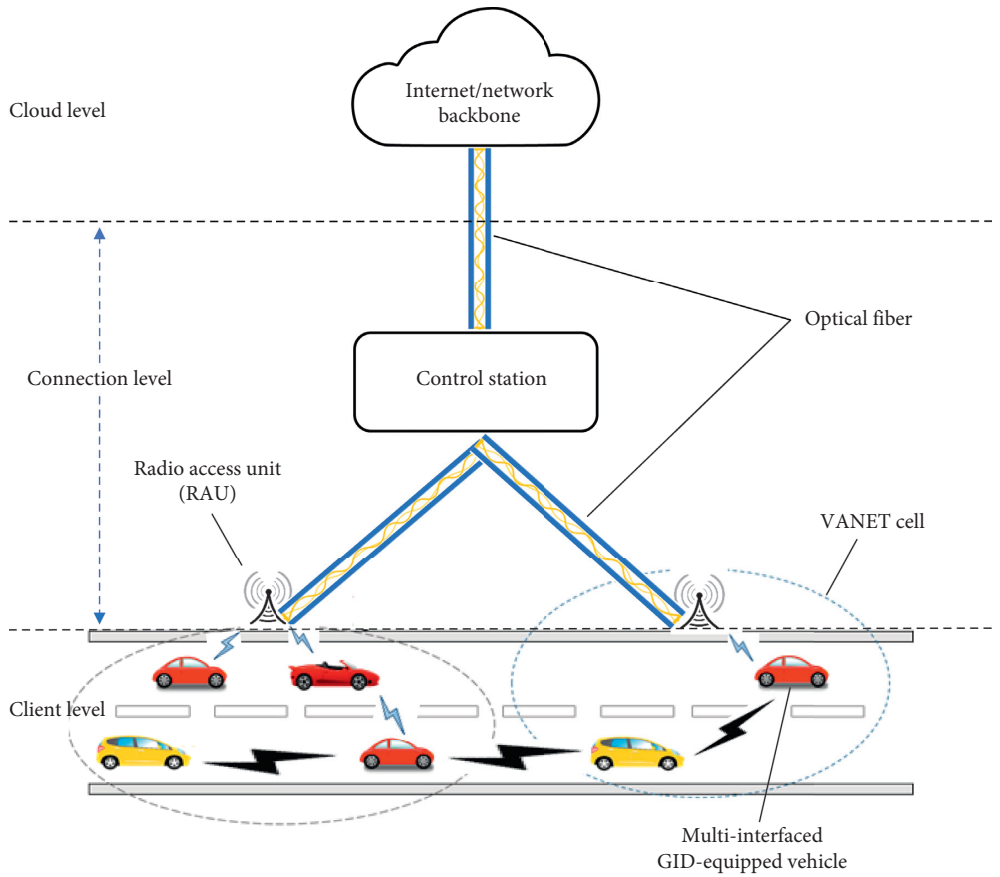


Figure 2: A generalized view of proposed heterogeneous VANETs architecture.

After the physical layer on the fiber channel (FC-0), the FC-1 layer performs the duty of data encoding and decoding. Similarly, framing is the responsibility of FC-2. Many other types of services related to different communication tasks are carried out at fiber channel 3 while layer 4 of the protocol stack performs protocol mapping. For vehicles using WAVE, long-range WiFi, or 4G/LTE interfaces at a particular instance, the data packets forwarding follows through all the layers of 802.11p, 802.11ah, and International Mobile Telecommunications (IMT) Advanced standard stacks, respectively. The summary of notations used throughout the paper is shown in Table 1.

3.3. Best Interface Selection (BIS) Algorithm. The idea of employing BIS interface permits the vehicular users to switch between the interfaces belonging to different technologies as per the best suitability of application requirements as shown in Table 2. In fact, the interface selection criterion for connectivity may depend on several QoS parameters such as throughput, delay, or other user preference like cost-effectiveness. Therefore, the presence of multiple wireless interfaces ensures services through always best-connected user interface at all the times.

The multiple interfaces (WAVE, long-range WiFi, and 4G/LTE) also serve as a back-up to each other in case one interface is a bottleneck for any reason for a certain type of services. There may be a variety of different applications running by vehicular users. The algorithm randomly selects the interface of an access network from the available options and checks if QoS requirements (in terms of bandwidth and/or delay) are successfully met by the chosen interface or it needs to switch over to some new interface. Cost may be another user-defined preference. If the QoS parameters are satisfied, the interface with lowest cost would be opted. The algorithm also serves the purpose to manage load sharing between different interfaces. For example, if an interface undergoing congestion can start causing longer delays, if it does not meet the maximum delay requirement, and the algorithm run will result in changing to some other interface.

4. Results and Discussion

4.1. Simulation Environment. In this section, the simulation environment is discussed in detail highlighting several application parameters. Each vehicle is equipped with multiple wireless interfaces that is (long-range WiFi [17], 4G/LTE [7], and WAVE [8]) installed on GID for establishing connectivity in the given simulation scenario. The performance of the proposed heterogeneous architecture is evaluated in comparison with existing wireless standards on the basis of different performance metrics such as throughput, delay, and server load. The general parameters for the simulation environment can be seen in Table 3.

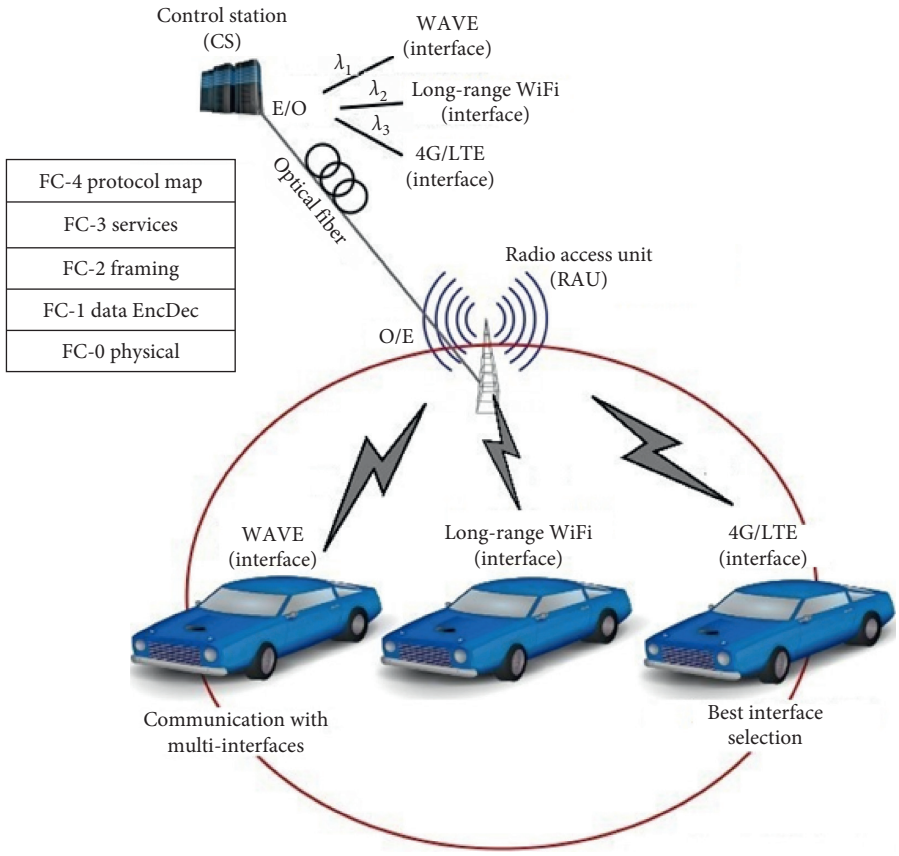


Figure 3: Protocol stack for multi-interfaced VANET.

In the first phase, all the available wireless interfaces are evaluated individually in a given scenario against a set of requirements imposed by various applications. Then, the proposed heterogeneous architecture is evaluated in the same scenario against the same set of requirements to identify the variation among different performance indicators. The detailed performance analysis based on the chosen indicators is presented in the following section.

4.2. Comparison of the Proposed Heterogeneous Architecture with Individual Wireless Interfaces

4.2.1. Analysis of Throughput Parameter with respect to Simulation Time. The simulation results in Figure 4 illustrated the throughput parameter using different communication technologies in a scenario compliant with the simulation parameters in Table 3. The graph shows that the heterogeneous architecture with dynamic and adaptive network selection outperformed WAVE and long-range WiFi standards and shows a high peak of 1100 packets/second at the beginning of the simulation time and then gradually goes on declining with time. Although proposed heterogeneous architecture selects the best network interface depending on the availability at that time with respect to several parameters (e.g., radio propagation and coverage, signal strength, sufficient bandwidth, higher data rate, and lower latency) but, heavy user applications such as, Voice over Internet Protocol (VoIP) and video conferencing, are continuously entertained, and thus the throughout tends to go down below to 30 packets/seconds in all the cases. Nevertheless, the proposed architecture remains in the leading role as compared to other counterparts throughout the simulation time.

4.2.2. Analysis of Delay Parameter with respect to Simulation Time. The graph in Figure 5 depicted the end-to-end delay offered by different communication standards. The figure clearly shows that the delay gradually increases above the simulation time of 15 seconds for all communication standards. Especially, the 4G/LTE standard shows higher delay peak of 1800 ms at 300 s simulation time than 1400.18 ms for the long-range WiFi standard at the same simulation time. However, heterogeneous architecture shows least delay of 451.80 ms at 300 s of simulation time. The reason for such a long delay shown in the case of the 4G/LTE standard might be the higher number of requests by data intensive applications such as VoIP of global system for mobile (GSM) quality and video conferencing, and hence, the network gets loaded causing congestion on the link. In case of the heterogeneous architecture, initially, the rapid switching of communication technologies based on number of requests from various applications with varying distances between the source and the destination causes similar latency as compared to other cases, but it soon

Table 1: A summary of notations used throughout the paper.

Symbol	Definition
d_{proc}	The processing delay is the time that a node spends processing a packet
d_{queue}	The queuing delay is the time required to put an entire packet into the communication media multiplied by an average length of the queue
D_{a}	Delay requirement of the application
d_{ltetotal}	Total delay of the LTE interface
$d_{\text{wavetotal}}$	Total delay of the WAVE interface
$D_{(m\times t)}$	Delay availability matrix for single hop communication
$d_{k,n}\ \varepsilon\ D_{(m\times t)}$	The delay of network interface k at time n
B	Bandwidth of the network interface
B_{wifi}	Bandwidth of the WiFi interface
$B_{(\text{m}\times\text{t})}$	Network availability matrix for single hop communication
c	Unit cost
$c_k\ \varepsilon\ C_{(\text{m})}$	Unit cost of any network interface k
$S_{(m\times t)}$	Network scheduling according to interface m in time slot t
N_n	Network utilization of the interface
N_{inclte}	Network utilization of the LTE interface
N_{incwave}	Network utilization of the WAVE interface
M	The number of network interfaces
$d_{\text{total},k}$	Total delay of the selected network interface k
T	The number of time slot periods
d_{trans}	The transmission delay is the time required to put an entire packet into the communication media
d_{prop}	The propagation delay is the time required for a packet to reach from vehicle to the RAU divided by propagation speed of the media or speed of light
d_{total}	Total delay
$d_{\text{wifitotal}}$	Total delay of the WiFi interface
$d_{\text{wifitotal}}$	Total delay of the WiFi interface
$d_{\text{wavetotal}}$	Total delay of the WAVE interface
$d_{k,n}\ \varepsilon\ D_{(m\times t)}$	The delay of network interface k at time n
B_{lte}	Bandwidth of the LTE interface
B_{wave}	Bandwidth of the WAVE interface
$b_{k,n}\ \varepsilon\ B_{(m\times t)}$	The bandwidth of that network interface k can provide at time n
$C_{(\text{m})}$	Vector of unit cost of all the available network interfaces
$C_{(\text{e})}$	Cost of all network interfaces e
$s_{k,n}\ \varepsilon\ S_{(m\times t)}$	Network k selected at time n
N_{a}	Network utilization by the application
N_{incwifi}	Network utilization of the WiFi interface
N_{inc}	Sum of bandwidth x delay product of all network interfaces
k	Current selected network interface
c_k	Unit cost of selected network interface k
b_{a}	Bandwidth requirement of the application

stabilizes itself after 60 s on the average value of 445.5 ms throughout the simulation time.

4.2.3. Analysis of the Server Load Parameter with respect to Simulation Time. As the number of requests per second on the server increases by the clients running Hypertext Transfer Protocol (HTTP), E-mail, File Transfer Protocol (FTP), VoIP of GSM quality, and video conferencing applications, Figure 6 shows a gradual decrease due to frequent switching between different technologies in the presence of a hard requirements imposed by a plethora of running applications. The heterogeneous architecture exhibits a higher server load starting from 27.6 requests per second that remains higher throughout the simulation as compared to long-range WiFi and other available interfaces. As the proposed heterogeneous architecture is an adaptive multi-interfaced architecture that selects best available interfaces, it is capable enough to serve a higher number of requests as compared to other counterparts.

4.2.4. Impact of Mobility Speed on the Throughput Parameter. As shown in Figure 7, by varying the mobility speed, the throughput parameter demonstrates relatively irregular trend in the graph. However, the proposed heterogeneous architecture offers a reasonable throughput of 101.55 packets/second at mobility speed of 55 kmph. Furthermore, it can also be seen from the figure that the throughput tends to decrease as mobility speed varies from 60 till 80 kmph. On the contrary, the WAVE standard demonstrates a significantly lower throughput of 58.41 packets/second at the same level of mobility. The main factor behind faded throughput is the increase in mobility speed of source and destination vehicles during communication. The heterogeneous architecture is able to cope well with increasing mobility speed as compared to other options due to dynamic interface selection based on application demand. Then, it goes on decreasing between 65 and 70 kmph due to frequent disconnections.

4.2.5. Impact of Mobility Speed on the Throughput Parameter. In Figure 8, the impact of mobility on delay is quite significant for all wireless options especially for 4G/LTE and long-range WiFi, that is, 1811.38 and 1402.18 ms at the speed of 80 kmph, respectively. The reason behind high delay is mainly due to sparseness of source and destination nodes as mobility speed goes on increasing. The demand for running user's applications (such as VoIP and video conference) causes congestion hindering the traffic flow and reduces bandwidth for delay intensive applications. However, heterogeneous architecture tackles the delay by dynamic switching to different available wireless interfaces as per mobility requirement and exhibits moderate delays.

4.2.6. Impact of Server Load with respect to Mobility Speed. The graph depicted the effect of varying mobility on server load for different wireless technologies. As shown in Figure 9, the server load can have huge impact on mobility speed from 55 kmph to 62 kmph. The proposed heterogeneous architecture serves the maximum number of client requests right from the start of the simulation time but goes down rapidly until the mobility speed of 62 kmph. Then, it starts stabilizing from approximately 9 request/s to less than 5 request/s as compared with other

Table 2: Best interface selection algorithm for IoV.

Procedure: $m(B, C, D, N)$ //selecting interface for an application requirement app
$B \longleftarrow$ set bandwidth requirement
$C \longleftarrow$ set cost requirement
$D \longleftarrow$ set delay requirement
$N \longleftarrow$ set network utilization requirement
SET $s_{k,n} = 1$ such that $s_{kn}\ \varepsilon\ S_{(m\times t)}$ //Interface $\longleftarrow$ select a random network ID for initialization
SWITCH app's access preferences (B, C, D, Nn)
CASE B:
IF $b_{kn} >= b$a such that $b_{k,n}\ \varepsilon\ B_{(m\times t)}$ //if the current network interface meets application bandwidth requirements then,
RETURN B
ELSE $B_{(m\times t)} >= b_{\mathrm{a}}$ such that $B_{(m\times t)} = B = B_{\mathrm{lte}} = B_{\mathrm{wave}} = B_{\mathrm{wifi}}$ //compare it with //the bandwidths available to other access networks
RETURN B //network interface with highest bandwidth support
BREAK;
CASE C:
$C_{(\mathrm{m})} = \sum_{c_{\mathrm{k}}\ \varepsilon\ C_{(\mathrm{m})}} C_{(\mathrm{e})}$ //sum of costs of all links "e"
For all $C_{(\mathrm{m})}$, $c_{\mathrm{k}}\ \varepsilon\ C_{(\mathrm{m})}$ do //FOR get the list of networks to iterate and sort in the increasing cost order
RETURN $(\min(\sum c_{\mathrm{k}}))$ //return the network interface with least cost. k, m
BREAK;
CASE D:
IF $d_{kn} <=$ da such that $d_{k,n}\ \varepsilon\ D_{(m\times t)}$ where $\sum d_{\mathrm{total,k}} = d_{\mathrm{proc}} + d_{\mathrm{queu}} + d_{\mathrm{trans}} + d_{\mathrm{prop}}$ //if the current network interface meets the delay requirements then, return void
ELSE $D_{(m\times t)} <= d_{\mathrm{a}}$ *such that* $D_{(m\times t)} = d_{\mathrm{total}} = d_{\mathrm{ltetotal}} = d_{\mathrm{wavetotal}} = d_{\mathrm{wifitotal}}$ //compare it with the delays of other access networks
RETURN $\forall\ d_{\mathrm{total}}\ e\ D$ $\min(\sum d_{\mathrm{total}})$ total, m //return the network interface with least delay
BREAK;
CASE default:
For all $c_k = 0$ to n, //where n is the nth cost amount subject to vector of unit cost, that is, $C_{(\mathrm{m})}$, $c_{\mathrm{k}}\ e\ C_{(\mathrm{m})}$ //FOR get the list of network interfaces to iterate and sort in an increasing cost order
IF $N_{\mathrm{n}} >= N_{\mathrm{a}}$ *such that* $b_{k,n}\ e\ B_{(m\times t)}$ and $d_{k,n}\ e\ D_{(m\times t)}$, where $N_{\mathrm{n}} = B * d_{\mathrm{total,n}}$ //if the current network interface meets bandwidth and delay requirements then,
RETURN N_{n}
ELSE $N_{\mathrm{n}} < N_{\mathrm{a}}$ such that $N_{\mathrm{n}} = N_{\mathrm{inclte}} = N_{\mathrm{incwave}} = N_{\mathrm{incwifi}}$ and $N_{\mathrm{inclte}} = B_{\mathrm{lte}} * d_{\mathrm{ltetotal}}$, $N_{\mathrm{incwave}} = B_{\mathrm{wave}} * d_{\mathrm{wavetotal}}$, $N_{\mathrm{incwifi}} = B_{\mathrm{wifi}} * d_{\mathrm{wifitotal}}$ //compare it with the bandwidth and delay for other available access networks, and
RETURN $(\max(\sum N_{\mathrm{inc}}))$ $N_{\mathrm{inc}}\ e\ N$ //the one with highest bandwidth and least delay
BREAK;
$F\ s_{k,n} = 0$ //no network interface is assigned then,
RETURN false;
ELSE RETURN true;

Table 3: Simulation parameters.

Parameters	Values
Simulator	NCTUns 6.0 [27], OPNET Modeler [28]
Wireless technologies	Long-range WiFi, 4G/LTE, WAVE
Standards	IEEE802.11ah, IMT advanced, IEEE 802.11p
Frequency bands	2.4 GHz, 700–2570 MHz, 5.9 GHz
Simulation time	300 sec
Number of vehicles	30
Acceleration	1
Deacceleration	4
Speed of vehicles	55–80 km/hour
Traffic type	TCP/UDP
Traffic application	VoIP, video, FTP, HTTP, E-mail
Scenario	Semi-Rural, Rural

counterparts which do not specifically perform better against increasing mobility speed.

4.3. Benefits of the Proposed Heterogeneous Architecture. This section presents some prevalent features of the proposed multi-interfaced architecture from various aspects of VANET. These features are enlisted as follows.

4.3.1. Cost-Effective Solution. The cost-effectiveness is of utmost significance in the multi-interfaced architecture. The effort was to make the design inexpensive introducing cheaper RAUs following a very simple transmission mechanism. It is pertinent to mention that the costs may be higher in the areas where the fiber needs to be installed from the scratch. The proposed RoF approach

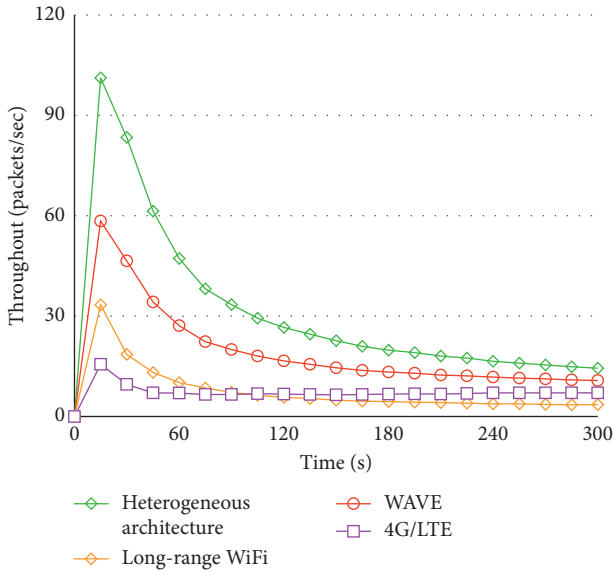


Figure 4: Throughput of RoF-based proposed heterogeneous architecture against other wireless interfaces.

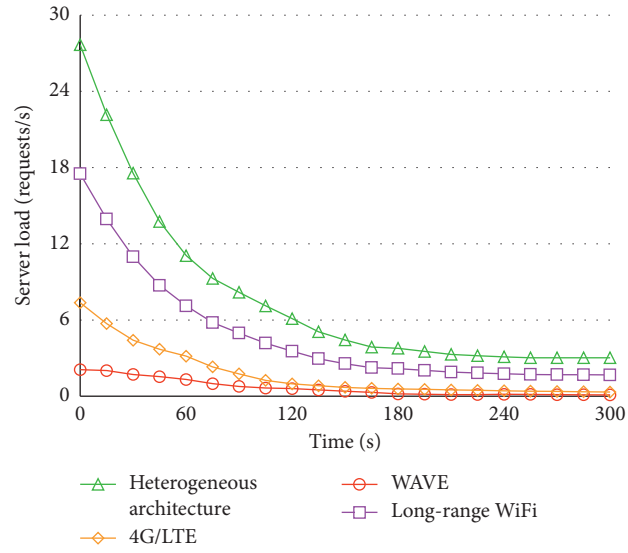


Figure 6: Server load of proposed RoF-based heterogeneous architecture against other wireless interfaces.

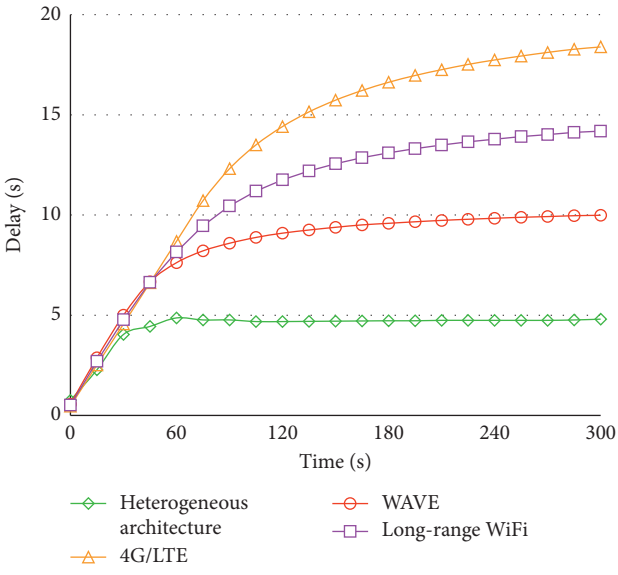


Figure 5: Delay of proposed RoF-based heterogeneous architecture against other wireless interfaces.

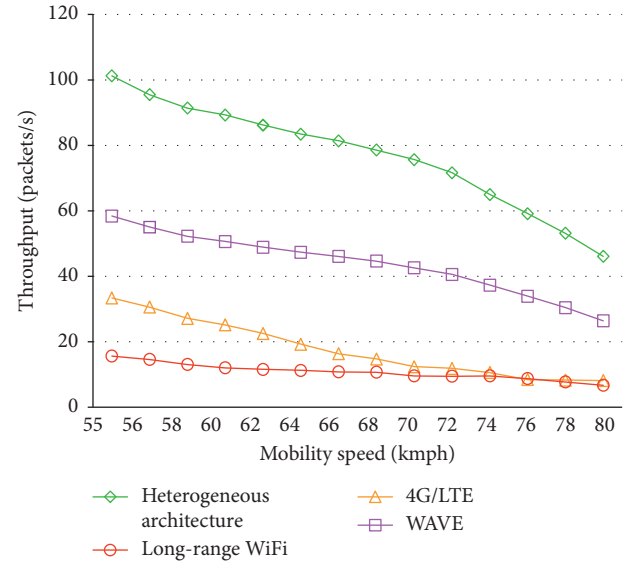


Figure 7: Throughout comparison of proposed RoF-based heterogeneous architecture with other wireless interfaces against different mobility speeds.

is robust than the existing architectures in terms of data rate, bandwidth availability, and quality of service provision. The overall cost factor depends on the existing infrastructure available. For example, if the proposed architecture is to be deployed in an area already covered by fiber services, the only major cost can be the RAU deployment which can be up to tens of USDs.

4.3.2. Congestion Control. Congestion on the network is one of the few troublesome aspects that may gradually lead to slower down the performance of overall network. Accidents, emergencies, or other mishaps usually cause this congestion in VANET as a single point of failure; the entire network appears to be bottleneck and goes down. As the proposed architecture supports many interfaces so if there is some problem with one interface, other nodes can carry on their communication by some other interfaces.

4.3.3. Support for Future Technologies. The proposed architecture demonstrates its compatibility to support many future technologies (such as Fifth Generation (5G) or HaLow) [29] as the RAU design can support a wide range of frequency bands irrespective of the wireless technology

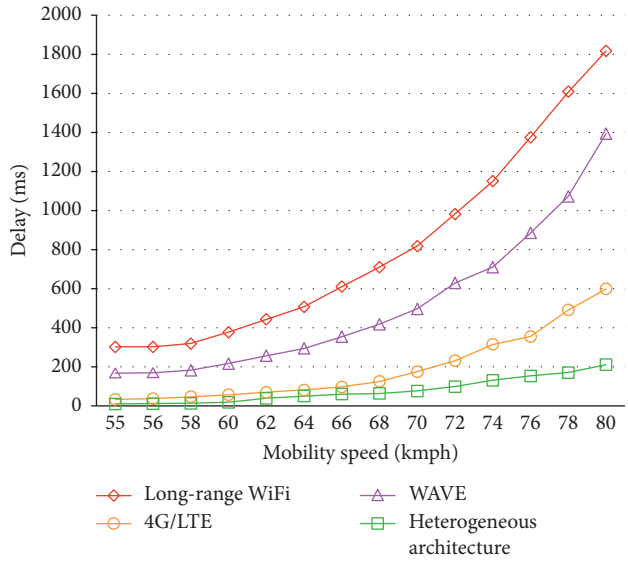


Figure 8: Delay comparison of the proposed RoF-based heterogeneous architecture with other wireless interfaces against different mobility speeds.

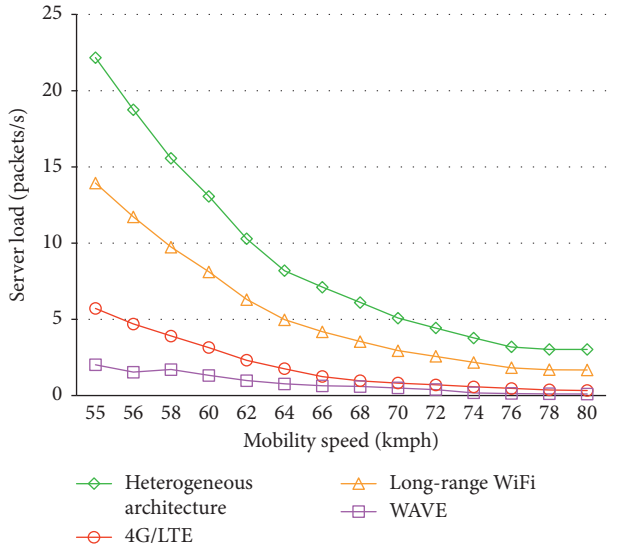


Figure 9: Server load comparison of the proposed RoF-based heterogeneous architecture with other wireless interfaces against different mobility speeds.

standard. Therefore, the deployed RAUs along the roadways can serve to listen on various frequency channels without fearing technology obsoleteness.

4.3.4. Capacity. Utilizing fiber as communication link between several RAUs and CS provides a large number of benefits to network providers because the existing fiber infrastructure spread over most of the areas in advanced countries can be shared for VANET services, and hence, higher throughputs can be achieved. Thanks to the availability of multiple interfaces at a time where each interface can support a bulk of nodes, the proposed architecture is more scalable as well.

4.3.5. Ease of Management. The regions where fiber is already deployed, the proposed architecture can be implemented rapidly with least control infrastructure. A small number of CS are enough to provide the infrastructure management facility due to the idea of fiber connectivity at the backhaul, and CS is the only centralized entity for all kind of processing on the user requests.

4.3.6. Carbon Footprint Savings. As per the statistics, ICT is accounted for 2% of the global carbon footprints, and this trend is going to continue with an annual increase of 10% [30]. Every effort made to minimize this effect would eventually prevent the environment. The proposed architecture employs fiber at the backhaul to connect with the network backbone. Hence, it would contribute in the carbon emission savings towards the phenomenon of Green Networks [3].

5. Conclusion

This paper proposes a novel heterogeneous architecture for Internet of vehicles based on multiple wireless interfaces available for communication. One of the critical requirements of the vehicular communication is the future compatibility for a variety of modern network standards. The proposed heterogeneous architecture outperformed the existing wireless technologies when evaluated individually on the basis of high throughput and low latency in comparison with long-range WiFi, 4G/LTE, and conventional WAVE architectures by varying simulation time and mobility speeds. Moreover, the performance of existing architecture compared to proposed architecture varies as per underlying application demands and network support (i.e. bandwidth intensive applications require high-speed network interface). The proposed architecture ensures the provision of best available connectivity that can fulfill users' demands frequently, thus serving higher number of clients. The proposed RoF-based architecture with multi-interfacing will be a promising solution for future vehicular networks which simultaneously ensures integrity, compatibility, and reliability of the interconnected devices in IoV environment. The work can further be extended towards the classification of vehicles on the basis of application requirements in order to minimize the access control issues as the number of vehicles and application demand increases, thereby reducing congestion on radio access units. Moreover, a more detailed analysis on the capital and operating costs of such approaches has been scheduled as a future work. Furthermore, several other themes can be integrated with the proposed architecture (such as, information centric networks (ICN) [31] and mobile edge computing (MEC) [32] paradigms) to further exploit the advantages of the proposed architecture.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was partly funded by EPSRC Global Challenges Research Fund (the DARE Project; no. EP/P028764/1). The work was also funded partially by Italian MIUR PON projects Pico&Pro (ARS01_01061), AGREED (ARS01_00254), FURTHER (ARS01_01283), and RAFAEL (ARS01_00305) and by Apulia Region (Italy) Research Project E-SHELF (OSW3NO1).

References

[1] J. Contreras, S. Zeadally, and J. A. Guerrero-Ibanez, "Internet of vehicles: architecture, protocols, and security," *IEEE Internet of Things Journal*, vol. 5, no. 5, 2017.

[2] M. Alam, J. Ferreira, and J. Fonseca, "Introduction to intelligent transportation systems," in *Intelligent Transportation Systems. Studies in Systems, Decision and Control*, M. Alam, J. Ferreira, and J. Fonseca, Eds., vol. 52, Springer, Cham, Switzerland, 2016.

[3] C. Xu, W. Quan, H. Zhang, and L. A. Grieco, "GrIMS: green information-centric multimedia streaming framework in vehicular ad hoc networks," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 2, pp. 483–498, 2018.

[4] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of network and computer applications*, vol. 37, pp. 380–392, 2014.

[5] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: a survey on architecture, challenges, and solutions," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2377–2396, 2015.

[6] Y. Fangchun, W. Shangguang, L. Jinglin, L. Zhihan, and S. Qibo, "An overview of internet of vehicles," *China Communications*, vol. 11, no. 10, pp. 1–15, 2014.

[7] J. Huang, F. Qian, A. Gerber, Z. M. Mao, S. Sen, and O. Spatscheck, "A close examination of performance and power characteristics of 4G LTE networks," in *Proceedings of 10th International Conference on Mobile Systems, Applications, and Services MobiSys'12*, pp. 225–238, Lake District, UK, June 2012.

[8] I. Al-Anbagi and H. T. Mouftah, "WAVE 4 V2G: wireless access in vehicular environments for vehicle-to-grid applications," *Vehicular Communications*, vol. 3, pp. 31–42, 2016.

[9] W. Zhu, D. Gao, C. H. Foh, H. Zhang, and H.-C. Chao, "Reliable emergency message dissemination protocol for urban internet of vehicles," *IET Communications*, vol. 11, no. 8, pp. 1275–1281, 2017.

[10] W. Zhu, D. Gao, W. Zhao, H. Zhang, and H.-P. Chiang, "SDN-enabled hybrid emergency message transmission architecture in internet-of-vehicles," *Enterprise Information Systems*, vol. 12, no. 4, pp. 471–491, 2017.

[11] Z. Ji and Q. Anwen, "The application of internet of things (IOT) in emergency management system in China," in *Proceedings of 2010 IEEE International Conference on Technologies for Homeland Security (HST)*, pp. 139–142, IEEE, Waltham, MA, USA, November 2010.

[12] Z. Andreopoulou, "Green informatics: ICT for green and sustainability," *Journal of Agricultural Informatics*, vol. 3, no. 2, pp. 1–8, 2012.

[13] M. Wellens, B. Westphal, and P. Mahonen, "Performance evaluation of IEEE 802.11-based WLANs in vehicular scenarios," in *Proceedings of 2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring*, pp. 1167–1171, IEEE, Dublin, Ireland, April 2007.

[14] A. Ghosh, D. R. Wolter, J. G. Andrews, and R. Chen, "Broadband wireless access with WiMax/802.16: current performance benchmarks and future potential," *IEEE Communications Magazine*, vol. 43, no. 2, pp. 129–136, 2005.

[15] H. H. R. Sherazi, I. Raza, M. H. Chaudary, S. A. Hussain, and M. H. Raza, "Multi-radio over fiber architecture for road vehicle communication in VANETs," *Procedia Computer Science*, vol. 32, pp. 1022–1029, 2014.

[16] Y. Yao, L. Rao, X. Liu, and X. Zhou, "Delay analysis and study of IEEE 802.11p based DSRC safety communication in a highway environment," in *Proceedings of 2013 IEEE INFOCOM*, pp. 1591–1599, IEEE, Turin, Italy, April 2013.

[17] A. Augustin, J. Yi, T. Clausen, and W. Townsley, "A study of LoRa: long range & low power networks for the internet of things," *Sensors*, vol. 16, no. 9, p. 1466, 2016.

[18] T. Adame, A. Bel, B. Bellalta, J. Barcelo, and M. Oliver, "IEEE 802.11AH: the WiFi approach for M2M communications," *IEEE Wireless Communications*, vol. 21, no. 6, pp. 144–152, 2014.

[19] S. M. Bhagat and V. Wadhai, "Performance evaluation of AODV routing protocol using WiMAX on VANET," *International Journal of Computer Applications*, vol. 108, no. 5, pp. 36–39, 2014.

[20] L. Jing-Lin, L. Zhi-Han, and Y. Fang-Chun, "Internet of vehicles: the framework and key technologies," *Journal of Beijing University of Posts and Telecom*, 2014.

[21] H. Guoqing, H. Anpeng, H. Ruisi, A. Bo, and C. Zhangyuan, "Theory analysis of the handover challenge in express train access networks (ETAN)," *China Communications*, vol. 11, no. 7, pp. 92–98, 2014.

[22] H. ElSawy, E. Hossain, and M.-S. Alouini, "Analytical modeling of mode selection and power control for underlay D2D communication in cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 11, pp. 4147–4161, 2014.

[23] E. Hossain, G. Chow, V. C. M. Leung et al., "Vehicular telematics over heterogeneous wireless networks: a survey," *Computer Communications*, vol. 33, no. 7, pp. 775–793, 2010.

[24] M. Bacco and A. Gotta, "RLNC in satellite networks: a cooperative scenario for delivering M2M traffic," *International Journal of Satellite Communications and Networking*, vol. 35, no. 6, pp. 605–620, 2017.

[25] O. Pedrola, A. Castro, L. Velasco, M. Ruiz, J. P. Fernández-Palacios, and D. Careglio, "CAPEX study for a multilayer IP/MPLS-over-flexgrid optical network," *Journal of Optical Communications and Networking*, vol. 4, no. 8, pp. 639–650, 2012.

[26] T. Joseph and J. John, "Modified twin-spot launching: an improved launching technique for enhancing data rates in multimode fiber," *Applied optics*, vol. 56, no. 4, pp. 838–846, 2017.

[27] S. Y. Wang, C. L. Chou, C. H. Huang et al., "The design and implementation of the NCTUns 1.0 network simulator," *Computer Networks*, vol. 42, no. 2, pp. 175–197, 2003.

[28] X. Chang, "Network simulations with OPNET," in *WSC'99. 1999 Winter Simulation Conference Proceedings. "Simulation - A Bridge to the Future" (Cat. No.99CH37038)*, pp. 307–314, ACM, Phoenix, AZ, USA, December 1999.

[29] W. Ejaz and M. Ibnkahla, "Multiband spectrum sensing and resource allocation for IoT in cognitive 5G networks," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 150–163, 2018.

[30] H. H. R. Sherazi, G. Piro, L. A. Grieco, and G. Boggia, "When renewable energy meets LoRa: a feasibility analysis on cableless deployments," *IEEE Internet of Things Journal*, 2018.

[31] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies-CoNEXT'09*, pp. 1–12, ACM, Atlanta, GA, USA, June 2009.

[32] C.-H. Hsu, S. Wang, Y. Zhang, and A. Kobusinska, "Mobile edge computing," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 7291954, 3 pages, 2018.

Hindawi
Mobile Information Systems
Volume 2019, Article ID 8278904, 11 pages
https://doi.org/10.1155/2019/8278904

Research Article

A Local Information Sensing-Based Broadcast Scheme for Disseminating Emergency Safety Messages in IoV

Wenjie Wang,[1,2] **Tao Luo**,[2] **and Hongxia Kang**[1]

[1]*National Engineering Laboratory for Transportation Safety and Emergency Informatics, China Transport Telecommunications and Information Center, Beijing, China*
[2]*Beijing Key Laboratory of Network System Architecture and Convergence, Beijing University of Posts and Telecommunications, Beijing, China*

Correspondence should be addressed to Tao Luo; tluo@bupt.edu.cn

Received 5 October 2018; Revised 22 December 2018; Accepted 30 December 2018; Published 3 February 2019

Guest Editor: Mohamed Elhoseny

Internet of Vehicle (IoV) is playing an increasingly important role in constructing an Intelligent Transport System (ITS) of safety, efficiency, and green. Safety applications such as emergency warning and collision avoidance require high reliability and timeliness for data transmission. In order to address the problems of *slow response* and *local broadcast storm* commonly existing among waiting-based relay schemes of emergency messages, a local topology information sensing technology-based broadcast (LISCast) protocol is proposed in this paper, making use of the advantage of probability-based forwarding scheme in redundancy inhibition. According to the beacon broadcasted periodically between vehicles, LISCast collects information about number and distribution of neighbor, from which the *characteristic information* such as effective candidate number, maximum forwarding distance, and global traffic density are extracted. Through embedding the characteristic information into the head of broadcast packets by the message sender for assisting in making relay decision, the alternative receivers uniformly schedule forwarding priorities in a distributed and adaptive way. LISCast works without the help of a roadside unit and generates a little more overhead. The simulation results show that LISCast improves the ability to adapt to dynamic topology by optimizing the performance of delay, redundancy, and broadcast efficiency upon the condition of satisfying the high level of transmission reliability.

1. Introduction

IoV is the most typical applications for the Internet of Things (IoT) technology [1] in the field of transportation. The communication networks of IoV mainly include vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle to pedestrian (V2P), vehicle to network (V2N), and so on [2]. Vehicles can communicate to each other and share data through the onboard devices, which are of great importance in reducing traffic accidents and improving road efficiency [3]. IoV is one of the most significant technologies to realize ITS, which attracts the increasing attentions from the industry and academia. Nowadays, there are two main standards [4] about IoV. One is the developed DSRC (dedicated short range communications) [5], which is proposed and carried out by American and Japan, in the way of ad hoc to generate network using 802.11p as the communication protocol. The other is C-V2X (cellular vehicle-to-everything), which is suggested at most by Europe and China, making use of developing and widely distributed cellular network to satisfy the low delay and high reliability of vehicular environment [6].

Emergency messages always contain information about life, which should be notified to the vehicles located behind in the range of several kilometers driving towards the accident place, for the purpose of avoiding the serial collision and improving driving safety [7, 8]. Because the communication range of vehicle devices is about 300 meters only, multihop forwarding will be used to spread the emergency messages to the risk of zone (RoZ). As is known the core of multihop routing protocols is how to select the relay nodes. According to the way of relay selection, the existing

broadcast strategies mainly include two kinds [9]: the sender-based forwarding scheme and receiver-based forwarding scheme.

The sender-based schemes specify relay nodes by the sender based on the neighbor information. The specified forwarder forwards packets as soon as possible once it receives emergency messages. This scheme can spread messages rapidly. Besides, no matter how to change for the density of traffic, the level of useless duplicates remains steady. It is an effective method to avoid broadcast storm, which is a common problem for designing broadcast protocols. However, these schemes depend on real time and precise neighbor information. As a matter of fact, it is a challenge for beacon to collect the accurate neighbor information because of the highly dynamic topology of IoV. The chosen relay node is not always the optimal candidate in geography, which means that covering the whole RoZ will experience more hops of forwarding. Actually, each time one hop increases in the process of multihop forwarding, more redundancy is produced and the probability for the broadcast to be interrupted increases as well. Furthermore, the reliability of sender-based schemes falls sharply when encountering channel fading and interference in the quickly changing topology of networks.

Receiver-based schemes do well in utilizing the sharing features of wireless channel to disseminate emergency messages. The candidate receivers cooperate with each other to forward packets in a distributed way according to certain rules. For example, the most popular broadcast protocols are farthest-first schemes, which are based on the position of vehicles. The priorities of candidates are directly proportional to the distance between the sender and receivers. The farthest node will forward packets preferentially. On the one hand, the nearer candidates will be suppressed to compete for forwarding, so that less redundancy will be produced. On the other hand, the farthest-first rule can ensure the most extensive coverage per hop, so that fewer hops will be needed to warn all the vehicles locating in the RoZ. Because the forwarding decision is made after receiving packets, the broadcasting continuity can be ensured to some extent, which is why receiver-based schemes attract so much attention from researchers. However, there exist problems of *slow response* and *local broadcast storm* [10] because of the receivers' lack of enough knowledge about the sender's topology, which will be discussed in detail in Section 3.

Based on the analysis of the requirements for disseminating emergency safety messages, this paper focuses on the receiver-based broadcasting scheme, which is one of the most promising protocols in IoV. The main contributions of this paper are two-fold:

(i) First, we highlight and indicate the problems of *slow response* and *local broadcast storm*, which commonly exist in the farthest-first waiting-based broadcasting protocols but are ignored.

(ii) Second, a fast and low overhead broadcasting scheme, called LISCast, is proposed based on the sensing of local topology information as a solution to the problems we analyzed.

The study is organized as following. Section 2 reviews the related works. Section 3 introduces the problems and challenges existing in the farthest-first broadcasting schemes. Section 4 describes in details the design of proposed broadcast protocol LISCast, including the technology of local information sensing, forwarding scheme, and retransmission strategy. Finally, simulation and results analysis are shown in Section 5, which is followed by conclusions in Section 6.

2. Related Works

In order to disseminate emergency messages quickly and reliably, many excellent broadcasting protocols have been proposed in the past years, among which waiting-based, contention-based, and probability-based schemes are the most popular ones.

The waiting-based broadcasting scheme was first introduced to IoV in [11]. All candidates configure their forwarding priorities by assigning different waiting times according to the distance from themselves to the previous forwarder. The famous priority schedule rule is seen in the following formula, which is shown as formula (2) in [11]:

$$D_{\text{wait}}^{\text{j}} = D_{\max} \cdot \left(1 - \frac{d_{\text{ij}}}{R}\right), \tag{1}$$

where d_{ij} is the distance between the receiver j and last forwarder i, R is the communication range, and $\text{D}_{\max}$ is the maximum waiting time. We can see from formula (1) that the larger distance from the receiver to sender, the less waiting time can be scheduled, suppressing the nearer receivers to rebroadcast. In this way, the geography progress of messages in each forwarding hop can be maximized. As a result, fewer hops will be needed to cover the whole RoZ.

Similarly, the authors in [12] allowed the candidates to wait some time before forwarding according to the farthest-first rule. But they did not give exact equations to calculate the waiting time. UMB [13] was first proposed to configure nodes' priorities in the MAC layer. RTS/CTS (Response To Send/Clear To Send), which was first used in unicast, was introduced into broadcast protocol to alleviate the impact of hidden terminal and to enhance broadcast continuity. However, frequent handoff caused by break link would increase extra control delay, preventing messages disseminating quickly. Besides, apart from distance, the speed of candidates was considered to schedule the forwarding priorities in [14]. Although in [15] the farthest-first forwarding scheme was extended to implement in multichannel operation. In the past few years, many other protocols have been proposed with the similar forwarding rule to optimize broadcast performance in certain scenarios such as OppCast [16], UV-CAST [17], ROFF [18], and so on.

Different from waiting-based forwarding schemes, contention-based forwarding schemes assign candidates' priorities using the size of Contention Window ($\text{CW}_{\min}$) rather than the waiting time. In [19], different values of $\text{CW}_{\min}$ are set to vehicles according to their distance from the sender. The longer distance between the receiver and

sender, the smaller CW_{min} value could be configured. In order to reduce redundancy furthermore, in [20] only vehicles falling in some narrow segments could join to compete channel access. Other similar contention-based broadcasting schemes could be seen in [21, 22]. Although the extra waiting delay was eliminated in contention-based schemes, the broadcast efficiency would decrease because the optimal candidates in geography may fail to access the contention channel. Furthermore, since the size of CW_{min} is limited, the number of candidates joining the program of channel competition is certain, leading to serious collision in the dense network, and expanding the size of CW_{min} would increase the delay of channel access.

The orobability-based scheme was firstly proposed on the basis of the farthest-first forwarding scheme by Wisitpongphan et al. [23]. It was an effective method to control redundancy. The well-known representatives are Weighted-*p* and Slotted*P*. The forwarding probability is directly proportional to the distance between the receivers and senders in Weighted-*p*, so that the farthest vehicles had higher probabilities to rebroadcast. To avoid erroneous forwarding judgment, vehicles in Slotted*P* firstly wait for some time according to formula (1) and then rebroadcast messages in a certain probability *P*. To improve the adaptive capacity of routing, many schemes were proposed. For example, in [24] dynamic density was estimated, while in [25] the usage of channel was monitored to adjust forwarding probability. Besides, in [26, 27], real-time vehicle density and distance between vehicles and other factors were combined to schedule rebroadcasting probability. The fewer the vehicles, or the longer the one hop distance, the higher the probability can be set. Although probability-based scheme can reduce packets collision caused by rebroadcasting of neighbors at the same time slot, it is at the cost of reducing broadcast efficiency, because the most optimal candidates do not always win the channel contention for they are forwarding data in some probability.

3. Problems and Challenges

As the popularization of positioning module and the continuous improvement of positioning accuracy, GPS (global positioning system) turns to be the standard configuration of automobile gradually. Position-based protocols have made a great progress in the past few years for disseminating emergency safety messages, among which waiting-based schemes were the most popular ones because they made fully use of the sharing feature of wireless channel and were easy to be realized in engineering. As is shown in formula (1), the priority was set in terms of a timer, by which the farthest candidates were configured the least waiting time to forward packets, so that the single hop progress was maximized and the nearer candidates were restrained to relay, resulting in less redundancy, less contention and fewer hops. However, the difference of waiting time between adjacent candidates was so small that they may forward simultaneously, leading to drastic collision and larger latency of channel access. The situation may be more serious especially in the dense networks. Take the Slotted-1 persistence scheme [23] as an example, without loss of generality, to discuss the problems that waiting-based schemes face.

As is shown in Figure 1, Slotted-1 divides communication range into N_s segments. Vehicles in the same segment have the same priority, and the priority is directly proportional to the distance from the center of segment to the last forwarder. So that vehicles in the farthest segment have the highest priorities in terms of waiting time to rebroadcast. Upon receiving a packet, a node checks the packet ID and rebroadcasts with probability 1 at the end of assigned time slot D_{wait} if it receives the packet for the first time and has not received any duplicates during D_{wait}; otherwise, it discards the packet. To avoid erroneous forwarding judgment when receiving duplicates from multisources, vehicles firstly wait for a regular duration *WAIT_TIME* before rebroadcasting, and the waiting time of candidate j is calculated by the following formula, which is shown as formula (2) in [23]:

$$D_{wait}^{j} = S_{ij} \cdot \sigma, \tag{2}$$

where σ is the one hop time slot and S_{ij} is the configured time slot number between candidate j and the previous forwarder i, which is cited from formula (3) of [23] as following:

$$S_{ij} = N_S \left(1 - \left\lceil \frac{\min\left(d_{ij}, R\right)}{R} \right\rceil\right). \tag{3}$$

Note that if node j receives duplicates from multiple forwarders within the duration of *WAIT_TIME*, it selects the largest D_{wait}^{j} value as its waiting time. In other words, each candidate should use the relative distance to the nearest forwarder to assign waiting time in order to ensure that the farthest receivers rebroadcast firstly. So that the nearer candidates are suppressed to relay. We can see from Figure 1 that vehicles E and F falling in the farthest segment are assigned the highest priority, and vehicle E will be chosen to calculate the waiting time of receiver of next hop so as to reduce the delay of single hop.

Note that the broadcast performance is easy to be affected by the fixed parameters such as *WAIT_TIME* and N_s. The larger the value of *WAIT_TIME*, the lesser the redundancy can be produced, and the higher broadcast reliability is achieved, but the longer extra end-to-end delay could be postponed. In addition, the larger N_s, the greater difference of waiting time between adjacent candidates will be set, hence the less collision will occur, but the longer waiting delay will be assigned for the low priority candidates. Moreover, the waiting-based schemes are weak to adapt to the rapid changing topology, which will be illustrated by the following two examples.

3.1. Slow Response Problem. As is shown in Figure 2, few vehicles locate on the road nonuniformly, which often happens on the highway or during the leisure time in urban scenarios such as morning or night. There are always many empty segments in the coverage of vehicle communications. The *farthest candidates* (e.g., yellow vehicles), even which are actually the optimal candidates in this situation, have to wait certain time to forward packets because it is the *farthest*

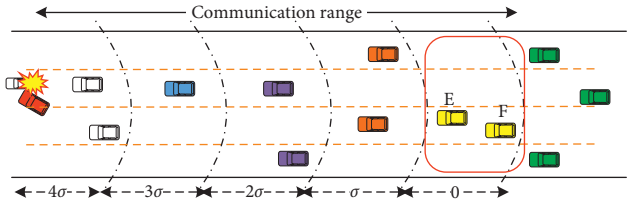


Figure 1: Priority schedule of Slotted-1.

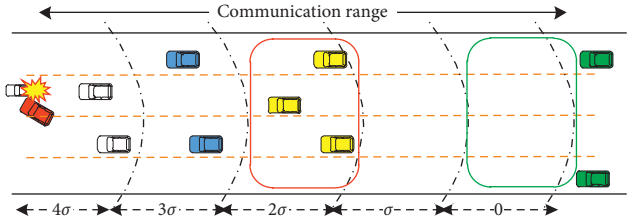


Figure 2: Slow response of Slotted-1.

segment (e.g., green box) that is set the highest priority according to formula (2). The reason is that candidate receivers' lack of enough knowledge about the topology of previous forwarder such as the number of candidates, their distribution and the real-time density, and so on to make more intelligent relay decision. This schedule scheme postpones packets disseminating quickly, and this phenomenon is called *slow response*.

3.2. Local Broadcast Storm. Meanwhile, as is shown in Figure 3, there are so many vehicles running here and there in the dense network such as rush hours in the urban or near toll station on the highway. Many vehicles locating in the same segment (e.g., yellow cars in red box) have the same priority to forward packets, according to the waiting time schedule rule, formula (2), for instance. The time difference of them is so little that they relay packets almost at the same time slots simultaneously, leading to more useless duplicates, higher probability of collision, longer channel access delay, and lower reliability, and this phenomenon is called *local broadcast storm*.

Different from mobile ad hoc network, vehicles in IoV move in high speed, resulting in highly dynamic topology, channel fading, and interference, which are serious challenges for data transmission. Besides, slow response and local broadcast storm problems of waiting-based forwarding schemes lead to obvious performance deterioration, which should be optimized so as to adapt to the dynamic characteristic of IoV.

4. Design of LISCcast

Since the typical waiting-based forwarding scheme lacks of enough knowledge about the topology characteristic of candidates, it is hard to adapt to the dynamic topology, leading to the problems of *slow response* and *local broadcast storm*. A local information sensing broadcast protocol is

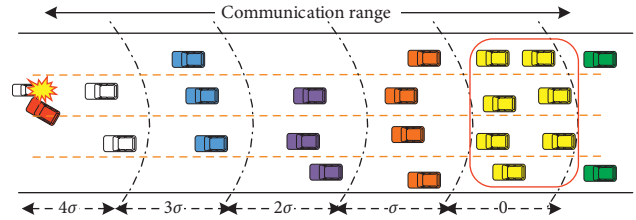


Figure 3: Local broadcast storm of Slotted-1.

proposed in this section to optimize the broadcast performance.

4.1. Overview of LISCast. The packet flow of LISCast can be seen in Figure 4. The flow of emergency packets works under two models. One model is the sender (called source for the first hop) sensing local topology information based on BSM, while the other model is the receivers completing forwarding packets. When receiving emergency packets on the network layer from upper layer, the sender calculates its characteristic information of topology using the local information sensing technology, which will be described in detail in the next Section 4.2. Together with other normal information about broadcast messages, the important characteristic information are embedded into the head of emergency packets before broadcasting around. Upon receiving emergency packets, the candidates assign the waiting time and forwarding probability according to the uniform characteristic information of the previous forwarder and separate distance from themselves to the sender. Only the candidates that pass the probability test can take part in the progress of waiting. If candidates do not receive any duplicate or ACK during the period of waiting time, they will relay packets; otherwise, the waiting progress will be canceled, which means other candidates have already rebroadcasted. The retransmission progress will be started at the end of the max waiting time if the sender (last forwarder) does not receive any ACK or duplicates. The packet will be disseminated hop by hop in this way, unless it covers the whole RoZ.

4.2. The Local Information-Sensing Technology. The wildly existed beacon (called BSM, Basic Safety Message in [5]) in IoV is used to sense the local topology information for relay decision. The local information sensing technology faces two aspects of challenges at least as follows:

Challenge 1: Low Overhead and Fully Distributed. As we know, it is better for safety messages to operate in a distributed way in the highly dynamic environment for satisfying the requirements of extremely low timeliness. It is difficult, if not infeasible, to design a centralized controller for safety data dissemination due to rapid mobility of vehicles. Frequent control information exchange will introduce heavy overhead and postpone emergency messages disseminating quickly. We need to design a fully distributed and lightweight protocol so that safety data can be efficiently spread to vehicles.

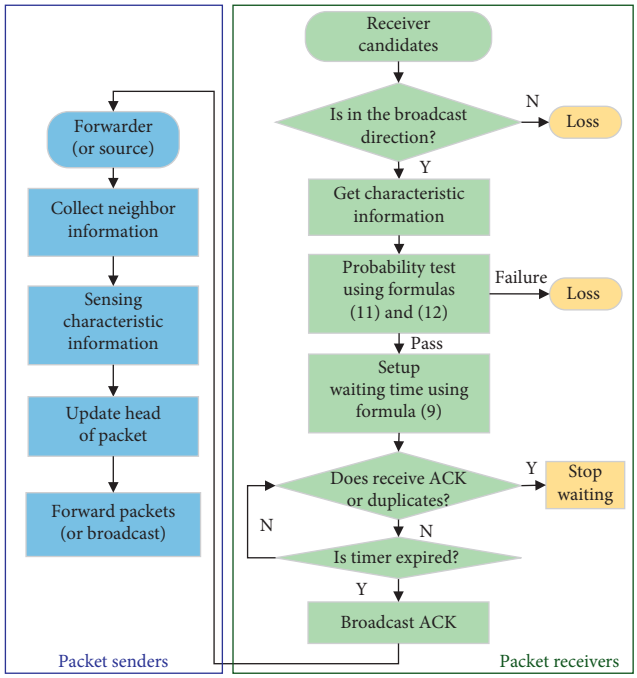


Figure 4: The packet flow of LISCast.

Challenge 2: Uniform Forwarding Rule. The characteristic information which is used by candidates to cooperate to assign priorities should be uniform. Because of the highly changing topology and packet loss, the characteristic information that each vehicle senses according to periodic beacons may be different from each other. If assigning priorities using vehicles' respective characteristic information, several candidates could be scheduled the same waiting time to forward packets simultaneously, intensifying packets collision and increasing channel accessing delay. Therefore, uniform characteristic information is beneficial to distinguish the forwarding priorities of candidates.

The following parts of this section discuss the design of local information sensing technology in detail.

Vehicles in the network periodically broadcast beacons to notify neighbors its basic status information such as ID, location, velocity, direction, and time stamp and so on. Through sensing the number and distribution of neighbors, vehicles can construct a local topology graph. According to the enough information about topology graph, it is easy for candidates to select the optimal relay nodes. However, sharing the topology graph costs heavy overhead, which is also easy to cause network congestion. In order to reduce the overhead, a tradeoff scheme can be available. Only a list of IDs ordered by descending priority in advance is embedded into the head of packets for relay decision. Although the size of IDs list is much smaller than that of topology graph, it still occupies several bytes which cannot be ignored, especially in the dense network where hundreds of neighbors running around. Broadcasting such large packet immensely increases the probability of channel congestion. To address the Challenge 1, a low overhead scheme is proposed in this section. Based on the neighbor information, only the characteristic information of local topology such as the *effective candidate number, the effective communication distance,* and *traffic density* are extracted and embedded into the head of packets. No matter how density of traffic is changed, the size of characteristic information remains unchanged. Therefore, the increased overhead is low and keeps stable when emergency events happen. Besides, the local information sensing technology operates only on the basis of beaconing messages, without any help of centralized controller, satisfying the distributed feature of IoV for disseminating safety messages.

The definitions of variables are given below.

Definition 1. Effective candidate number (ECN): the number of candidates located in the broadcast direction considering the distribution of vehicles.

ECN is used to adjust the number of segments that the communication range is divided into, taking the changing distribution of vehicles into consideration. In fact, we mainly care about the number of vehicles locating in the farthest segment. Thus, positive distance weighting coefficient [28] is used to calculate the value of ECN, which is shown in the following equation:

$$N_{\mathrm{ECN}} = \sum_{k=1}^{N_s} \lambda_k \cdot N_k, \tag{4}$$

where N_k is the number of vehicles in the k_{th} segment and λ_k is the weighting coefficient of the k_{th} segment, which is expressed as

$$\lambda_k = \frac{d_{k\mathrm{S}}^q}{R}, \tag{5}$$

where $d_{k\mathrm{S}}$ is the distance from the k_{th} segment to the sender, and q is a positive integer.

We can see from formula (4) that the more vehicles far away from the sender, the larger ECN can be set. For example, in the situation of dense traffic, more segments will be beneficial to differentiate the priorities of adjacent candidates, mitigating the *local broadcast storm* caused by simultaneous rebroadcasting. On the contrary, the less vehicles locate in the farther segments, in the sparse network for instance, the smaller ECN can be configured, and the fewer empty segments turns up where with no vehicles locating. So that at least one vehicle can be assigned into the optimal segment, avoiding unnecessary waiting time before forwarding.

Definition 2. Effective communication distance (ECD): the distance from the farthest neighbor to the sender.

The relative distance from candidates to previous forwarder is the key to calculate the priorities of candidates. Using ECD to substitute the fixed parameter R for assigning the waiting time for each candidate can improve the adaptability of routing protocol against the dynamic of topology.

ECN represents the changing number of candidates, while ECD reflects the dynamic distribution of candidates. With the help of ECN and ECD in LISCast, there are always

candidates locating in the dynamic farthest segment and they can rapidly relay packets without any delay, no matter the density of topology how to change. Thus, the *slow response* problem can be solved mostly.

Definition 3. Effective traffic density (ETD): the estimated density with the consideration of vehicle distribution.

Due to the high mobility of vehicles, it is hard to collect the precise neighbor information for designing the exact values of ECD and ECN. Hence, there may be no less than one candidate locating at the farthest segment for competing channel access, which still leads to collision. ETD is proposed in this section to provide the changing topology information for supporting prediction of ECN and ECD and assignment of forwarding probability.

The speed-density liner model [29] is used in this section to estimate the real time traffic density $\overline{\rho}$, which is expressed as

$$\overline{V} = V_{\mathrm{f}}\left(1 - \frac{\rho}{\rho_0}\right), \tag{6}$$

where V_{f} is the limited velocity when vehicle drives freely, ρ_0 is the maximum density that the road can support, and $\overline{V}$ is the average velocity of target vehicle, which can be estimated by the neighbor information.

Given a velocity set of target vehicle at the moment t, $\{V_{h0}, V_{h1}, V_{h2}, V_{h3}, \ldots, V_{hm}\}$, where h is the h_{th} broadcasting period, V_{h0} is the velocity of target vehicle, V_{hl} is the velocity of neighbor l, and m is the number of neighbors. Then, the average velocity of target vehicle at this moment considering vehicles' distribution can be expressed as

$$\overline{V_h} = \sum_{k=1}^{m} \lambda_k V_{hk}, \tag{7}$$

where λ_k is the weighting coefficient of the k_{th} neighbor, which can be calculated by formula (5) similarly. After broadcasting beacons for T times, a set of average velocity can be produced, and the average velocity of target vehicle during period T can be expressed as

$$\overline{V} = \frac{\sum_{h=1}^{T} \overline{V}_h}{T}. \tag{8}$$

Gathering formulas (6)–(8) can calculate the estimated density, as the indicator of real-time traffic flow.

In addition, because of the channel fading and dynamic topology, the characteristic information that single vehicle senses is different from each other. The priorities of some candidates scheduled by the single characteristic information of themselves may turn to be the same, which will lead to packet collision and interrupt broadcast progress. Therefore, to solve the Challenge 2, LISCast assigns the priorities of all candidates using the same characteristic information, which represents the main topology information of previous forwarder and is embedded into the head of packet itself. Scheduling the waiting time according to the uniform information and the same rule, the candidates will compete to forward packets orderly.

After sensing the local topology information based on the neighbor information collecting from beacons, the data frame in LISCast is designed in Figure 5.

The head of LISCast packet includes three parts. The first part is main information about emergency events such as the type of message, the time and location of emergency events, the time stamp and position of last forwarder, broadcast direction, and so on. The second part is characteristic information of candidate topology, which is used for forwarding cooperation including the effective communication distance, the effective candidate number, and the effective traffic density. The last is the extension field.

In LISCast, the precise of neighbor information collecting from periodic beacon is the key. Many schemes were proposed to ensure the reliability of beacons [30]. The most popular method is repeating broadcasting several times during the period of beacon, and the packet reception ratio could reach more than 90% through test [31].

4.3. Relay Strategy. LISCast is improved from the typical formula (2) of waiting-based forwarding scheme, for the purpose of optimizing the performance of delay and redundancy and enhancing the adaptability of routing protocol against the dynamic topology. The priority schedule rule is shown as follows:

$$T_{\mathrm{wait}}^{\mathrm{j}} = N_{\mathrm{S}}^{\mathrm{j}} \cdot \sigma, \tag{9}$$

where $T_{\mathrm{wait}}^{\mathrm{j}}$ is the waiting time of candidate j, and $N_{\mathrm{S}}^{\mathrm{j}}$ is the number of segment that candidate j belongs to in the communication range of previous forwarder, which is expressed as

$$N_{\mathrm{S}}^{\mathrm{j}} = \left\lceil N_{\mathrm{ECN}} \cdot \frac{\max\left(0, d_{\mathrm{ECD}} - d_{\mathrm{ij}}\right)}{d_{\mathrm{ECD}}} \right\rceil, \tag{10}$$

where d_{ECD} is the ECD of previous forwarder i, d_{ij} is distance between candidate j and i, and N_{ECN} is the ECN of i.

When receiving emergency messages carrying the characteristic information of last forwarder, all the receivers calculate their waiting time using formula (9). Both of the characteristic information d_{ECD} and N_{ECN} are used by LISCast to make sure that one candidate at least but not so much candidates are falling in the farthest segment ready to forwarding messages with the least waiting delay, which is always set as zero.

Furthermore, in order to restraint the useless redundancy, a probability-based scheme is introduced to suppress the nearer candidates to compete to rebroadcast. The probability is directly proportional to the distance between the receivers and senders, which is shown in formula (11).

$$P_{\mathrm{j}} = \min\left(1, \frac{d_{\mathrm{ij}}}{d_{\mathrm{ECD}}}\right), \tag{11}$$

where P_{j} is the forwarding probability of candidate j. In order to balance the waiting delay and redundancy, the value of N_{ECN} is always not larger enough in LISCast to differentiate all the candidates. As a matter of fact, there are still

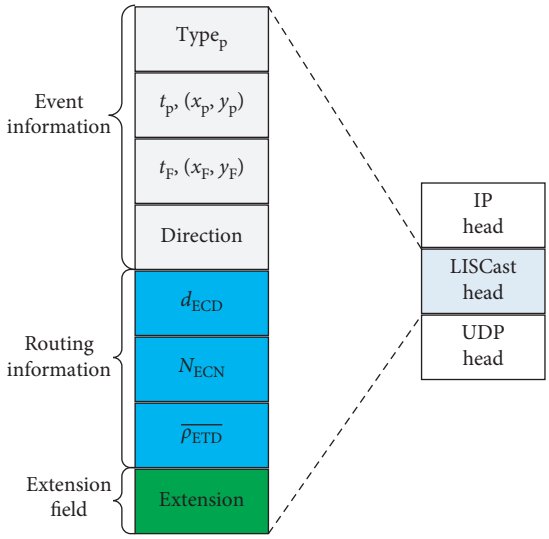


Figure 5: Data frame of LISCast.

many candidates with the same priorities colliding to each other when rebroadcasting packets simultaneously in the extremely dense network. Therefore, the estimated density indicator ETD is used by LISCast to mitigate collision through suppressing some candidates relaying together with distance-based probability P_j, which is shown as formula (12).

$$P_d = \begin{cases} P_{d1}, \overline{\rho_{ETD}} \in \{\text{sparse traffic}\}, \\ P_{d2}, \overline{\rho_{ETD}} \in \{\text{medium traffic}\}, \\ P_{d3}, \overline{\rho_{ETD}} \in \{\text{dense traffic}\}, \end{cases} \quad (12)$$

where $1 \geq P_{d1} \geq P_{d2} \geq P_{d3} \geq 0$ is the forwarding probability assigned through the estimated density indicator $\overline{\rho_{ETD}}$, which is used here to schedule forwarding probability roughly. $\overline{\rho_{ETD}}$ can be used to adjust the dynamic N_{ECN} more precisely in the future.

In particular, the mechanism of LISCast depends on the precise of neighbor information collecting from periodic beacon, which is near real time. So it is normal that the distance between the candidates and sender is larger than d_{ECD}. In this situation, the waiting time is set zero and the forwarding probability only relays on the P_d, which reflects the global traffic density in the perspective of the previous forwarder. So that LISCast can adapt to the dynamic topology to some extent. Besides, the farthest-first forwarding rule in LISCast can also maximize the coverage of each hop, realizing rapid dissemination of emergency messages.

4.4. Retransmission Mechanism. As we know, there is no handoff or retransmission mechanism like unicast adopted in broadcast scheme of 802.11p MAC layer, so the broadcast reliability may not be ensured. The simplest method to improve reliability is repeating broadcasting emergency messages many times. It will produce heavy redundancy and exhaust the limited spectrum. A retransmission mechanism is proposed by LISCast to ensure the continuance of broadcast. The last forwarder (including the source node) will start the retransmission progress only in the case of monitoring none duplicates or ACK at the end of the maximum waiting time.

5. Simulation and Results Analysis

The popular network simulator NS2 and transportation simulator SUMO [32] are introduced in this section to illustrate and analyze the performance of LISCast.

5.1. Simulation Scenario. Take a bidirectional highway with six lanes and 3 km long as an example of scenario. The width of the single lane is ignored comparing to the communication range of 300 meters. 20~100 vehicles enter the highway randomly and drive at the speed of 30–100 km/h using SUMO. Vehicles generate one emergency packet per one second at the probability of 0.5. The other main parameters are summarized in Table 1.

5.2. Performance Metrics. To illustrate the effectiveness and feasibility of the proposed broadcast scheme, the following typical protocols are studied comparatively.

5.2.1. Mflood. The most original receiver-based protocol is implemented into VANET. Upon receiving a packet, vehicles only in the direction of broadcast in this paper forward it immediately if the packet is new. Broadcast storm in the scenario of dense network needs to be optimized.

5.2.2. FARTHEST. The farthest-first scheme is first proposed in [11] for VANET. The vehicles that are farther to the sender are assigned higher priority to access the channel in terms of less waiting time, optimizing hop progress and forwarding latency. That is why farthest is suggested as the basic idea of many protocols.

5.2.3. Slotted-1. This is one of the most representative waiting-based schemes in IoV. Slotted-1 firstly waits for the period time *WAIT_TIME* for receiving packets form multi forwarders and then configures waiting time using farthest-first rule for the candidates locating in the divided narrow segments.

5.2.4. SlottedP. This is one of the typical probability-based schemes. Similar to Slotted-1, Slotted*P* assigns priorities of candidates through relative distance between the receivers and forwarders, but forwards packets with a probability (e.g., 50%).

5.2.5. Mflood, FARTHEST, Slotted-1, and SlottedP. Represent the most familiar design principles of safety messages dissemination schemes in IoV and have served as benchmarks for quite a few researches, e.g., [9, 16–18]. In LISCast, we configure the forwarding probability P_d as {0.95, 0.85, 0.75} according to the estimated traffic density, for the purpose of mitigating collision roughly in dense network. As

Table 1: Parameters of simulation.

Parameter	Value
Car following model	Krauss
PHY model	TwoRayGround
MAC model	802.11 DCF
Size of CBR	512 bytes
Maximum waiting time	25, 100 ms
Number of segments	5
Forwarding probability, P_d	{0.95, 0.85, 0.75}
Simulation time	200 seconds

a matter of fact, this probability-based scheme that LISCast uses in this paper is only an ordinary advice for reducing redundancy, which should be meticulously designed together with the developed density estimation method in the future.

The following performance metrics are evaluated for comprehensively understanding the benefits of LISCast.

5.2.6. Packet Delivery Ratio (PDR). It is the percentage of packets covering the whole RoZ among the total packets the sources generate.

5.2.7. End-to-End Delay (E2ED). It is the time difference between generating time and receiving time when the messages reach the end of RoZ.

5.2.8. Broadcast Redundancy (BR). It is the number of duplicates generating per packet.

5.2.9. Forwarding Efficiency (FE). FE is the contribution yields to PDR each hop.

5.3. Results Analysis. First of all, this section configures the maximum waiting time as 25 ms and runs the simulation 10 times with different initialization and gets the average values in NS2.

As is shown in Figure 6 that as the increase of vehicle number, the PDR of all the protocols increase as well, because the connectivity of network becomes better, and more vehicles are available to rebroadcast messages. When the number reaches 80 vehicles/3 km, the PDR of most protocols begins to decline, because more frequent collision causes high packet loss due to simultaneous forwarding. Probability scheme are introduced by Slotted*P* and LISCast to mitigate collision and reduce redundancy, so their PDRs keep increasing even in dense network. Because candidates in Slotted*P* forward messages in the fixed probability, the PDR is lower than other protocols in the sparse network. On the contrary, LISCast adjusts the forwarding probability according to the estimated real time density and the dynamic distribution of candidates, thus its PDR keeps at the high level. However, the PDR of LISCast is still inferior to that of Slotted-1 when the number is less than 80 per 3 km. That is because the candidates with lower priorities fail to hear the rebroadcasting due to channel fading and interference. And

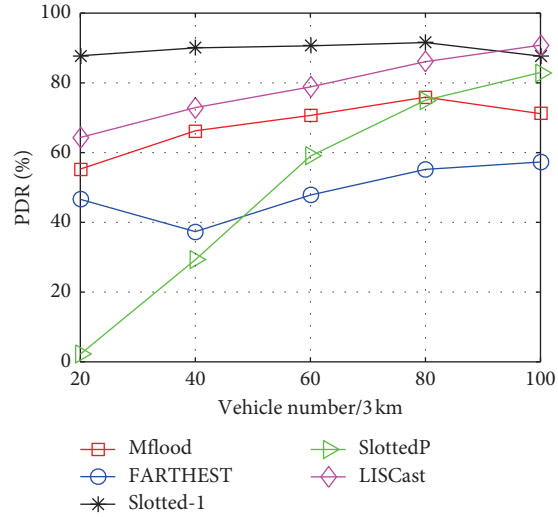


Figure 6: Packet delivery ratio vs vehicle number.

they still take part in forwarding, leading to more collision and packet loss. Furthermore, Slotted-1 improves PDR through mitigating erroneous forwarding judgment in the way of waiting for a period of *WAIT_TIME* for receiving message from multisources. Hence, the PDR of Slotted-1 plays best among the chosen protocols. Nevertheless, none measure is adopted by FARTHEST to reduce collision and erroneous judgment, thus its PDR is the worst of all in the most density scenarios.

We can see from Figure 7 that the E2ED of all protocols keeps increasing as the increase of vehicle number. That is because more vehicles compete to forward messages, leading to longer access delay of wireless channel. In particular, the E2ED of FARTHEST, Slotted-1, and Slotted*P*, which belong to waiting-based forwarding schemes, in the extremely sparse network such as 20 vehicles per 3 km is much larger than that in other density scenarios, 40–60 vehicles per 3 km, for instance. That is because the lower priorities candidates have to wait for the extra time before forwarding, while the higher priorities positions locating none candidates due to nonuniform distribution, which phenomenon is slow response we have discussed in detail in Section 3. Therefore, LISCast uses characteristic information such as effective candidate number and the maximum forwarding distance to assist to assign waiting time for receivers in a distributed way, ensuring the optimal candidates forwarding messages without any extra delay even in the situation of sparse network. Besides, in order to avoid erroneous judgment, Slotted-1 and Slotted*P* introduce *WAIT_TIME* before forwarding, thus their E2ED is much larger than the three other protocols in which candidates do not have to wait for the extra time. Indeed, the PDR is improved in this way, but is at the cost of increasing delay. On the contrary, LISCast innovatively makes use of effective candidate number to mitigate collision and designs effective forwarding distance to ensure the optimal candidates forwarding without any latency. Hence, its E2ED is much less than other protocols. At the point of 20 vehicles per 3 km, the E2ED of LISCast is 3 times less than that of Slotted-1. The problem of *slow*

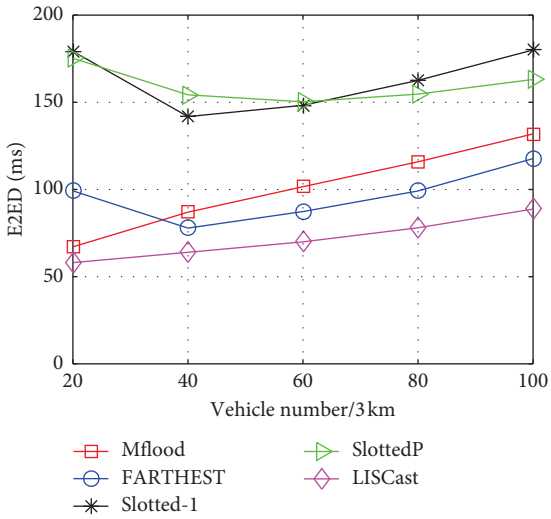


Figure 7: End-to-end delay vs vehicle number.

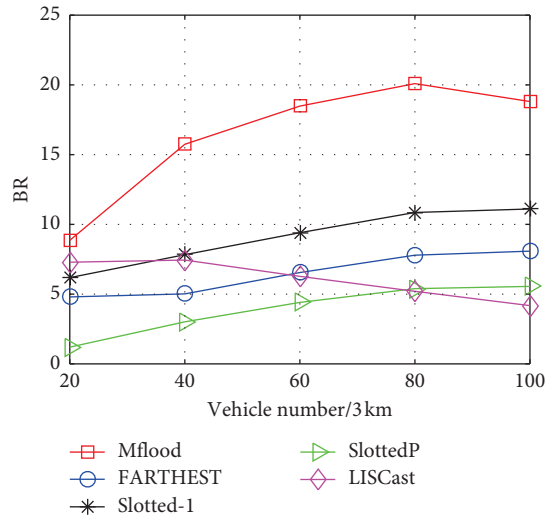


Figure 8: Broadcast redundancy vs vehicle number.

response discussed in Section 3 is addressed in LISCast reasonably.

Figures 8 and 9 show the broadcast redundancy and forwarding efficiency vs the number of vehicles. We can see that as the increase of density of vehicles, the connectivity of network gets better, and more vehicles joins to forward packets. Thus, the increasing rebroadcasting aggravates channel contention and packets collision, leading to more redundancy and bringing down the increasing speed of PDR. As a result, all the existed protocols' BR (Figure 8) increase and the FE (Figure 9) decrease inversely, and the descending speed increases with the number of vehicles. This is the problem of *local broadcast storm*. FARTHEST schedules priorities based on the distance between the sender and receivers to restrain near candidates forwarding, so its BR and FE outperform Mflood. Moreover, Slotted-1 divides communication range into some segments to differentiate candidates' priorities so as to reduce redundancy, so its BR and FE are superior to that of FARTHEST, but worse than Slotted*P*, in which probability forwarding scheme is proposed to alleviate collision in dense network. However, the configuration of fixed probability in Slotted*P* losses the PDR, especially in the situation of sparse network. Correspondingly, LISCast makes use of characteristic information about dynamic topology such as the maximum forwarding distance, and candidate number and distribution to adjust the number of segments at which candidates locating, and to assign forwarding probability according to sensing traffic density and distribution. As a result, the performance of BR and FE are improved tremendously compared to the other schemes. In this way, the problem of *local broadcast storm* we have analyzed in Section 3 is solved in LISCast with low overhead and in a fully distributed way. Nevertheless, in the sparse network, the performance of LISCast does not very well. That is because the precise of neighbor information, based on which the sensing technology collects characteristic information for forwarding decision, gets worse due to quick mobility of vehicles. So that the adaptive beacon broadcasting scheme is necessary for LISCast to grantee accurate services.

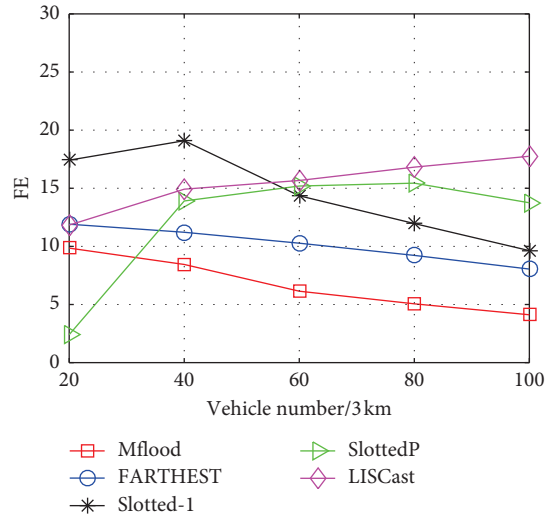


Figure 9: Forwarding efficiency vs vehicle number.

Furthermore, we configure the maximum waiting time as 100 ms in the simulation to explore the performance of the proposed scheme, compared with the Slotted-1 in the case of 25 ms.

Figures 10–12 show the delay, broadcast redundancy, and forwarding efficiency of LISCast and Slotted-1 in the case of 25 ms and 100 ms, respectively. We can see from these figures that in the situation of 100 ms, the performance of BR and FE of Slotted-1 is much better than that in the case of 25 ms, but the E2ED is larger. That is because the larger maximum waiting time is beneficial to differentiate the priorities of forwarding, reducing collision caused by simultaneous rebroadcasting, but is at the cost of longer E2ED. Accordingly, in order to balance the broadcast reliability, timeliness and efficiency, LISCast makes use of characteristic information to adjust the waiting delay and probability dynamically according to the local topology sensing technology. As is shown in Figures 10–12 that

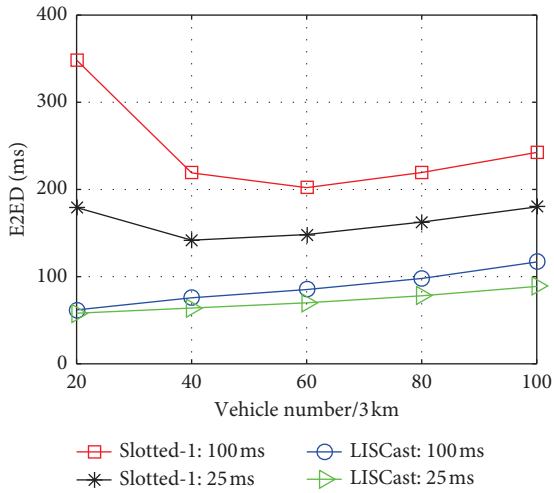


Figure 10: End-to-end delay in 100/25 ms vs vehicle number.

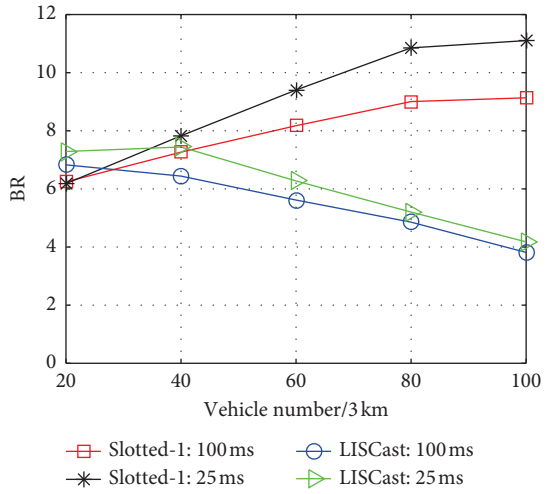


Figure 11: Broadcast redundancy in 100/25 ms vs vehicle number.

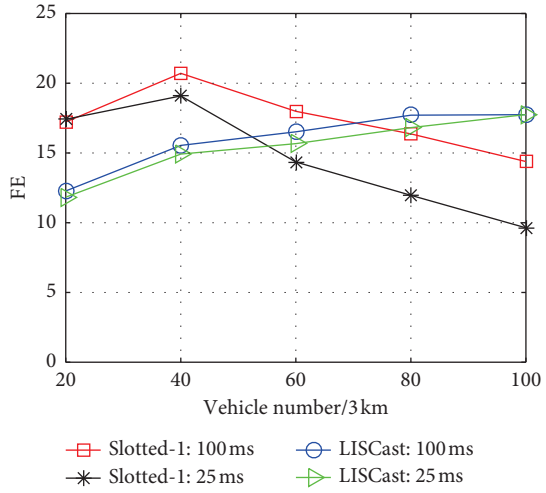


Figure 12: Forwarding efficiency in 100/25 ms vs vehicle number.

LISCast perform well both in the two waiting time configurations and is not sensitive to the changing topology. In the case of 100 ms, the E2ED of LISCast is 7 times better than that of Slotted-1 in the sparse network, while in the situation of 25 ms, the BR of LISCast is 3 times better than that of Slotted-1 in the dense network. This observation can show that it is beneficial and feasible for LISCast to optimize the performance using local information sensing technology.

6. Conclusions

A local topology information sensing technology based broadcast scheme is proposed in this paper to address the slow response and local broadcast storm problems existing in the typical protocols. LISCast makes use of periodic beacon to collect neighbor information, through which the characteristic information of topology are extracted such as effective candidate number, effective forwarding distance, and effective traffic density. The original information of emergency messages and uniform characteristic topology information of the sender are gathered together for the purpose of assisting receivers to rebroadcast messages in a fully distributed way. The simulation results show that the proposed scheme is effective and feasible on improving the broadcast performance with little overhead. Compared with the typical waiting-based and probability based protocols, LISCast plays the best on end-to-end delay in most kinds of density scenarios and outperforms on broadcast redundancy and forwarding efficiency in the dense networks. However, LISCast does not always work the best, in the sparse networks, for instance, because the characteristic information that BSM provides is not so precise. Therefore, beacon adaptive technology is necessary in the future for the proposed scheme to support more precise services and to improve the availability to adapt to the highly dynamic topology.

Data Availability

Readers can access the data underlying the findings of the study by sending email to the author Wenjie Wang at isa_guet@163.com or the corresponding author Tao Luo at tluo@bupt.edu.cn.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported in part by the National Natural Science Foundation of China under Grant no. 61571065.

References

[1] S. Kuutti, S. Fallah, K. Katsaros, M. Dianati, F. Mccullough, and A. Mouzakitis, "A survey of the state-of-the-art localization techniques and their potentials for autonomous vehicle applications," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 829–846, 2018.

[2] Y. J. Choi, J. Hur, H. Y. Jeong et al., "Special issue on V2X communications and networks," *Journal of Communications & Networks*, vol. 19, no. 3, pp. 205–208, 2017.
[3] E. Eze, S. Zhang, E. Liu et al., "Achieving reliable communication in vehicular ad-hoc networks (VANETs): a survey," in *Proceedings of International Conference on Automation and Computing*, pp. 1–6, Huddersfield, UK, September 2017.
[4] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, no. 99, pp. 1–17, 2018.
[5] B. Li, G. J. Sutton, H. Bo et al., "Modeling and QoS analysis of the IEEE 802.11p broadcast scheme in vehicular ad hoc networks," *Journal of Communications & Networks*, vol. 19, no. 2, pp. 169–179, 2017.
[6] G. Naik, J. Liu, and J.-M. J. Park, "Coexistence of wireless technologies in the 5 GHz bands: a survey of existing solutions and a roadmap for future research," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1777–1798, 2018.
[7] G. Luo, Q. Yuan, H. Zhou et al., "Cooperative vehicular content distribution in edge computing assisted 5G-VANET," *China Communications*, vol. 15, no. 7, pp. 1–17, 2018.
[8] X. Zhang, Q. Miao, and Y. Li, "An adaptive link quality based safety message dissemination scheme for urban VANETs," *IEEE Communications Letters*, vol. 22, no. 10, pp. 2104–2107.
[9] W. Wang, "Quality of forwarding-based data disseminating strategy in urban VANET," *Journal of China Universities of Posts and Telecommunications*, vol. 22, no. 6, pp. 50–59, 2015.
[10] G. Li, W. Wang, X. Yao, and W. Chen, "SOBP: a sender-designated opportunistic broadcast protocol for VANET," *Telecommunication Systems*, vol. 53, no. 4, pp. 453–467, 2013.
[11] L. Briesemeister and G. Hommel, "Role-based multicast in highly mobile but sparsely connected ad hoc networks," in *Proceedings of First Annual Workshop on Mobile and Ad Hoc Networking and Computing. MobiHOC*, pp. 45–50, Boston, MA, USA, August 2000.
[12] T. Osafune, L. Lin, and M. Lenardi, "Multi-hop vehicular broadcast (MHVB)," in *Proceedings of International Conference on ITS Telecommunications*, pp. 757–760, IEEE, Chengdu, China, June 2007.
[13] G. Korkmaz and E. Ekici, "Urban multi-hop broadcast protocol for inter-vehicle communication systems," in *Proceedings of ACM Workshop on Vehicular Ad Hoc Networks*, pp. 76–85, Philadelphia, PA, USA, October 2004.
[14] Y. T. Yang and L. D. Chou, "Position-based adaptive broadcast for inter-vehicle communications," in *Proceedings of IEEE International Conference on Communications Workshops*, pp. 410–414, IEEE, Beijing, China, May 2008.
[15] P. Akkhara, Y. Sekiya, and Y. Wakahara, "Efficient alarm messaging by multi-channel cut-through rebroadcasting based on inter-vehicle communication," *IAENG International Journal of Computer Science*, vol. 36, no. 2, 2009.
[16] M. Li, W. Lou, and K. Zeng, "OppCast: opportunistic broadcast of warning messages in VANETs with unreliable links," in *Proceedings of International Conference on Mobile Adhoc and Sensor Systems*, pp. 534–543, Macau, China, October 2009.
[17] W. Viriyasitavat, O. Tonguz, and F. Bai, "UV-CAST: an urban vehicular broadcast protocol," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 116–124, 2011.
[18] H. Yoo and D. Kim, "ROFF: RObust and fast forwarding in vehicular ad-hoc networks," *IEEE Transactions on Mobile Computing*, vol. 14, no. 7, pp. 1490–1502, 2015.
[19] C. F. Chiasserini, E. Fasolo, R. Furiato et al., "Smart broadcast of warning messages in vehicular ad hoc networks," in *Proceedings of Workshop Interno Progetto NEWCOM (NoE)*, Turin, Italy, November 2005.
[20] K. A. Hafeez, L. Zhao, Z. Liao et al., "A new broadcast protocol for vehicular ad hoc networks safety applications," in *Proceedings of Global Telecommunications Conference*, pp. 1–5, Miami, FL, USA, December 2010.
[21] S. Panichpapiboon and W. Pattara-Atikom, "A review of information dissemination protocols for vehicular ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 3, pp. 784–798, 2012.
[22] R. Chen, W.-L. Jin, and A. Regan, "Broadcasting safety information in vehicular networks: issues and approaches," *IEEE Network*, vol. 24, no. 1, pp. 20–25, 2010.
[23] N. Wisitpongphan, O. K. Tonguz, J. S. Parikh et al., "Broadcast storm mitigation techniques in vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 14, no. 6, pp. 84–94, 2007.
[24] I. Ibrahim, M. C. Weigle, and M. Abuelela, "Probabilistic inter-vehicle geocast for dense vehicular networks," in *Proceedings of IEEE 69th Vehicular Technology Conference*, pp. 1–5, Barcelona, Spain, April 2009.
[25] S. Oh, J. Kang, and M. Gruteser, "Location-based flooding techniques for vehicular emergency messaging," in *Proceedings of International Conference on Mobile & Ubiquitous Systems*, pp. 1–9, San Jose, CA, USA, July 2006.
[26] D. P. Agrawal, A. Mostafa, and A. M. Vegni, "CAREFOR: collision-aware reliable forwarding technique for vehicular ad hoc networks," in *Proceedings of International Conference on Computing, Networking and Communications*, pp. 773–777, Honolulu, HI, USA, January 2013.
[27] K. A. Hafeez, L. Zhao, Z. Liao et al., "A new broadcast protocol for vehicular ad hoc networks safety applications, global telecommunications conference," in *Proceedings of IEEE Global Telecommunications Conference GLOBECOM*, pp. 1–5, Miami, FL, USA, December 2010.
[28] U. Schirpke, S. Hölzler, G. Leitinger, M. Bacher, U. Tappeiner, and E. Tasser, "Can we model the scenic beauty of an alpine landscape?," *Sustainability*, vol. 5, no. 3, pp. 1080–1094, 2013.
[29] C. F. Shao, C. Z. Xiao, B. B. Wang et al., "Speed-density relation model of congested traffic flow under minimum safety distance constraint," *Journal of Traffic and Transportation Engineering*, vol. 15, no. 1, pp. 92–99, 2015.
[30] F. Farnoud and S. Valaee, "Reliable broadcast of safety messages in vehicular ad hoc networks," in *Proceedings of Conference on Computer Communications*, pp. 226–234, Rio de Janeiro, Brazil, April 2009.
[31] Q. Xu, T. Mak, J. Ko et al., "Medium access control protocol design for vehicle–vehicle safety messages," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 2, pp. 499–518, 2007.
[32] R. Riebl, H. J. Günther, C. Facchi et al., "Artery: extending veins for VANET applications," in *Proceedings of International Conference on Models and Technologies for Intelligent Transportation Systems*, pp. 450–456, Budapest, Hungary, June 2015.

Hindawi
Mobile Information Systems
Volume 2019, Article ID 9892512, 9 pages
https://doi.org/10.1155/2019/9892512

Research Article

A New Distance Vector-Hop Localization Algorithm Based on Half-Measure Weighted Centroid

Lu Jian Yin

College of Information Engineering, Chao Hu University, Hefei, China

Correspondence should be addressed to Lu Jian Yin; jianyinlu@163.com

Received 11 September 2018; Revised 26 November 2018; Accepted 10 December 2018; Published 3 January 2019

Guest Editor: Mohamed Elhoseny

Considering the defects of the Distance Vector-Hop (DV-Hop) localization algorithm making errors and having error accumulation in wireless sensor network (WSN), we proposed a new DV-Hop localization algorithm based on half-measure weighted centroid. This algorithm followed the two-dimensional position distribution, designed the minimum communication radius, and formed a reasonable network connectivity firstly. Then, the algorithm corrected the distance between the beacon node and its neighbour node to form a more accurate jump distance so that the shortest path can be optimized. Finally, we theorized the proposed localization algorithm and verified it in simulation experiments, including same communication radius, different communication radii, and different node densities in same communication radius, and have compared the localization error and localization accuracy, respectively, between the proposed algorithm and the DV-Hop localization algorithm. The experiment's result shows that the proposed localization algorithm have reduced the localization's average error and improved the localization's accuracy.

1. Introduction

As there is rapid development in wireless communication, the rapid development of low energy, low cost, intensive, multifunctional tiny wireless sensor network is promoted. And a large number of wireless sensor nodes are one of the key elements of wireless sensor networks [1, 2]; therefore, research on location technology in wireless sensor networks is one of the key issues in the research of wireless sensor networks, which is of great significance.

The DV-Hop localization algorithm [3] was first proposed by Dragos Niculescu et al. of Rutgers, USA, which is a distributed localization algorithm based on distance vector routing protocol without ranging [4]. Many scholars and scientific research institutions have carried out in-depth research on the DV-Hop Localization algorithm. In reference [5], in order to reduce the DV-Hop error, the ideal beacon node spacing is introduced to eliminate the larger error in the average single-hop distance calculated by the beacon node, and the average single-hop distance of the whole network is corrected. Then, the unknown node coordinates calculated by the least squares method are corrected. In reference [6], the weighted average of distance error and estimation distance error is proposed to correct the original average hop distance. The weight of the particle group is improved by using the subsection index and logarithmic decrement weight. In reference [7], for each beacon node, the weight of each beacon node is added to calculate the average hop distance. The main node definition is proposed, the network topology structure will be considered more comprehensively, and the local and global characteristics will be weighed better; in order to calculate the estimated distance of nodes, the improved particle swarm optimization algorithm is used instead of the maximum likelihood estimation method to locate the node coordinates. In reference [3], the range of broadcasting information of beacon nodes is limited by the threshold of the hop number; the average distance of each anchor node is corrected by the average distance error of each beacon node; the unknown node of this round is upgraded to a new anchor node for the next round of positioning. In reference [8], the multi-communication radius method is introduced to refine the hops between nodes. When calculating the average hop distance of unknown nodes, the isolated nodes are

eliminated, and the average hop distance obtained by beacon nodes is weighted and normalized to improve the localization accuracy of unknown nodes. In reference [9], the distance between the unknown nodes and the beacon nodes is calculated using different average hop distances. Using the Galactic Swarm Optimization thought of beacon nodes in the network is divided into different species: the particle swarm optimization algorithm is used to estimate the unknown node in each population, which is the optimal location, and the weighted centroid algorithm is used to optimize the suboptimal solution which is set as the coordinates of the unknown node.

All of the above studies give a good research idea for the DV-Hop localization algorithm. This paper proposes another improvement scheme based on the DV-Hop algorithm. This algorithm followed the two-dimensional position distribution, designed the minimum communication radius, and formed a reasonable network connectivity firstly. Then, the algorithm corrected the distance between the beacon node and its neighbour node to form a more accurate jump distance so that the shortest path can be optimized. Finally, we theorized the proposed localization algorithm and verified it in simulation experiments, including same communication radius, different communication radii, and different node density with same communication radius, and have compared the localization error and localization accuracy, respectively, between the proposed algorithm and the DV-Hop localization algorithm. The experimental result shows that the proposed localization algorithm have reduced the localization's average error and improved the localization's accuracy. Compared with the DV-Hop algorithm, whose localization accuracy increases from 0.6 to 0.7, other DV-HOP is about 0.3; and new DV-Hop shows a localization accuracy fluctuating stably within 0.1.

2. Analysis of the DV-Hop Localization Algorithm

The DV-Hop localization algorithm is a distributed range-free localization algorithm based on the distance vector routing protocol [5]. The main principle therein is to calculate the distances between beacon nodes and unknown nodes by multiplying the average hop distance in WSNs by the hop count of the beacon nodes. Then, the position information of unknown nodes is obtained through trilateration, triangulation, and multilateration [10], thus realizing localization. For a network topology established by a random arrangement of wireless sensor nodes, the 40 paths from beacon nodes to unknown nodes are possibly not straight. Hence, some errors are likely to exist in the node localization process when using the DV-Hop algorithm [11]. Moreover, the more numerous the hop counts, the larger the errors (i.e., error accumulation occurs).

2.1. Basic Procedure of the DV-Hop Algorithm. The localization of nodes using the DV-Hop [12, 13] algorithm is mainly divided into three steps.

Step 1. Calculating the minimum hop count between beacon nodes and unknown nodes. Beacon nodes broadcast information which shows their positions to neighbouring nodes by using the classical distance vector routing protocol [14]. The information contains {id, x_i, y_i, H_i}, where id, (x_i, y_i), and H_i represent the identifier, the coordinate, and the hop count of beacon nodes i, respectively. Moreover, the initial value of H_i is set to zero. The nodes receiving the broadcast information record the localization and hop counts of beacon nodes as vectors, which are then transmitted to neighbouring nodes (the value of hop count is incremented by one). When a node receives the same id group, it is supposed to compare the newly obtained value of H_i with the original value and then select the minimum value to replace and update the original group; otherwise, the newly obtained group is abandoned. The position information and minimum hop count of all beacon nodes are obtained by this communication mode in WSNs.

Step 2. Estimating the average hop distance. The purpose of calculating the average hop distance and minimum hop count first is to estimate the distance between unknown nodes and beacon nodes. After acquiring the localization and the hop count of beacon nodes in the first stage, the average hop distance of whole networks can be computed. The information is then broadcast to the whole network, or all networks. Furthermore, most nodes are required to receive the average hop distance from their nearest beacon nodes. The distances between beacon nodes and unknown nodes can be calculated by multiplying the average hop distance by the hop count. Here, hd_i and $h(ij)$ denote the average hop distance and the hop distance between a beacon node i (x_i, y_i) and an unknown node j (x_j, y_j), respectively, as shown in the following formula:

$$hd_i = \frac{\sum \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2}}{\sum h(ij)}. \tag{1}$$

The distances between unknown nodes and beacon nodes are calculated using the following formula:

$$d_i = hd_i \times \text{Hop}, \tag{2}$$

where hd_i signifies the average hop distance, while Hop is the minimum hop count between unknown nodes i and beacon nodes.

As shown in Figure 1, which shows the network topology of the DV-Hop localization algorithm, the red and the blue circles indicate beacon nodes and unknown nodes, respectively. The distances and hop counts among beacon nodes $L1$, $L2$, and $L3$ are known, and A represents an unknown node. According to formula (1), the average hop distance can be calculated as $(40 + 75)/(2 + 5) = 16.42$ m. In Figure 1, unknown node A receives the average hop distance from beacon node $L2$. On this basis, according to formula (2), the distances between the three beacon nodes $L1$, $L2$, and $L3$ and the unknown node A are 3×16.42 m, 2×16.42 m, and 3×16.42 m, respectively.

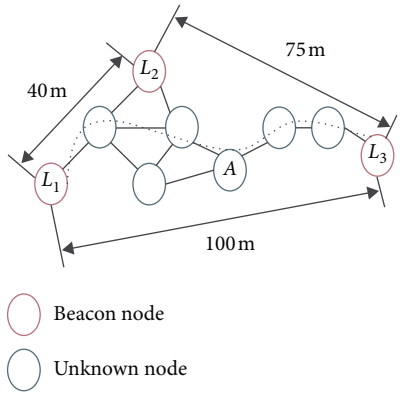


Figure 1: Network topology.

Step 3. Based on plane geometry, the coordinates of unknown nodes can be acquired in the case of knowing the coordinates and distances between three beacon nodes. Suppose that the coordinates of three beacon nodes are (x_1, y_1), (x_2, y_2), and (x_3, y_3), respectively, and the distances between these three beacon nodes and an unknown node D (x, y) are expressed as d_1, d_2, and d_3, separately, then, the following formula is obtained:

$$\begin{cases} (x_1 - x)^2 + (y_1 - y)^2 = d_1^2, \\ (x_2 - x)^2 + (y_2 - y)^2 = d_2^2, \\ (x_3 - x)^2 + (y_3 - y)^2 = d_3^2. \end{cases} \tag{3}$$

Meanwhile, the coordinate of node D can be calculated by using the following formula:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2(x_1 - x_3) & 2(y_1 - y_3) \\ 2(x_2 - x_3) & 2(y_2 - y_3) \end{bmatrix}^{-1} \cdot \begin{bmatrix} x_1^2 - x_3^2 + y_1^2 - y_3^2 + d_3^2 - d_1^2 \\ x_2^2 - x_3^2 + y_2^2 - y_3^2 + d_3^2 - d_2^2 \end{bmatrix}. \tag{4}$$

In this way, the coordinates of unknown nodes can be computed. For a network topology established by a random arrangement of wireless sensor nodes, the paths from beacon nodes to unknown nodes are possibly not straight. Hence, some errors likely exist in the node localization process when using the DV-Hop algorithm. Moreover, the more numerous the hop counts, the larger the errors (i.e., error accumulation occurs).

2.2. Error Analysis for the DV-Hop Algorithm. The DV-Hop algorithm is based on the shortest path first mechanism. Nodes in WSNs broadcast their localization information and calculate distances to other nodes so that beacon nodes acquire the least hop counts required to reach other nodes and known position information. Meanwhile, the real paths between nodes are regarded as approximately straight lines to calculate the average hop distance, which is applied as the average hop distance of node localization in networks, while unknown nodes are expected to obtain the average hop distance from the nearest beacon nodes with favorable communication conditions to estimate their self-localization positions. Therefore, in the localization process, various factors can make localization errors exceed the actual demand. These factors include the fact that network nodes are distributed unevenly, the actual hop distances between nodes are far longer than, or less than, the communication radius, and there are no beacon nodes which can be used for communication near unknown nodes. However, the centroid localization algorithm [15] takes the coordinates of a polygon centroid as a reference position and has low requirements for the actual distances between nodes, the communication radius, and the density of beacon nodes. Therefore, the cost of network construction can be reduced by using the algorithm. Hence, the authors proposed a new DV-Hop localization algorithm based on the half-measure weighted centroid [16].

3. Half-Measure Weighted Centroid Localization Algorithm

3.1. Improving the Algorithm. In computational geometry, the centroid of a polygon can be obtained by calculating the average coordinate of the vertices. Suppose that the position vector of a polygon with N edges satisfies the following equation, that is, $p_i = (x_i, y_i)^{\mathrm{T}}$, then the coordinate $(X_{\mathrm{est}}, Y_{\mathrm{est}})$ of its centroid [17, 18] is expressed as shown below:

$$(X_{\mathrm{est}}, Y_{\mathrm{est}}) = \left(\frac{1}{N} \sum_i^N X_i, \frac{1}{N} \sum_i^N Y \right). \tag{5}$$

Theorem 1. *Given the network node G with N nodes, the node density and the node distribution follow the two-dimensional Possion point process with density; to ensure that the probability P (G connectivity) $p \geq (0 \leq p < 1)$ is established, the optimal communication radius of nodes is*

$$R_{\min} = \sqrt{\frac{-\ln(1 - P^{1/N})}{\rho\pi}}. \tag{6}$$

Certificate. If the network G is connected, $\forall i \in V$, i, it is not an isolated node; that is, the node degree $d(i) \geq 1$, then the minimum node degree of graph G $d_{\min} \geq 1$.

Because nodes are distributed as two-dimensional Poisson points,

$$P(d(i) = 0) = P\left(N\left(\pi R^2(i)\right) = 0\right) = \frac{\left(\rho\pi R^2(i)\right)^0}{0!} e^{-\rho\pi R^2(i)} = e^{-\rho\pi R^2(i)}. \tag{7}$$

Therefore, $P(d(i) \geq 1) = 1 - P(d(i) = 0) = 1 - e^{-\rho\pi R^2(i)}$.

According to the independence of Poisson process events,

$$P(d_{\min} \geq 1) = \binom{N}{N} P(d(i) \geq 1)^N P(d(i) = 0)^0 = \left(1 - e^{-\rho\pi R^{2(i)}}\right)^N. \quad (8)$$

Therefore, according to the probability P (G connectivity) $\geq p\,(0 \leq P \leq 1)$, then $(1 - e^{-\rho\pi R^{2(i)}})^N \geq p$, and it can be reasoned. $R_{(i)} \geq \sqrt{(-\ln(1 - p^{(1/N)})/\rho\pi)}$, and the minimum communication radius of nodes can be obtained, $R_{\min} = \sqrt{-\ln(1 - P^{(1/N)})/\rho\pi}$·QED.

Definition 1. Regions are chosen, the neighbourhood h of node $M \in R^n$ relative to node set S is

$$U(M;\ h) = \{y \in S, \|M - y\|1 < h/2\}. \quad (9)$$

The advantage of using 1-norm is saving calculation time, so square regions are chosen.

Definition 2. The α-order node density of node M relative to set S is

$$\frac{1}{h(M; S, \alpha)}. \quad (10)$$

In the equation,

$$h(S; M,\ \alpha) = \min\{h : U(M, h), \text{the node number is } \alpha \text{ at least } a\}, \quad (11)$$

Since M's neighbourhood $h(S; M, \alpha)$ is an open set, so it has at least $\alpha - 1$ nodes in the node set S.

Definition 3. Assume M_i as the neighbourhood set of node i, M_{ij} as the Euclidean distance between node i and node j, R as the network communication radius, then the neighbourhood distance model is

$$M_i = \{j \mid j \neq i \text{ and } d_{ij} \leq R\}. \quad (12)$$

Definition 4. Assume M_i and M_j are chance variables in a network of random uniform distribution, there exists $M_i \neq M_j$, M_{ij} is all the nodes within the common area of $M_i \,\&\, M_j$, i.e., $M_{ij} = |M_i \cap M_j|$, then the neighbourhood distance $\mathrm{ND}(i, j)$ is

$$\mathrm{ND}(i, j) = 1 - \frac{m_{ij}}{M_j}, \quad j \in R. \quad (13)$$

There may exist $M_i \neq M_j$, $\mathrm{ND}(i, j) \neq \mathrm{ND}(j, i)$, but $d_{ij} = d_{ji}$, and the neighbouthood distance $\mathrm{CHND}(i, j)$ of half-measure weighted centroid proposed in this paper is

$$\mathrm{CHND}(i, j) = \frac{1}{2}[\mathrm{ND}(i, j) + \mathrm{ND}(j, i)] = 1 - \frac{M_i + M_j}{2M_iM_j} m_{ij}. \quad (14)$$

3.1.1. Half-Measure Weighted Centroid Localization Communication Model. The adopted log-normal shadow fading model is an empirical model based on experiments:

$$p(d) = p(d_0) - 10n_p \log\left(\frac{d}{d_0}\right) + X_\sigma. \quad (15)$$

Theoretically, the weight factor reflects the influence of all beacon nodes on centroid position. The positioning weight weight_i is

$$\mathrm{weight}_i = \left(\frac{1}{\widehat{d_{ij}}}\right)^g, \quad i \in U, \quad (16)$$

where $\widehat{d_{ij}}$ is the estimated distance between unknown node i and beacon node j. However, g is the weight factor (Figure 2).

3.1.2. Localization Model. Assume path (S_1, S_n) to be the path from node S_1 to node S_n, S_i and S_{i+1} are neighbours, and the localization distance of path S_1, S_n is

$$\mathrm{RND}(\mathrm{path}(S_1 + S_n)) = \sum_{i=1}^{n-1} \mathrm{RND}(S_i, S_{i+1}). \quad (17)$$

Path between S_1 and S_n is not unique, but there exists a shortest path that satisfies the $\mathrm{RND}(\mathrm{path}(S_1, S_n))$ value. Assume $\mathrm{RND}_{\min}(S_1, S_n)$ to be the shortest RND path distance,

$$\mathrm{RND}_{\min} = \left\{\sum_{i=1}^{n-1} \mathrm{RND}(S_i, S_{i+1})\right\}. \quad (18)$$

Choose the optimized weight within the communication range of unknown nodes and calculate d_{ij}, the estimated distance from the unknown node i to the beacon node j is

$$d_{ij} = \mathrm{RND}(S_i, S_j) \times \mathrm{weight}_i. \quad (19)$$

Calculating error and accuracy, while calculating the average hop distance, K beacon nodes adjacent to beacon nodes i (x_i, y_i) are searched to obtain error factors, which are expressed by error_i, as shown in formula:

$$\mathrm{error}_i = \frac{\sum_{i=1}^{k} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}}{K}. \quad (20)$$

Calculating the localization accuracy for the centroid of a beacon node i, denoted as $\mathrm{accuracy}_i$, and then, the normalized average localization error:

$$\mathrm{accuracy}_i = \frac{\mathrm{error}_i}{R}. \quad (21)$$

3.1.3. Computing Coordinates of Nodes. By using the least squares method (LSM), the distance from the unknown

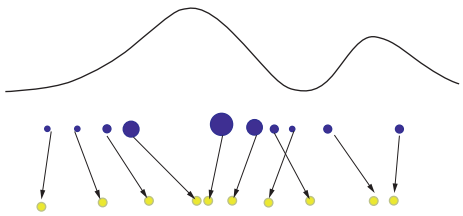


Figure 2: Weight factor.

node i (x_i, y_i) to beacon node $j(x_j, y_j)$ is calculated, and then the distance d_{ij} between the two nodes can be calculated from the following formula:

$$d_{ij} = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2}. \tag{22}$$

Accordingly,

$$x_i^2 + y_i^2 - 2x_i y_i + x_j^2 + y_j^2 = d_{ij}^2. \tag{23}$$

Let,

$$\begin{aligned} A_i &= x_i^2 + y_i^2, \\ B_j &= x_j^2 + y_j^2. \end{aligned} \tag{24}$$

Then,

$$d_{ij}^2 - A_i = -2x_i y_j - 2x_j y_i + B_j. \tag{25}$$

It can be found from formula (20) that

$$Z = \begin{bmatrix} x_j \\ y_j \\ \vdots \\ B_j \end{bmatrix},$$

$$A = \begin{bmatrix} -2x_1 & -2y_1 & 1 \\ -2x_2 & -2y_2 & 1 \\ \vdots & \vdots & \vdots \\ 2x_i & -2y_i & 1 \end{bmatrix}, \tag{26}$$

$$B = \begin{bmatrix} d_1^2 - A_1 \\ d_2^2 - A_2 \\ \vdots \\ d_i^2 - A_i \end{bmatrix}.$$

The coordinates of the nodes are

$$\begin{aligned} B &= A \times Z, \\ Z &= \left(A^{\mathrm{T}} A\right)^{-1} A^{\mathrm{T}} B, \end{aligned} \tag{27}$$

unknown node j is

$$\begin{cases} x_j = Z(1,1), \\ y_j = Z(2,1). \end{cases} \tag{28}$$

3.2. Procedures of the Improved Algorithm

Step 1. The hop count in the shortest path is acquired by broadcasting information among nodes, which is the same as the procedure used in the DV-Hop localization algorithm.

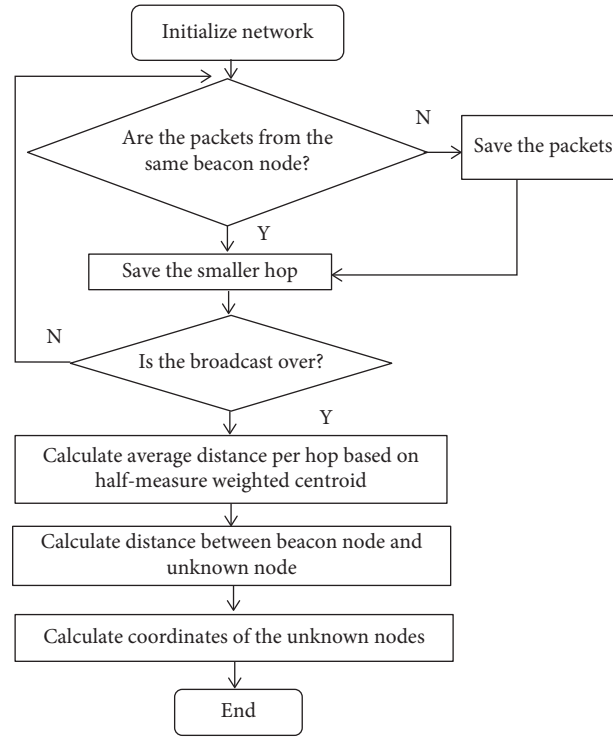


Figure 3: Flowchart.

Step 2. Based on half-measure weighted centroid neighbourhood distance model, calculate neighbourhood distance, weight factor, shortest path, and optimize.

Step 3. The distances from the unknown nodes to the beacon nodes are calculated by using formulas (6)–(25). Then, by using LSM, the coordinates of unknown nodes are obtained, and the flowchart is shown in Figure 3.

4. Simulation and Data Analysis

4.1. Establishing a Network Simulation Environment. Assess the efficacy and practicability of the improved algorithm proposed here, carry out system level simulation with MATLAB software and analyze and compare test data. One hundred wireless sensor nodes are arranged randomly in a square region of 100 m × 100 m, including 40 beacon nodes and 60 unknown nodes. Other parameters are set as shown in Table 1.

4.2. Simulation and Performance Analysis. The network topology of the DV-Hop localization algorithm based on the half-measure weighted centroid. Thereinto, the red ○ and the black + denote beacon nodes and unknown nodes, respectively (Figure 4). Distance estimation between unknown nodes and beacon nodes is obtained by the product of the minimum hop and the average hop distance between the two nodes; however, the minimum number of hops between

Table 1: Simulation parameters.

Area of the square region: BorderLength = 100
Total number of network nodes: NodeAmount = 100
Number of beacon nodes: BeaconAmount = 40
Number of unknown nodes: UNAmount = NodeAmount−BeaconAmount
The communication radius of each sensor: $R = 50$
The number of network nodes generated at random: C=BorderLength.*rand(2, NodeAmount)
A matrix for storing the coordinates of network nodes: Sxy = [1: NodeAmount; C]
A matrix containing the coordinates of beacon nodes: Beacon = [Sxy(2,1: BeaconAmount); Sxy(3,1:BeaconAmount)]
A matrix containing the coordinates of unknown nodes: UN = [Sxy(2,(BeaconAmount + 1):NodeAmount); Sxy(3,(BeaconAmount + 1): Node amount)]

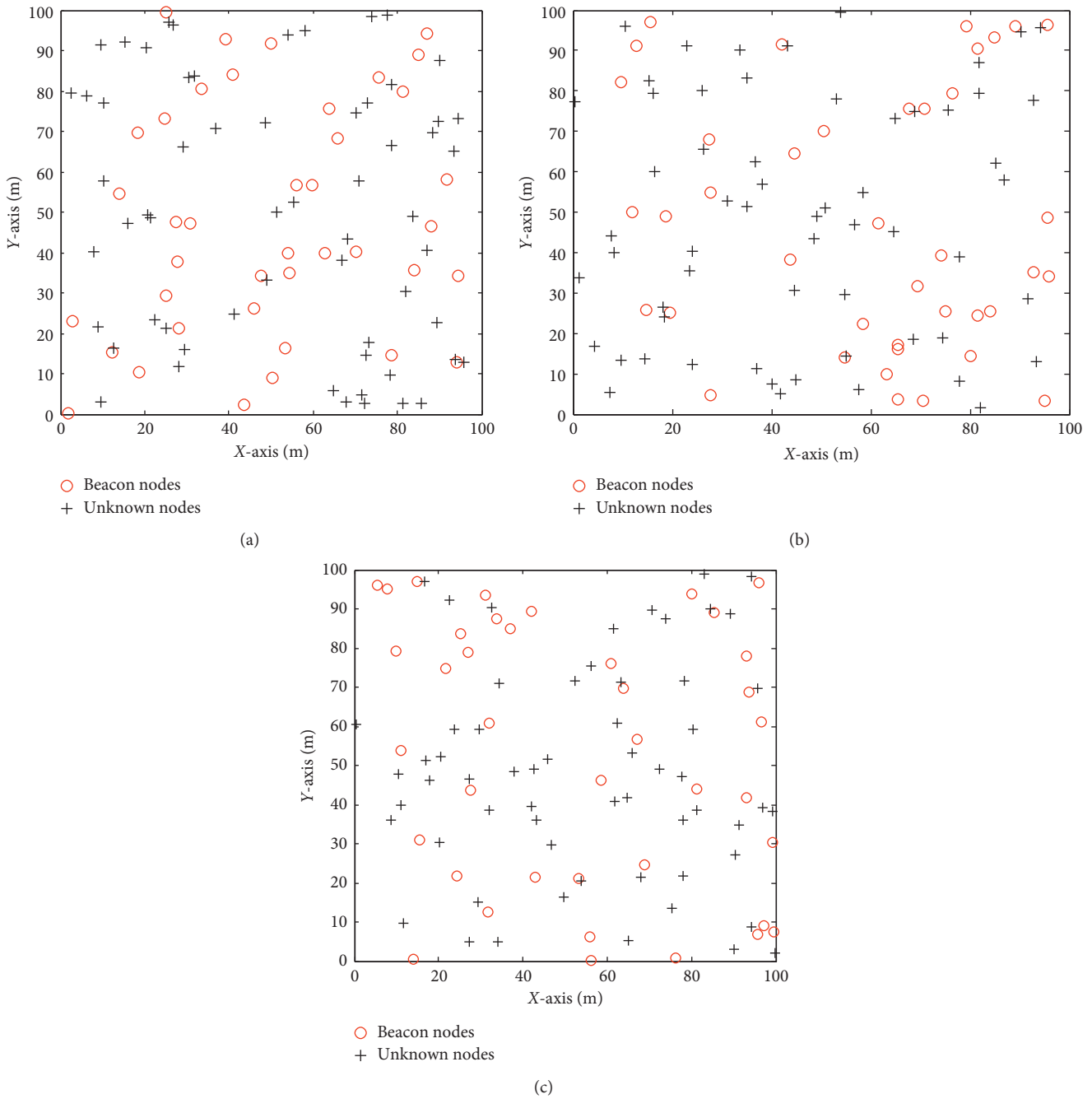


Figure 4: Network topology. (a) Same communication radius. (b) Different communication radii. (c) Same communication radius, but different densities.

nodes is largely determined by the communication radius of the nodes. Different communication radii will have different hop distances, which will also lead to different node locations; as shown in Figures 4(a)–4(c), the larger the node density, the smaller the communication radius, and the topology is closer to the actual location. In addition, optimizing network topology can save network energy consumption and prolong network lifetime.

The localization errors arising from the DV-Hop localization algorithm and the proposed localization algorithm are compared over the same communication radius ($R = 50$ m), and the node localization error of the DV-Hop localization algorithm fluctuates within the range 15 to 60, while that of the proposed algorithm ranges between 2 and 15 and is more stable. The main reason is that the increase of the number of unknown nodes will reduce the minimum communication radius. The number of unknown nodes is equivalent to the total number of nodes (fewer beacon nodes) which is an important factor affecting the current network connectivity. The localization errors arising from the DV-Hop localization algorithm and the proposed localization algorithm are compared over the same communication radius ($R = 50$ m), and the node localization error of the DV-Hop localization algorithm fluctuates within the range 15 to 60, while that of the proposed algorithm ranges between 2 and 15 and is more stable (Figure 5).

It shows the comparison of average localization accuracy of DV-Hop algorithm with that of the proposed localization algorithm. It shows that the localization accuracy of the DV-Hop localization algorithm varies within the range 0.3 to 1.2, while that of the improved localization algorithm fluctuates between 0.1 and 0.2. The main reason is that the location accuracy of New DV-Hop algorithm is higher with the increase of the number of communication radius (Figure 6).

The comparison of the average localization errors arising from the DV-Hop localization algorithm with those of the proposed localization algorithm under different communication radii is done. A total of 100 groups of experiments were carried out as the communication radius R was increased from 10 m to 80 m. In the new DV-Hop localization algorithm, when the node communication radius increases, the positioning accuracy is smaller and the positioning performance is better (Figure 7).

The localization accuracy of the DV-Hop algorithm are compared with that of the DV-Hop localization algorithm based on the half-measure weighted centroid, and other DV-Hop. To obtain the results, 100 groups of experiments were conducted with increasing communication radius R ($10\text{ m} \le R \le 80\text{ m}$) (Figure 8).

At the same communication radius, and for different densities of beacon nodes, the comparison of the average localization errors of the two algorithms is done. Similarly, the communication radius R was fixed at 50 m, while the number of beacon nodes was increased from 10 to 80 in the 50 groups of experiments. The average localization error of the DV-Hop algorithm increased gradually from 30. While other DV-Hop localization algorithm is about 15, and the

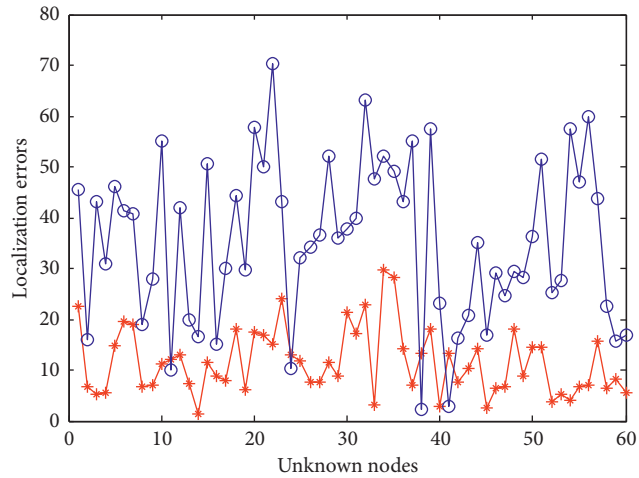


Figure 5: Comparison of the localization errors over the same communication radius.

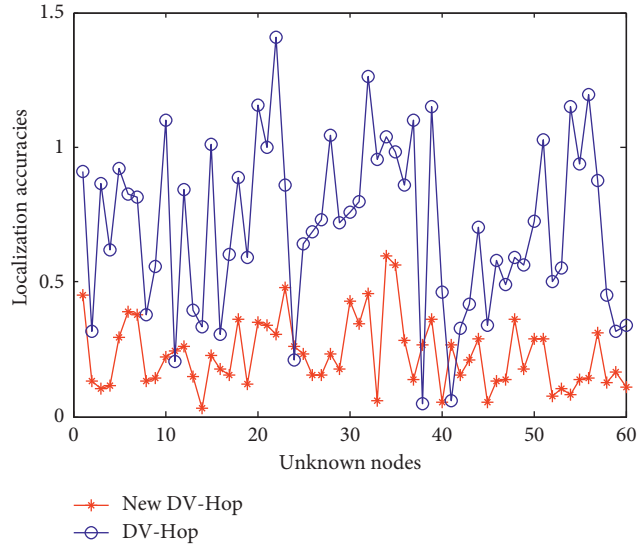


Figure 6: Comparison of the localization accuracies over the same communication radius.

new DV-Hop localization algorithm based on a half-measure weighted centroid was below 5; in particular, its localization performance was optimal for between 30 and 60 beacon nodes. It is almost unaffected by the communication radius and the total number of nodes. The main reason is that the more accurate distance between beacon nodes and their neighbours can be obtained by optimizing equations (13) and (14), which can undoubtedly reduce the positioning error of all unknown nodes (Figure 9).

The comparison of localization accuracies of the two algorithms at the same communication radius, but for different densities of beacon nodes, is done. The communication radius R was set to 50 m, and the number of beacon nodes was increased gradually from 10 to 80 in the 50 groups of experiments. Compared with the DV-Hop algorithm, whose localization accuracy increases

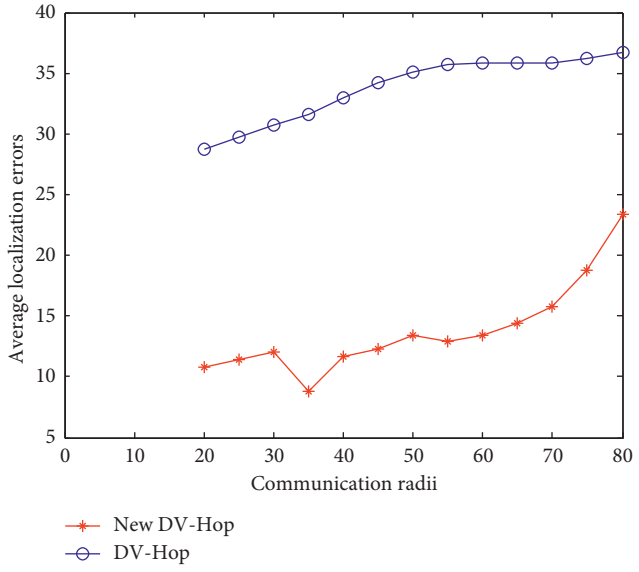


Figure 7: Comparison of localization errors over different communication radii.

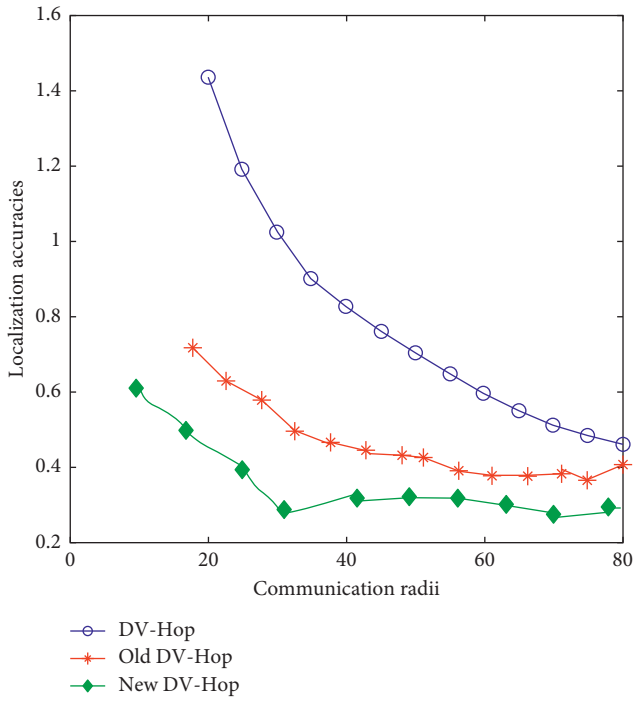


Figure 8: Comparison of localization accuracies over different communication radii.

from 0.6 to 0.7, other DV-HOP is about 0.3; and new DV-Hop shows a localization accuracy fluctuating stably within 0.1. Beacon nodes are calculated by the half-measure weighted centroid localization model, next step is to design optimized weight, and optimize the shortest path. The higher the density of beacon nodes and the more reasonable the distribution, the higher the positioning accuracy and the better the positioning performance (Figure 10).

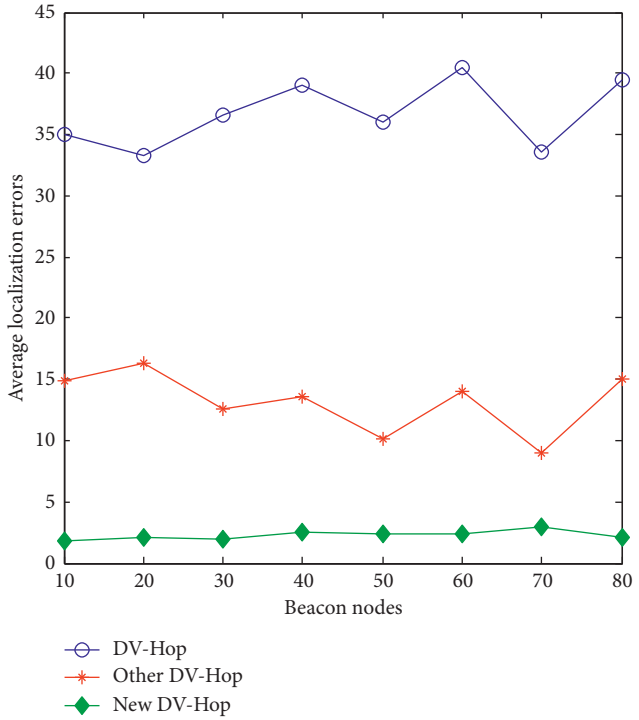


Figure 9: Comparison of the average localization errors at the same communication radius, and different densities of beacon nodes.

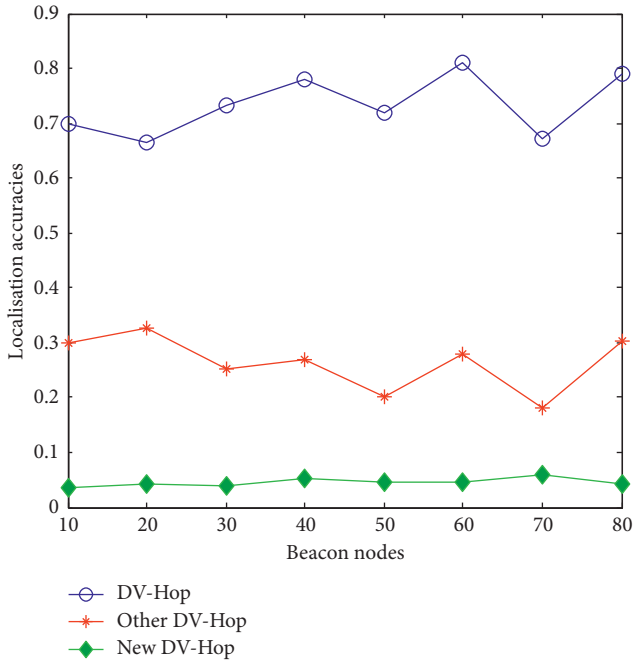


Figure 10: Comparison of the localization accuracies at the same communication radius, but with different densities of beacon nodes.

5. Conclusion

In view of the disadvantages in the practical application of the DV-Hop algorithm in WSNs, such as the uneven distribution of nodes, holes, and large errors in the average hop

distance, a novel localization algorithm, combining the DV-Hop algorithm with a half-measure weighted centroid, was proposed. Beacon nodes realize their localization by using the centroid algorithm and then use the localized accuracy as the weight for localizing unknown nodes. Through theoretical reasoning and simulation experiments, it was found that the improved localization algorithm reduced the localization errors and improved the localization accuracy of unknown nodes compared with the DV-Hop algorithm whether used in the same networks or not. Compared with the DV-Hop algorithm, whose localization accuracy increases from 0.6 to 0.7, other DV-HOP is about 0.3; and new DV-Hop shows a localization accuracy fluctuating stably within 0.1. It was worth noting that the study was performed in an ideal network simulation environment, so there remains the need to research the application of the improved algorithm under realistic network environments in the future.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares no conflicts of interest.

Acknowledgments

The research was funded with the project no. KJ2014A096 entitled "Intelligent Tourism Platform—application of Internet of things location perception service in tourism industry," supported by funds for a key project from the Natural Science Foundation in Anhui Province, China.

References

[1] S. Chatterjea and P. Havinga, "A dynamic data aggregation scheme for wireless sensor networks," *Proc Program for Research on Integrated Systems and Circuits*, vol. 41, no. 2, pp. 116–125, 2017.

[2] B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: a survey," *Journal of Network and Computer Applications*, vol. 60, pp. 192–219, 2016.

[3] M. Mehrabi, H. Taheri, and P. Taghdiri, "An improved DV-hop localization algorithm based on evolutionary algorithms," *Telecommunication Systems*, vol. 64, no. 4, pp. 639–647, 2017.

[4] A. M. A. A. Znaid, M. Y. I. Idris, A. W. A. Wahab et al., "Low communication cost (LCC) scheme for localizing mobile wireless sensor networks," *Wireless Networks*, vol. 23, no. 3, pp. 737–747, 2017.

[5] L. Gui, X. Zhang, Q. Ding, F. Shu, and A. Wei, "Reference anchor selection and global optimized solution for DV-hop localization in wireless sensor networks," *Wireless Personal Communications*, vol. 96, no. 4, pp. 5995–6005, 2017.

[6] X. Yang and W. Zhang, "An improved DV-hop localization algorithm based on hop distance and hops correction," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 11, no. 6, pp. 319–328, 2016.

[7] S. Tomic and I. Mezei, "Improvements of DV-hop localization algorithm for wireless sensor networks," *Telecommunication Systems*, vol. 61, no. 1, pp. 93–106, 2015.

[8] G. Sharma and A. Kumar, "Improved DV-hop localization algorithm using teaching learning based optimization for wireless sensor networks," *Telecommunication Systems*, vol. 67, no. 2, pp. 163–178, 2018.

[9] L. Cui, C. Xu, G. Li et al., "A high accurate localization algorithm with DV-hop and differential evolution for wireless sensor network," *Applied Soft Computing*, vol. 68, 2018.

[10] S. Kumar and D. K. Lobiyal, "An advanced DV-hop localization algorithm for wireless sensor networks," *Wireless Personal Communications*, vol. 71, no. 2, pp. 1365–1385, 2013.

[11] M. M. Ren, Z. J. Xie, G. Jin et al., "DV-hop localization algorithm based on multi-mobile beacon," *Computer Engineering*, vol. 40, no. 10, pp. 92–97, 2014.

[12] F. Shahzad, T. R. Sheltami, and E. M. Shakshuki, "DV-maxHop: a fast and accurate range-free localization algorithm for anisotropic wireless networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 99, pp. 2494–2505, 2017.

[13] X. L. Cui, W. B. Chen, and C. Hao, "Research on DV-HOP algorithm for wireless sensor networks," in *Proceedings of International Conference on Knowledge Management in Organizations*, Beijing, China, August 2017.

[14] J. G. Ko and M. Chang, "MoMoRo: providing mobility support for low-power wireless applications," *IEEE Systems Journal*, vol. 9, no. 2, pp. 585–594, 2017.

[15] A. Ademuwagun and V. Fabio, "Reach centroid localization algorithm," *Wireless Sensor Network*, vol. 9, no. 2, pp. 87–101, 2017.

[16] K.-Y. Kim and Y. Shin, "A distance boundary with virtual nodes for the weighted centroid localization algorithm," *Sensors*, vol. 18, no. 4, p. 1054, 2018.

[17] J. Mass-Sanchez, E. Ruiz-Ibarra, J. Cortez-González et al., "Weighted hyperbolic DV-hop positioning node localization algorithm in WSNs," *Wireless Personal Communications*, vol. 96, no. 4, pp. 5011–5033, 2017.

[18] T. Wang, X. Wei, J. Fan, and T. Liang, "Adaptive jammer localization in wireless networks," *Computer Networks*, vol. 141, pp. 17–30, 2018.

Hindawi
Mobile Information Systems
Volume 2019, Article ID 2741323, 15 pages
https://doi.org/10.1155/2019/2741323

Research Article

Predicting the Route of the Longest Lifetime and the Data Packet Delivery Time between Two Vehicles in VANET

Mohamed Nabil,[1] **Abdelmajid Hajami**,[2] **and Abdelkrim Haqiq**[1]

[1]*Computer, Networks, Mobility and Modeling Laboratory, FST, Hassan 1st University, Settat, Morocco*
[2]*LAVETE Laboratory, FST, Hassan 1st University, Settat, Morocco*

Correspondence should be addressed to Mohamed Nabil; nabilmed77@gmail.com

Received 30 May 2018; Revised 8 November 2018; Accepted 28 November 2018; Published 2 January 2019

Guest Editor: Ali K. Bashir

Among the most critical issues in VANET are the frequent failures of the route caused by the high mobility of vehicles, the increase of the network overload caused by control messages, and the increase of the data packet delivery time. Short communication route lifetime often breaks down during data packet transmission between the source and the destination vehicles, which results in a relaunch of a new route reconstruction that becomes more frequent and depletes a significant amount of network resources. To face these issues, much research has considered the route stability and the route lifetime determination between source and destination vehicles as important factors to improve the quality of service in the VANET network. However, this research did not take into account the route that has the longest lifetime as the most stable route and assumes that vehicles move at a constant speed during a direct communication between them. Furthermore, it did not model the data packet delivery time between the source and the destination vehicles. For this reason, we propose two protocols that use vehicles density to predict the data packet delivery time before sending the data and use vehicles movement information to determine the longest lifetime route, taking into account the variation of the vehicles velocity for comfort applications on highway. Our schemes are evaluated in function of vehicles density by measuring the average route lifetime, the percentage of packets delivery, the control overhead, the average end-to-end delay, the throughput, and the average number of route failures generated during the transmission of data packets.

1. Introduction

Vehicular ad hoc networks (VANETs) allow vehicles to communicate each other directly through the On Board Unit (OBU) device forming vehicle-to-vehicle communication, or with existing infrastructure via fixed equipment beside the road called Road Side Unit (RSU) forming vehicle-to-infrastructure communication [1, 2]; and they are a key component of intelligent transportation systems (ITS) [3]. VANETs support a wide range of safety applications to make accurate decisions by drivers and to help road traffic authorities for better control and mitigation of traffic congestion. Hence, the number of accidents on the roads will be reduced. Besides, they provide many nonsafety applications that supply the passengers with the capability to communicate with other passengers traveling in other vehicles, sharing multimedia content, playing online games, accessing the Internet, checking emails, etc. [4–6].

Unfortunately, intrinsic characteristics of the highly dynamic network topology cause several challenges to develop the previous applications. Among these challenges are the frequent breakages of links building the path between two vehicles because of their short lifetimes. This situation leads to a more frequent reconstruction of routes. Besides, the network fragmentation and the route rupture lead to an increase of the data packet delivery time between the source and the destination vehicles (packet wait time in queue). This issue results into a low data packet delivery ratio, an increase of end-to-end delay, an increase of control packets, and a depletion of a significant amount of network resources. To improve these metrics for achieving the sought quality of service, an efficient and reliable routing protocol is needed to

provide the most stable routes for supporting the nonsafety applications exchange in VANETs.

Numerous protocols have been proposed in the literature to improve the communication efficiency between two communicating vehicles. These protocols try to find more stable routes by choosing vehicles that travel in the same direction [7], or by dividing the vehicles in groups [8], or by building stable backbones on road using connected dominating sets (CDS) [9], or by using an evolving graph from the source to the destination vehicles [10], or by dividing the moving vehicles to several clusters [11, 12]. All these protocols do not really determine the most stable route and their performance is still far from the sought level of quality of service. This research assumes that vehicles move at a constant speed during the link lifetime calculation between two vehicles in direct communication. In this case, link lifetime is not accurate due to the variation of the vehicles' velocity during the route establishment. Hence, the accurate link lifetime is an important metric that significantly affects the stability of multihop routing protocols in VANETs. Furthermore, this research did not predict the packet delivery time which is also an important metric for decreasing the number of lost data packets and the network overload.

To overcome these limitations, we propose two schemes for nonsafety applications in a highway environment. These schemes predict the most stable route relaying two communicating vehicles and take into account the data packet delivery time before sending data, so as to avoid the frequent failures of the route. Thus, there is the decrease of both lost data packets and control messages. The main contributions of the paper are as follows:

(i) To insure that the route which has the longest lifetime will be chosen during the route establishment; that is, our schemes determine the route that has the longest lifetime among all possible routes between the source and the destination vehicles during the route request.

(ii) To model the data packet delivery time between source and destination vehicles using a mathematical calculation. In other words, the source vehicle predicts the delivery time of the data packet to destination vehicle before sending data in order to know how many data packets to send before the route rupture.

(iii) To predict the link lifetime, taking into account the acceleration and deceleration of vehicles' speed in a direct communication between two vehicles, namely, we consider the acceleration or deceleration of vehicles' speed at the moment the calculation of the time in which two vehicles stay in direct communication.

The remainder of this paper is organized as follows: Section 2 presents related work. Section 3 presents link lifetime prediction model. Section 4 presents data packet delivery average time prediction model. Section 5 shows the most stable route construction. Section 6 presents simulation and results. Finally, we give a conclusion in Section 7.

2. Related Work

The challenges of network routing protocols in VANETs have been attracting more research efforts, and a number of routing protocols have been proposed to determine the route based on the route lifetime.

Menouar et al. [13] propose a movement-prediction-based routing (MOPR) to avoid the link rupture until the end of data transmission. MOPR predicts the future nodes' positions in order to choose the most stable route that has enough lifetime for data transmission. The performance of the MOPR depends on the prediction accuracy and the estimation of the data transmission time that depends on various components such as network bandwidth and driver's behavior.

To determine a more stable route, Taleb et al. [8] proposed the scheme ROMSGP that groups vehicles according to their movement directions. The most stable route is determined by selecting the path that has the longest link expiration time. The authors did not take into consideration the case where there are no vehicles traveling in the same direction of group movement.

Namboordiri and Gao [14] proposed a prediction-based routing (PBR) protocol that determines a stable route on highway giving priority to vehicles that travel in the same direction of source motion. This protocol predicts the route lifetime and preemptively determines new routes prior to old ones break. These authors assumed that vehicles travel at a constant velocity at the duration of the link.

Liu et al. [15] proposed a stable direction-based routing protocol (SDR) that combines direction broadcast and path duration prediction into AODV [16]. In SDR, vehicles are grouped based on the position, and the route selection is based on the link duration. The authors did not take into consideration the case where there are not enough vehicles in a given direction range participating in the route discovery process.

Eiza and Ni [10]proposed an evolving graph-reliable ad hoc on-demand distance vector (EG-RAODV) that allows finding the most reliable route from the source to the destination. They proposed an extended version of the evolving graph model to model and formalize the VANET communication graph (VoEG), and they developed a new evolving graph Dijkstras algorithm (EG-Dijkstra) to find the most reliable journey (MRJ) based on the journey reliability in VoEG. The problem of this protocol is that at each any given time, the source vehicle must have full knowledge of a VANET communication graph. Furthermore, the authors assumed that vehicles travel at a constant velocity along the same direction on the highway and they did not take into account the vehicles density.

In [17], authors proposed the scheme ARP-QD which is a QoS-based routing protocol in terms of hop count, link duration and connectivity so as to cope with dynamic topology and keep the balance between stability and efficiency of the algorithm. However, it is not enough to use only a global distance to reflect the overall QoS of a routing path.

Authors of [18] proposed an enhanced version of AODV protocol, named En-AODV, to deal with routes instability

issues for multimedia applications requirements. En-AODV leverages cross-layer information on the link quality combined with the knowledge of the final destination of the receiver vehicle to establish the most stable path relaying the source and destination vehicles and quickly react to the occurrence of a link failure in this path and provide an alternative link of good quality. The authors did not take into consideration the case where there are no vehicles moving towards the destination region.

Authors in [12] proposed a new clustering-based reliable low-latency multipath routing scheme by employing Ant Colony Optimization technique to compute the optimal routes among the communicating vehicles in terms of reliability, end-to-end latency, throughput, and energy consumption. Although the scheme reduces the end-to-end latency and RREQ messages, it does not determine the most stable route and does not take into account the variation of velocity during a direct communication between vehicles.

Authors of [19] proposed a reliable routing protocol to establish a more reliable route between the source and the destination vehicles, known as AODV-R. They incorporate link reliability metric in the original AODV routing protocol. In this scheme, the source vehicle chooses the route based on the maximum reliability value among all received route reply messages. They assumed that vehicles will not change their velocities either by accelerating or decelerating during time period T. Also, this scheme does not determine the most stable route.

In [20], authors proposed a novel reactive routing protocol for vehicle-to-vehicle networks, named MA-DP-AODV-AHM. The latter is based on the AODV routing protocol in which the modifications made are related to the hello message and route discovery procedures, in order to establish reliable and stable routes from source to destination vehicles. In this scheme, the intermediate vehicle rebroadcasts the route request message if the speed is lower than a threshold and both forwarding and receiving vehicles are not diverging. Moreover, this scheme adapts the frequency of broadcasting the periodic "hello message" to suppress broadcasted unnecessary and redundant hello messages. Authors of this work did not take into consideration the case where there are not enough vehicles that respect the constraints (speed is lower than a threshold and vehicles are not diverging) of broadcasting the route request message. Besides, they have not determined the most stable route and have not taken into account the variation of velocity during a direct communication between vehicles.

The link lifetime of all these schemes is not accurate because these schemes assume that speed of vehicles is constant during the calculation of direct link lifetime between vehicles. Furthermore, they do not select the route that has the longest lifetime and do not take into account the data packet delivery time before sending data, except MOPR and ROMSGP. Besides, all these schemes do not model this data packet delivery time and did not take into consideration the case where there are no vehicles moving in the same direction or towards the destination, except MOPR, ARP-QD, and CRLLR. Therefore, the goal of this work is first to predict the route that has the longest lifetime whatever the direction of the vehicles on highway. And second, to model the data packet delivery average time for nonsafety applications.

Table 1 provides the comparison of the existing schemes in terms of accurate link lifetime, route lifetime, data packet delivery time, and participating vehicles during the build of route.

3. Link Lifetime Prediction

Let (X_m, Y_m), V_m, and A_m are the position, the speed, and the acceleration of the vehicle m at moment t_0, respectively. (X_n, Y_n), V_n, and A_n are the position, the speed, and the acceleration of the vehicle n at time t_0, respectively. (X'_m, Y'_m) and (X'_n, Y'_n) are positions of vehicles m and n at moment t_1, respectively.

We assume that the acceleration of each vehicle is constant during a direct communication. The abscissa axis is parallel to the direction of movement of vehicles m and n to facility the calculation. The distance between vehicles m and n on the ordinate axis is negligible per report to the radius (R) of the coverage area of each vehicle (i.e., $|Y_m - Y_n| \approx 0$).

3.1. Vehicles m and n Travel in Same Direction. It is assumed that the vehicles m and n travel in the positive sense of the abscissa axis. Therefore, distances traveled by vehicles m and n during the delay t $(t_1 - t_0)$ are represented by the following equations [21, 22]:

$$X'_m - X_m = \frac{1}{2}A_m t^2 + V_m t, \tag{1}$$

$$X'_n - X_n = \frac{1}{2}A_n t^2 + V_n t. \tag{2}$$

We can write again

$$X'_m - X_m = -(X_m - X_n) + (X'_n - X_n) + (X'_m - X'_n). \tag{3}$$

So from (1)–(3), we represent the time t, during which the distance between vehicles m and n will be $|X'_m - X'_n|$ on the x-axis, by the following equation:

$$\frac{1}{2}(A_m - A_n)t^2 + (V_m - V_n)t + d - d' = 0, \tag{4}$$

where $d = X_m - X_n$ and $d' = X'_m - X'_n$.

If vehicles m and n have the same acceleration, then the time which vehicles stay in communication direct is formulated by

$$t = \frac{d' - d}{V_m - V_n}, \tag{5}$$

where $V_m \neq V_n$ and $|d'| \approx R$.

If vehicles m and n have not the same acceleration, then in this case, we calculate the delta of equation (4), that is,

$$\Delta = (V_m - V_n)^2 - 2(A_m - A_n) * (d - d'). \tag{6}$$

(i) Si ($V_m > V_n$ and $A_m > A_n$) or ($V_m < V_n$ and $A_m < A_n$): the maximum time in which the vehicles m and n remain in direct communication is the time t in

Table 1: Comparison of existing schemes.

Scheme	Link lifetime: accurate or not accurate	The selected route has the longest lifetime: yes/no	Data packet delivery time		Participating vehicles
			Considered or not considered	Modeled or not modeled	
MOPR [13]	Not calculated	No	Considered and not accurate	Not modeled	All vehicles
ROMSGP [8]	Not accurate	No	Considered and not accurate	Not modeled	Just vehicles that travel in the same group
PBR [14]	Not accurate	No	Not considered	Not modeled	Giving priority to vehicles that travel in the same direction
SDR [15]	Not accurate	No	Not considered	Not modeled	Only vehicles that travel in the same direction
EG-RAODV [10]	Not accurate	No	Not considered	Not modeled	All vehicles
ARP-QD [17]	Not accurate	No	Not considered	Not modeled	All vehicles
En-AODV [18]	Not accurate	No	Not considered	Not modeled	Only vehicles moving towards the destination region
CRLLR [12]	Not accurate	No	Not considered	Not modeled	All vehicles
AODV-R [19]	Not accurate	No	Not considered	Not modeled	All vehicles
MA-DP-AODV-AHM [20]	Not calculated	No	Not considered	Not modeled	Vehicles that their speed is lower than a threshold and they are not diverging
Our schemes	Accurate	Yes	Considered	Modeled	All vehicles

which the distance between these vehicles will be R (i.e., $|d'| \approx R$). This time is represented by the following formula:

$$t = \frac{-|V_m - V_n| + \sqrt{\Delta}}{|A_m - A_n|}. \tag{7}$$

(ii) Si ($V_m > V_n$ and $A_m < A_n$) or ($V_m < V_n$ and $A_m > A_n$): in this case, there are two possibilities.

First case: one vehicle leaves the coverage area of the other before their speeds become equal (i.e., $|d'| > R$). In this case, the maximum time t in which the two vehicles remain in direct communication ($|d'| \approx R$) is formulated by

$$t = \frac{|V_m - V_n| + \sqrt{\Delta}}{|A_m - A_n|}. \tag{8}$$

Second case: vehicles m and n stay in direct communication (i.e., $|d'| \leq R$) at the moment when their speeds are the same. In this case, the maximum time in which the two vehicles remain in direct communication ($|d''| \approx R$) is $t + t'$, where $t = t_1 - t_0$ is the time in which the speed of one is inferior or equal to the other and $t' = t_2 - t_1$ is the time in which these vehicles stay in direct communication after the speed of one overtakes the other. Thus

$$t = \frac{|V_m - V_n|}{|A_m - A_n|}, \qquad \frac{1}{2}(A_m - A_n)t'^2 + d' - d'' = 0, \tag{9}$$

where $d' = -(1/2)((V_m - V_n)^2/A_m - A_n) + d$ and $d'' = X_m'' - X_n''$ (X_m'' and X_n'' are positions of vehicles m and n at moment t_2, respectively). The time t_{fi} in which the distance between the two vehicles becomes R ($|d''| \approx R$) is

$$t' = \frac{\sqrt{-2(A_m - A_n) * (d' - d'')}}{|A_m - A_n|}. \tag{10}$$

Hence

$$t + t' = \frac{|V_m - V_n| + \sqrt{-2(A_m - A_n) * (d' - d'')}}{|A_m - A_n|}. \tag{11}$$

Remark: in the case where vehicles m and n travel in the negative direction of the x-axis, we change $d - d'$ by $d' - d$ and $d' - d''$ by $d'' - d'$ in previous formulas.

3.2. Vehicles m and n Travel in Opposite Direction of Each Other. The time t during which the distance between vehicles m and n will be $|X_m' - X_n'|$ on the x-axis is represented by the following equation:

$$\frac{1}{2}(A_m - A_n)t^2 + (V_m - V_n)t + d - d' = 0, \tag{12}$$

where $d = X_m - X_n$ and $d' = X_m' - X_n'$.

The maximum time t in which the two vehicles remain in direct communication ($|d'| \approx R$) is formulated by

$$t = \begin{cases} \dfrac{d' - d}{V_m + V_n}, & \text{if } A_m = A_n, \\ \dfrac{-(V_m + V_n) + \sqrt{\Delta}}{A_m + A_n}, & \text{otherwise,} \end{cases} \tag{13}$$

where $\Delta = (V_m + V_n)^2 + 2(A_m + A_n) * (d' - d)$.

4. The Data Packet Delivery Time Prediction

To model the data packet delivery time, we, first of all, determine the number of vehicles on road. For determining this number of vehicles, each one broadcasts periodically a message of existence on the length of road; and each one receives a new message of existence and updates the number of vehicles on the road in its table which is called the vehicles density on the road (VDR). A vehicle waits two consecutive messages of existence intervals to hear from a vehicle. If no message was received, the vehicle number is decreased in VDR.

We assume that vehicles are uniformly distributed on the road. Therefore, the average number of vehicles in the communication range of each vehicle is the integer part of the following formula:

$$n = \frac{2 * R * N}{L}, \tag{14}$$

where R is the radius of the communication range, N is the number of vehicles on the road, and L is the road length.

Let T_i is the data packet delivery time to a neighbor i. So T_i is the sum of the packet transmission time and the propagation time of a bit through a medium. Therefore [23–25]

$$T_i = \frac{S_{\text{packet}}}{B_{\text{rate}}} + \frac{d_i}{V_{\text{prop}}}, \tag{15}$$

where S_{packet} is the size of the packet, B_{rate} is the bit rate in the medium, d_i is the distance between the forwarder and its neighbor i, and V_{prop} is the propagation velocity in the medium.

We consider the propagation time through a medium is constant between a forwarder and their neighbors whatever their positions in the forwarder's coverage area. Because, the propagation speed is too great compared to the distance between a forwarder and their neighbors. Therefore, we consider the data packet delivery time to a neighbor i is constant, i.e., $T_i = T \ \forall \ i \in \{1, 2, 3, \ldots, n\}$, where n is the number of neighbors of the forwarder.

We assume the worst case in which, at any time, each vehicle has a packet for sending it to a neighbor; and all vehicles have the same opportunity to send a data packet to a neighbor. So, the waiting time to send a data packet in the ith order by the forwarder is

$$T_{w,i} = (i - 1) * T. \tag{16}$$

For example, if the forwarder is the first that will send a packet of data, then the waiting time is 0 s ($(1 - 1) * T$); and the wait time to be the last that will send a packet of data among n neighbors is $n * T$ ($(n + 1 - 1) * T$).

Hence, the waiting average time to send a data packet by the forwarder among n neighbors is

$$T_{w,\text{avg}} = \sum_{i=0}^{n} \frac{i * T}{n + 1} = \frac{n * T}{2}. \tag{17}$$

Thus, the data packet delivery average time to a neighbor among n neighbors is

$$T_{\text{avg}} = t_{w,\text{avg}} + T = \frac{n + 1}{2} * T. \tag{18}$$

Therefore, the data packet delivery average time from the source vehicle to the destination one is

$$t_{\text{avg}} = N_{\text{vih}} * \frac{n + 1}{2} * T, \tag{19}$$

where N_{vih} is the number of vehicles that build the route between the source and the destination vehicles.

When the source vehicle has a data packet to send to the destination vehicle, it calculates the remaining time of route between itself and the destination vehicle. If this left time of route is less than the data packet delivery average time, the source vehicle launches a new route request; otherwise, it sends the data packet.

To verify the delivery time of the data packets of formula (19), we simulated (using NS2) the delivery time of the data packets between the source and the destination vehicles according to the density of the vehicles on highway of 5 km with 4 lanes in two opposite directions as shown in Figure 1. The speed of the vehicles varies between 0 km and 100 km. Our simulation does not take into account the waiting time of data packets in the queue at the source vehicles.

Figure 2 shows that the delivery time of the data packets of formula (19) and the simulated delivery time of the data packets are very close.

5. The Most Stable Route Construction

The network model consists of one road ended by two intersections in highway environment or in urban environment for road segments. This road has the same characteristics such as length, width, and number of lanes. Each lane has a distinctive traffic density (Figure 2). Each vehicle is equipped with a global positioning system (GPS) that provides information about its location, speed, and direction. Finally, each source vehicle knows the location of the destination by using a location service such as RLSMP [26] and ZGLS [27].

Given a directed graph G(V, E) that is defined by a finite set $V = \{v_1, v_2, v_3, \ldots, v_n\}$ of vertices, where v_i is a vehicle and by finite set $E = \{t_1, t_2, t_3, \ldots, t_m\}$ of edges, where t_j is the remaining time between any two vehicles to stay in direct communication with each other.

Whenever a vehicle receives a discovery message of route, it saves message's identifier and the traveled route lifetime in a table, called Route Request Table (RRT).

We seek to determine the most stable route between the source and the destination vehicles. The route lifetime (RLT) is the minimum link lifetime (LLT) between links that build the route between source and destination vehicles. As in Figure 3, the most stable route is the one which is built by vehicles S-A-I-K-D, and the lifetime of this route is 4 s at instant t.

When the source vehicle wants to determine a new route between itself and the destination vehicle, it broadcasts a new route discovery message in the side close to destination of its communication range. Then, when the destination

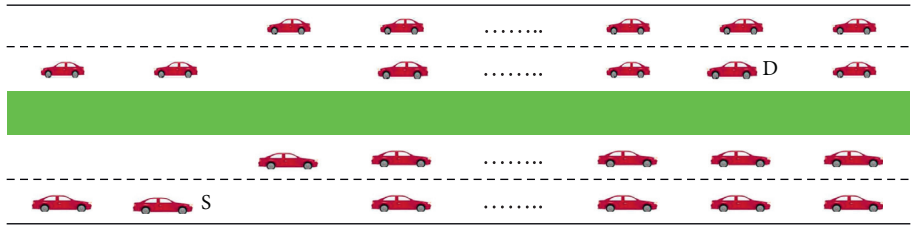


Figure 1: Bidirectional highway model.

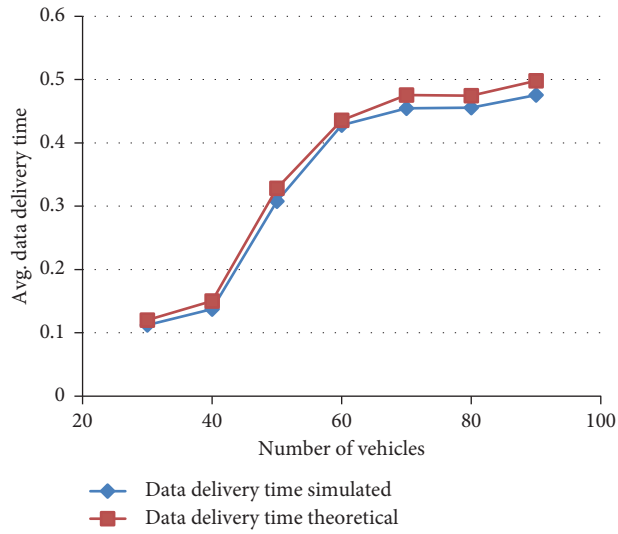


Figure 2: Delivery time of the data packets between the source and the destination vehicles.

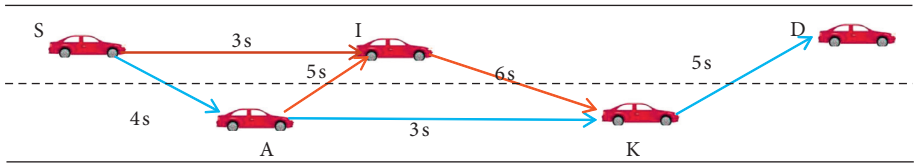


Figure 3: Most route lifetime.

vehicle receives this route request message, it copies the route lifetime and the moment of calculation of this lifetime in the route reply. Next, it sends the latter to the source vehicle.

To determine this route, we propose two schemes: the first one uses beacon message and the other does not use it. These schemes are an extension of our work [28].

The idea of these schemes is that each vehicle can retransmit again the same route request message if it allows to the increase of the route lifetime.

5.1. Scheme without Beacon Message. Each source vehicle (s) knows the distance d(s, d) between itself and the destination vehicle (d) because each source vehicle knows the location of the destination vehicle by using a location service. We use this distance to determine the expiration parameter for the route request message so that it will not be rebroadcasted indefinitely on the entire network.

When the source vehicle wants to determine a new route to the destination vehicle, it adds its information (identifier, location, d(s, d), speed, direction, and RLT that is 0 s at the source vehicle) in the route request message (RRM) and broadcasts it in its communication range.

Each receiver vehicle (r), on the side close to destination vehicle of its communication range, calculates the link lifetime (LLT) and d(f, r) between itself and the previous forwarder vehicle (f). Then, it checks whether it is not the destination and d(r, d) (d(f, d)–d(f, r)) is less than or equal to zero meter. If it is, it deletes the RRM. Otherwise, it calculates the new RLT (which is the LLT if the previous forwarder is the source vehicle; otherwise, the new RLT is the minimum between the LLT and the RLT in the RRM). Next, it checks its RRT whether it has not already received the same RRM. If it has not, it saves the new RLT and RRM's id in its RRT, and then it puts its information (id, location, d(r, d), speed, direction, and new RLT) in place of those of the previous forwarder vehicle in the RRM. Next, it

```
(1) Notations;
(2) SV: source vehicle; DV: destination vehicle; FV: forwarder vehicle;
(3) RV: Receiver Vehicle on the side close to the destination of the forwarder's coverage area;
(4) RRM: Route Request Message;
(5) RRMID: RRM id;
(6) RRT: Route Request Table;
(7) LLT(FV, RV): Link LifeTime between forwarder vehicle and receiver vehicle;
(8) RLT: Route LifeTime;
(9) d(FV, RV): distance between forwarder vehicle and receiver vehicle;
(10) Information: id, location, speed, direction, RLT, d(FV, DV);
(11) R: communication range;
(12) Initialization;
(13) RLT = 0; d(FV, DV) = d(SV, DV);
(14) SV adds its information in RRM;
(15) SV broadcasts RRM;
(16) RV calculates LLT(FV, RV) and d(FV, RV);
(17) d(RV, DV) = d(FV, DV) − d(FV, RV);
(18) if d(RV, DV) ≤ 0 and RV ≠ DV then
(19)    RV deletes RRM;
(20) else
(21)    if FV == SV then
(22)       newRLT = LLT(FV, RV);
(23)    else
(24)       newRLT = min(LLT(FV, RV), RLT in RRM);
(25)    end
(26)    if RRMID is not in RRT of RV then
(27)       RV saves newRLT and RRMID in its RRT;
(28)       if RV == DV then
(29)          DV replies by RRP;
(30)       else
(31)          RV modifies FV information in RRM by its information;
(32)          RV broadcasts RRM;
(33)       end
(34)    else
(35)       if newRLT ≤ RLT in RRT of RV then
(36)          RV deletes RRM;
(37)       else
(38)          RV modifies RLT in its RRT by newRLT;
(39)          if RV == DV then
(40)             DV replies by RRP;
(41)          else
(42)             RV modifies FV information in RRM by its information;
(43)             RV broadcasts RRM;
(44)          end
(45)       end
(46)    end
(47) end
```

Algorithm 1: MSRP: most stable route prediction.

broadcasts the latter in its communication range in the side close to the destination. Otherwise, it checks whether the new RLT is greater than the RLT in its RRT. If it is the case, it modifies the RLT in its RRT by the new RLT. Then, it puts its information instead of those of the previous forwarder vehicle in the RRM. Next, it broadcasts the latter in its communication range in the side close to the destination. Otherwise, it deletes it.

Each next receiving vehicle will do the same operations that have been done by the previous receiving vehicle until the route discovery message arrives to the destination or the distance between the source and the destination vehicles becomes less or equal to zero meters (Algorithm 1).

5.2. Scheme with Beacon Message. It is assumed that each vehicle periodically sends its information in beacon message (location, speed, direction of movement, identifier, and current time) to its neighbors. Then, each vehicle constructs its neighboring list by information extracted from beacon messages. Whenever a new neighbor is discovered, a new entry is added and a timer is set. A vehicle waits two

```
(1) Notations;
(2) SV: source vehicle; DV: destination vehicle; FV: forwarder vehicle;
(3) RV: Receiver Vehicle on the side close to destination of the communication range;
(4) NRV: Next RV on the side close to destination of the communication range;
(5) RRM: Route Request Message;
(6) RRMID: RRM id;
(7) RRT: Route Request Table;
(8) LLT(FV, RV): Link LifeTime between FV and RV;
(9) RLT: Route LifeTime;
(10) DPDT(SV, DV): The data packets delivery time between the SV and the DV;
(11) information: id, RLT;
(12) Initialization;
(13) RLT = 0; FV = SV;
(14) if DV is neighbor of SV and LLT(SV, DV) > DPDT(SV, DV) then
(15)    SV sends DATA to DV;
(16) else
(17)    SV adds its information in RRM;
(18)    SV broadcasts RRM;
(19)    RV calculates LLT(FV, RV);
(20)    if FV == SV then
(21)       new RLT = LLT(FV, RV);
(22)    else
(23)       new RLT = min(LLT(FV, RV), RLT in RRM);
(24)    end
(25)    if RRMID is not in RRT of RV then
(26)       RV saves new RLT and RRMID in its table RRT;
(27)       RV modifies FV information in RRM by its information;
(28)       if DV is neighbor of RV then
(29)          RV sends RRM to DV;
(30)       else
(31)          RV broadcasts RRM;
(32)       end
(33)    else
(34)       if new RLT > RLT in RRT of RV and LLT(RV, NRV) > RLT in RRT of RV then
(35)          RV modifies RLT in its RRT by new RLT;
(36)          RV modifies FV information in RRM by its information;
(37)          if DV is neighbor of RV and LLT(RV, DV) > RLT in RRT of RV then
(38)             RV sends RRM to DV;
(39)          else
(40)             if DV is neighbor of RV then
(41)                RV deletes RRM;
(42)             else
(43)                RV broadcasts RRM;
(44)             end
(45)          end
(46)       else
(47)          RV deletes RRM;
(48)       end
(49)    end
(50) end
```

Algorithm 2: MSRP-BM: most stable route prediction using beacon message.

consecutive beacon intervals to hear from its neighbor. If no message was received, the neighbors' entry is deleted.

In this scheme, when the source vehicle wants to send a data packet to destination, it checks if the latter is among its neighbors. If it is, it send it the data packet. Otherwise, it adds its information (identifier, and RLT that is 0 s at the source vehicle) in the route request message (RRM) and broadcasts it in its communication range.

Then, each receiver vehicle (r), on the side close to destination vehicle of its communication range, calculates the LLT between itself and the previous forwarder vehicle (f). Then, it determines the new RLT (which is the LLT if the previous forwarder is the source vehicle; otherwise, the new RLT is the minimum between the LLT and the RLT in the RRM). Next, it checks its RRT whether it has not already received the same RRM. If it has not, it saves the new RLT

and RRM's id in its RRT and then it puts its information (identifier and new RLT) in place of those of the previous forwarder in the RRM. After that, it checks whether the destination vehicle is among its neighbors. If it is, it sends to it the RRM. Otherwise, it broadcasts the latter in its communication range on the side close to the destination. Otherwise, it checks whether the new RLT is not strictly greater than the RLT in its RRT. If it is not, it deletes it. Otherwise, it checks if there is a next receiver that remains (in direct communication with the current receiver) a time strictly greater than the RLT in its RRT. If this is not the case, it deletes the RRM. Otherwise, it modifies the RLT in its RRT by the new RLT. Then, it puts its information instead of those of the previous forwarder in the RRM. Next, it checks whether the destination is among its neighbors. If it is, it sends to it the RRM. Otherwise, it broadcasts the latter in its communication range on the side close to the destination.

Each next receiving vehicle will do the same operations that have been done by the previous receiving vehicle until the route discovery message arrives to the destination (Algorithm 2).

6. Simulation and Results

We have used the pattern IDM-LC which is a microscopic mobility model in the tool vehicular ad hoc networks mobility simulator (VanetMobiSim), and we have used NS2 to implement our protocols. Vehicles are deployed in a 5000 m × 80 m area. This area is a highway with four lanes bidirectional. Vehicles are able to communicate with each other using the IEEE 802.11p MAC layer. The vehicles' speed fluctuates between 0 m/s and 27 m/s. We have considered packet size of 512 bytes, simulation time of 400 s, hello interval of 1 s, and packet rate of 4 packets per second. We setup ten multihop CBR flow vehicles over the network and start at different time instances and continue throughout the remaining time of the simulation. The transmission range is kept at 250 m. Simulation results are averaged over 20 simulation runs.

We evaluate the performance of our routing schemes MSRP-BM and MSRP against of ROMSGP which more closely resembles to the nature of our algorithms, and location-aided routing (LAR1) [29] that selects the shortest path. These schemes are evaluated for the average routes lifetime, the percentage of packets delivery, the control overhead, the average end-to-end delay, the throughput, and the average routes failures number generated during the transmission of data packets.

Simulation parameters are summarized in Table 2.

Figures 4 and 5 show the higher stability of MSRP and MSRP-BM compared to that of ROMSGP and LAR1 because our schemes determine the route that has the longest lifetime. Hence, it becomes more stable compared to others, where LAR1 gets the lowest route lifetime value. LAR1 chooses the shortest route that breaks quickly when the speed of vehicles and their number increase. ROMSGP chooses the shortest route among the vehicles belonging to the same group; for this reason, its route is stable compared to that of LAR1.

Table 2: Simulation parameters.

Parameter	Value
Simulation time	400 s
Simulation area	5000 m × 80 m
No. of vehicles	30–90
Transmission range	250 m
Packet rate	4 packets/s
Packet size	512 bytes
Traffic type	CBR
Mobility model	IDM-LC
Speed	0–100 km/h

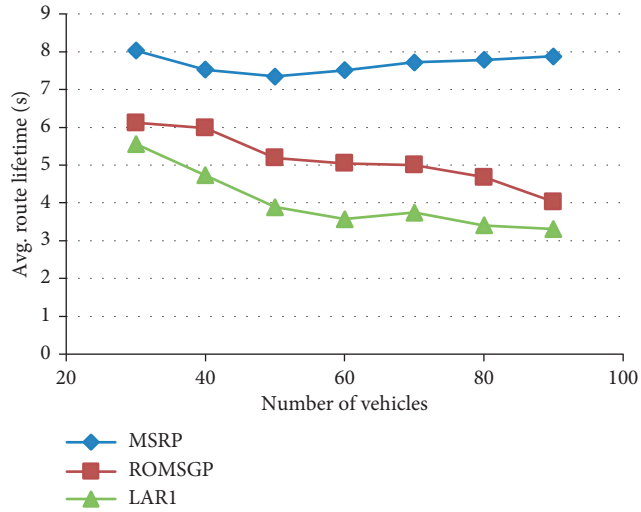


Figure 4: Average route lifetime versus vehicles density.

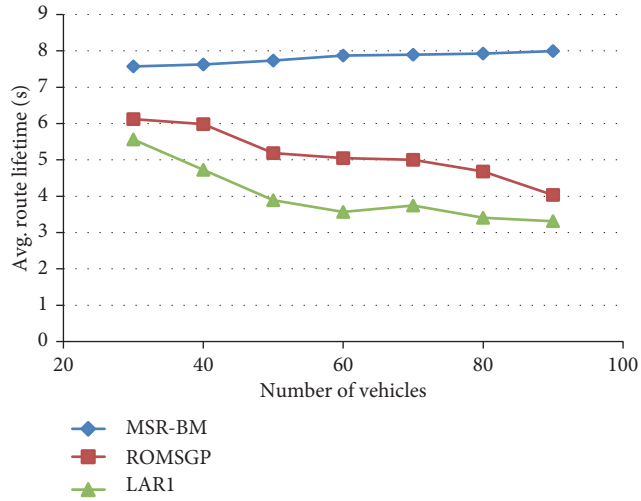


Figure 5: Average route lifetime versus vehicles density.

Figures 6 and 7 show the delay is maximal for a minimum number of vehicles, and it is linearly decreased with the increase of number of vehicles because of the reduction of the number of disconnections. The average end-to-end delay of our schemes is the lowest (notably when the vehicles

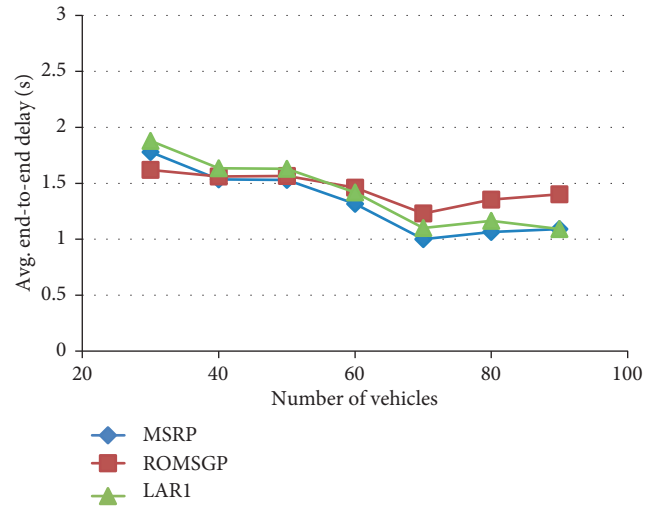


Figure 6: Average end-to-end delay versus vehicles density.

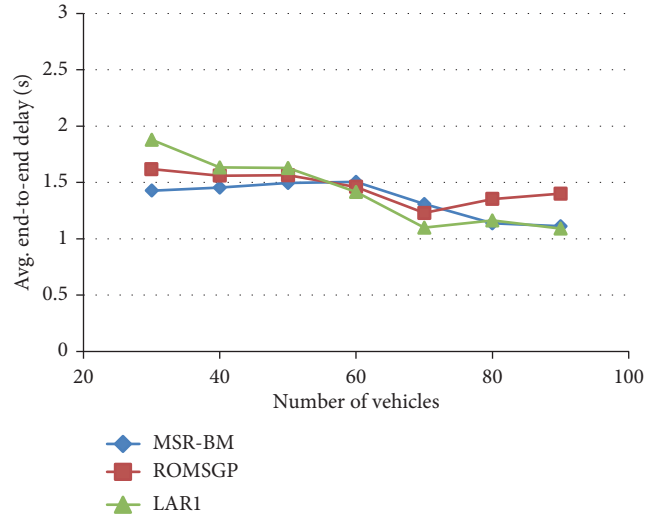


Figure 7: Average end-to-end delay versus vehicles density.

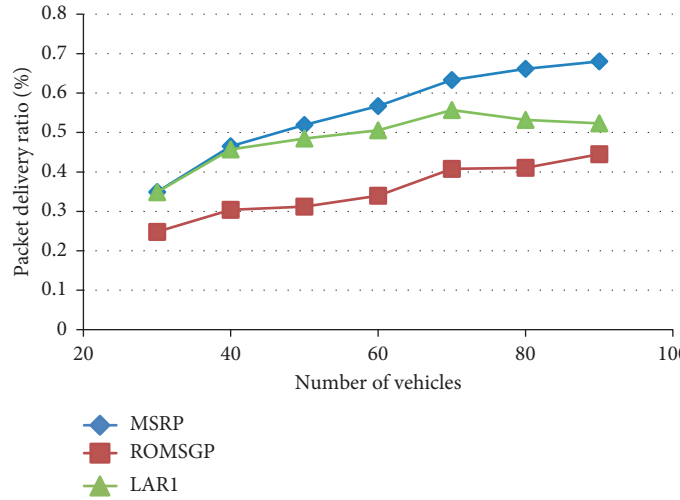


Figure 8: Packet delivery ratio versus vehicles density.

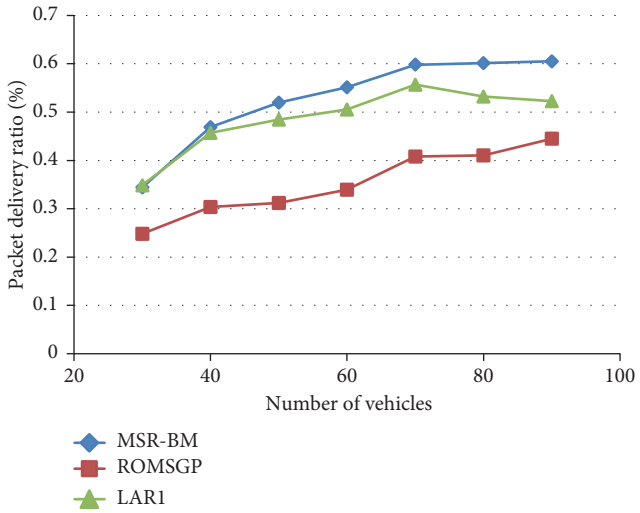


Figure 9: Packet delivery ratio versus vehicles density.

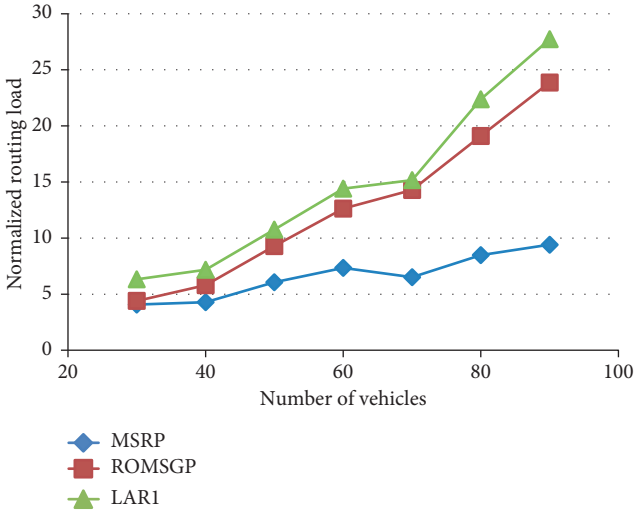


Figure 10: Normalized routing load versus vehicles density.

number is increasing) compared to those of ROMSGP and LAR1 because of the stability of route that reduces the number of data packets in queue, and thus, the delivery delay of data packet between the source and the destination vehicles.

Figures 8 and 9 exhibit that the packet delivery ratio of all schemes increases with the increase of vehicles density on the road and that our schemes achieve a good packet delivery ratio than both ROMSGP and LAR1. This is because our schemes forward data packets on road by predicting the most stable route taking into account the velocity variation; on the contrary of ROMSGP that determines a stable route by selecting the shortest route among the vehicles belonging to the same group and LAR1 that selects the shortest path. The selection of the most stable route allows the decrease of the number of route breakage and the number of data packets in queue. The packet delivery ratio is not better because of the nonuniform distribution of vehicles in our mobility model. Moreover, we have not yet used a method which keeps the data until the destination vehicle, as in the case of the carry-and-forward mechanism [30].

In Figures 10 and 11, we consider all control packets used in the routing process, except beacon messages for our MSR-BM scheme. The control overheads of all routing protocols increase according to the increase of number of vehicles. LAR1 does not predict a stable route; hence, it generates more control overhead because of the frequent route reconstruction. ROMSGP determines a stable route by building the route by vehicles of the same group; hence, it provides less control overhead compared with LAR1. Our schemes predict the most stable route that decreases to a high extent the reconstruction of route; for this reason, they have much less control overhead than the other compared routing protocols.

In Figures 12 and 13, our schemes have better throughput than ROMSGP and LAR1. Because in MSRP and MSR-BM, the duration of the paths is longer, the number of path breaks is reduced, and also the control overhead is decreased compared with the other routing protocols.

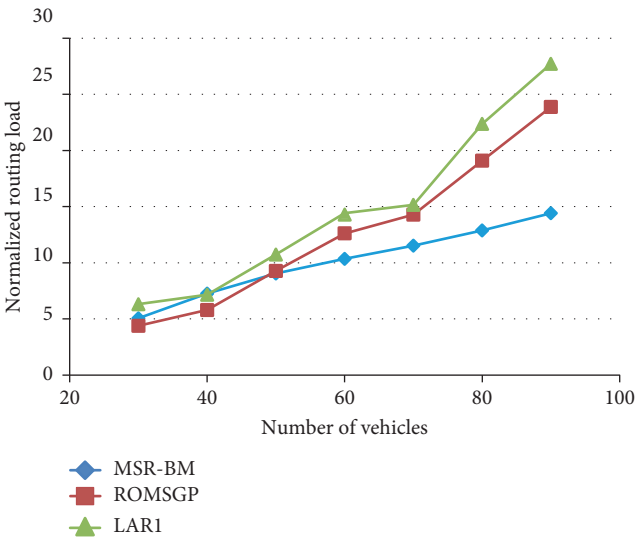


Figure 11: Normalized routing load versus vehicles density.

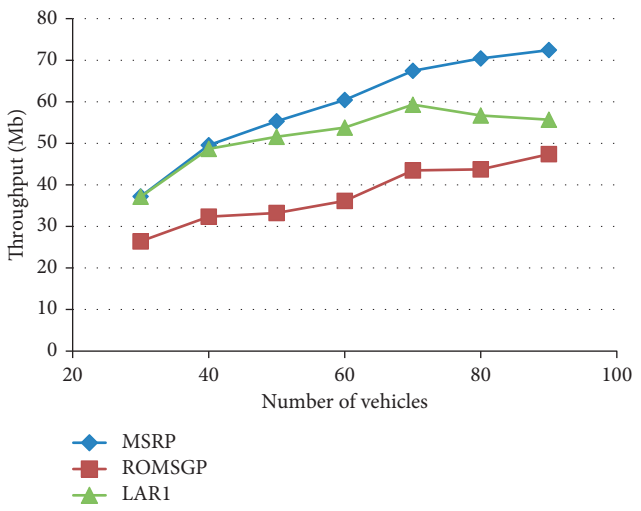


Figure 12: Throughput versus vehicles density.

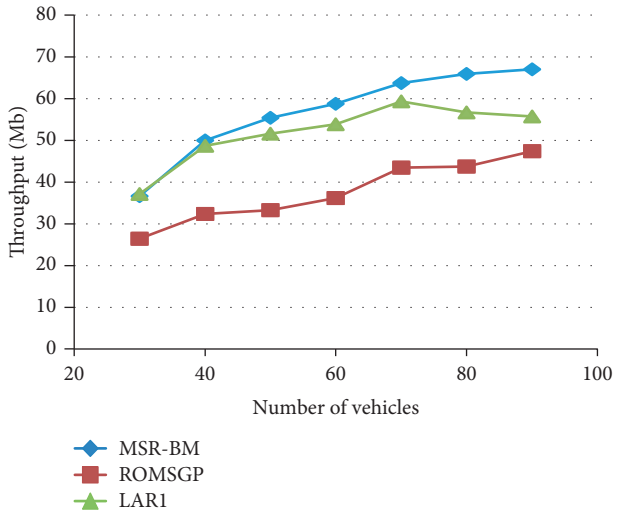


Figure 13: Throughput versus vehicles density.

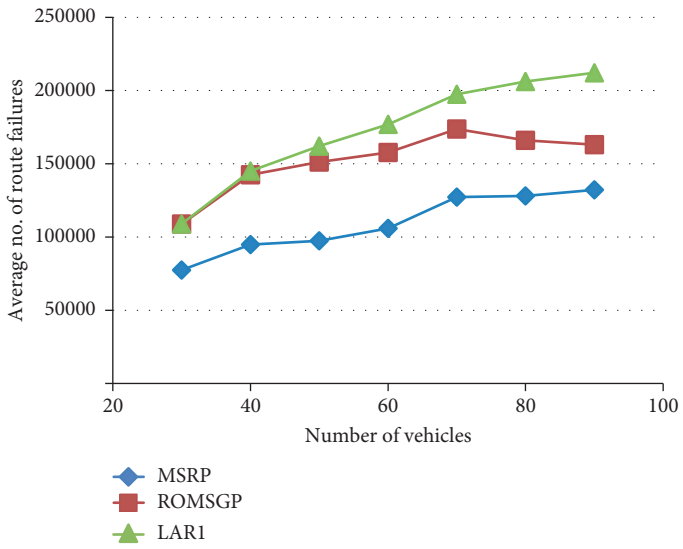


Figure 14: Average of routes failures versus vehicles density.

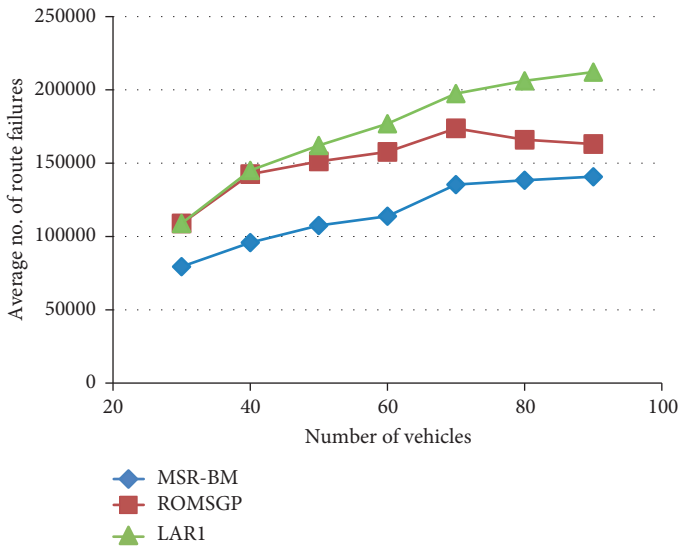


Figure 15: Average of routes failures versus vehicles density.

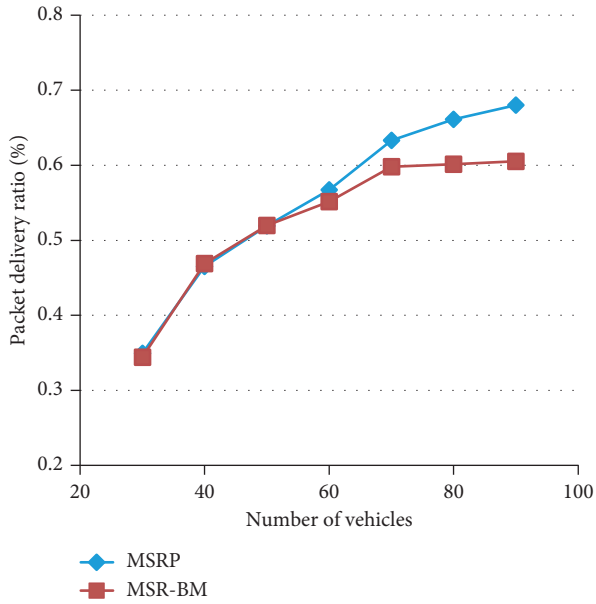


Figure 16: PDR between our schemes versus vehicles density.

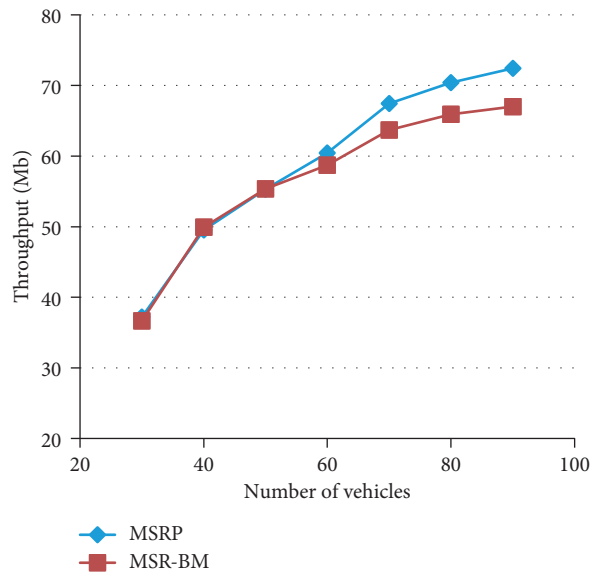


Figure 17: Throughput between our schemes versus vehicles density.

ROMSGP has the lowest throughput compared to LAR1. This is because ROMSGP determines the route by vehicles that travel in the same group (they are not enough) on the contrary of our schemes and LAR1 that do not take into account the direction of movement. When the number of vehicles increases, the ROMSGP throughput increases rapidly compared to that of LAR1. This is because ROMSGP has enough number of vehicles to select a stable route versus LAR1 that determines the shortest path.

As shown in Figures 14 and 15, the average number of route breaks (number of errors) of our protocols is lower than those of both ROMSGP and LAR1, because our schemes choose the most stable route and predict the data

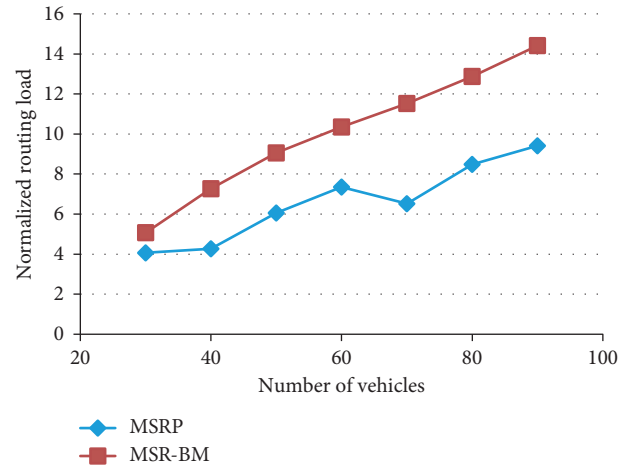


Figure 18: NRL between our schemes versus vehicles density.

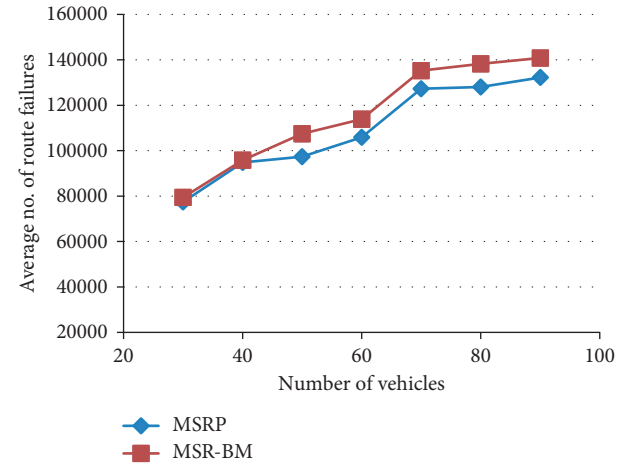


Figure 19: Average of routes failures between our schemes versus vehicles density.

packet delivery time before sending data. LAR1 chooses the shortest path, regardless of whether it is reliable or not. ROMSGP outperforms LAR1 because it predicts a stable route by building it by vehicles belonging to the same group, and it creates a new alternative route before a route breakage.

As shown in Figures 16–19, according to the vehicles density, our scheme with beacon message (MSRP-BM) has the lowest packet delivery ratio and throughput. Besides, MSRP-BM has the highest normalized routing load and the highest average number of route failure compared to our scheme without beacon message (MSRP). This is explained by periodicity of beacon messages that charge the bandwidth.

7. Conclusion

Our schemes are designed to enhance the communication on highway for the comfort applications. They predict the most stable route by selecting the route that has the longest lifetime. They are based on the prediction of the link lifetime and the route lifetime taking into account the velocity

variation. Moreover, our schemes predict the data packet delivery time before sending the data. They are compared to ROMSGP and LAR1 in highway environment. The results showed that our schemes have higher average route lifetime, higher percentage of packet delivery, higher throughput, lower average end-to-end delay, and lower average route failures number compared to existing schemes.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. A. Hussain, M. Iqbal, A. Saeed et al., "An efficient channel access scheme for vehicular ad hoc networks," *Mobile Information Systems*, vol. 2017, Article ID 8246050, 10 pages, 2017.

[2] A. Zekri and W. Jia, "Heterogeneous vehicular communications: a comprehensive study," *Ad Hoc Networks*, vol. 75-76, pp. 52–79, 2018.

[3] T. S. J. Darwish, K. Abu Bakar, and K. Haseeb, "Reliable intersection-based traffic aware routing protocol for urban areas vehicular ad hoc networks," *IEEE Intelligent Transportation Systems Magazine*, vol. 10, no. 1, pp. 60–73, 2018.

[4] S. Sultan, M. Doori, A. Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc networks," *Journal of Network and Computer Applications*, vol. 37, pp. 380–392, 2014.

[5] A. Dua, N. Kumar, and S. Bawa, "A systematic review on routing protocols for vehicular ad hoc networks," *Vehicular Communications*, vol. 1, no. 1, pp. 33–52, 2014.

[6] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2010.

[7] D. Tian, K. Shafiee, and V. C. M. Leung, "Position-based directional vehicular routing," in *Proceedings of GLOBECOM 2009, IEEE Global Telecommunications Conference*, pp. 1–6, Honolulu, HI, USA, November-December 2009.

[8] T. Taleb, E. Sakhaee, A. Jamalipour, K. Hashimoto, N. Kato, and Y. Nemoto, "A stable routing protocol to support ITS services in VANET networks," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3337–3347, 2007.

[9] M. A. Togou, A. Hafid, and L. Khoukhi, "SCRP: stable CDS-based routing protocol for urban vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1298–1307, 2016.

[10] M. H. Eiza and Q. Ni, "An evolving graph-based reliable routing scheme for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 4, pp. 1493–1504, 2013.

[11] Z. Wang, L. Liu, M. Zhou, and N. Ansari, "A position-based clustering technique for ad hoc intervehicle communication," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 38, no. 2, pp. 201–208, 2008.

[12] F. Abbas and P. Fan, "Clustering-based reliable low-latency routing scheme using ACO method for vehicular networks," *Vehicular Communications*, vol. 12, pp. 66–74, 2018.

[13] H. Menouar, M. Lenardi, and F. Filali, "A movement prediction based routing protocol for vehicle-to-vehicle communications," in *Proceedings of V2VCOM*, San Diego, CA, USA, July 2005.

[14] V. Namboordiri and L. Gao, "Prediction-based routing for vehicular ad hoc networks," *IEEE Transaction on Vehicular Technology*, vol. 56, no. 4, pp. 2332–2345, 2007.

[15] C. Liu, Y. Shu, O. Yang, Z. Xia, and R. Xia, "SDR: a stable direction-based routing for vehicular ad hoc networks," *Wireless Personal Communications*, vol. 73, no. 3, pp. 1289–1308, 2013.

[16] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of WMCSA'99 Second IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90–100, New Orleans, LA, USA, February 1999.

[17] Y. Sun, S. Luo, Q. Dai, and Y. Ji, "An adaptive routing protocol based on QoS and vehicular density in urban VANETs," *International Journal of Distributed Sensor Networks*, vol. 11, no. 6, 2015.

[18] B. Moussaoui, S. Djahel, M. Smati, and J. Murphy, "A cross layer approach for efficient multimedia data dissemination in VANETs," *Vehicular Communications*, vol. 9, pp. 127–134, 2017.

[19] M. H. Eiza, Q. Ni, T. Owens, and G. Min, "Investigation of routing reliability of vehicular ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, pp. 1–15, 2013.

[20] K. A. Darabkh, M. S. E. Judeh, H. Bany Salameh, and S. Althunibat, "Mobility aware and dual phase AODV protocol with adaptive hello messages over vehicular adhoc networks," *International Journal of Electronics and Communications*, vol. 94, pp. 277–292, 2018.

[21] M. M. Alotaibi and H. T. Mouftah, "Adaptive expiration time for dynamic beacon scheduling in vehicular ad-hoc networks," in *Proceedings of 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, pp. 1–6, Boston, MA, USA, September 2015.

[22] Q. Guan, F. R. Yu, and S. Jiang, "Prediction-based topology control and routing in cognitive radio mobile ad hoc networks," in *Proceedings of 2010 INFOCOM IEEE Conference on Computer Communications Workshops*, pp. 1–6, San Diego, CA, USA, March 2010.

[23] O. Kaiwartya and S. Kumar, "Guaranteed geocast routing protocol for vehicular adhoc networks in highway traffic environment," *Wireless Personal Communications*, vol. 83, no. 4, pp. 257–2682, 2015.

[24] K. L. K. Sudheera, M. Ma, G. G. M. N. Ali, and P. H. J. Chong, "Delay efficient software defined networking based architecture for vehicular networks," in *Proceedings of 2016 IEEE International Conference on Communication Systems, ICCS*, pp. 1–6, Shenzhen, China, December 2016.

[25] B. A. Forouzan and S. C. Fegan, *Data Communications and Networking*, McGraw-Hill Higher Education, New York, NY, USA, 2007.

[26] H. Saleet, O. Basir, R. Langar, and R. Boutaba, "Region-based location-service-management protocol for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 917–931, 2010.

[27] M. Rehan, H. Hasbullah, I. Faye et al., "ZGLS: a novel flat quorum-based and reliable location management protocol for VANETs," *Wireless Network*, vol. 24, no. 6, pp. 1885–1903, 2017.

[28] M. Nabil, A. Hajami, and A. Haqiq, "Determining and evaluating the most route lifetime as the most stable route

between two vehicles in VANET," in *Proceedings of the 8th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2017)*, pp. 125–132, Springer International Publishing, Marrakech, Morocco, December 2017.

[29] Y. B. Ko and N. H. Vaidya, "Location-Aided Routing (LAR) in mobile ad hoc networks," *Wireless Networks*, vol. 6, no. 4, pp. 307–321, 2000.

[30] N. Alsharif, S. Cspedes, and X. S. Shen, "iCAR: Intersection-based connectivity aware routing in vehicular ad hoc networks," in *Proceedings of 2013 IEEE International Conference on Communications (ICC)*, pp. 1736–1741, Budapest, Hungary, June 2013.

Hindawi
Mobile Information Systems
Volume 2018, Article ID 9093139, 6 pages
https://doi.org/10.1155/2018/9093139

Research Article

Uplink Resource Allocation for Interference Mitigation in Two-Tier Femtocell Networks

Sung-Yeop Pyun,[1] Woongsup Lee,[2] and Ohyun Jo[3]

[1]*Korea Telecom, Seoul, Republic of Korea*
[2]*Department of Information and Communication Engineering, Gyeongsang National University, Tongyeong 53064, Republic of Korea*
[3]*Department of Computer Science, College of Electrical and Computer Engineering, Chungbuk National University, Cheongju 28644, Republic of Korea*

Correspondence should be addressed to Ohyun Jo; jjo9804@gmail.com

Received 6 August 2018; Revised 8 October 2018; Accepted 31 October 2018; Published 2 December 2018

Guest Editor: Safdar H. Bouk

Two-tier femtocell networks, in which a large number of femto base stations (BSs) are deployed within a region overlapping with a macrocell, can provide an economical means of increasing user capacity and coverage. Given that femto BSs may be deployed with no cell planning, cross-tier interference generated from a number of macrocells and femtocells can cause severe problems. In particular, a macro mobile station (MS) that transmits uplink data may generate severe interference with adjacent femtocells, which causes performance degradation. In order to solve these problems, two novel resource allocation schemes, *optimization* and *heuristic*, are proposed, which efficiently reduce uplink interference in two-tier femtocell networks. Simulation results at the system level verify that both proposed schemes can improve the average capacity of the femtocells, but the heuristic scheme outperforms the optimization scheme in terms of computational complexity.

1. Introduction

With the increasing popularity of high data rate wireless services, a number of communication techniques have been proposed to cope with the increase in mobile traffic. One simple yet powerful means of increasing the capacity of wireless networks involves decreasing the size of the cell because a small cell is perfectly adequate for providing high data rate services for multiple users through more efficient wireless environments. Accordingly, femtocells, which have a small cell coverage, have been regarded as a key element in providing high-quality services in homes or small offices [1].

Femto base stations (BSs) are low-transmit power BSs with restricted indoor service coverage. Femto BSs provide connections between mobile devices and service providers using a licensed band [2]. They provide an efficient way of achieving a high data rate and increased service area, especially in places where radio connection would otherwise not be supportable. In two-tier femtocell networks, a large number of femtocells may be overlapping in the service area of a conventional macrocell, which has a large service coverage.

Given that femtocells are usually deployed without any cell planning, macrocells and femtocells can interfere with each other, probably leading to severe performance degradation in two-tier femtocell networks, especially if the spectrum is shared among femtocells and macrocells [3, 4]. For example, a mobile station (MS) of a macro BS that transmits with a high power or is located near the femto BS may cause severe uplink interference with neighboring femtocells, and accordingly, the capacity of the femtocells can deteriorate.

The importance of uplink interference in two-tier femtocell networks means that its mitigation has been extensively investigated in the previous literature [5–7]. Uplink capacity in CDMA-based two-tier femtocell networks was analyzed in [5], in which a technique for avoiding interference using sectorization and CDMA hopping was also presented. In [6], the uplink capacity of TDMA-based

two-tier femtocell networks was analyzed by distinguishing between those cases where macro- and femtocells share the same frequency and those where the frequency is divided. When the frequency is divided, the interference generated between macrocells and femtocells may not occur when the spectral efficiency is reduced. However, when the frequency is shared, the uplink throughput may be increased by the proper allocation of transmit power. In [7], an uplink power control scheme was proposed, in which the maximum transmit power of femtocell users is adjusted, in an effort to mitigate cross-tier interference at a macro BS. Finally, efficient power control schemes in dense and small-cell networks are studied in [4, 8, 9]. The interference management algorithms for improvement of practical LTE and LTE-A mobile networks are studied and adopted practically as shown in [10–15].

We present efficient resource allocation algorithms that can reduce uplink interference in two-tier femtocell networks. To this end, we formulate an optimization scheme using integer programming (IP), but this turns out to be somewhat impractical due to its complexity. In order to provide a practical solution, we propose a heuristic scheme with low complexity in which femtocells and a macrocell perform resource allocation cooperatively.

2. System Model

We consider two-tier femtocell networks in which a set of femto BSs $\mathbf{K} = \{1, \ldots, K\}$ are deployed in the coverage of a macro MB. Both macro BS and femto BSs use the same frequency band, and the bandwidths of the macro BS and the femto BS_k are denoted by W and W_k, respectively. A set of macro MSs $\mathbf{M} = \{1, \ldots, M\}$ communicate with the macro BS. A set of femto MSs $\mathbf{M}_k = \{1, \ldots, M_k\}$ communicate with the femto BS_k, where $k = 1, \ldots, K$ that denotes the index of the femto BS.

Each frame containing downlink and uplink subframes has the same duration, where $t = 1, 2, \ldots$ is the index of the frame. Each uplink subframe is divided into a set $\mathbf{N} = \{1, \ldots, N\}$ of time slots, each of which has a fixed interval. Each femto BS may be synchronized with the overlay macro BS in the frames using GPS or the IEEE 1588 PTP (Precision Time Protocol) [16]. A quasistatic flat fading channel is assumed, in which the channel state is constant within a unit frame duration and can vary frame by frame. A BS is made aware of the state of the channels from channel feedback information.

The signal to interference/noise ratio (SINR) of femto MS_i belonging to femto BS_k in slot j at time t is given by

$$\gamma_{ij}^{k}(t) = \frac{p_i^k(t) h_i^k(t)}{W_k N_0 + I_j^k(t)}, \tag{1}$$

where $p_i^k(t)$ is the transmitted power of femto MS_i belonging to femto BS_k, $h_i^k(t)$ is the gain experienced in the channel between femto MS_i and femto BS_k, and N_0 denotes the amount of noise per hertz.

The amount of interference in the uplink of femto BS_k in slot j at time t is described as

$$\begin{aligned} I_j^k(t) &= I_{\text{macro}\longrightarrow j}^k + I_{\text{femto}\longrightarrow j}^k, \\ I_{\text{macro}\longrightarrow j}^k &= \sum_{m\in M} p_m(t) h_{mk}(t) b_{mj}(t), \\ I_{\text{femto}\longrightarrow j}^k &= \sum_{k'\in K, k'\neq k} \sum_{i'\in M_{k'}} p_{i'}^{k'}(t) h_{i'k}^{k'}(t) b_{i'j}^{k'}(t), \end{aligned} \tag{2}$$

where $I_{\text{macro}\longrightarrow j}^k$ is the amount of interference from the macro MSs to femto BS_k where $p_m(t)$ is the transmitted power of macro MS m, $h_{mk}(t)$ is the gain experienced in the channel between macro MS m and femto BS_k, and $b_{mj}(t)$ is the indicator of resource allocation for the macro BS. If the slot j at frame t is allocated for macro MS m, $b_{mj}(t)$ is 1; otherwise, it is 0.

$I_{\text{femto}\longrightarrow j}^k$ is the amount of interference from the MSs located in the other femto BSs with femto BS_k where $p_{i'}^{k'}(t)$ is the transmitted power of femto MS i' in the femto BS k', $h_{i'k}^{k'}(t)$ is the gain experienced in the channel between femto MS i' located in femto $\mathrm{BS}_{k'}$ and femto BS_k, and $b_{i'j}^{k'}(t)$ is the indicator of resource allocation for femto $\mathrm{BS}_{k'}$. If the slot j at frame t is allocated to femto MS i', $b_{i'j}^{k'}(t)$ is 1; otherwise, it is 0. Given that the interference between femtocells can be mitigated using either transmit power control or fractional frequency reuse [17], the interference generated in the uplink between macro MSs and femtocells can be minimized.

Using uplink open-loop transmit power control [18], which was devised to compensate the propagation loss and channel fluctuation due to shadowing, a BS determines the transmit power of subordinated MSs such that the target SINR can be satisfied. Therefore, the transmitted power of the subordinated MSs can be estimated by the macro/femto BSs. The MS i's target SINR, $\gamma_i^{\text{target}}(t)$, can be determined from the MS's rate requirement.

3. Efficient Resource Allocation

Figure 1 shows how the BS operates under the proposed schemes. A scheduler conventionally selects a number of MSs from those connected to the BS and then decides on the number of slots for the selected MSs. Note that a variety of scheduling policies can be chosen, as in the conventional scheduler. The proposed schemes are then used to determine which time slots are allocated for the selected MSs.

$r_m(t)$ and $r_i^k(t)$ denote the number of time slots allocated to macro MS m and femto MS i located in femto BS_k, respectively. Then, $R(t) = \sum_{m\in\mathbf{M}} r_m(t)$ and $R^k(t) = \sum_{i\in\mathbf{M}_k} r_i^k(t)$ are defined by the number of time slots allocated by a macro BS and femto BS_k, respectively, where $0 \le R(t) \le N$ and $0 \le R^k(t) \le N$. The uplink resource utilization of macro BS $\lambda(t)$ and femto BS_k $\lambda^k(t)$ can be expressed as

$$\begin{aligned} \lambda(t) &= \frac{R(t)}{N}, \quad \text{where } 0 \le \lambda(t) \le 1, \\ \lambda^k(t) &= \frac{R^k(t)}{N}, \quad \text{where } 0 \le \lambda^k(t) \le 1 \text{ for } \quad k = 1, \ldots, K, \end{aligned} \tag{3}$$

which is the number of allocated time slots as a proportion of the total time slots.

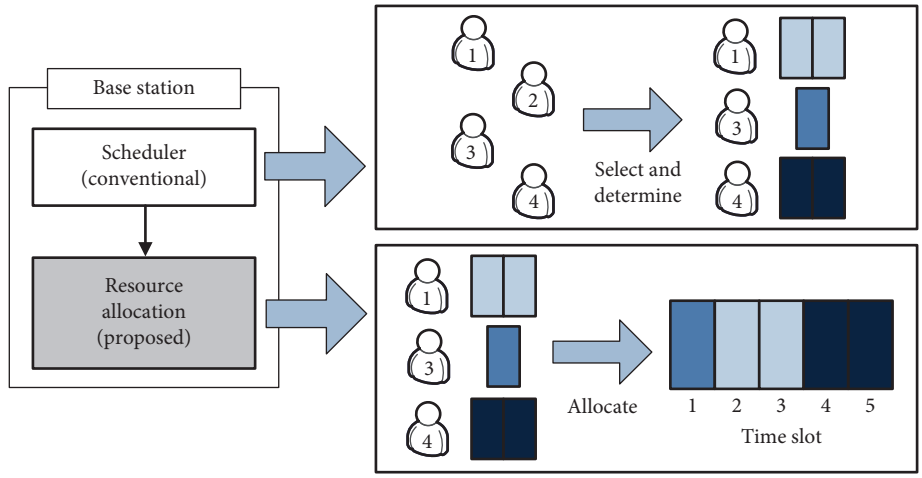


Figure 1: BS operation including scheduler and resource allocation. The term BS refers both macro and femto BSs.

3.1. Resource Allocation Using Optimization Scheme. In the optimization scheme, the uplink interference from macro MSs is supposed to be known to each femto BS_k through its backhaul link. Therefore, the optimization scheme can maximize the capacity of femto BS_k regardless of any resource allocation of a macro BS, $b_{mj}(t)$. We devise the optimization scheme using the following integer programming method:

$$\max_{\mathbf{b}_k} \sum_{i\in\mathbf{M}_k} \sum_{j\in\mathbf{N}} b_{ij}^k(t)\log_2\left(1+\gamma_{ij}^k(t)\right) \tag{4}$$

subject to

$$\sum_{i\in\mathbf{M}_k} b_{ij}^k(t) \le 1, \quad \forall j \in \mathbf{N}, \tag{5}$$

$$\sum_{j\in\mathbf{N}} b_{ij}^k(t) = r_i^k(t), \quad \forall i \in \mathbf{M}_k, \tag{6}$$

$$b_{ij}^k(t) \in \{0,1\}, \quad \forall i \in \mathbf{M}_k,\ j \in \mathbf{N}, \tag{7}$$

$$b_{mj}(t) \in \{0,1\}, \quad \forall m \in \mathbf{M},\ \forall j \in \mathbf{N}, \tag{8}$$

where $\mathbf{b}_k$ is an $M_k \times N$ matrix, the elements of which denote the resource allocators of the femto BS_k, $b_{ij}^k(t)$. The objective function (4) is intended to maximize the total sum capacity of all femto MSs belonging to the femto BS_k. Moreover, equation (5) describes the constraint that a single time slot cannot be shared for multiple femto MSs simultaneously. Furthermore, equation (6) indicates that the total number of allocated time slots of femto MS i is $r_i^k(t)$. Equations (7) and (8), respectively, describe the binary resource allocator of femto BS_k $b_{ij}^k(t)$ and macro BS $b_{mj}(t)$.

From the solution of the formulated problem, each femto BS_k can obtain the optimal resource allocator $\mathbf{b}_k$. However, a huge signaling overhead is required to ascertain the uplink interference $I_j^k(t)$ at the femto BS. In addition, the femto BS needs to solve an integer programming problem, which also entails a large number of computations.

2.2. Resource Allocation Using Heuristic Scheme. To avoid the problems encountered with the optimization scheme, a heuristic scheme is proposed, which reduces the computational complexity by operating in a distributed way. Also, in the conventional OFDM-based two-tier/multitier resource allocation algorithms which are adopted in standards, macro BS and femto BSs use the separated resources or frequency bands to avoid and mitigate intercell interference. In this manner, the network-wise capacity cannot be optimized. Also, the cooperation of macro BS and femto BSs is hardly possible in the practical deployment scenarios because the vendors of macro BS and the vendors of femto BSs are not same generally. Thus, it is very important that the resource management algorithms between macro BS and femto BSs should work in a distributed manner. The system model in which the proposed scheme is working is exactly the same to the system model of the optimization scheme. Given that a macro MS that uses a great amount of power when transmitting may severely interfere with neighboring femtocells; by using the proposed heuristic algorithm, femto BSs can cooperate with the overlaid macro BS in resource allocation.

We describe how the macro BS operates in the heuristic scheme. First, the index of time slot $j = 1$ and the resource allocator of macro BS $b_{mj}(t) = 0$ are initialized. Second, the macro BS classifies the MSs scheduled at time t, $\mathbf{M}'$. Third, the macro BS allocates time slots to the scheduled macro MSs based on the transmit power in the descending order. The macro MS m' with the largest transmit power is chosen from the scheduled macro MSs, $\mathbf{M}'$. A slot j is then allocated for the chosen macro MS m' ($b_{m'j}(t) = 1$). Finally, the index of slot j and the number of slots allocated to macro MS m', $r_{m'}(t)$, are updated. The macro BS may continue allocating slots to the chosen macro MS m' in the ascending order of the slot index (from 1 to N) until the number of slots allocated to macro MS m' is satisfied ($r_{m'}(t) = 0$). This operation is summarized in Algorithm 1.

The operation of femto BS_k in the heuristic scheme is described as follows. First, the index of time slot $j = N$ and the resource allocator of femto BS $b_{ij}^k(t) = 0$ are initialized.

(1) Parameter initialization

(i) $j = 1$: slot index
(ii) $b_{mj}(t) = 0$, $\forall m \in \mathbf{M}$, $\forall j \in \mathbf{N}$: resource allocator

(2) Compute scheduled macro MS set

(i) $\mathbf{M}' = \{m \in \mathbf{M} \mid r_m(t) > 0\}$

(3) Choose a macro MS m'

(i) $m' = \arg\max_{m \in M'} p_m(t)$

(4) Time slot allocation for the macro MS m'

(i) $b_{m'j}(t) = 1$

(5) Parameter update

(i) $j = j + 1$ and $r_{m'}(t) = r_{m'}(t) - 1$

(6) If $r_{m'}(t) = 0$, go to step (7); otherwise, go back to step (4)
(7) Update the macro MS scheduling set

(i) $\mathbf{M}' = \mathbf{M}' - m'$

(8) If $\mathbf{M}' = \varnothing$, stop; otherwise, go back to step (3)

Algorithm 1: Macro BS operation in the heuristic scheme.

(1) Parameter initialization

(i) $j = N$: index of time slot
(ii) $b_{ij}^k(t) = 0$, $\forall i \in \mathbf{M}_k$, $\forall j \in \mathbf{N}$: resource allocator

(2) Compute scheduled macro MS set

(i) $\mathbf{M}_k' = \{i \in \mathbf{M}_k \mid r_i^k(t) > 0\}$

(3) Choose a femto MS i'

$i' = \arg\min_{i \in \mathbf{M}_k'} \gamma_i^{\text{target}}(t)$

(4) Time slot allocation for femto MS i'

(i) $b_{i'j}^k(t) = 1$

(5) Parameter update

(ii) $j = j - 1$ and $r_{i'}^k(t) = r_{i'}^k(t) - 1$

(6) If $r_{i'}^k(t) = 0$, go to (7); otherwise, go back to step (4)
(7) Update the femto MS scheduling set

(i) $\mathbf{M}_k' = \mathbf{M}_k' - i'$

(8) If $\mathbf{M}_k' = \varnothing$, stop; otherwise, go back to step (3)

Algorithm 2: Femto BS BS_k operation in the heuristic scheme.

Second, the femto BS classifies the femto MS scheduling set at time t, $\mathbf{M}_k'$. Third, given that the macro BS allocates slots to the scheduled macro MSs based on the transmit power in the descending order, the femto BS allocates slots to the scheduled femto MS in the descending order of the time slot (from N to 1) in order to minimize interference from macro MSs, as follows. Even if the amount of interference from macro MSs is the same, a femto MS with a low target SINR may experience more capacity degradation than a femto MS with a high target SINR. Therefore, femto MS i' with the smallest target SINR is chosen from the scheduled femto MSs, $\mathbf{M}_k'$. The femto BS then assigns a slot j for the chosen femto MS i' ($b_{i'j}^k(t) = 1$). Finally, the index of slot j and the number of slots to be allocated to macro MS i' $r_{i'}^k(t)$ are updated. The femto BS may keep allocating slots to the chosen femto MS i' in the descending order of the slot (from N to 1) until the number of slots allocated to femto MS i' is satisfied ($r_{i'}^k(t) = 0$). The operation of a femto BS is summarized in Algorithm 2.

Using the heuristic scheme means that the capacity of the femtocells may be lower than in cases where the optimization scheme is used because resources are allocated heuristically. However, because the femtocells do not need to receive any information about the interference generated in the uplink of macro MSs, the heuristic scheme can operate in a distributed manner. The computational complexity of the heuristic scheme, which can be derived as $O(NM_k)$, is also much lower than that of the optimization scheme. Even though the macro BS requires additional computations whose complexity is $O(NM)$ for cooperative resource allocation, the overall computational complexity is low such that the heuristic scheme is potentially affordable and takes place in real time. And the mobile station which generates intercell interference significantly can be efficiently taken account into the resource allocations for macro BS and femto BSs in a distributed manner.

4. Simulation Results and Conclusions

For our simulation environment, we consider a two-tier femtocell network where K femto BSs are uniformly located in the coverage of a macro BS. In our performance evaluation, we only consider the capacity of femto BSs located in the outer area of a macrocell. In the simulation, a proportional fair scheduler was used for the conventional scheduler of a BS. The channel gains ($h_i^k(t)$, $h_{mk}(t)$, and $h_{ik}(t)$), and the location of the MSs, were decided in the simulations with reference to the scenario in [19]. The detailed parameters are summarized in Table 1. We found out the solution of the optimization problem which is described in equations (4)–(8) by using MATLAB and then compared to the performance of the proposed algorithm evaluated also by MATLAB simulations.

Figure 2 describes the average capacity of an outer femto BS according to the uplink resource utilization $\lambda^k(t)$ in the case where the uplink resource utilization of macro BS is $\lambda(t) = 0.4$. The proposed schemes evidently yield capacity enhancement over a random scheme in which time slots are randomly allocated to femto MSs. When the uplink resource utilization of femto BS $\lambda^k(t)$ increases, it is obvious that the amount of interference in the uplink increases as well. As a consequence, the amount of capacity enhancement by the proposed schemes falls from 41% to 4% because the scheduling gain decreases. When the resource utilization of the femto BS is at a maximum ($\lambda^k(t) = 1$), the gain of the proposed schemes is at a minimum.

Figure 3 describes the average capacity of the outer femto BS according to the uplink resource utilization $\lambda^k(t)$ in the case where the uplink resource utilization of the macro BS is $\lambda(t) = 0.6$. When the uplink resource utilization of macro BS

Table 1: Simulation parameters.

Macro cell coverage	700 m
Femtocell coverage	20 m
Number of femto BSs (K)	50
Number of macro MSs (M)	15
Number of femto MSs in femto BS$_k$ (M_k)	2
System bandwidth of macro BS (W)	5 MHz
System bandwidth of femto BS (W_k)	1 Hz
Distance between macro BS and outer femto BS	600 m
Number of time slots (N)	5
Target SINR of macro MSs	10 dB
Target SINR of femto MSs	10, 20 dB
Max TX power of MSs	23 dBm
External wall loss of femtocells	10 dB

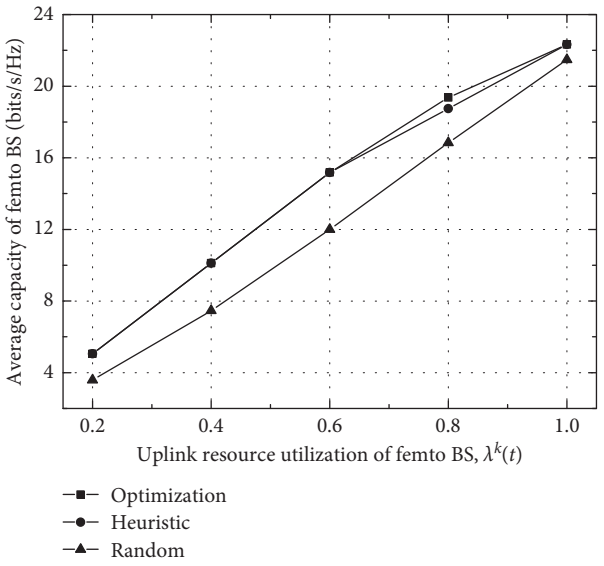


Figure 2: Average capacity of outer femto BS in the case where uplink resource utilization of macro BS $\lambda(t) = 0.4$.

$\lambda(t)$ increases, the amount of uplink interference with the femto BSs also increases. As a consequence, the capacity enhancements of both heuristic scheme and random scheme decrease compared to those of the optimization scheme. When the resource utilization of femto BS$_k$ is less than the unused resource utilization of the macro BS ($\lambda^k(t) \leq 1 - \lambda(t)$), the heuristic scheme can allocate the uplink resources that are not used by the macro MSs to femto MSs belonging to femto BS$_k$. In this case, the heuristic scheme shows the same performance as the optimization scheme because it can avoid strong uplink interference.

Figure 4 describes the average capacity of the outer femto BS according to the uplink resource utilization $\lambda^k(t)$ in the case that the uplink resource utilization of macro BS is $\lambda(t) = 0.8$. Even for the case that the resource utilization of a macro BS is higher, the proposed heuristic scheme still outperforms the random scheme.

Performance evaluation using intensive system level simulations verified that both proposed heuristic scheme and optimization scheme are efficient in improving the capacity of femtocells. The optimization scheme showed

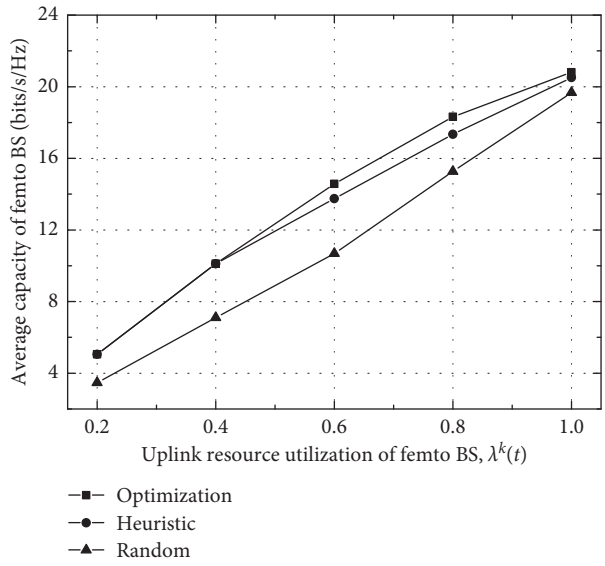


Figure 3: Average capacity of outer femto BS in the case where uplink resource utilization of macro BS $\lambda(t) = 0.6$.

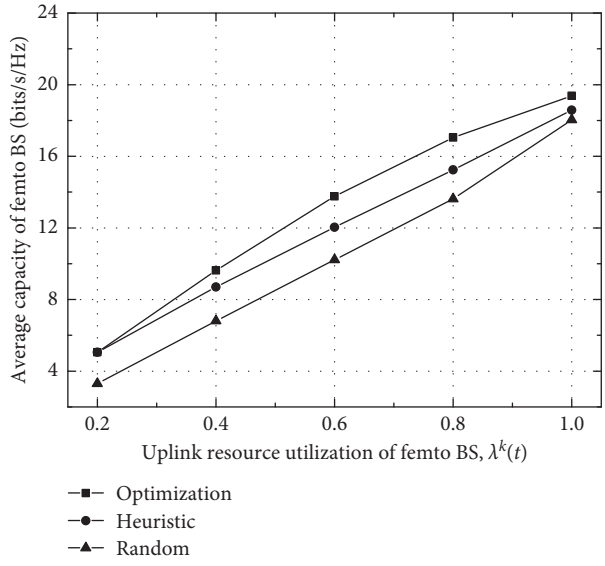


Figure 4: Average capacity of outer femto BS in the case where uplink resource utilization of macro BS $\lambda(t) = 0.8$.

the best performance for all cases, and the performance of the heuristic scheme is comparable to that of the optimization scheme when the uplink resource utilization of the macro BS is lower. The heuristic scheme is more feasible in terms of its complexity for practical implementations because the femtocells do not need the additional procedure regarding the measurement and report of uplink interference from the macro MSs, which enables real-time implementation.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was a part of the project titled Development of Distributed Underwater Monitoring and Control Networks, funded by the Ministry of Oceans and Fisheries, Korea. In part, this work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIT) (No. NRF-2018R1C1B5045013), and this work was supported by the research grant of Chungbuk National University in 2018.

References

[1] V. Chandrasekhar, J. Andrews, and A. Gatherer, "Femtocell networks: a survey," *IEEE Communications Magazine*, vol. 46, no. 9, pp. 59–67, 2008.

[2] S. Pyun and D. Cho, "Resource allocation scheme for minimizing uplink interference in hierarchical cellular networks," in *Proceedings of 2010 IEEE 71st Vehicular Technology Conference*, Taipei, Taiwan, May 2010.

[3] J. Kim and D. Cho, "A joint power and subchannel allocation scheme maximizing system capacity in indoor dense mobile communication systems," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 9, pp. 4340–4353, 2010.

[4] H. Zhang, S. Huang, C. Jiang, K. Long, V. C. M. Leung, and H. V. Poor, "Energy efficient user association and power allocation in millimeter wave based ultra dense networks with energy harvesting base stations," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 9, pp. 1936–1947, 2017.

[5] V. Chandrasekhar and J. Andrews, "Uplink capacity and interference avoidance for two-tier femtocell networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 7, pp. 3498–3509, 2009.

[6] R. S. Karlsson, "Radio resource sharing and capacity of some multiple access methods in hierarchical cell structures," in *Proceedings of IEEE VTS 50th Vehicular Technology Conference*, Amsterdam, Netherlands, September 1999.

[7] H. Jo, C. Mun, J. Moon, and J. Yook, "Interference mitigation using uplink power control for two-tier femtocell networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 4906–4910, 2009.

[8] H. Zhang, H. Liu, J. Cheng, and V. C. M. Leung, "Downlink energy efficiency of power allocation and wireless backhaul bandwidth allocation in heterogeneous small cell networks," *IEEE Transactions on Communications*, vol. 66, no. 4, pp. 1705–1716, 2018.

[9] H. Zhang, Y. Nie, J. Cheng, V. C. M. Leung, and A. Nallanathan, "Sensing time optimization and power control for energy efficient cognitive small cell with imperfect hybrid spectrum sensing," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 730–743, 2017.

[10] S. Mumtaz, J. Rodriguez, and I. Otung, "Smart resource allocation scheme for fair coexistence in LTE-U and WiFi," in *Proceedings of 35th AIAA International Communications Satellite Systems Conference*, , Trieste, Italy, October 2017.

[11] N. Abedini, B. Sadiq, and J. Li, "Uplink scheduling with power control command in an FDD half-duplex network," U.S. Patent, vol. 9, p. 949, 2018.

[12] R. Estrada Pico, *Optimization models for resource management in two-tier cellular networks*, Ph.D. thesis, Ecole de technologie superieure, 2014.

[13] D. Gonzalez, M. Garcia-Lozano, and S. R. Boque, "Intercell interference coordination for control channels in LTE and LTE-A: an optimization scheme based on evolutionary algorithms," *Wireless Personal Communications*, vol. 93, no. 3, pp. 687–708, 2017.

[14] C. Kosta, B. Hunt, A. U. Quddus, and R. Tafazolli, "On interference avoidance through inter-cell interference coordination (ICIC) based on OFDMA mobile systems," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 973–995, 2013.

[15] D. Lee, G. Y. Li, and S. Tang, "Intercell interference coordination for LTE systems," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 9, pp. 4408–4420, 2013.

[16] IEEE P802.16m/D12, *DRAFT Amendment: Air Interface for Broadband Wireless Access Systems-Advanced Air Interface*, IEEE, Piscataway, NJ, USA, 2011.

[17] H. Lee, D. Oh, and Y. Lee, "Mitigation of inter-femtocell interference with adaptive fractional frequency reuse," in *Proceedings of IEEE International Conference on Communications*, Cape Town, South Africa, May 2010.

[18] L. K. Tee, C. Van Rensburg, and J. Tsai, "Uplink power control for an OFDMA mobile cellular system," in *Proceedings of IEEE 66th Vehicular Technology Conference*, Baltimore, MD, USA, October 2007.

[19] T. Nihtila, "Increasing femto cell throughput with HSDPA using higher order modulation," in *Proceedings of IEEE International Networking and Communications Conference*, Lahore, Pakistan, May 2008.

Hindawi
Mobile Information Systems
Volume 2018, Article ID 9876437, 13 pages
https://doi.org/10.1155/2018/9876437

Research Article

CMD: A Multichannel Coordination Scheme for Emergency Message Dissemination in IEEE 1609.4

Odongo Steven Eyobu,[1,2] **Jhihoon Joo**,[1] **and Dong Seog Han**[1]

[1]*School of Electronics Engineering, Kyungpook National University, 80 Daehak-ro, Buk-gu, Daegu 41566, Republic of Korea*
[2]*School of Computing & Informatics Technology, Makerere University, Plot 56, Pool Road, P.O. Box 7062, Kampala, Uganda*

Correspondence should be addressed to Dong Seog Han; dshan@knu.ac.kr

Received 2 August 2018; Accepted 21 October 2018; Published 21 November 2018

Guest Editor: Mohamed Elhoseny

The IEEE 1609.4 legacy standard for multichannel communications in vehicular ad hoc networks (VANETs), specifies that the control channel (CCH) is dedicated to broadcast safety messages, while the service channels (SCHs) are dedicated to transmit infotainment service content. However, the SCHs can be used as an alternative to transmit high priority safety messages in the event that they are invoked during the service channel interval (SCHI). This implies that there is a need to transmit safety messages across multiple available utilized channels to ensure that all vehicles receive the safety message. Transmission across multiple SCHs using the legacy IEEE 1609.4 requires multiple channel switching and therefore introduces further end-to-end delays. Given that safety messaging is a life critical application, it is important that optimal end-to-end delay performance is derived in multichannel VANET scenarios to ensure reliable safety message dissemination. To tackle this challenge, three primary contributions are in this article: first, a cooperative multichannel coordinator (CMD) selection approach based on the least average separation distance (LAD) to the vehicles that expect to tune to other SCHs and operates during the control channel interval (CCHI) is proposed. Second, a model to determine the optimal time intervals in which CMD operates during the CCHI is proposed. Third, a contention back-off mechanism for safety message transmission during the SCHI is proposed. Computer simulations and mathematical analysis show that CMD performs better than the legacy IEEE 1609.4 and a selected state-of-the-art multichannel message dissemination scheme in terms of end-to-end delay and packet reception ratio.

1. Introduction

Nowadays, intelligent transport systems (ITS) are one of the key drivers for the evolution of smart cities. Among the major enabling technologies to realize this evolution is vehicular communications technology (VCT). VCTs should be able to provide services such as safety on the road and in-vehicle on-demand infotainment content. The IEEE 1609.4 standard [1] is the basic technology designed to achieve and enable the implementation of both cooperative safety message dissemination and provision of infotainment services through multichannel communications. Seven 10 MHz channels have been reserved in the 5.9 GHz frequency band [2] for this purpose.

The multichannels defined therein are the control channel (CCH) and six service channels (SCHs), all operating at fixed intervals. The CCH is dedicated to broadcast safety messages while the SCHs are dedicated to transmit infotainment service content. During the CCH interval (CCHI), all vehicles must tune to the CCH unlike during the SCH interval (SCHI). Furthermore, the standard defines the continuous and alternating channel access modes. In the continuous channel access mode, vehicles tune to the CCH until they demand for a service that has been advertised. The alternating channel access mode allows vehicles to always switch between the CCH and their desired advertised SCH after an interval of 50 ms.

When the different vehicles switch to their desired SCHs during the SCHI, it limits the possibility of transmitting safety broadcast messages to all vehicles in the event of an emergency during the SCHI. This is a threat to the reliability of safety message transmission especially because further end-to-end delays are introduced. Therefore, it is necessary to design interchannel communication mechanisms across

service channels which should be able to meet requirements such as minimum end-to-end delay for emergency safety message transmission and delivery.

Various studies [3–11] have proposed approaches on improving end-to-end delay performance for vehicular ad hoc network (VANET) in multichannel conditions. The major considerations in these previous studies include the following: (1) using channel coordination vehicles [6], (2) using road side units (RSUs) as coordinators [10, 11], (3) dynamic variable CCHI and SCHI [5], and (4) time slot utilization based on peer-to-peer negotiation as a multichannel coordination function [4]. A detailed review of studies [3–11] is covered in Section 2. However, for the purpose of this study, the wireless access to vehicular environments—enhanced safety message delivery approach (WSD) [6] is used for comparison with the proposed scheme. During the CCHI, in the WSD approach, each vehicle collects data including the expected SCH that the vehicles in its communication range expect to tune to during the SCHI and computes the delay in each SCH and the number of vehicles expected to tune to a given SCHI. In the event of a high priority message during the SCHI, the invoking vehicle schedules the transmission of the emergency message across all the SCHs based on a schedule determined by the SCH which has the smallest fraction of the delay divided by the number of vehicles in the SCH. This implies that in WSD, the emergency message-invoking vehicle performs the channel coordination function.

In this paper, the information collection routine during the CCHI based on the service advertisements is the same as that of the WSD except that each vehicle only collects the separation distance information between the vehicles in its communication range and the expected SCH they expect to tune to during the SCHI. We consider vehicles expecting to tune to similar specific SCHs as belonging to the same SCH cluster, and for each SCH cluster, a coordinator for each of the other SCH clusters is selected. The cooperative multichannel coordinator (CMD) selection is based on the least average separation distance (LAD). This description of our scheme was first introduced in our paper [12]. Therefore, we extend the concept by (1) detailing the proposed scheme, (2) performing an extensive literature survey of multichannel MAC schemes in VANETs, (3) proposing a Markov chain for the back-off procedure during the SCHI, (4) a mathematical analysis of end-to-end delay which incorporates a proposed model for the optimal slot length when CMD operates during the CCHI, (5) and additional end-to-end delay performance tests in single-hop blind flooding scenarios. The results of the study show that the proposed scheme has a lower end-to-end delay in both non-rebroadcast scenarios and single-hop flooding scenarios when compared to the WSD approach [6]. The original contributions of this article are summarized as follows:

(i) A multichannel coordinator selection approach based on the LAD to vehicles tuned to other SCHs with the purpose of forwarding emergency messages with minimum end-to-end delay

(ii) A Markov chain for the back-off procedure during contention for transmission of safety messages in the SCHI

(iii) A model to determine the optimal slot length in which the proposed CMD operates during the CCHI

(iv) A queueing delay model that depends on the number of vehicles within the carrier sensing range to determine the queue length

(v) A mathematical analysis of the message dissemination end-to-end delay for the proposed CMD scheme and WSD

(vi) A simulation analysis of end-to-end delay while comparing the proposed CMD scheme, WSD, and the legacy IEEE 1609.4

The remainder of this paper is organized as follows. Section 2 discusses the related works. Section 3 describes the proposed CMD system model. Section 4 describes the numerical analysis. Section 5 describes shows the simulation setup and performance analysis. Finally, the conclusion is given in Section 6.

2. Related Work

Various state-of-the-art approaches designed for multichannel VANET scenarios are discussed in this section. The review covers adaptive interval approaches and coordination based approaches used in multichannel VANETs.

Pal et al. [3] proposed to eliminate the fixed CCHI and SCHI intervals by introducing a triggered multichannel medium access control (MAC) scheme where the CCHI is triggered each time there exists an emergency message with the objective of minimizing the end-to-end-delay. Similarly, Chantaraskul et al. [13] and Wang et al. [5] also proposed approaches to dynamically adjust the CCHI based on the channel congestion condition. This approach offers a high trade-off against infotainment content delivery in environments where both safety and content delivery are highly required.

Almohammedi et al. [4] proposed an adaptive multichannel assignment and coordination (AMAC) scheme in VANETs which exploits channel access scheduling and channel switching. The channel access scheduling is done by the RSU based on the traffic conditions to guarantee that all safety messages are disseminated during the CCHI and also achieve higher throughput of the infotainment content. The AMAC scheme also uses a peer-to-peer (PNP) negotiation mechanism between service providers and users for the SCH reservations to adaptively transmit safety messages based on the CCH conditions and the traffic safety state. The PNP negotiation process results into (1) transmission of safety messages over the CCH if the traffic condition is light and (2) transmission over the SCH if the traffic condition is heavy to avoid extended end-to-end delays of safety message delivery. Transmission over the SCH involves negotiating for a time slot during the SCHI. Generally, the PNP negotiation process is an additional process in the synchronization interval (SI) and naturally extends end-to-end delays. Additionally, AMAC uses different adaptive contention windows for safety message and service message transmission in

order to minimize on packet collision in the multichannel environment.

Similarly, Wang et al. [5] proposed a variable CCHI (VCI) multichannel MAC which dynamically adjusts the length ratio between the CCH and the SCH mainly for the transmission of safety messages. In the VCI approach, when wireless service advertisements (WSAs) are transmitted during the CCHI, interested nodes request the service provider to reserve a specified content transmission time interval in the SCHI within which they shall receive content. This reservation approach is quite similar to the PNP time slot negotiated for in [4]. The only difference is that in [5], the time slot is used for transmitting infotainment content while in [4], the time slot is used for transmitting safety messages.

The hidden node problem in multichannel VANETS can be minimized using the request to send (RTS)/clear to send (CTS)/data/acknowledgement (ACK) handshake. However, this causes the exposed node problem that hinders concurrent transmissions especially in dynamic environments like VANETs. In particular, SCH selection in multichannel VANETS can result into an exposed node problem hence hindering concurrent transmissions. Lee et al. [8] proposed a scheme based on piggybacking of selected SCHs in the safety message in multichannel VANETs to minimize the exposed node problem. In this case the piggybacked message acts as a coordination agent so that the exposed vehicles do not select a common SCH.

Yao et al. [9] proposed a flexible multichannel MAC (FM-MAC) protocol which allows safety messages to be broadcasted on the service channel and nonsafety messages to be transmitted on the control channel in a flexible way. The SCHI and CCHI are not adjusted dynamically but instead both are utilized for transmitting safety and nonsafety messages. In FM-MAC, finding the optimal bandwidth resource allocation was key in determining the flexibility of using both the SCHI and CCHI. The RSU in [9] performs the major coordination function by the following: (1) setting up a coordination period for the RSU to broadcast frames to all vehicles in range informing them of a contention period to transmit safety messages, (2) safety message broadcasts and SCH service reservation requests are made by vehicles, (3) the RSU as well broadcasts a scheduling period to all vehicles in its range informing them of the schedule assignments and schedule orders, (4) and finally all nonsafety messages are exchanged based on the SCH schedules and assignments which were broadcasted by the RSU. Zhao et al. [10] proposed the demand-aware MAC (DA-MAC) protocol which follows quite a similar criteria like in [9], though DA-MAC does not consider the coordination frames broadcast by the RSU in FM-MAC.

The multichannel coordination schemes in [9–11] seem attractive, but mainly depend on the RSU. It has been reported that RSUs may sometimes face unavailable grid power connection challenges [14], and hence may require being battery powered. The major issue is ensuring that they are power charged. This limitation is the reason for the advocacy of vehicle-to-vehicle (V2V) target multichannel coordination schemes.

The WSD algorithm proposed by Ghandour et al. [6] targets transmitting event driven high priority messages to all service channels with a minimized delay to its neighbours. During the CCHI, WSD operates at each node by gathering information about its neighbours through hello messages thereby forming a database comprising of the available service channels and available vehicles. In case there exists an emergency message event trigger during the SCHI, the SCH with the least average ratio of the channel average delay and the number of nodes is first tuned to by the source vehicle of the emergency message event trigger for message dissemination. SCH switching continues in the order of the least ratio until all SCHs are exhausted. The major point of interest in the WSD protocol is to disseminate information to its neighbours with minimum delay. Due to the multiple switches to different SCHs by the nearest vehicle that acts as a coordinator, WSD logically poses a large total dissemination delay in order to transmit to all the other service channels. The WSD design is based on the argument that nearer vehicles are a greater point of interest for safety.

The scheduling algorithm for high priority message dissemination (SAEMD) proposed by Joo et al. [15] operates by selecting and switching to a SCH belonging to the nearest vehicle. Similar to WSD in [6], SAEMD uses a data collection routine in the CCHI and uses the separation distance data for deciding on the nearest vehicles hence the next SCH to be tuned to for message transmission. Summarily, WSD [6] and SAEMD [15] were designed to work in multichannel WAVE conditions. However, both WSD and SAEMD provide a minimum end-to-end delay benefit in the SCH which the nearest neighbouring vehicles tunes to first. In the case where most SCHs have vehicles tuned to them, the overall total dissemination delay is expected to be larger due to the need to do multiple switching to the different SCHs. Based on WSD and SAEMD, the total end-to-end delay for emergency message dissemination in multichannel WAVE conditions needs to be improved. In our previous work [12], we presented a cooperative multicoordinator scheme (CMD) for multichannel communication in VANETs to take care of the large total dissemination delay in multiple service channels. The proposed CMD addresses multichannel communications in VANETs and uses acquired knowledge from the CCHI.

Like in Dang et al. [16], the proposed CMD advocates for the utilization of the SCH in case an emergency message is invoked towards the time the SCHI takes over in the SI. Utilization of the both the CCHI and SCHI increases the reliability of safety message broadcasting. In the proposed CMD approach, each vehicle maintains a single radio, and the channel coordinator selection approach is distance based. CMD also makes use of multiple coordinators for each SCH cluster based on the available advertised SCHs hereafter referred to as Y. Table 1 shows the comparisons of different state-of-the-art multichannel access schemes used in VANETs.

3. Cooperative Multichannel Emergency Message Dissemination Protocol (CMD)

CMD operates in vehicular multichannel communications with the goal of achieving a low end-to-end delay in the dissemination of messages throughout the entire set of

Table 1: Comparison of existing multichannel VANET schemes.

Scheme	Utilizes RSU for coordination?	Nodes hosting the coordination function	Switching times per coordinator
Pal et al. [3]	No	1	Y-1
Chantaraskul et al. [13]	No	1	Y-1
VCI: [5]	No	1	Y-1
AMAC: [4]	Yes	1	Y-1
Lee et al. [8]	No	1	Y-1
FM-MAC: [9]	Yes	1	Y-1
DA-MAC: [10]	Yes	1	Y-1
Li et al. [11]	Yes	1	Y-1
WSD: [6]	No	1	Y-1
SAEMD: [15]	No	1	Y-1
Proposed CMD	No	Y-1	1

Switching times refers to the number of times a coordinator node must switch to different SCHs to transmit a single emergency message until all SCHs receive the message.

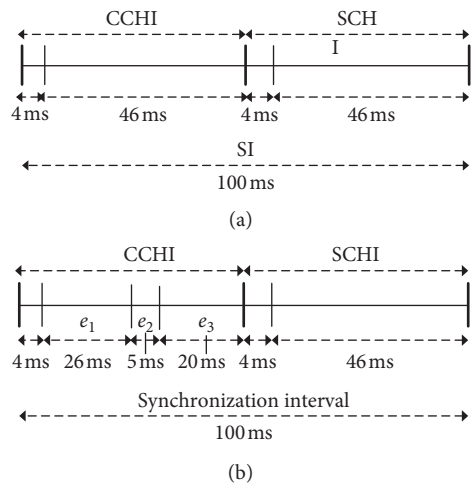


Figure 1: (a) Standard channel access in IEEE 1609.4. (b) The SI utilization based on CMD.

vehicles tuned to different SCHs without changing much on the IEEE 1609.4 standard. Like some of the presented multichannel approaches in [6] and [15], the CMD protocol follows the channel coordination principle where the coordinator vehicles are selected using the distance to vehicles tuned to other SCHs. A channel coordinator selection algorithm is presented later in this section.

Figure 1(a) shows the standard IEEE 1609.4 channel access, and Figure 1(b) shows the synchronization interval (SI) utilization based on the proposed CMD which can be described in the following steps:

(1) At the start of the CCHI and after the guard interval, 26 ms are used for broadcasting basic safety messages (BSMs) and advertising available services by service provider nodes. The BSMs broadcasted at this stage includes the vehicle location information and the SCH which a node will use to in order to receive nonsafety data.

(2) In the next 5 ms, using the location information received and piggybacked SCHs from the other nodes, each node calculates the average distance it has from nodes which intend to use each of the different SCHs, respectively.

(3) The calculated average distance to vehicles intending to tune to each SCH is appended to the BSM and broadcasted by each vehicle. In the last 20 ms of the CCHI, the vehicles then broadcast their BSMs. On receipt of each BSM, each vehicle compares its own average separation distances with that in the received BSM if the SCH in the BSM is the same. A node autonomously qualifies itself to be the best fit coordinator if it has the LAD compared to all the other nodes intending to use the same SCH.

(4) During the SCHI, in the event of an emergency event message transmission, the best fit vehicles with the LAD to other SCHs forward the emergency message to the vehicles which tuned to the other SCH by switching to the target SCH.

3.1. Channel Coordinator Selection. In this subsection, the CMD protocol is described in detail and illustrated by Figure 2. Figure 2 shows three channels SCH1, SCH2, and SCH3 which were advertised during the CCHI and logically clustered to represent the vehicles tuned to the different SCHs during the SCHI. The vehicles selected the advertised SCHs in the CCHI in a random manner. Each vehicle while in the CCHI received and selected an SCH from the WAVE service advertisements (WSAs) and also received and transmitted location information together with their selected SCH. With the received location information and SCH at every instance, each receiving vehicle computes the separation distances in relation to each SCH with the objective of finding the least separation distance to vehicles expecting to tune to a specific SCH.

Considering each SCH as a cluster, the channel coordinator vehicles in each cluster are such that for all vehicles in a given cluster, they have LAD of the connectivity to nodes in another SCH compared to the other vehicles it will share with the same SCH. If Y SCHs were advertised, then there should exist $Y-1$ SCH coordinators in each cluster. Table 2 describes the notations used in formulating the channel coordinator selection approach. The channel coordinator selection model can be formulated as

$$\exists C_{k\_z} \in \text{SCH}k \text{ s.t.} D_{c\_z} \le d_{i\_z} \quad \forall d_{i\_z}, \quad i = 1, 2, \ldots, m, \quad k = 1, 2, 3, \ldots, 6, \tag{1}$$

where

$$d_{i\_z} = \frac{d_1 + d_2 + \cdots + d_m}{m} \quad \text{for} \quad z = 1, 2, 3, \ldots, 6. \tag{2}$$

Each vehicle keeps the broadcasted SCHz and its associated d_{i_z} in its coordination fitness information base (CFIB) as seen in Table 3. After the d_{i_z} calculation stage by each receiving vehicle, each vehicle again broadcasts its local d_{i_z} and is received through the periodic broadcast BSM. Each incoming d_{i_z}'s is compared with the local d_{i_z}'s as long as the SCHz is the same. The comparison is such that

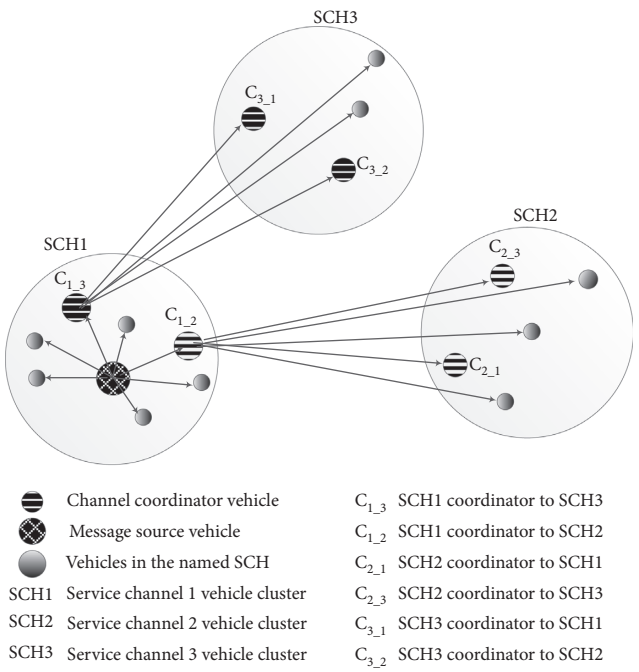


Figure 2: A logical view of the CMD structure with the emergency message generated from SCH1 and broadcasted to its members and then relayed by the channel coordinators to SCH3 and SCH2.

Table 2: Notations used in channel coordinator selection.

Acronym	Description
k	An advertised SCH which a vehicle intends to switch to during the SCHI
z	Any other advertised SCH apart from the one which a given vehicle intends to switch to during the SCHI
c	An SCH coordinator vehicle
c_{k_z}	The channel coordinator for forwarding messages from SCHk to SCHz
Y	The number of advertised SCHs to provide nonsafety services
m	The number of vehicles expecting to switch to SCHz
d_i	The V2V separation distance. $i = 1, \ldots, m$
d_{i_z}	The average d_i for a given vehicle considering the vehicles expecting to switch to SCHz
D_{c_z}	The LAD for the coordinator vehicle in SCHk to SCHz
$f_{\text{SCH}z}$	The coordination fitness value for a given vehicle considering the d_{i_z} to SCHz

Table 3: Coordination fitness information base.

Gossiped SCHz	Average d_{i_z}	$f_{\text{SCH}z}$
SCH 1	d_{i_1}	≥ 1
SCH 2	d_{i_2}	≥ 1
SCH 3	d_{i_3}	≥ 1
SCH 4	d_{i_4}	≥ 1
SCH 5	d_{i_5}	≥ 1
SCH 6	d_{i_6}	≥ 1

when d_{i_z} is the least among the incoming d_{i_z}'s for the common SCHz, then the coordination fitness (CF) is 1. Implying that the vehicle i has the least average distance to SCHz and hence is the service coordinator of its SCH to SCHz. Generally, the value of CF is determined based on the order of greatness of d_{i_z}. That is, the least d_{i_z} has CF equals to 1 and the greatest d_{i_z} has CF equals to m. For clarity, the CF range is $i = 1, 2, 3, \ldots, m$. The least d_{i_z} which represents the coordinators' average distance is then represented as D_{c_z} for purposes of clarity as seen in Equation (1).

Again, as seen in Table 3, the CF value in SCHk is represented as $f_{\text{SCH}z}$. The general representation in Figure 2 shows the vehicle coordinators $C_{k\_1}, C_{k\_2}, C_{k\_3}$ which have the least CF values to the advertised SCHs. It should however be noted that although C_{2_3} and C_{3_2} are represented a SCH coordinators in Figure 2, only C_{1_3} and C_{1_2} are functionally operational as channel coordinators because the emergency message is triggered in SH1. Algorithm 1 elaborates on the CMD channel coordinator selection procedure.

3.2. Challenges in the Proposed CMD. In the CCHI, while transmitting BSMs containing the average separation distance to other vehicles, conditions such as the hidden node problem and shadowing may hinder the BSM delivery to some vehicles. In such a case, more than one vehicle may assume the position of the channel coordinator to a given SCH cluster. During the SCHI, it is also possible that a channel coordinator vehicle may not receive an emergency message from the affected source vehicle due to the hidden node problem.

This is a prominent problem in single-hop broadcast scenarios. To alleviate this reachability problem, the single-hop blind flooding based approach of broadcasting was implemented, and simulation results are shown later in Section 5.4 to describe its impact on delay in each WAVE channel. In single-hop blind flooding, when vehicles receive a message, they rebroadcast it only once. That is, the vehicles receiving the rebroadcasted message do not broadcast the retransmitted message. A comparison of the proposed CMD with WSD is also done for the single-hop flooding scenario.

Again, by applying CMD, it is possible that only one in a given SCH may qualify to be the channel coordinator to all other SCHs by having the LAD to all advertised SCHs. This scenario exists when one node is isolated from its SCH members yet near to all the other SCH cluster members. Another issue about CMD is that when a cluster has less than $Y - 1$ members, then some members will act as coordinators for more than one SCH. These two mentioned scenarios would cause an increase in the total dissemination delay because such coordinators will have to switch between multiple channels.

3.3. Proposed Back-Off Model for Emergency Message Transmission during the SCHI. Figure 3(a) represents the standard back-off process to be adopted in the CCHI and for nonsafety data transmission in the SCHI. The Markov chain proposed and presented in Figure 3(b) operates in the

(1) **while** in CCHI vehicles receive WSA's and broadcast their location information
(2) Select an SCH to be tuned to
(3) Append selected SCH and location information to all BSM's and broadcast
(4) **while** periodic safety messages are received
(4a) **for** each vehicle
(4b) **for** each SCH advertised
(4c) Compute d_{i_z}
(4d) Append d_{i_z} to the BSM and then broadcast
end for
(4e) **if** (BSM is received) **then**
for each similar SCHz
(4f) **if** (all the d_{i_z} values are greater than the local average d_{i_z}) **then**
(4g) Vehicle is the channel coordinator C_{k_z}
(4h) **else**
(4i) Vehicle is just a member of its selected SCHk cluster.
(4j) **end if**
end for
(4k) **end if**
(4l) **end for**
(4m) **end while**
(5) **end while**

Algorithm 1: Channel coordinator selection algorithm.

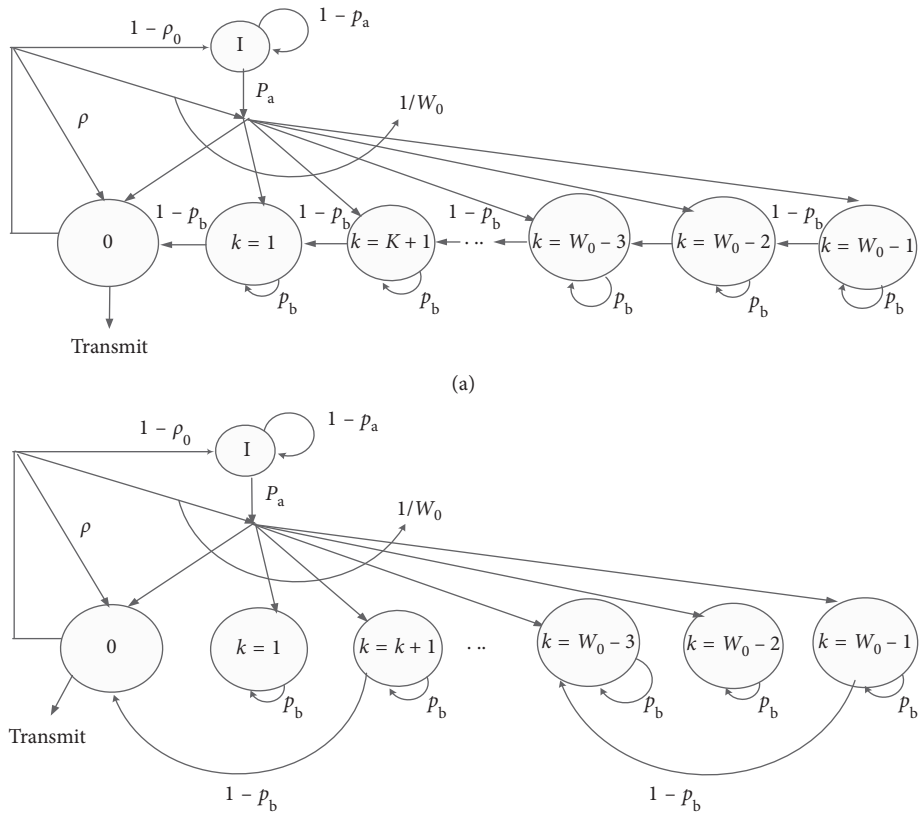


Figure 3: One-dimensional Markov chain model for a back-off instance. (a) Standard back-off process to be adopted in the CCHI and for nonsafety data transmission in the SCHI. (b) Proposed back-off process for emergency safety message transmission during the SCHI.

SCHI showing the back-off process when an emergency message is invoked. Safety emergency messages are considered high priority messages during the SCHI; therefore, the model design is tailored to minimize their contention delay. In the standard back-off criteria, waiting state transitions are marked by uniformly reducing contention window sizes.

In the proposed criteria seen in Figure 3(b) the same phenomenon is followed but the size of the reducing contention window (RCW) is two times the size of the RCW compared to when transmitting WSAs, safety messages in the CCHI, and data services during the SCHI.

Let $s_i(t)$ and $b_i(t)$ represent the back-off stage and the back-off counter, respectively at time t. Hence, the state of the Markov chain can be expressed as a two-tuple $\{s_i(t), b_i(t)\}$, and the back-off state of the high priority emergency messages can be simplified as a one-tuple $\{b_i(t)\}$ for $s_0(t) \equiv 0$. Table 4 defines all the probabilities shown in the Markov chains in Figures 3(a) and 3(b). Each of the one-time transition probabilities in Figure 3(b) is described below:

(i) The idle state $\{I\} \longrightarrow$ the back-off state $\{0\}$: node transmits a packet if the channel is sensed as idle: $P\{0|I\} = p_a$

(ii) The idle state $\{I\} \longrightarrow$ the state back-off $\{k\}$: this occurs if a new packet arrives in the queue: $P\{k|I\} = p_a/W_i, k \in (0, W_0 - 1)$

(iii) The back-off state $\{k\} \longrightarrow$ the state back-off $\{k\}$: occurs if the channel is sensed to be busy and in this case the back-off counter freezes: $P\{k|k\} = p_b, k \in (1, W_0 - 1)$

(iv) The back-off state $\{k+2\} \longrightarrow$ the state back-off $\{k\}$: if the channel is sensed to be idle, the back-off counter decrements by two steps: $P\{k|k+2\} = 1 - p_b, k \in (0, W_0 - 2)$

(v) The back-off state $\{0\} \longrightarrow$ the idle state $\{I\}$: node returns to idle state if it has no packet to send: $1 - \rho$.

(vi) The back-off state $\{0\} \longrightarrow$ the idle state $\{k\}$: nodes start back-off procedure if at least one packet is in the queue: $P\{k|0\} = \rho_0/W_0, k \in (0, W_0 - 1)$

In summary, the one-step transition probabilities are as follows:

$$\begin{cases} P\{0 \mid I\} = p_a, \\ P\{k \mid I\} = p_a/W_i, \quad k \in (0, W_0 - 1), \\ P\{k \mid k\} = p_b, \quad k \in (1, W_0 - 1), \\ P\{k \mid k+2\} = 1 - p_b, \quad k \in (0, W_0 - 2), \\ P\{I \mid 0\} = 1 - \rho_0, \\ P\{k \mid 0\} = \rho_0/W_0, \quad k \in (0, W_0 - 1). \end{cases} \tag{3}$$

The stationary distribution of the Markov chain is defined as

$$b_0 = \lim_{t \longrightarrow \infty} P\{b(t) = k\}, \quad k \in (0, W_0 - 1). \tag{4}$$

Table 4: Notations.

Acronym	Description
λ	The packet arrival rate
μ	Average service rate of the queue in packets per second
ρ	The probability that at least one packet is in the queue = λ/μ
p_b	Is the back-off blocking probability
p_a	The packet arrival probability = $1 - e^{-\lambda\sigma}$
W_0	Contention window size for back-off
k	Current window size state as an effect of exponential back-off
I	Idle state
β	Traffic density
d_0	The reference distance used in calculating the received signal strength at a particular distance
$P_r(.)$	The received signal strength at specified distance
d_c	The critical distance that refers to the distance where the first Fresnel zone touches the ground and is also referred to as the Fresnel distance
γ_1	Path loss exponent
γ_2	Path loss exponent
h_T	Transmitter height
h_R	Receiver height
ψ	Electromagnetic wavelength fixed at 5.9 GHz
B	The number of vehicles in carrier sensing range
$X_{\sigma 1}$	The zero mean, normally distributed random variables with standard deviation $\sigma 1$
$X_{\sigma 2}$	The zero mean, normally distributed random variables with standard deviation $\sigma 2$
L_{CS}	The carrier sensing range defined as the average distance for a node to detect the other nodes transmissions
c_{th}	The carrier sensing threshold which indicates the receive sensitivity of the radio and is a constant and radio dependent

Given the one-step probabilities, the stationary probabilities can be expressed as

$$b_k = \frac{(W_0 - k)}{W_0(1 - p_b)} b_0,$$
$$b_I = \frac{(1 - \rho)}{p_a} b_0. \tag{5}$$

The sum of the stationary probabilities for the states should be equal to one, therefore,

$$\frac{(W_0 - 1)}{W_0(1 - p_b)} b_0 + \frac{(1 - \rho)}{p_a} b_0 = 1,$$
$$b_0 = \left[\frac{(W_0 + 1)}{2(1 - p_b)} + \frac{1 - \rho}{p_a} \right]. \tag{6}$$

Since transmission occurs when the back-off counter value $k = 0$, the transmission probability τ can be defined as

$$\tau = b_0 = \left[\frac{(W_0+1)}{2(1-p_b)} + \frac{1-\rho}{p_a}\right], \quad (7)$$

τ is very important as it is later used in the end-to-end delay analysis seen in the next section.

4. End-to-End Delay Analysis

The key performance indicator in this study is end-to-end delay. The goal of this section is to numerically derive the end-to-end delay while considering the mechanism of the proposed CMD scheme. Generally, the performance of the proposed CMD depends on the communication performance during the 26 ms of transmitting the location information and then the 20 ms of sharing the average separation distances to determine the SCH coordinators. The two decision time slots (26 ms and 20 ms) in this article from now onwards shall be referred to as e_1 and e_3 respectively as shown in Figure 1(b).

Most importantly, all or most of the vehicles should transmit their information within e_1 and e_3 for the channel coordinator selection to be efficient. Therefore, one eminent optimization parameter in this problem is the length of e_1 and e_3 which we believe should depend on the length of an arbitrary time slot T_{slot} existing during the interval e_1 and e_3. And since T_{slot} is one parameter that determines the end-to-end delay of a transmission, and we start by defining the end-to-end delay $E[d]$ model as follows:

$$E[d] = E[q] + E[c] + E[t], \quad (8)$$

where $E[q]$, $E[c]$, and $E[t]$ represent the average queueing delay, average contention delay, and average transmission delay, respectively.

4.1. Contention Delay Model. The average contention $E[c]$ is defined as

$$E[c] = E[CW] = \left(\frac{CW_{min}-1}{2}\right)T_{slot}, \quad (9)$$

where $E[CW]$ is the average contention window size. The size of T_{slot} is relevant for the derivation of the optimal period for e_1 and e_3 for the proposed CMD. Finding T_{slot} requires that (1) we define the stationary probability that a node transmits a BSM in the arbitrary time slot T_{slot} and (2) the time it takes to yield a successful transmission $T_{success}$, collision time T_{coll}, and the idle time σ.

By using the transmission probability τ, the following probabilities can be found:

$$\begin{aligned} p_{idle} &= (1-\tau)^N, \\ p_{busy} &= 1 - p_{idle}, \\ p_{success} &= N\tau(1-\tau)^{N-1}, \\ p_{coll} &= 1 - p_{idle} - p_{success}, \end{aligned} \quad (10)$$

where p_{idle} is the probability that a channel is in an idle state and not being utilized, p_{busy} is the probability that a transmission is occupying the channel, $p_{success}$ is the probability of having a successful transmission, and p_{coll} is the probability of having a collision in the channel.

The transmission time slot duration T_{slot} is defined as

$$T_{slot} = (1-p_{busy})\sigma + T_{success}\cdot p_{success} + T_{coll}\cdot p_{coll}, \quad (11)$$

where σ is the duration of an empty slot. $T_{success}$ is the time required for a successful transmission, and T_{coll} is the average time of a collision event:

$$\begin{aligned} T_{success} &= \text{DIFS} + \sigma + E[t], \\ T_{coll} &= \text{EIFS} + \sigma + E[t]. \end{aligned} \quad (12)$$

The average transmission delay can be expressed as $E[t] = S/R$, with S representing the message size and R representing the data rate, respectively. DIFS and EIFS are the distributed coordination function interframe space time and extended interframe space time, respectively.

4.2. Optimal Slot Period Allocation Model. At this stage, since T_{slot} has been mathematically defined by Equation (11), the task is now to define the optimal period of that each of e_1 and e_3 slot shall take. In other words, we need to find how many T_{slot}'s should exist in either the 1st or 2nd time slot to enable sufficient coordination selection functionality.

The objective to achieve during e_1 and e_3 is to have most or all of the vehicles to transmit their location, desired SCH and LAD information. In this article, we consider that e_1 and e_3 period should just be long enough to allow all the vehicles denoted by B within the carrier sensing range to transmit their information. The duration V representing either e_1 or e_3 can therefore be defined as

$$V = B \times T_{slot}. \quad (13)$$

In this article, we define the number of vehicles B in carrier sensing range based on [9] as

$$B = 2\beta L_{cs}. \quad (14)$$

L_{cs} is given by

$$L_{cs} = \begin{cases} E\left[d_0 10^{(p_r(d_0) - c_{th} + X_{\sigma 1})/10\gamma_1}\right], & d_0 \le L_{cs} \le d_c, \\ E\left[d_0 10^{(p_r(d_0) - 10\gamma_1 \log_{10}(d_c/d_0) - c_{th} + X_{\sigma 2})/10\gamma_1}\right], & L_{cs} > d_c, \end{cases} \quad (15)$$

d_c can be calculated as $d_c = 4h_T h_R/\psi$.

4.3. Queueing Delay Model. In this paper, the queueing delay $E[q]$ is formulated considering that a VANET communication system is best modeled as an M/M/1/B queueing system [17]. In this case, the arrivals are considered to be distributed exponentially through a Poisson process, the service times are exponentially distributed and independent of each other, and a single communication channel acting as a server has a finite queue length B. Where we define B in this article as the number of vehicles within the carrier sensing range. Based on Equation (14), B can be calculated. The expected queue length can therefore be calculated as

$$E[b] = \frac{\rho}{1-\rho^{B+1}} \cdot \left(\frac{1-\rho^{B}}{1-\rho} - B\rho^{B} \right). \quad (16)$$

Using Little's law, the queueing delay can be represented as

$$Q_d = \frac{E[b]}{\lambda(1-P_B)}, \quad (17)$$

where P_B is the probability that the queue is full and $\lambda(1-P_B)$ represents the effective arrival rate which the packets are put into the queue. When $\rho = (\lambda/\mu) \neq 1$, the queueing delay is defined as

$$E[q] = Q_d = \frac{E[b]}{\lambda\left(1-\left(1-\rho/1-\rho^{B+1}\right)\cdot\rho^{B}\right)} = \frac{1}{\mu-\lambda} - \frac{1}{\mu}\cdot\frac{B\rho^{B}}{1-\rho^{B}}, \quad (18)$$

when

$$\rho = 1,$$

$$Q_d = \frac{E[b]}{\lambda\{1-[1/(B+1)]\}} = \frac{(B+1)}{2\lambda} = \frac{(B+1)}{2\mu}. \quad (19)$$

At this stage, all the parameters for numerically finding $E[d]$ using Equation (8) can be computed.

5. Simulation

5.1. Mobility Model and Network Simulator. The Manhattan model is used to emulate the movement pattern of vehicle nodes on streets defined by a map. The map is composed of a number of horizontal and vertical streets. Each street has one lane. The mobile vehicle node moves along the horizontal and vertical grids on the map. At an intersection of horizontal and vertical streets, the mobile node can turn left, right, or goes straight. This choice is probabilistic. The vehicle turn probability is set to 0.5. We consider a two-dimensional 1,500 m by 1,500 m fully connected road network in a Manhattan grid with vehicles moving at a mean speed of 40 km/h. The grid offers a total of 6 km for vehicular motion for the single-lane scenario. Our mobility trace for the vehicles is generated using BonnMotion-2.1.3.

To analyze the performance of CMD, we simulated its system dynamics with the NS-3 simulator, version ns-3-dev. Table 5 summarizes the general simulation parameters, and Table 6 defines the simulation performance metrics.

5.2. End-to-End Delay. In a typical VANET scenario, not all vehicles may demand for the advertised infotainment services. This means that not all SCHs will be utilized during the SCHI. In Figure 4, the total end-to-end dissemination delay is shown for WSD, IEEE 1609.4, and the proposed CMD. Only 5 SCHs were advertised during the CCHI.

Observations show that the proposed CMD maintains lower total end-to-end delays compared to WSD and the legacy IEEE 1609.4 when more than two SCHs are utilized during the SCHI. This observation is true for both the analytical and simulation results. In the legacy IEEE 1609.4, a vehicle with an emergency message during the SCHI must wait for the CCHI in order to transmit an emergency message. This is the major cause for the much end-to-end delay exhibited by the legacy IEEE 1609.4 system. The better

Table 5: Simulation parameters.

Description	Value
Message payload size S	200 bytes
Fading model	Nakagami
Packet interval	100 ms
Data rate R	3 Mbps
Content window size: Min, max	15, 256
Slot time σ	16 μs
Arbitrary interframe space number (AIFSN)	2
Short interframe space (SIFS) time	32 μs
Antenna height	1.5 m
Frequency	5.9 GHz
Transmitter and receiver gain	3 dB
Number of vehicles	50
Vehicle speed	40 m/s
Vehicle mobility model	Manhattan-grid highway

Table 6: Simulation performance metrics.

Metric	Description
End-to-end delay	The safety message dissemination single-hop delay
Packet reception ratio (PRR)	The percentage of nodes that successfully receive a packet from a tagged node given that all the receivers are within the transmission range of the sender at the moment that the packet is sent out [18]
Packet transmission ratio (PTR)	The percentage of nodes that successfully transmit a packet given the prevailing contention for channel access

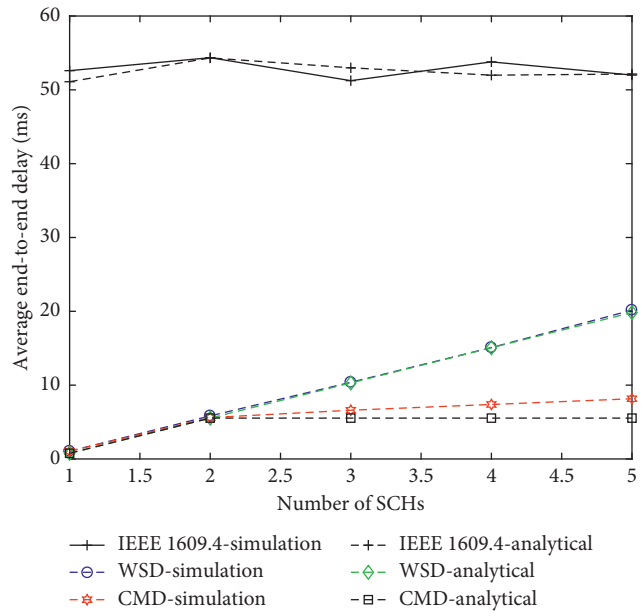


Figure 4: Analytical and simulation results of average end-to-end delay versus number of channels.

performance realized by the CMD is the effect of using multiple coordinators whereby each coordinator switches to a specific SCH in order to relay a BSM during the SCHI. In WSD, only one channel coordinator is used, hence the need for multiple channel switching in order to relay the BSM to all the SCHs. Therefore, there is an additional delay introduced by the multiple switching and the transmission delays.

The slight differences seen in the theoretical and simulation results are a result of the system dynamics used in generating the results both in theory and in the simulation. In WSD, the theoretical results are generated based on the derivation of a single channel end-to-end delay $E[d]$. We then use the number of SCHs Y as a factor to fix the multichannel condition to find the total message dissemination end-to-end delay T_d as follows:

$$T_d = \begin{cases} E[d], & Y = 1, \\ YE[d], & Y > 1. \end{cases} \quad (20)$$

In the proposed CMD, the theoretical T_d is defined by

$$T_d = \begin{cases} E[d], & Y = 1, \\ 2E[d], & Y > 1. \end{cases} \quad (21)$$

In the simulation, the frequency of each of the SCHs defined by the WAVE standard is different. This has an impact on the end-to-end delay results thus causing the slight differences observed between the theoretical and simulation results. It should be noted that the final T_d represented in the results of Figures 4–6 includes the switching delay where multiple channels are involved. Theoretically, the switching delay was arbitrarily fixed at 2 ms.

5.3. PRR and PTR. The proposed CMD first operates during the CCHI within the time durations, e_1, e_2, and e_3. During the time durations e_1 and e_3, it is important that all or most vehicles transmit and receive the BSMs in order to enable efficient channel coordinator selection. Therefore, Figure 7 is shown to provide an understanding of the PRR and the PTR during the time intervals e_1 and e_3.

It is observed in Figure 7 that as the slot duration of e_1 or e_3 increases, the PRR and PTR also increases. Generally, an increase in the slot duration gives room for more contending nodes to transmit as the available transmission time slots σ would also increase.

Figure 8 represents the PRR and PTR realized when the proposed optimal e_1 model is used. The optimal length in time for e_1 is 8.38 ms given the simulation scenario and settings seen in Table 7. The parameter settings seen in Table 6 are based on realistic channel measurements which were attained in [19].

The key observation in Figures 7 and 8 is that e_1 values greater than 8.38 ms result into relatively the same PRR and PTR values with insignificant differences. This therefore means that lengthening e_1 or e_3 beyond 8.38 ms would simply be a waste in the CCHI.

Figure 5 represents the PRR attained against the total end-to-end delay achieved when transmitting a BSM over single and multiple SCHs. The result shows that the

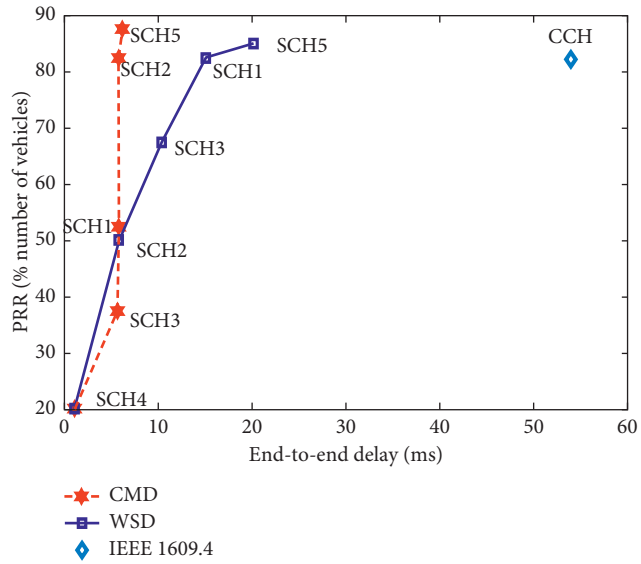


Figure 5: PRR versus end-to-end delay: understanding the BSM proliferation rate across various channels.

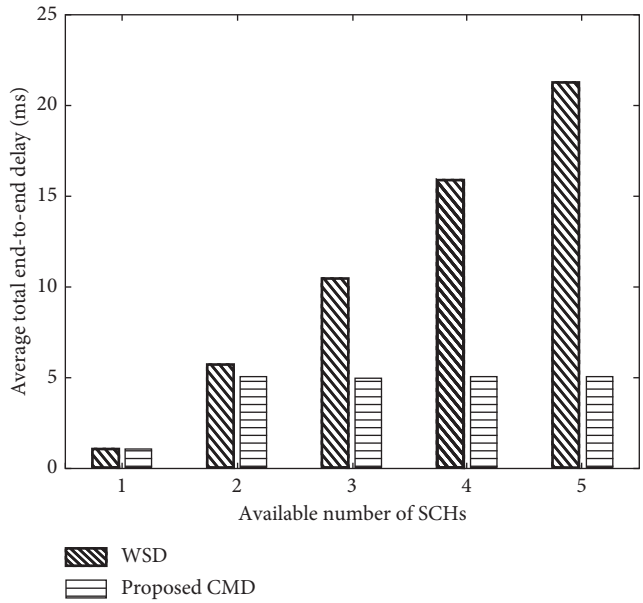


Figure 6: Average total dissemination delay in the single-hop flooding scenario given varying numbers of available SCHs.

proposed CMD offers a greater PRR within a shorter end-to-end delay compared to the WSD and IEEE 1609.4 legacy system especially when considering total coverage of all SCHs with the BSM. The order of the SCH switching represented in Figure 5 for each approach depends on the channel switching dynamics of each.

At about 6 ms, CMD covered slightly over 50% of the vehicles and served 3 SCHs while WSD served lesser. The good performance exhibited by CMD is based on the multicoordinator functionality in a scenario where multiple services are demanded and offered by different SCHs. It is important to note again that the IEEE 1609.4 would wait for

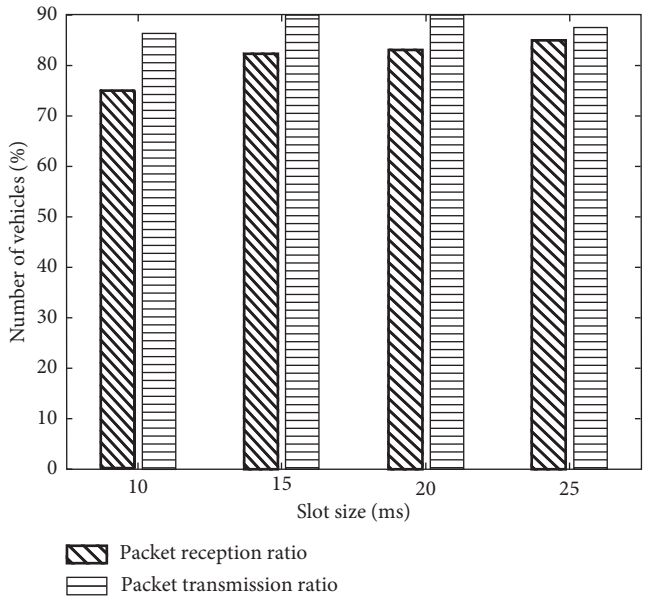


Figure 7: PRR and PTR simulation results for various sizes of e_1.

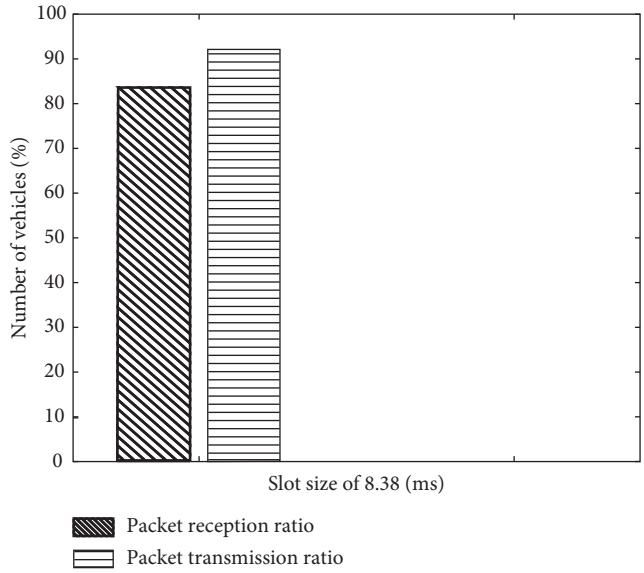


Figure 8: PRR and PTR simulation results based on the derived optimal e_1 interval.

Table 7: Parameter settings for optimal e_1 determination.

Description	Value
d_0	10 m
$P_r(d_0)$	−60 dB
c_{th}	−85 dB
$X_{\sigma 1}$	5.6 dBm
γ_1	1.9
β	25 vehicles/km

the CCHI to transmit BSMs in case of an emergency during the SCHI. It is for this reason that the end-to-end delay for the legacy system is not better than CMD and WSD.

5.4. Improving Reachability for Reliability by Single-Hop Blind Flooding. In order to provide insights on how to alleviate the hidden node problem which can be a hindrance to the effectiveness of the proposed approach during the channel coordinator selection process, we have implemented the single-hop bind flooding approach well knowing that blind flooding approaches introduce the broadcast storm problem [20] which may affect the end-to-end delay.

The purpose of experimenting the single-hop blind flooding (SHBF) is to provide an understanding that even though using SHBF introduces further end-to-end delays, it can be used as a factor in further determining the optimal size of e_1 and e_3 with the benefit of having a higher reachability during e_1 and e_3.

However, in this study, we have not divulged into further formulating another model for determining the optimal size of e_1 and e_2 based on the SHBF end-to-end delay results. We only present SHBF-based results.

Figure 9 shows the cumulative distribution function of the reachability in both flooding and no flooding conditions in the CCHI given a period of 8 ms. The results captured in Figure 9 are for the first SI in our simulation experiment particularly to understand the influence of the number of vehicles in the simulation playground especially given the fact that the vehicle node generation in the simulation is based on a Poisson process.

Four sections of reachability for analysis can be observed in Figure 9. These are between 0 and 10%, between 10% and 38%, between 38% and 68%, and >68%.

The reachability range between 0% and 10% is realized during the starting period of the SI when few vehicle nodes have been ushered into the simulation environment based on a Poisson process. It can be observed that the no-flooding scenario offers a better reachability compared to the SHBF scenario. This is because at the start, there are few vehicles which are all able to be reached and therefore, introducing the SHBF simply causes unnecessary contention.

As the number of vehicles increases in the simulation environment, the sparsity of the vehicles is larger given the vehicle mobility. This sparsity leads to reduced reachability. This can be observed between 10% and 38% where the SHBF scenario offers a better reachability compared to the no-flooding scenario.

The number of vehicles in the simulation environment increases to a point whereby there is a level of stability in the reachability which can be observed between 38% and 68%. This stability scenario is true for both the SHBF and the nonflooding scenario. This means that SHBF has no effect in the CMD process in dense vehicular scenarios.

After 68% reachability is achieved, using the SHBF scenario does not offer better reachability results because of the broadcast storm. At this moment, all vehicles are in the playground of the simulation environment.

We can generally affirm from the observations that the SHBF is indeed suitable to improve on reachability in sparsely dense vehicular scenarios as seen in the region between 10% and 38%. Therefore, the SHBF is useful in the CMD process in sparsely dense vehicular scenarios.

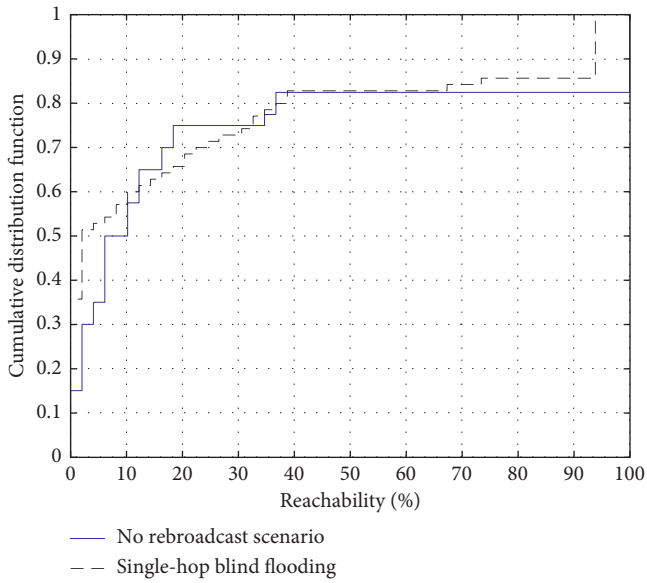


Figure 9: Cumulative distribution function of the percentage number of vehicles receiving message transmission during the CCHI.

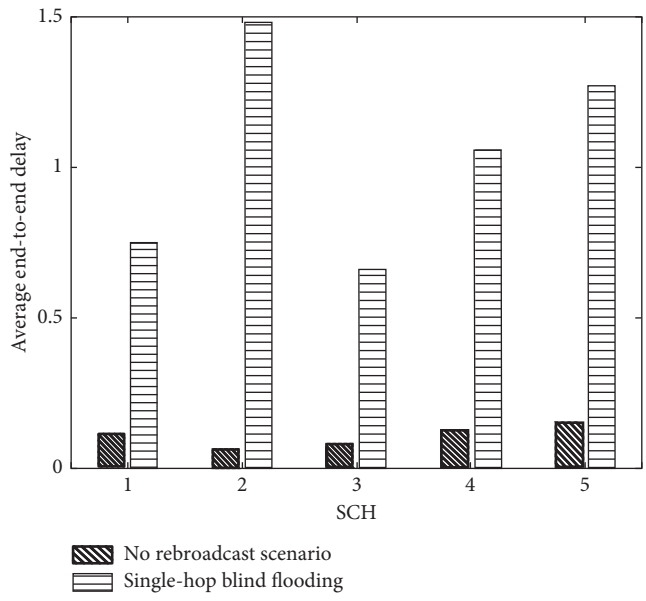


Figure 10: Average dissemination delay in each channel while comparing the blind flooding scenario with the non-rebroadcast scenario at each SCH.

To investigate the effect of flooding on delay, the single-hop blind flooding was implemented in five WAVE SCHs with the objective that during the SCHI, there should be a higher guarantee of emergency message delivery to the channel coordinator once invoked by any vehicle.

By observing Figure 10, it is clear that the single-hop blind forwarding introduces a further delay in the message dissemination time compared to when no blind flooding is applied.

Observations in Figure 6 also indicate that as a result of single-hop blind flooding, the average total dissemination end-to-end delay over multiple channels will also increase compared to what was earlier realized in Figure 5 when no flooding was applied. However, it is worth noting that in scenarios of no flooding and single-hop blind flooding, CMD still exhibits a delay lesser than WSD which is desirable for our design goal.

The negative impact of single-hop blind flooding observed in Figures 10 and 6 imply that a good minimum delay flooding mechanism once utilized would further improve the performance of our proposed CMD protocol in the process of disseminating BSMs.

6. Conclusion

In this paper, we proposed a cooperative multichannel message dissemination scheme called CMD for safety message dissemination in the IEEE 1609.4 standard with the goal of improving on the reliability of safety messaging in multichannel scenarios. In order to achieve this, a cooperative SCH coordinator selection approach was developed. The SCH coordinator selection is based on the vehicle which has the LAD to vehicles that expect to tune to other SCHs and operate during the CCHI.

In order to improve on the efficiency of the channel coordinator selection process during the CCHI, a model to determine the optimal slot duration was developed. A channel contention back-off Markov model was developed to operate during the SCHI in order to improve on the transmission of high priority safety messages in the event that they are invoked. Additionally, a queueing delay model that depends on the number of vehicles within the carrier sensing range was proposed and developed to determine the queue length.

Through mathematical and simulation analysis, the proposed CMD achieves lower end-to-end delay and PRR compared to the legacy IEEE 1609.4 system and WSD, which is one of the state-of-the-art multichannel schemes for WAVE.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was partially supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2016R1D1A3B03934420) and the Korea Institute for Advancement of Technology (KIAT) grant funded by the Korean Government (MOTIE) (no. P0000535, multichannel telecommunications control unit and associated software).

References

[1] IEEE, "IEEE standard for wireless access in vehicular environments (WAVE)-multi-channel operation," IEEE 1609.4-2010, 2010.

[2] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[3] R. Pal, A. Prakash, and R. Tripathi, "Triggered CCHI multichannel MAC protocol for vehicular ad hoc networks," *Vehicular Communications*, vol. 12, pp. 14–22, 2018.

[4] A. A. Almohammedi, N. K. Noordin, A. Sali, F. Hashim, and M. Balfaqih, "An adaptive Multi-Channel assignment and coordination scheme for IEEE 802.11 P/1609.4 in vehicular Ad-Hoc networks," *IEEE Access*, vol. 6, pp. 2781–2802, 2018.

[5] Q. Wang, S. Leng, H. Fu, and Y. Zhang, "An IEEE 802.11 p-based multichannel MAC scheme with channel coordination for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 2, pp. 449–458, 2012.

[6] A. J. Ghandour, M. Di Felice, H. Artail, and L. Bononi, "Dissemination of safety messages in IEEE 802.11 p/WAVE vehicular network: analytical study and protocol enhancements," *Pervasive and Mobile Computing*, vol. 11, pp. 3–18, 2014.

[7] R. Huang, J. Wu, C. Long, Y. Zhu, B. Li, and Y. B. Lin, "SPRCA: distributed multisource information propagation in multichannel VANETs," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 11306–11316, 2017.

[8] D. Lee, S. H. Ahmed, D. Kim, J. Copeland, and Y. Chang, "Distributed SCH selection for concurrent transmissions in IEEE 1609.4 multi-channel VANETs," in *Proceedings of 2017 IEEE International Conference on Communications (ICC)*, pp. 1–6, Paris, France, 2017.

[9] Y. Yao, K. Zhang, and X. Zhou, "A flexible Multi-Channel coordination MAC protocol for vehicular ad hoc networks," *IEEE Communications Letters*, vol. 21, no. 6, pp. 1305–1308, 2017.

[10] H. Zhao, K. Gao, M. Zhang, D. Li, and H. Zhu, "A demand-aware transmission optimization control scheme based on multichannel coordination," in *Proceedings of 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 373–377, Nanjing, China, October 2017.

[11] X. Li, B. J. Hu, H. Chen, G. Andrieux, Y. Wang, and Z. H. Wei, "An RSU-coordinated synchronous multi-channel MAC scheme for vehicular ad hoc networks," *IEEE Access*, vol. 3, pp. 2794–2802, 2015.

[12] O. S. Eyobu, J. Joo, and D. S. Han, "Cooperative multi-channel dissemination of safety messages in VANETs," in *Proceedings of 2016 IEEE Region 10 Conference (TENCON)*, pp. 1867–1870, Singapore, 2016.

[13] S. Chantaraskul, K. Chaitien, A. Nirapai, and C. Tanwongvarl, "Safety communication based adaptive multi-channel assignment for VANETs," *Wireless Personal Communications*, vol. 94, no. 1, pp. 83–98, 2017.

[14] K. Tweed, "Why cellular towers in developing nations are making the move to solar power," *Scientific American*, 2013.

[15] J. Joo, H. Lee, and D. S. Han, "SAEMD: a scheduling algorithm for emergency message dissemination in vehicular ad hoc networks," in *Proceedings of 2014 Sixth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 501–504, Shanghai, China, 2014.

[16] D. N. M. Dang, C. S. Hong, S. Lee, and E. N. Huh, "An efficient and reliable MAC in VANETs," *IEEE Communications Letters*, vol. 18, no. 4, pp. 616–619, 2014.

[17] J. Li and C. Chiga, "Delay-aware transmission range control for VANETs," in *Proceedings of 2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pp. 1–6, Houghton, MI, USA, December 2010.

[18] X. Ma, X. Chen, and H. H. Refai, "On the broadcast packet reception rates in one-dimensional MANETs," in *Proceedings of IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*, pp. 1–5, New Orleans, LA, USA, November 2008.

[19] L. Cheng, B. Henty, D. Stancil, F. Bai, and P. Mudalige, "Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 GHz dedicated short range communication (DSRC) frequency band," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, 2007.

[20] Y. Yi, M. Gerla, and T. J. Kwon, "Efficient flooding in ad hoc networks using on-demand (passive) cluster formation," *Contract*, vol. 14, p. 0016, 2002.

Hindawi
Mobile Information Systems
Volume 2018, Article ID 5957412, 10 pages
https://doi.org/10.1155/2018/5957412

Research Article

Integrated Packet Classification to Support Multiple Security Policies for Robust and Low Delay V2X Services

Jaehyeong Wee and Wooguil Pak

Department of Computer Engineering, Keimyung University, Daegu 704-701, Republic of Korea

Correspondence should be addressed to Wooguil Pak; wooguilpak@kmu.ac.kr

Received 19 June 2018; Revised 28 September 2018; Accepted 3 October 2018; Published 1 November 2018

Guest Editor: Safdar H. Bouk

One of the key applications in the 5G system is Vehicle-to-Everything (V2X). Ultra-low delay communication is essential for the safety of users and pedestrians in V2X. However, as sophisticated and various cyberattacks are increasing, it becomes hard to satisfy low delay constraints. To protect networks from such attacks, even single network security equipment provides multiple security functions, resulting in the inevitable additive delay in packet processing. In this paper, we suggest a new packet classification paradigm to resolve this issue. The proposed algorithm integrates multiple policy rule-sets into a single rule-set and classifies incoming packets using the integrated rule-set. Thus, it has a unique feature providing high classification performance regardless of the number of security policies. Through extensive performance evaluations, we confirm that the performance improvement is also increased with the total rule-set number increasing without the significant overhead of memory cost. We expect that it will mitigate the delay issue of existing network equipment for upcoming services such as V2X.

1. Introduction

Vehicle-to-Everything (V2X) service is one of the most promising applications in the 5G system. It frequently exchanges information between drivers, pedestrians, vehicles, and transportation infrasystems [1–6], and the information should be delivered with low delay and high reliability for the safety of involved persons.

Modern cyberattacks have become more sophisticated and diverse, and as a result, security functions installed in modern security equipment also become more complex and various. For protecting networks from various cyberattacks, single multifunction network equipment has been introduced [7]. For example, unified threat management (UTM) supports multiple rule-sets using multiple policy tables as shown in Figure 1. Such integrated network equipment has advantages in security but disadvantages in strict delay requirements of V2X. Each security policy is implemented by complicate packet classification that searches a matching rule with the highest priority by comparing each field of every rule with the incoming packet header. As the integrated equipment should independently perform packet classification for each policy rule-set, the classification cost increases as the number of rule-sets increases [8–14]. Multiple classifications are a bottleneck of network performance, especially in terms of the delay [15–20]. Therefore, the high performance and scalable packet classification is essential for supporting V2X.

In this paper, we propose a new packet classification algorithm that has a distinct feature against other competitors. Although most existing classification algorithms suffer from deteriorated performance as the total rule-set number increases, the proposed algorithm can achieve high classification performance regardless of the total rule-set number. It can effectively support reliable and low delay V2X services. Figure 2 shows the overall architecture of the software-defined networking (SDN) for V2X. Packet classification is a basic function of OpenFlow controller and SDN switch.

To increase the performance of packet classification, high-end SDN switches adopt the expensive hardware-based solution. However, the OpenFlow controller usually adopts software-based packet classification since hardware solution cannot achieve high flexibility to support various security requirements from customers. This algorithm targets OpenFlow controllers and software-based SDN switches to reduce the burden of packet classification. It can play a very

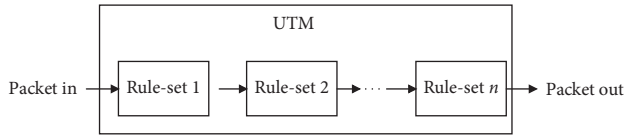


Figure 1: Multiple packet classification using multiple rule-sets in UTM equipment.

important role in them to provide high performance and high security, simultaneously.

The remainder of this paper is organized as follows: Section 2 briefly presents related work, and the motivation of this research is explained in Section 3. In Section 4, the proposed algorithm is described in detail. The performance evaluation results are compared with those of competitors in Section 5. Finally, Section 6 concludes.

2. Related Work

Although many factors can be used to evaluate the performance of packet classification algorithms, packet classification speed and memory requirements are most important factors. However, most algorithms cannot support high classification speed with low memory requirement.

Packet classification is classified into hardware- and software-based approaches [21–27]. Hardware-based packet classification can achieve very high classification speed that is impossible for the software-based one. Most modern network equipment adopts hardware packet accelerators to provide 100 Gbps performance with multiple rule-sets. However, the hardware should be redesigned to satisfy the various requirements of users such as adding a new field in the rule structure. Moreover, hardware-based solutions usually adopt expensive memory called ternary-content addressable memory (T-CAM) for classification. Since supported rule-set size is determined by the size of T-CAM, it costs very high to support large rule-sets.

The strongest advantage in the software-based approach is flexibility. If the structure of field should be changed, it can be easily supported by modifying software. Another merit of the software-based approach is cost. If larger rule-set is needed, the user can increase the rule-set capacity of the network equipment by just adding much cheaper dynamic random-access memory (DRAM) compared to T-CAM.

Well-known algorithms belonging to the software-based approach are exhaustive search, cross-producting-based classification, tuple space search, and decision tree-based algorithms [21]. Now, we will briefly describe each software-based algorithm.

Exhaustive search linearly compares each rule with keys from highest to lowest priority to find the matching rule. Due to the searching procedure, the packet classification performance is degraded as the rule-set size increases. However, it requires smallest memory among all packet classifications and supports very fast update. Most of all, it can be easily implementable. As a result, it is suitable for a system with a small rule-set.

Cross-producting-based classification independently performs searching for each field, and it merges intermediate results [28–33]. This procedure is repeated until the final matching rule is found. It is one of fastest classification algorithms but it requires a huge amount of memory and time to build a classification table. Since it cannot support incremental update, it needs to rebuild entire table whenever a rule-set is updated. Although it has such critical weaknesses, it can support the classification performance almost similar to that of the hardware-based approach. Therefore, a lot of research is still going on to improve the weaknesses.

Tuple space search probes each sub-rule-set called tuple space to find the matching rule [34–37]. A tuple is defined by combination of each prefix length for five tuples, and the set of tuples are called tuple space. Since each rule of a rule-set belongs to only one of the tuples, tuple space has a good scalability in terms of a rule-set size. Although it achieves a moderate classification performance, it supports fast update, i.e., inserting or deleting a rule. Therefore, it has been adopted in Open vSwitch [38]. However, the classification performance is decreased proportional to the number of tuples, thus requiring further research to improve the performance.

Decision tree-based algorithm recursively chooses a child node according to the predefined policy on decision tree built based on a rule-set until it reaches a leaf node [39–47]. If it reaches, it searches the matching rule with the highest priority among all rules stored in the leaf node. The overall classification performance is known to have log complexity in terms of the rule-set size.

Decision tree-based algorithm provides a comparable classification performance with that of cross-producting-based classification algorithm but requires much smaller memory size. Thus, the decision tree-based algorithm is one of the most actively researched algorithms at present. When a decision tree-based algorithm partitions a rule-set into multiple sub-rule-sets, partitioning criteria is controlled by two factors: *space factor*, the maximum ratio of the sum of all rules belong to all sub-rule-sets to the original rule-set size, and *binth*, the maximum allowed rule size in the leaf node. Hence, the classification performance and the table size can be adjusted according to the requirements of applications.

Large *space factor* increases partitioning number but decreases the height of a decision tree, resulting in fast classification performance. However, the total number of duplicate rules is increased, and therefore, generating a large decision tree. On the other hand, large *binth* reduces partitioning number, so the tree size is decreased but the searching cost in the leaf node increases, and thus, providing low classification performance.

Well-known algorithms belonging to the decision tree-based approach are HiCuts and HyperCuts [39, 40]. Although they provide high classification performance, they still suffer from a large decision tree due to significant rule duplications. Recently, EffiCuts was introduced to decreasing rule duplications [41]. EffiCuts is based on HyperCuts but groups rules by fields with wildcard and generates a separate tree for each group. This approach significantly reduces rule duplications, so the total tree size is greatly decreased. However, separate tree deteriorates the classification performance. As a mitigation, trees with similar wildcard characteristics can be merged to increase classification performance while the overall tree

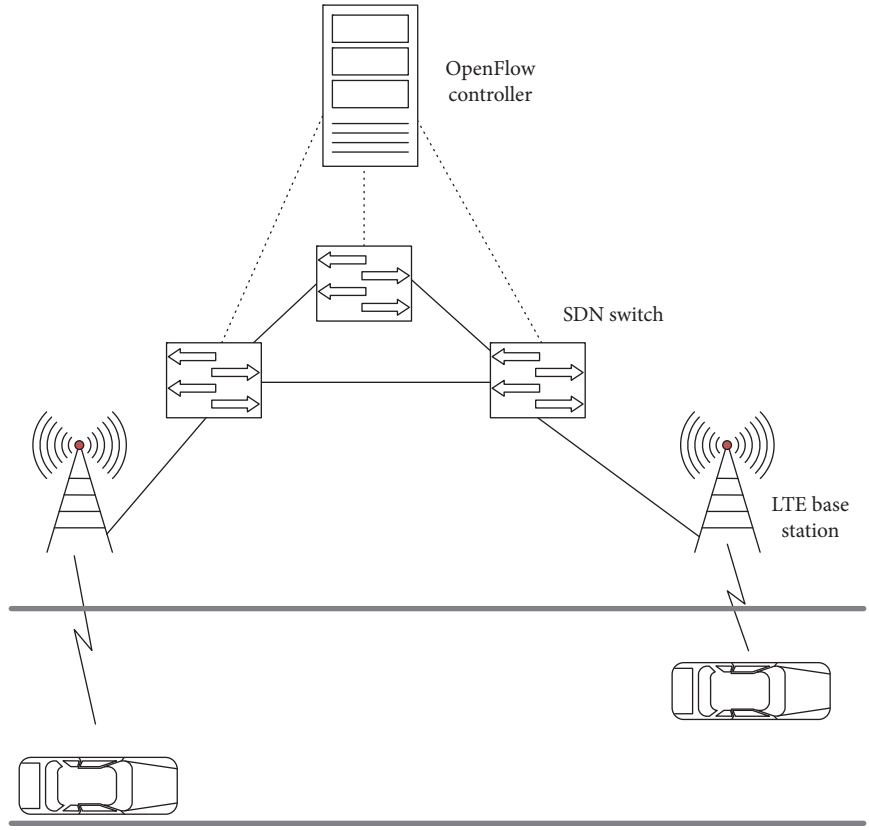


Figure 2: Overall architecture of V2X networks.

size is almost the same. EffiCuts is known to support fast updating [48, 49].

We will describe the operation of EffiCuts in detail. At first, EffiCuts splits the total rule-set into some predefined categories according to how many wildcard field each rule contains, where wildcard field is a field on which the rule has a large matching range, typically at least 50% of the total range of the field. For 5-tuple rule-set, we have four cases as follows:

(i) Category 1: four wildcard field rules
(ii) Category 2: three wildcard field rules
(iii) Category 3: two wildcard field rules
(iv) Category 4: one or zero wildcard field rules

For example, assuming that matching ranges of a rule for source IP, destination IP, source port, destination port, and protocol are ANY, ANY, 0 to 32768, 80, 0 to 128, it has four wildcard fields except for destination port, and therefore belonging to Category 1. Since each category contains similar rules only, EffiCuts builds a decision tree for sub-rule-set belonging to the same category and reduces replicated rules during building a decision tree. Although EffiCuts generates multiple decision trees, the total tree size is very small compared to the original HyperCuts. However, the number of decision tree affects the total classification performance. To reduce the number of trees, EffiCuts merges similar categories. This tree merging process increases the total tree size but it can still avoid excessive replication of rules. By doing so, EffiCuts achieves high classification performance and low memory requirement, simultaneously.

Table 1 summarizes each feature of packet classification algorithms.

3. Motivation

As shown in Table 1, the software-based approach consumes much memory to achieve high classification performance. However, high complexity of memory requirement results in low scalability in terms of rule-set size. Although decision tree-based algorithms have a high complexity of memory requirement, i.e., $O(N^D)$, latest decision tree algorithms show very low memory requirements, where N and D denotes the total dimension number and the rule-set size, respectively.

To verify the memory requirement, we performed the following experiment. We synthesized multiple firewall rule-sets whose size is from 20K to 100K using ClassBench [50]. Then, we built the total decision tree and calculated the ratio of the tree size to the rule-set size for each rule-set, where space factor and binth were configured to the best values. Figure 3 shows the experimental results obtained from EffiCuts. EffiCuts shows almost the same ratio regardless of the rule-set size, which means EffiCuts achieves almost $O(N)$ for memory requirement. Thus, it can decrease the decision tree size by 100 times for 100,000 rules compared to HiCuts or HyperCuts [41].

Figure 4 shows the ratio of the average memory access number and the rule-set size on the same configuration.

Table 1: Comparison features of software-based packet classification algorithms according to algorithm type.

Algorithm	Classification performance	Memory requirement	Incremental update
Exhaustive	O(N)	O(N)	Possible
Cross-producting	O(DW)	O(N^D)	Impossible
Tuple space	O(N)	O(N)	Possible
Decision tree	O(D)	O(N^D)	Partially possible

Note: rule-set size, total bit length of all keys, and the size of dimension of rule are denoted by N, W, and D, respectively

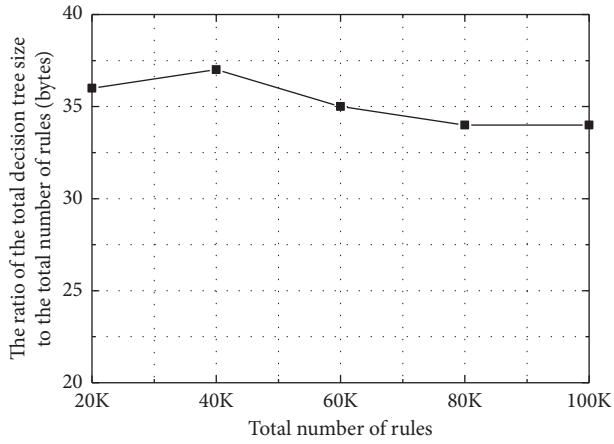


Figure 3: The ratio of the total decision tree size for EffiCuts to the total number of rules as the number of rules increases.

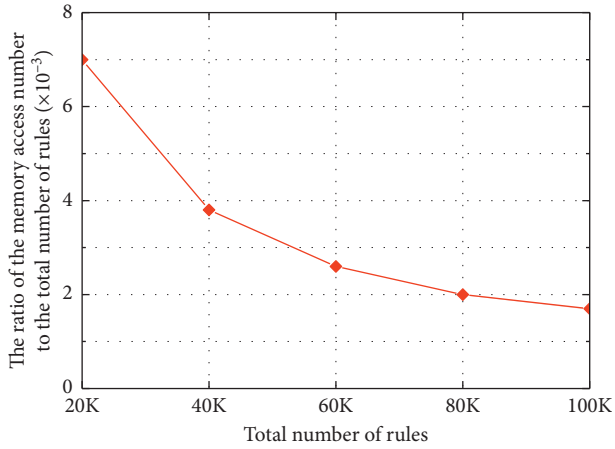


Figure 4: The average ratio of memory access number to the total number of rules as the number of rules increases.

We synthesized the packet data using each rule-set and searched the decision tree to find every packet in the data. We counted the total number of memory accesses during searching process and obtained the ratio of the total number and the total packet number. As the rule-set size increases, the number of memory access for EffiCuts also increases in Figure 4. However, the ratio of the access number to the rule-set size decreases as shown in Figure 4. From Figures 3 and 4, we can finally find two characteristics as follows:

Characteristic 1: $M(R_1) + M(R_2) > M(R_1 + R_2)$, where $M(R)$ is the average memory access number for rule-set R.

Characteristic 2: $S(R_1) + S(R_2) \cong S(R_1 + R_2)$, where $S(R)$ is the size of decision tree for rule-set R.

For example, we can see that $M(T_{20K}) + M(T_{40K}) > M(T_{20K} + T_{40K}) \cong M(T_{60K})$ from Figure 4 and $S(T_{20K}) + S(T_{40K}) \cong S(T_{20K} + T_{40K}) \sim S(T_{60K})$ from Figure 3, respectively, where T_n denotes the testing rule-set with a size of n used in the experiment and where K means 1,000.

Until now, existing research studies for packet classification focus on classification with a single rule-set. However, network systems with multiple rule-sets become popular, and fast classification algorithm oriented on a single rule-set has limitation to achieve high performance for multiple rule-sets. Thereby, it is required to consider multiple rule-sets for designing high performance classification algorithms. Hence, Characteristics 1 and 2 suggest a new guideline for developing packet classification algorithms. According to Characteristic 1, if a system has multiple rule-sets, it is advantageous to integrate them into one rule-set to construct a decision tree for improving classification speed. Characteristic 2 also implies that the size of the decision tree for integrated rule-sets is not larger than the sum of sizes for each decision tree for all rule-sets.

We finally conclude that packet classification algorithm based on integrated rule-sets has many advantages and suggest a new classification algorithm utilizing the features of integrated rule-sets.

4. Proposed Algorithm

The proposed algorithm performs packet classification using an integrated rule-set that combines all rule-sets in a system. At first, we briefly show the features of the proposed algorithm, and then, describe the algorithm in detail. For simple explanation, we assume that the rule consists of five tuples but it can be easily extended to more field cases.

4.1. Features of the Proposed Algorithm

4.1.1. Minimized Classification Cost. The proposed algorithm can complete total packet classification for all rule-sets with one search. Therefore, it can minimize the increased overhead due to the repetitive classification. Since it can maintain the high packet classification performance regardless of the number of rule-sets, it is very important feature of the proposed algorithm.

4.1.2. Early Packet Drop. Integrated rule-set has not only advantage to decrease classifying overhead but also to remove unnecessary classifying. For example, Figure 5 shows existing and proposed packet classifications. Assume that an incoming packet is allowed by rule-sets 0 to $k - 1$, but it is rejected by rule-set k. In this case, packet classifications for rule-sets 0 to $k - 1$ are eventually unnecessary since the packet cannot be forwarded due to rule-set k. However, packet classification for each rule-set is performed in sequence, so it cannot avoid

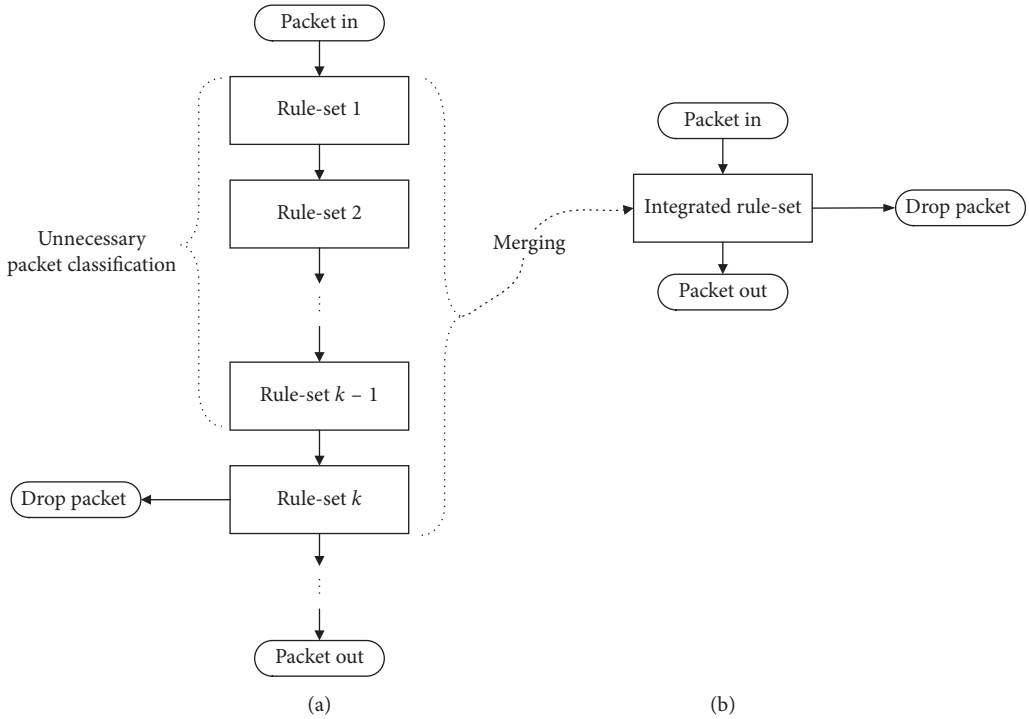


Figure 5: Packet classifications of existing and proposed algorithm. (a) Previous packet. (b) Proposed packet.

the unnecessary classifications for rule-sets 0 to $k-1$ for existing classification. For the proposed classification algorithm, all rule-sets are integrated into one larger rule-set, making almost the same effect as searching multiple rule-sets, simultaneously. Thereby, the problem of existing classification is mitigated in the proposed one.

4.2. Building Decision Tree. The proposed algorithm builds a decision tree using EffiCuts after merging each rule-set into a large rule-set. However, it needs unique procedure called "fast rule skipping" and "early drop marking" in each leaf node for improving the searching performance.

4.2.1. Fast Rule Skipping. The proposed algorithm requires an additional table called "rule-set starting index table" to store all indexes of the first rule in each rule-set. If we reach a leaf node during traversing the tree, we should find matching rules for each rule-set. Original EffiCuts linearly searches matching rules, so it will take a long time. To increase searching performance, we need to skip unvisited rules in rule-set k and go to the next rule-set $k+1$ when we find matching rule in the rule-set k. It is called "rule skipping." For example, if we find a matching rule r_2 for ACL rule-set in the leaf node as shown in Figure 6, we do not need to check rules r_3 and r_5 anymore. In this case, we can find the index number for firewall rule-set, i.e., 4, and skip r_3 and r_5. Thus, we can directly start searching the matching rule for firewall rule-set.

4.2.2. Early Packet Drop Marking. Assume that we build a node of a decision tree. Each node corresponds to disjoint hypercube searching space. Let us define some notations for describing "early packet drop marking":

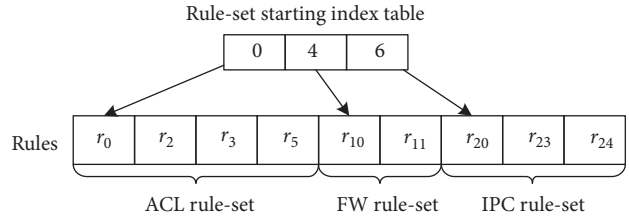


Figure 6: An example of a leaf node that contains 9 rules, i.e., 4, 2, and 3 rules for access control list (ACL), firewall (FW), and IP chain (IPC) rule-sets, respectively. Rules in each rule-set are arranged in order of increasing priority.

(i) Δ_v: the searching space for node v

(ii) k: the total rule-set number

(iii) n_p^v: the total number of rules for rule-set p belong to node v

(iv) $r_p^v[i]$: ith rule of rule-set p belonging to node v when the rules are sorted in the order of decreasing priority

(v) $S(\cdot)$: a set of all matching keys with given rule

(vi) $S_p^v[i] \triangleq S(r_p^v[i]) \cap \Delta_v$

We define $D_p^v(j)$ as a set of all keys matching with action "drop" from first to ith rules of the rule-set p belonging to node v when the rules are sorted in the order of decreasing priority. Then, it is recursively defined as

$$D_p^v(j) = \begin{cases} D_p^v(j-1) \cup S_p^v[j] & \text{if action of } r_p^v[i] \text{ is "drop",} \\ D_p^v(j-1) - S_p^v[j] & \text{otherwise,} \end{cases} \tag{1}$$

where $D_p^v(0) = \varnothing$.

Assume that an incoming packet is, respectively, matched with $r_p^v[i]$ and $r_q^v[j]$ for rule-sets i and j, where the actions of $r_p^v[i]$ and $r_q^v[j]$ are "allow" and "drop." In this case, the packet should be dropped by the rule-set j. If all packets matching with $r_p^v[i]$ are always matched with rules in other rule-set with action "drop," it will be very helpful to know that the packet will be dropped for increasing classification performance. This idea can be generalized as follows.

If $S_p^v[i] \subset D_q^v(n_q^v)$, any packet matched with $r_p^v[i]$ in node v is dropped, where $p \neq q$. Thus, while building a node v, the proposed algorithm finds any rule $r_p^v[i]$ s.t. $S_p^v[i] \subset D_q^v(n_q^v)$, where $p < q$, and mark $r_p^v[i]$ with "early packet drop." If a packet matches with a rule that has a mark "early packet drop" during searching, the searching procedure is finished and the packet is dropped. This "early packet drop marking" significantly increases the performance.

4.3. Proposed Packet Classification Performance Analysis. The proposed algorithm merges multiple rule-sets into an integrated one and constructs a decision tree. Now, we will show numerical analysis results for our algorithm. Assume that rules are homogeneous, and the decision tree is perfectly balanced B-tree for easy analysis. Let us define some notations as follows:

(i) k: the total rule-set number.

(ii) B: binth, the maximum allowed rule size in the leaf node.

(iii) c: the child number of each node. For easy analysis, we assume that c is fixed.

(iv) s: space factor. The maximum ratio of the sum of all rules belongs to all sub-rule-sets to the original rule-set size.

(v) N: the total rule number for each rule-set size. We also assume that N is fixed.

4.3.1. Total Packet Classification Cost Analysis. Assume that EffiCuts has N rules in a root node. If it has c child nodes and the space factor is s, the first level child node has at most sN/c rules. In a similar way, we can calculate the rule number in the leaf node as follows:

$$\frac{s^h N}{c^h} \leq B, \tag{2}$$

and it should be equal to or less than B, where the height of the decision tree is h_{EffiCuts}. From (2), we can find the height as follows:

$$h_{\text{EffiCuts}} \cong \log_{(c/s)}\left(\frac{N}{B}\right). \tag{3}$$

For the proposed algorithm, we can similarly obtain the height as

$$h_{\text{proposed}} \cong \log_{(c/s)}\frac{kN}{B}. \tag{4}$$

Thus, the total packet classification cost for EffiCuts is approximated as follows:

$$kh_{\text{EffiCuts}} \cong k \cdot \log_{(c/s)}\frac{N}{B}. \tag{5}$$

Now, we calculate the difference between two costs:

$$\begin{aligned} kh_{\text{EffiCuts}} - h_{\text{proposed}} &= k \cdot \log_{(c/s)}\frac{N}{B} - \log_{(c/s)}\frac{kN}{B}, \\ &= (k-1) \cdot \log_{(c/s)}\frac{N}{B} \\ &\quad - \log_{(c/s)}k > 0 \because \mathrm{k} > 1 \text{ and } \frac{N}{B} \gg k. \end{aligned} \tag{6}$$

Then, we can conclude that the proposed algorithm can always provide higher classification performance than EffiCuts.

4.3.2. Total Decision Tree Size Analysis. Since we assume that the decision tree is a perfectly balanced B-tree, EffiCuts requires at most $2^{h_{\text{EffiCuts}}} - 1$ nodes for one rule-set, so the total number of nodes is $k(2^{h_{\text{EffiCuts}}} - 1)$. Similarly, the proposed algorithm requires $2^{h_{\text{proposed}}} - 1$. If we calculate the difference between two node sizes,

$$\begin{aligned} &k\left(2^{h_{\text{EffiCuts}}} - 1\right) - \left(2^{h_{\text{proposed}}} - 1\right) \\ &= k\left(2^{\log_{(c/s)}(N/B)} - 1\right) - \left(2^{\log_{(c/s)}(kN/B)} - 1\right) \\ &= k\left(2^{\log_{(c/s)}(N/B)} - 1\right) - \left(2^{\log_{(c/s)}(kN/B)} - 1\right) \\ &= k\left(2^{\log_{(c/s)}(N/B)} - 1\right) - \left(2^{\log_{(c/s)}k + \log_{(c/s)}(N/B)} - 1\right) \\ &= 2^{\log_{(c/s)}(N/B)}\left(k - 2^{\log_{(c/s)}k}\right) - k + 1 \\ &= 2^{\log_{(c/s)}(N/B)}\left(k - k^{\log_{(c/s)}2}\right) - k + 1. \end{aligned} \tag{7}$$

Since $2^{\log_{(c/s)}(N/B)}(k - k^{\log_{(c/s)}2}) - k + 1 < 0$, if $1 < (c/s) < 2$, the proposed algorithm creates larger tree than EffiCuts, where $1 < (c/s) < 2$. However, we found that $c \gg s$ for most nodes in a decision tree. It means that the proposed algorithm builds a tree which size is not significantly large compared to EffiCuts.

5. Performance Evaluation

We compared the performance of the proposed algorithm with EffiCuts. Since EffiCuts is almost an unique decision tree-based packet classification algorithm to support fast classification and large rule-set size simultaneously, we choose it as a competitor. We measured average and worst case classification memory access numbers, and decision tree size using the optimal bucket size and space factor for each evaluation. Since the average classification memory access number defines the overall performance of the network equipment, it is the most important metric. The worst case classification memory access number represents the maximum queuing delay required to guarantee in-order packet forwarding. Last, the total decision tree size is also a critical factor to represent the scalability in terms of rule-set size. Considering modern network traffic increases

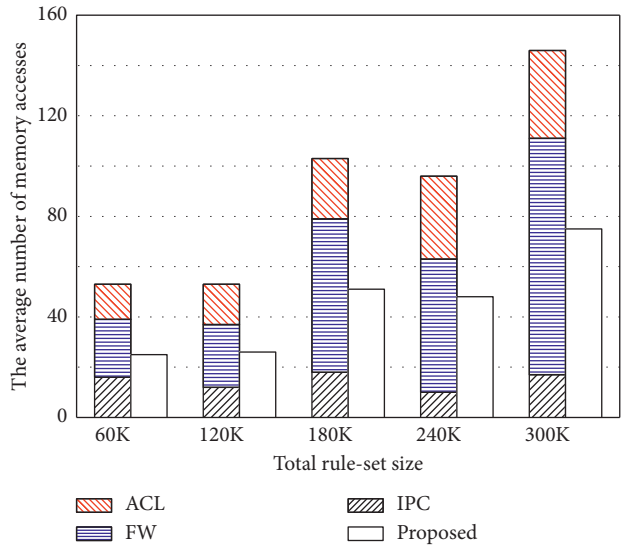


Figure 7: The comparison results of EffiCuts and the proposed algorithm for the average number of memory accesses as total rule-set size increases, where three rule-sets are used.

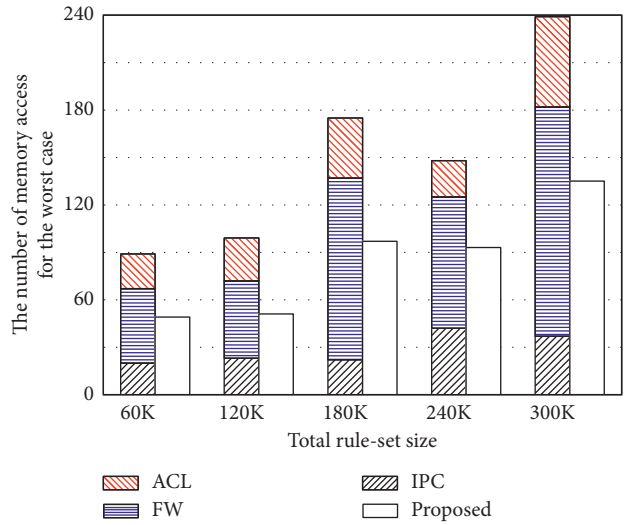


Figure 8: The comparison results of EffiCuts and the proposed algorithm for the worst case number of memory accesses as total rule-set size increases, where three rule-sets are used.

exponentially and rule-set becomes larger and more complicated to support various services, we choose these three metrics for performance evaluation.

For evaluating performance of the proposed algorithm, multiple rule-sets are needed. Thus, three rule-set types such as FW, ACL, and IPC were generated using Classbench [50]. Each rule consists of five tuples, and the rule-set size was set to 20K to 100K increasing by 20K where K means 1,000. Thus, the integrated rule-set size was to 60K to 300K. For each evaluation, binth and space factor were set to the optimal values, i.e., 30 and 2, respectively.

Figure 7 shows the average classification performance in terms of the average number of memory accesses according to the size of the total integrated rule-set. The proposed algorithm achieves about 2.5 times lower memory access number regardless of the rule-set size compared to EffiCuts. It is almost similar to the memory access number of each rule-set. It confirms that integrated rule-set has many benefits to increase the classification performance.

Figure 8 shows results for the worst case packet classification performance. The proposed algorithm decreases the memory access number by 2.2 times regardless of the total rule-set size compared to competitor. Although the improvement is slightly smaller than that for average memory access number, it also confirms that the proposed algorithm is very effective to increase the packet classification performance for the worst case.

The worst case performance actually affects the packet processing delay since most network equipment should guarantee that the packets are processed in sequence, keeping that the orders of incoming and outgoing packets are the same. As the worst classification performance is improved, it can efficiently provide in-order packet forwarding while minimizing packet queuing delay.

Figure 9 shows the comparison results between proposed and EffiCuts for decision tree size. As mentioned earlier as

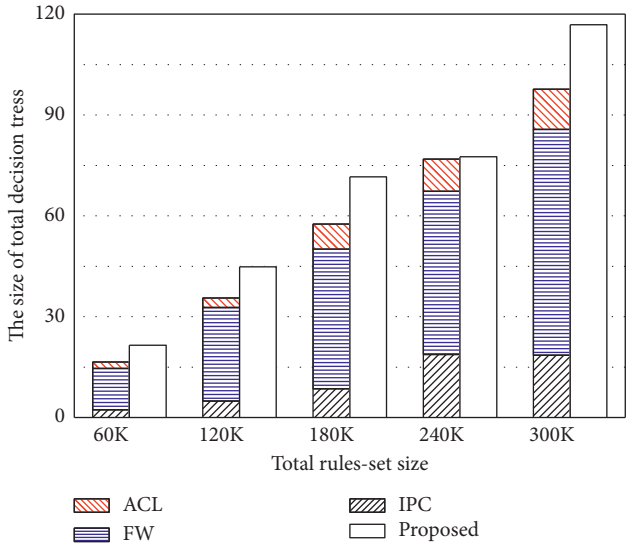


Figure 9: The comparison results of EffiCuts and the proposed algorithm for the decision tree size as total rule-set size increases, where three rule-sets are used.

Characteristic 2, the proposed algorithm generates a decision tree whose size about 20% is larger than that of EffiCuts for 300K rules. Therefore, the proposed algorithm does not suffer from significantly increased tree size caused by rule-set integration.

Although we used three rule-sets for most performance evaluations, it is also important to investigate the performance as the rule-set number increases for evaluating scalability in terms of the rule-set number. Figure 10 shows the ratio of the results of EffiCuts to those of the proposed algorithm for the memory access and the decision tree sizes as the rule-set size increases from 1 to 10.

As shown in Figure 10, the decision tree size of the proposed algorithm is almost the same to that of EffiCuts

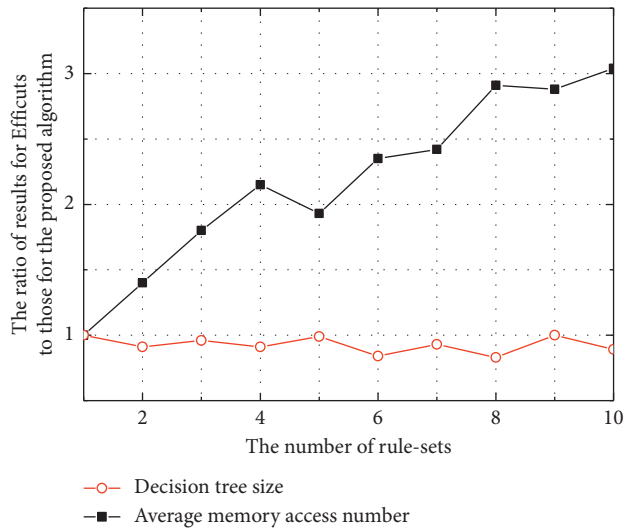


FIGURE 10: The ratio of results for EffiCuts to those for the proposed algorithm for decision tree and average memory access number as the number of rule-set increases, where each rule-set size is fixed to 20K.

regardless of rule-set size but the memory access size is decreased fast compared to EffiCuts. For 10 rule-sets, the proposed algorithm achieves 3 times higher classification performance while the decision tree size is just increased by 10%. Thus, we can see that our proposed algorithm can provide high classification performance without any cost of decision tree size.

6. Conclusions

In this paper, we proposed a new packet classification algorithm to achieve high packet classification performance without significant increasing of memory requirement. It can be adopted in modern high performance network equipment that use various classification rule-sets such as routing, switching, QoS, and other rule-sets. Existing network equipment with multiple rule-sets independently perform classification for each rule-set, thus resulting in deteriorated performance as the rule-set number increases. Our algorithm combines each rule-set and achieves high performance that cannot be provided by existing algorithms. We expect that it will help to enable robust and low delay V2X services in modern networks.

Data Availability

The source code data used to support the findings of this study are currently under embargo while the research findings are commercialized. Requests for data, 12 months after publication of this article, will be considered by the corresponding author.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] O. O. Fagbohun, "Comparative studies on 3G, 4G and 5G wireless technology," *IOSR Journal of Electronics and Communication Engineering*, vol. 9, no. 2, pp. 133–139, 2014.

[2] H. Tullberg, P. Popovski, Z. Li et al., "METIS system concept: the shape of 5G to come," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 132–139, 2016.

[3] P. K. Agyapong, M. Iwamura, D. Staehle, W. Kiess, and A. Benjebbour, "Design considerations for a 5G network architecture," *IEEE Communications Magazine*, vol. 52, no. 11, pp. 65–75, 2014.

[4] T. Janevski, "A system for PLMN-WLAN internetworking," *Journal of Communications and Networks*, vol. 7, no. 2, pp. 192–206, 2005.

[5] M. Hata, "Fourth generation mobile communication systems beyond IMT-2000," in *Proceedings of Fifth Asia-Pacific Conference on Communications and Fourth Optoelectronics and Communications Conference (APCC/OECC '99)*, pp. 765–767, Beijing, China, October 2002.

[6] A. Gohil, H. Modi, and S. K. Patel, "5G technology of mobile communication: a survey," in *Proceedings of International Conference on Intelligent Systems and Signal Processing ISSP-2013*, pp. 288–292, Anand, Gujarat, March 2013.

[7] *The Benefits of Multiple Flow Tables and TTPs Version Number 1.0 February 2*, 2015, https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_Multiple_Flow_Tables_and_TTPs.pdf.

[8] Z. Chen, Y. Wu, J. Ge, and E. Yuepeng, "A new lookup model for multiple flow tables of OpenFlow with implementation and optimization considerations," in *Proceedings of IEEE International Conference on Computer and Information Technology (CIT)*, pp. 528–532, Xi'an, China, September 2014.

[9] N. Gude, T. Koponen, J. Pettit et al., "Nox: towards an operating system for networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 3, pp. 105–110, 2008.

[10] Y. Kanizo, D. Hay, and I. Keslassy, "Palette: distributing tables in software-defined networks," in *Proceedings of IEEE INFOCOM*, pp. 545–549, Turin, Italy, April 2013.

[11] N. Sarrar, S. Uhlig, A. Feldmann, R. Sherwood, and X. Huang, "Leveraging zipf's law for traffic offloading," *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 1, pp. 16–22, 2012.

[12] Z. Wu, Y. Jiang, and S. Yang, "An efficiency pipeline processing approach for OpenFlow switch," in *Proceedings of 41st IEEE Conference on Local Computer Networks (LCN)*, pp. 204–207, Dubai, UAE, November 2016.

[13] *Flow Table Explosion with Openflow 1.0 (And Why We Need Openflow 1.3)*, http://blog.ipspace.net/2013/10/flow-table-explosion-with-openflow-10.html.

[14] X.-N. Nguyen, D. Saucez, C. Barakat, and T. Turletti, "Rules placement problem in OpenFlow networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1273–1286, 2016.

[15] M. Zolanvari, "SDN for 5G," http://www.cs.wustl.edu/~jain/cse570-15/ftp/sdnfor5g.pdf.

[16] *OpenFlow Switch Specification Version 1.5.0*, 2014, https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-switch-v1.5.0.noipr.pdf.

[17] N. Landage and T. Dhope, "Survey of SDN based packet classification techniques," *International Journal of Science and Research (IJSR)*, vol. 5, no. 7, pp. 1113–1115, 2016.

[18] N. McKeown, T. Anderson, H. Balakrishnan et al., "OpenFlow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.

[19] S. Agarwal, M. Kodialam, and T. Lakshman, "Traffic engineering in software defined networks," in *Proceedings of IEEE INFOCOM*, pp. 2211–2219, Turin, Italy, April 2013.

[20] T. Inoue, T. Mano, K. Mizutani, S.-I. Minato, and O. Akashi, "Rethinking packet classification for global network view of software-defined networking," in *Proceedings of IEEE 22nd International Conference on Network Protocols (ICNP)*, pp. 296–307, Raleigh, NC, USA, October 2014.

[21] A. Yahya, D. Al-Nejadi, and N. Shaikh-Husin, "Survey on multi field packet classification techniques," *Research Journal of Recent Sciences*, vol. 4, no. 2, pp. 98–106, 2015.

[22] P. Gupta and N. McKeown, "Algorithms for packet classification," *IEEE Network*, vol. 15, no. 2, pp. 24–32, 2002.

[23] K. Pagiamtzis and A. Sheikholeslami, "Content-addressable memory (CAM) circuits and architectures: a tutorial and survey," *IEEE Journal of Solid-State Circuits*, vol. 41, no. 3, pp. 712–727, 2006.

[24] K. G. Pérez, X. Yang, S. Scott-Hayward, and S. Sezer, "A configurable packet classification architecture for Software-Defined Networking," in *Proceedings of 27th IEEE International System-on-Chip Conference (SOCC)*, pp. 353–358, Las Vegas, Nevada, USA, September 2014.

[25] K. G. Perez, X. Yang, S. Scott-Hayward, and S. Sezer, "Optimized packet classification for software-defined networking," in *Proceedings of IEEE International Conference on Communications (ICC)*, pp. 859–864, Sydney, Australia, June 2014.

[26] H. Lim, "Survey and proposal on packet classification algorithms," in *Proceedings of International Conference on High Performance Switching and Routing (HPSR)*, Richardson, Texas, USA, June 2010.

[27] D. E. Taylor, "Survey and taxonomy of packet classification techniques," *ACM Computing Surveys*, vol. 37, no. 3, pp. 238–275, 2005.

[28] P. Gupta and N. McKeown, "Packet classification on multiple fields," in *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, pp. 147–160, Cambridge, MA, USA, August 1999.

[29] B. Xu, D. Jiang, and J. Li, "HSM: a fast packet classification algorithm," in *Proceedings of 19th International Conference on Advanced Information Networking and Applications (AINA, 2005)*, pp. 1–6, Taipei, Taiwan, March 2005.

[30] D. E. Taylor and J. S. Turner, "Scalable packet classification using distributed crossproducting of field labels," in *Proceedings of IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM, 2005)*, pp. 269–280, New York, NY, USA, March 2005.

[31] G. S. Jedhe, A. Ramamoorthy, and K. Varghese, "A scalable high throughput firewall in FPGA view document," in *Proceedings of 16th International Symposium on Field-Programmable Custom Computing Machines*, pp. 43–52, Palo Alto, California, USA, April 2008.

[32] Y. Pan, B. Chen, and T. Xu, "A timesaving recursive flow packet classification algorithm," in *Proceedings of International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC '09)*, pp. 442–445, Wuhan, China, April 2009.

[33] P.-C. Wang, C.-L. Lee, C.-T. Chan, and H.-Y. Chang, "Hardware-based packet classification made fast and efficient," in *Proceedings of 11th International Conference on Parallel and Distributed Systems*, Fuduoka, Japan, July 2005.

[34] V. Srinivasan, S. Suri, and G. Varghese, "Packet classification using tuple space search," *ACM SIGCOMM Computer Communication Review*, vol. 29, no. 4, pp. 135–146, 1999.

[35] M. Alutoin and P. Raatikainen, "Diagonal tuple space search," in *Proceedings of Global Telecommunications Conference (GLOBECOM '04)*, pp. 719–724, IEEE, Dallas, Texas, USA, November 1999.

[36] M. Alutoin and P. Raatikainen, "Diagonal tuple space search in two dimensions," in *Proceedings of 3rd International Networking Conference Networking (IFIP-TP6)*, pp. 308–319, Athens, Greece, May 2004.

[37] P.-C. Ting, Y.-S. Hsu, and T.-H. Lee, "Fast tuple space based packet classification algorithm for two-field conflict free filters," in *Proceedings of IEEE International Conference on Communications (ICC '03)*, pp. 325–331, Anchorage, AK, USA, May 2003.

[38] B. Pfaff, J. Pettit, T. Koponen et al., "The design and implementation of open vSwitch," in *Proceedings of 12th USENIX Symposium on Networked Systems Design and Implementation (NSDI '15)*, pp. 117–130, Oakland, CA, USA, May 2015.

[39] P. Gupta and N. McKeawn, "Classifying packets with hierarchical intelligent cuttings," *IEEE Micro*, vol. 20, no. 1, pp. 34–41, 2000.

[40] S. Singh, F. Baboescu, G. Varghese, and J. Wang, "Packet classification using multidimensional cutting," in *Proceedings of ACM Conference Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '03)*, pp. 213–224, Karlsruhe, Germany, Auguest 2003.

[41] B. Vamanan, G. Voskuilen, and T. N. Vijaykumar, "Efficuts: optimizing packet classification for memory and throughput," *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 4, pp. 207–218, 2010.

[42] H. Lu and S. Sahni, "O(logW) multidimensional packet classification," *IEEE/ACM Transactions on Networking*, vol. 15, no. 2, pp. 462–472, 2007.

[43] G. Antichi, C. Callegari, A. W. Moore, S. Giordano, and E. Anastasi, "JA-trie: entropy-based packet classification," in *Proceedings of IEEE 15th International Conference on High Performance Switching and Routing, HPSR 2014*, vol. 15, pp. 32–37, Vancouver, BC, Canada, July 2014.

[44] Y.-K. Chang and Y.-H. Wang, "CubeCuts: a novel cutting scheme for packet classification," in *Proceedings of 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pp. 274–279, Fukuoka, Japan, March 2012.

[45] H. Song and J. S. Turner, "ABC: adaptive binary cuttings for multidimensional packet classification," *IEEE/ACM Transactions on Networking*, vol. 21, no. 1, pp. 98–109, 2013.

[46] M. Kathuria and S. Gambhir, "Genetic binary decision tree based packet handling schema for WBAN system," in *Proceedings of Recent Advances in Engineering and Computational Sciences (RAECS)*, Chadigarh, India, March 2014.

[47] W. Pak and Y.-J. Choi, "High performance and high scalable packet classification algorithm for network security systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 1, pp. 37–49, 2017.

[48] T. S. Urmila, "Decision tree based network packet classification algorithms," *International Journal of Advanced Networking and Applications (IJANA)*, Special issue, pp. 28–34, 2015.

[49] B. Vamanan and T. N. Vijaykumar, "TreeCAM: decoupling updates and lookups in packet classification," in *Proceedings of the Seventh Conference on emerging Networking Experiments and Technologies*, Tokyo, Japan, December 2011.

[50] D. E. Taylor and J. S. Turner, "ClassBench: a packet classification benchmark," *IEEE/ACM Transactions on Networking (TON)*, vol. 15, no. 3, pp. 499–511, 2007.

Hindawi
Mobile Information Systems
Volume 2018, Article ID 5672154, 11 pages
https://doi.org/10.1155/2018/5672154

Review Article

Security and Privacy Issues in Vehicular Named Data Networks: An Overview

Hakima Khelifi,[1] **Senlin Luo**,[1] **Boubakr Nour**,[2] **and Sayed Chhattan Shah**[3]

[1]*School of Information and Electronics, Beijing Institute of Technology, Beijing, China*
[2]*School of Computer Science, Beijing Institute of Technology, Beijing, China*
[3]*Department of Information Communication Engineering, Hankuk University of Foreign Studies, Seoul, Republic of Korea*

Correspondence should be addressed to Senlin Luo; luosenlin2012@gmail.com

Received 6 July 2018; Accepted 30 August 2018; Published 30 September 2018

Academic Editor: Mohamed Elhoseny

A tremendous amount of content and information are exchanging in a vehicular environment between vehicles, roadside units, and the Internet. This information aims to improve the driving experience and human safety. Due to the VANET's properties and application characteristics, the security becomes an essential aspect and a more challenging task. On the contrary, named data networking has been proposed as a future Internet architecture that may improve the network performance, enhance content access and dissemination, and decrease the communication delay. NDN uses a clean design based on content names and Interest-Data exchange model. In this paper, we focus on the vehicular named data networking environment, targeting the security attacks and privacy issues. We present a state of the art of existing VANET attacks and how NDN can deal with them. We classified these attacks based on the NDN perspective. Furthermore, we define various challenges and issues faced by NDN-based VANET and highlight future research directions that should be addressed by the research community.

1. Introduction

During the past two decades, research academies and industrials focused their attention on vehicular ad hoc networks (VANETs) [1] in order to provide safety and assistance applications, improve the driving experience, and control the road traffic. Towards this goal, several protocols are proposed such as dedicated short-range communication (DSRC), wireless access in vehicular environment (WAVE), and other protocols that run as an overlay on DSRC/WAVE rather than the IP protocol [2]. In a vehicular environment, a huge amount of data are exchanged under different types of communication such as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and with pedestrian, satellite, charging stations, and smart grids (V2U). V2I communication can be used in applications that support Internet access, while V2V is mostly used in real applications that need to send emergency and real-time information about an accident or traffic information [3].

However, exchanging information and sharing data in VANET under the use of IP protocol have been a challenging task [4] due to the nature of this network that frequently and quickly changes under the use of poor-quality wireless link which makes VANET more complex in terms of routing, mobility, and security. Also, due to the fact that vehicles may exchange personal and sensitive information, securing the content and communication and preserving user and data privacy are indispensable [5]. VANET communication must ensure different security requirements including privacy, confidentiality, integrity, and nonrepudiation.

Meanwhile, different solutions have been proposed in the literature as future Internet architectures [6]. Information-centric networking (ICN) [7] has been proposed as one of the promising paradigms to replace the current host-centric network. Hereby, many solutions under the name of ICN have been implemented, such as named data networking (NDN) [8]. NDN replaces the IP address with the name of the content and implements a simple content discovery and data delivery mechanism using an Interest-Data exchange model. NDN aims to improve that data dissemination and facilitates content access. Also, it may enhance mobility support and intermittent connectivity

challenge that are difficult to provide through traditional IP networks, by merely re-requesting any unsatisfied request during the mobility and enabling vehicles to retrieve content from the most convenient cache store. Additionally, NDN follows a content-based security concept by protecting the content at the packet level instead of the communication channel level.

Security and privacy are one of the most critical aspects of the whole Internet and not only VANET. Bringing NDN in the vehicular environment has already been introduced in the literature [9]. However, most of the existing works focus on the NDN forwarding plane [10, 11] where the security solutions are rarely elaborated.

1.1. Motivation and Main Contributions. Despite the existing efforts on security, most of them did not consider the nature of VANET communication and attacks in their study [12]; they generally focused on denial of service (DoS) ignoring other attacks. Thus, the main motivation behind this work is to discuss and uncover VANET attacks and security issues from the NDN perspective. Also, as ICN/NDN and VANET merging is still on its first stage and taking a shape, it is quite important to focus on the security and privacy concerns in this phase. It is worth noting that we take VANET as the main network environment, studying its security issues using NDN as a communication model, and not the inverse. To our best knowledge, our work is the first one focusing on VANET security using NDN as a communication plane. Thus, we classify all existing VANET attacks and issues based on the NDN point of view. We overview each one of them and map it to NDN communication. Also, we provide research directions aiming to overcome these attacks and helping the research community to investigate more in this context.

1.2. Organization of the Paper. The rest of the paper is organized as follows: in the following section, we discuss the transaction from current host-centric vehicular networks toward the information-centric paradigm and overview the VANET and NDN architecture, focusing on security issues. Then, in Section 3, we categorize each VANET attack from the NDN perspective and present the existing efforts and summary for each category. Later, we highlight various future research directions in Section 4 and conclude our paper in Section 5.

2. From Host-Centric to Information-Centric Vehicular Networks

ICN is a new communication paradigm that aims to replace the current host-centric model. Shifting from the current IP-based solutions to ICN is not an easy task. Table 1 provides a comparison of host-centric and information-centric paradigms. Regardless of the deployment and transaction methods, mapping ICN communication logic to the existing Internet applications and networks needs more investigation. In this section, we present a quick overview of both VANET and NDN and discuss the mapping between them and the advantages that can be ported by NDN to the vehicular environment. Also, as this work focuses on security, we discuss also some of the security issues related to NDN design.

2.1. Vehicular Ad Hoc Network Overview. Vehicular ad hoc network (VANET) [13] is a part of mobile ad hoc network (MANET) where the node could be a *vehicle* or *roadside unit* (RSU) [14]. Vehicles exchange data with other vehicles (V2V), with RSU (V2I), or with charging stations, personal communication devices, and smart grids (vehicle to uniform) using different VANET applications. Each type of application has its particular features regarding content properties and the way the VANET applications consume it. These characteristics make VANET a challenging environment in terms of security and privacy.

2.1.1. VANET Security and Privacy Problems. As in any communication domain, security requirements in VANET should guarantee authentication, nonrepudiation, integrity, data availability, and confidentiality [15] in order to protect the exchanged messages in the network from modification, deletion, and delay by attackers. The vehicular communication characteristics and application properties have major effects on the security and privacy and make a more challenging environment. The security challenges caused by VANET characteristics are the following:

(1) *Scalability*. VANET is considered as an unbounded network that can be scalable from a small town to a big city until country [16]. It is growing larger and faster with no authority which makes the security enforcement and standardized rules and policies more challenging.

(2) *Mobility*. Due to the high speed of vehicles, the VANET topology can face quick and frequent changes, especially on the highway. Therefore, a very short connection duration and frequently disconnection may occur. Hence, it is very hard to prevent malicious nodes and mitigate attacks in time.

(3) *Time Constraints*. One of the most important of VANET's use cases is safety applications that aim to prevent crashes when an accident happens. These applications require reliable and real-time message delivery. However, due to the possibility of launching denial of service attacks, providing such time constraint services needs more efforts.

(4) *Data Dissemination*. Most of the information and messages in VANET are usually disseminated through vehicles; herein, several applications are vulnerable to attacks to modify, delete, or resend the information at the inappropriate time.

(5) *Privacy*. Preserving data and user privacy is an open issue in the whole Internet including VANET. Vehicles should trust the sender that may have an identity or not, as well as trust the intermediate forwarder vehicles. Thus, trade-off mechanisms are

Table 1: Comparison of host-centric and information-centric models.

Aspect	Host-centric model	Information-centric model
Addressing	(1) Host addresses (2) DNS for host resolution	(1) Content name (2) No DNS required
Routing	(1) Sends packets to the destination address (2) Stateless data plane (3) Point-to-point connectivity (4) Maintains one routing table (5) Routing is based only on the next hop information	(1) Uses Interest packets to fetch the data (2) Stateful data plane (3) Supports multipoint connection (4) Maintains three tables: FIB, PIT, and CS (5) FIB table contains multiple-hop information
Security	(1) Secures the communication channel	(1) Secures the content (content-based security)
Caching	(1) No caching concept	(1) Buffers data packets and reuses them
Mobility	(1) Resends packets to destination addresses	(1) Uses in-network caching and fetches data packets from the most convenient cache point

required between anonymity communication and privacy with the possibility to show real vehicle identity.

2.2. Named Data Networking Overview. Named data networking (NDN) [17] is a promising ICN architecture [18] that follows the content-based paradigm. NDN uses the content name to forward and deliver data between consumers and a producer, with a clean design based on the Interest-Data exchange model. Data packets are sent by a producer/replica node only when receiving an Interest packet triggered by the consumer for the existing content. Both Interest and Data packets contain the same content name.

Every NDN node maintains three data structures: content store (CS), pending interest table (PIT), and forwarding information base (FIB). The CS maintains the locally cached data that can be served for future requests, while the PIT is used to track the received Interest packets, aggregate them, and forward the Data packet downstream. It maintains *content name*, *list of incoming interfaces*, and *nonce* tuple. Similar Interests for the same requests are aggregated within the same PIT entry by pending only the received interface, whereas the FIB table acts as the routing database that contains a list of reachable prefix-names with the outgoing interfaces.

2.2.1. NDN Working Principle. Interest packets are triggered by consumers to discover the content in the network that can be satisfied by either a replica node or the original content producer, where a Data packet is used to deliver the content. Thus, the NDN working principle can be divided into two phases: Interest forwarding and Data forwarding, as illustrated on the right side in Figure 1:

(1) *Interest Forwarding*. When an NDN node receives an Interest packet, it checks its CS whether it already has the requested content. If the content exists on the CS, a Data packet is sent back using the same interface from where the Interest has arrived. Otherwise, PIT exact match is done. When a match is found, it means the same request has already been treated, and the interface name from where the Interest has been received will be appended to the PIT entry; otherwise, a new PIT entry is created for that request by recording the content name and the incoming interface and then performing the FIB longest prefix-name lookup: if a match is found, the Interest will be forwarded to the appropriate interface; otherwise, based on the network policies, the Interest will be either dropped or broadcasted to all interfaces.

(2) *Data Forwarding*. When a Data packet is created by a replica node or the original producer, it carries the same name as in the Interest packet. Hence, the NDN node checks its PIT to verify if the requests have already been treated by him; if a match is found, the Data packet will be sent out to all interfaces listed in the PIT entry (multicast). Otherwise, the packet is considered an unsolicited packet and dropped immediately by the node. During the Data forwarding, the node decides based on its local caching policies, if the content should be cached or not.

It is important to highlight here that all NDN components (CS, PIT, and FIB) are involved in the Interest forwarding phase, while only PIT and CS are used in the Data forwarding.

2.2.2. Security and Privacy in NDN. Preserving data security and preserving user privacy are the most important aspect of any of the today's network architecture and protocol [19]. As the content in NDN is decoupled from its original location, NDN follows a content-based security concept [20] that consists of securing the content among different network elements regardless of the used communication channel:

(1) *Security*. To ensure data authenticity, every Data packet is signed by the original producer using a public key. Thus, any node in the network can verify the data authenticity. Moreover, as Data can be cached in any place in the network, all necessary security-related information is traversed with the Data packets. Furthermore, data confidentiality and access control are supported by content encryption.

(2) *Privacy*. As compared to IP-based networks, any intermediate node can monitor user activities, by knowing who is requesting and what has been requested. However, in NDN, due to the use of

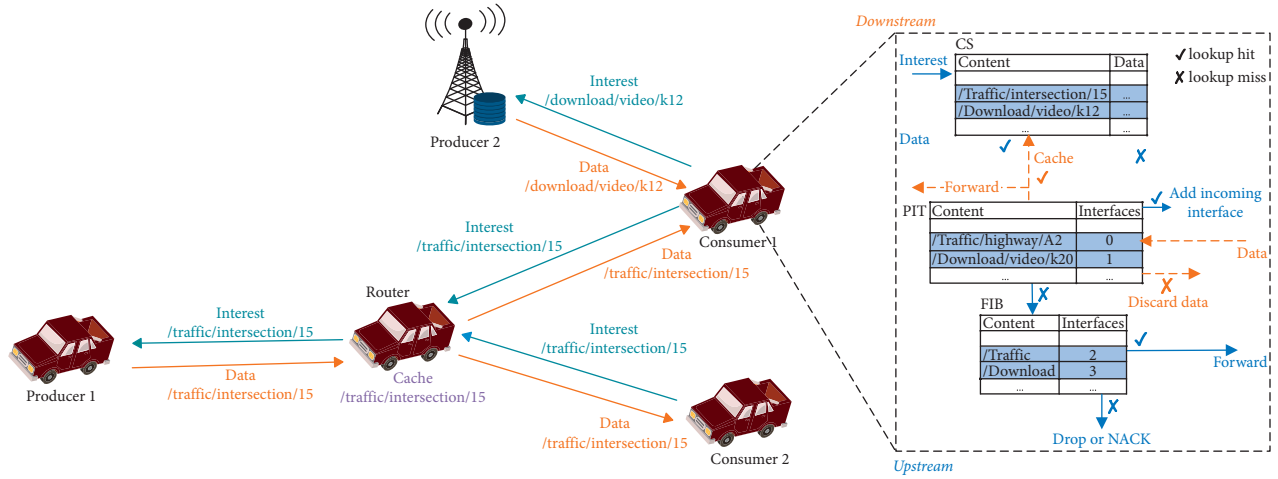


Figure 1: NDN-based VANET.

content names instead of host address, it is not an easy task to know who is requesting, but it is quite easy to know the requested content by monitoring the content names, where various attacks may be launched from different network levels using this vulnerability. Thus, both content and its name should be encrypted to provide high-level privacy.

2.3. NDN Advantages in VANETs. Due to the change of user and application requirements in today's Internet, NDN aims to improve the network scalability and reliability. Towards this, various efforts have been shown tending to bring NDN to vehicular environments [21, 22]. Vehicles in such a merging network can act as data consumers, producers, and intermediates nodes at the same time. Figure 1 shows an example or running NDN architecture on top of the VANET network.

2.3.1. Content Naming. NDN offers a clean, simple, and scale design that can support a large amount of content exchange among vehicles and with infrastructure. Hierarchical NDN names provide a wide addressing range that can be customized by network designers and carry different application semantics [23, 24]. Hence, different application properties can be integrated into the naming scheme to enhance the communication and improve users' needs.

2.3.2. Data Forwarding. The clean content discovery and data delivery mechanisms in NDN make it a suitable solution for VANET [25–27] that can improve the content access among multiple consumers by aggregating the Interests in the first edge node and inherently support multicast communication without the need of extra management protocols. Also, native support of multiple physical interfaces at the same time promotes the necessity of NDN.

2.3.3. In-Network Caching. The time and location decoupling concept in NDN enhances the data availability and improves the overall network performance [28–30]. Data producers are not required to be connected all time to satisfy consumer requests, where the network layer can fulfill different demands especially the hot ones, by retrieving the content from the most closer cache stores.

2.3.4. Data Security. NDN is a session-less architecture, where no session is required to fetch the content from producers or cache store. Also, all security mechanisms are applied to the content itself, by binding the content with its name using the public-private key concept. Hence, securing the communication channel in NDN is not an issue [31].

2.3.5. Mobility Enhancement. By using only the content name to fetch content from the network, NDN aims to enhance node mobility [32]. Mobile nodes are not required to ask for a new address when connecting with the new network. They only need to resend the nonsatisfied Interest by specifying the content name.

3. Security and Privacy Challenges in NDN-Based Vehicular Networks

By moving from a host-centric model to the information-centric concept and using NDN as the primary communication model in VANET, most of the traditional networking aspects will be changed. This also leads to changes in the security and privacy concerns [20]. Also, as ICN/NDN is still taking a shape, more issues will appear when running a large-scale NDN-VANET or fully deployed NDN without overlay protocols. Thus, it is very important to focus on security and privacy in the first design phase. In this section, we first discuss the security and privacy issues in the NDN architecture, and then we classify the existing VANET attacks based on NDN and target only those attacks affecting networking and NDN aspects such as content, routing and forwarding, and caching.

3.1. NDN Security and Privacy Issues. Despite the efforts shown in the NDN project and the research contributions, different security issues still exist in NDN [19]. In the following, we discuss briefly the most critical security issues.

As the network layer takes the responsibilities to satisfy the consumer requests via the ubiquitous in-network caching, different attacks may be launched from different network layers and entities for various goals such as interest flooding attack (due the use of content name), content poisoning attack, and cache poisoning/pollution attack (in-network caching). Hence, the NDN layer should tackle DoS attacks and validate the requested content name.

3.1.1. Content-Name Binding. The content name is the pillar element in ICN/NDN. All network-layer functionalities such as routing, forwarding, mobility, and security are based on the content name. The security of names reflects the network security. In NDN, content and name are bound and validated using the cryptographic function (e.g., public key and signature). Using this secure binding may prove the content ownership. However, in a large-scale network, content may be assigned to different names, which will affect the network scalability especially the routing plane. Thus, a secure control plane to assign names and validate content ownership is required.

3.1.2. Architecture Design. Despite the clean NDN architecture design, some security issues may occur. As NDN communication is based on content name where no host addresses are included, the use of one single interface such as a wireless interface on a vehicle or another device may create a problem of looping in both Interest and Data packets. Even adding a sequence number may solve this problem, however, and according to in-network caching, any node in the network may satisfy the demands. Assuming a malicious node receives all other demands because of the explicit broadcast, it can reply with false content and satisfy these demands, and other nodes in the same rang will receive the Data packets, that by consequence remove the PIT entry where the correct data will be considered unsolicited and dropped by the NDN forwarding plane. In such a scenario, the original requester receives wrong data and will never receive the correct content. Another issue can occur on a node with multiple interfaces: as the Data forwarding plane involves only PIT, a Data packet can be delivered from an interface not indexed in the FIB table but valid on the PIT. Malicious nodes may use this vulnerability to purge all demands on PIT.

3.1.3. Coexistence Issues. NDN can be deployed in three different modes: (a) overlay mode: running NDN on top of the TCP or IP protocol as an overlay layer; (b) coexistence with IP: a node may use the two stacks IP and NDN; and (c) clean-slate mode that consists of running NDN directly. The security of each mode depends on the security of the layer (e.g., IP or TCP). However, to show the real performance of NDN, a clean-slate deployment is required.

In the following sections, we classify VANET attacks into three categories: infrastructure attacks, content protection and access control, and content and user privacy. We overview each attack from both VANET and NDN perspectives and provide a review of existing solutions available.

3.2. Infrastructure Protection. Protecting the infrastructure will by consequence provide high availability and resilience by guaranteeing that only the accurate data are available. Although NDN does not address the hosts directly, securing the infrastructure hosts and endpoints is intuitive, as they are responsible for providing the content. Furthermore, as NDN allows a distributed content caching, this by consequence will increase the content availability and mitigate DoS attacks, which is not always applicable in case of dynamic content that may be generated dynamically only by its original provider.

3.2.1. Denial of Service. Denial of service (DoS) attack [33] is the most famous and dangerous one in the vehicular network, where the attackers send huge requests to the system in order to shut down the network and stop the communication between vehicles and between vehicles and RSUs. The goal of DoS is to stop sending or receiving information to vehicles about the network such as road status.

As NDN deals with content names instead of IP addresses, DoS attacks are based on the use of names [34] and may target consumers, producers, or intermediate nodes. From the NDN point of view, a basic DoS attack can be an *Interest flooding*, where an attacker sends a storm of Interest asking for a different content that may not be available in the cache store.

Figure 2 depicts a simple DoS attack; vehicles, RSUs, and other network infrastructure elements are involved in this scenario. However, due to the *Interest aggregation* feature, intermediate nodes may have more chance to be targeted compared to the content provider, especially when requesting a fake content (i.e., content with a valid name prefix and invalid suffix). The result of that is Interest dropping at the provider level and PIT entries after lifetime expiration at the intermediate nodes level. However, requesting a dynamic content that should be generated by the original content provider upon receiving the Interest (e.g., asking for a fresh patient report) may cause DoS at the provider level due to the fact that dynamic content is not popular and may not be aggregated by intermediate nodes.

A malicious vehicle sends a storm of different Interests asking for different content names, as RSU does not have the content, and it forwards the request and creates a new PIT. Because of the huge number of malicious Interests, the PIT is fitted, where a legitimate vehicle cannot send more requests, and may not benefit of the cache capabilities of the RSU or event forwarding its requests to other nodes. The attack is more severe when it comes to sensitive and urgent communications that may affect people's life.

Various countermeasure solutions have been proposed to overcome and mitigate DoS attacks, by using either rate-limiting mechanisms (e.g., per face or per name-prefix)

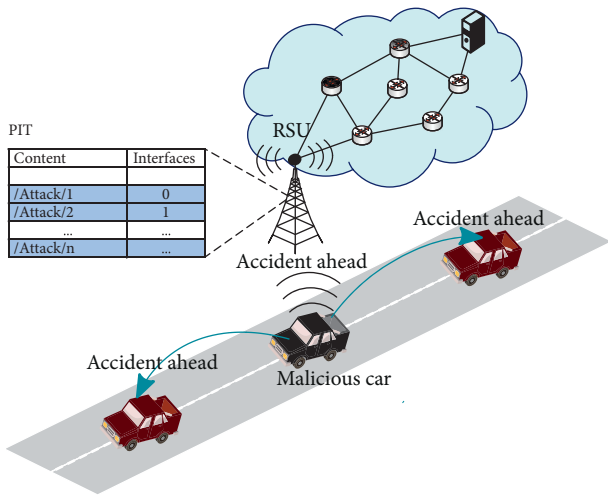


Figure 2: Denial of service attack.

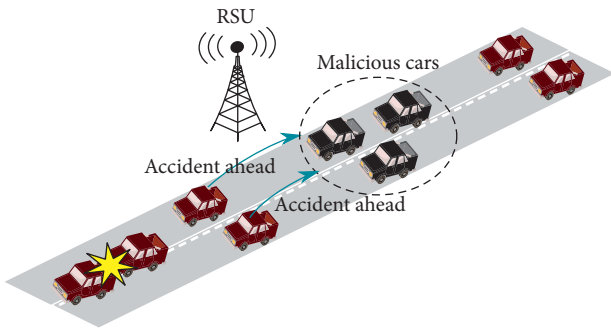


Figure 3: Black-hole attack.

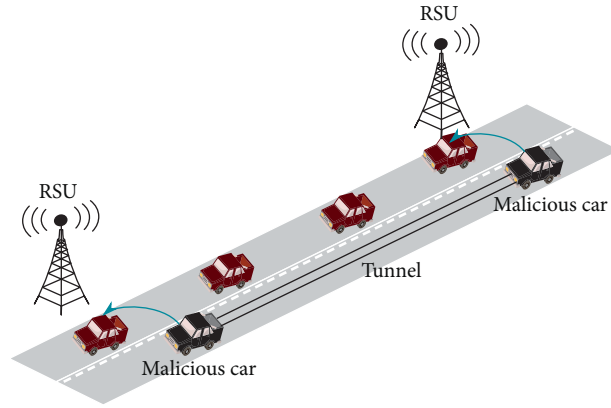


Figure 4: Wormhole attack.

In a nutshell, NDN uses a name-based forwarding scheme to forward the requests and deliver data back to consumers. Solving the black-hole and gray-hole attacks can be achieved either by securing the forwarding plane itself or by using secure namespaces to forward name-prefixes that do not exist in the FIB table. Furthermore, as the NDN forwarding plane forwards Interest/Data packets without knowing who is requesting or who will serve, these attacks may not affect VANET-based NDN even by announcing that they have the best route. However, as NDN uses hierarchical names to identify content and services, a malicious node can easily monitor the forwarding system and filter based on content names that allowed and denied packets, which makes these attacks hard to solve in such cases especially when a group of malicious vehicles launches the attack.

[35, 36] or statistical modeling approaches [37, 38]. The former consists of monitoring the face/name-prefix timeout rates and/or the PIT size, when detecting a DoS attack, and the router limits the interest arrival rate (IAR) on the suspicious face, while the latter relies on statistical information about the PIT and interfaces to identify the abnormal traffic pattern. However, these solutions need to make an extensive modification of the regular PIT structure or excessive storage statistics.

3.2.2. Black-Hole and Gray-Hole Attacks. Another dangerous attack, shown in Figure 3, that especially affects safety applications is the black-hole attack [39], where vehicle attackers engage other vehicles by claiming that they have the best route to the destination or have the best position to forward the packet. After the other vehicles send their packet to attackers, the malicious vehicle discards all packets from the network which caused lose of huge packets including critical information and safety messages. Similarly to the black-hole attack, in gray-hole attack, malicious vehicles act as black nodes and misguiding packets, filtering them according to their benefits. A single malicious node or a set of malicious nodes selects some packets to forward and drops others.

3.2.3. Wormhole Attack. The wormhole attack consists of creating a tunnel between two or more collaborative malicious vehicles, aiming to record and transmit data packets between them. Similarly to the black-hole attack, malicious vehicles engage other neighbor vehicles about the link between them as the best path to fetch the data instead of using the original trust path. After malicious vehicles receive packets from victim vehicles (Figure 4), they encapsulate and tunnel to another malicious vehicle, where the latter opens the encapsulated packets and spreads them in the network. The main objective of this attack is to change the network logical topology and make lose the important information that is sent through the tunnel, as well as creating a private network among the malicious vehicles. In an IP-based network, attackers use their IP addresses to create the tunnel. However, due to the use of names instead of addresses and forwarding packets without the need to know who is requesting and to whom should forward, wormhole attack may not be successfully executed in NDN-based networks.

3.2.4. Man-in-the-Middle Attack (MiMA). In man-in-the-middle attack, a malicious vehicle in the communication path keeps listing to all traversed information and injects

false information between vehicles. This attack, as shown in Figure 5, has serious effects on the safety applications especially if the injected information is about accidents that may cause life-endangering accidents.

Thanks to the content-based security, all information is signed by the original producer during its creation, and any changes in the data payload during the communication will be exposed to changes in the original signatures [40].

3.2.5. Summary and Insight. In this section, we have reviewed the existing VANET attacks that may affect the network infrastructure including DoS, black-hole, worm-hole, gray-hole, and man-in-the-middle attacks. We found that because of using the content name instead of host addresses, many issues can be overcome, especially when binding the content name with the shared information. Also, providing content security at the packet level enhances the communication security.

3.3. Content Protection. As each Data packet is self-signed in NDN, content requesters verify the content signature before consuming the content. Signature verification can also be done by intermediate nodes. However, it will cost more overhead and communication delay. The content signature may ensure *data integrity*, *authentication*, and *correctness*.

3.3.1. Bogus Information. In this type of attack, a malicious vehicle may generate false or wrong information and send it to the network in order to manipulate other vehicles. We find other attacks that can be classified as bogus information attacks, such as the following:

(1) *False Position Information*. Most of the safety applications are based on the particular position, where broadcasting false position information is a hard and critical issue in VANETs. A strong trust and validation model is needed to prevent such false information.

(2) *GPS Spoofing*. A malicious node utilizes the GPS satellite simulator to produce signals which are stronger than the actual satellite signals, tending to deceive vehicles to accept the false position information. This attack is related to physical devices. However, NDN should deal with trust in such data propagation, where collaborative vehicles may detect this information and stop it.

(3) *Illusion Attack*. Attackers disseminate wrong messages to create an illusion to vehicles by exploiting the current road conditions, like a group of cars moves slowly in order to deceive drivers to believe in this wrong information. This attack is hard to detect as the physical vehicle's sensors are used to create and spread the wrong traffic information.

Bogus information attack is usually associated with authentication security conditions, which is an easy task to deal with NDN, as the content is protected and authenticated at the packet level with a secure content-name binding

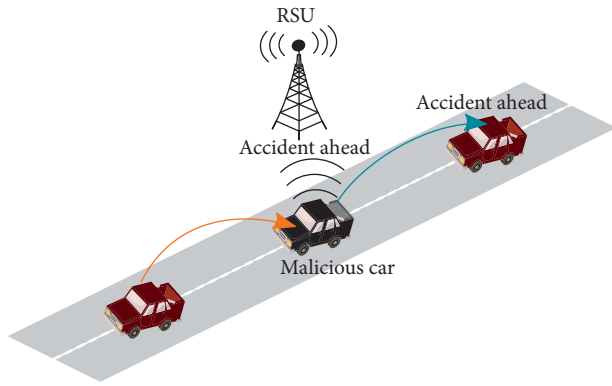


Figure 5: Man-in-the-middle attack.

of mechanisms based on hashing techniques and public-private keys.

3.3.2. Replay Attack. In the replay attack, a malicious vehicle saves a copy of the message and resends it later in the network in order to deceive other vehicles, making unnecessary stopping. As NDN is a cache-based network, this attack can be overcome by using the content name and checking the lifetime value in Data packets to know the data freshness, compared with the requested content.

3.3.3. Summary and Insight. Most of the existing NDN attacks related to content in VANETs can be solved by following the content-based security concept. Indeed, securing the content after its creation helps the content security life cycle. Also, when securing the content, access control rules and policies can be used to enforce who can access the content. Moreover, a robust trust model with the validation system is required in NDN to enforce content security and mitigate false content created by malicious nodes.

3.4. Content and User Privacy. Regardless of the content protection level, the user and content privacy still can be compromised in NDN, especially by using plain-text names. Any malicious node may receive the traversing requests and data back. By monitoring the content names, attackers can create a fake content and cache it in any near cache store, that by consequence will be served for future requests.

3.4.1. Sybil and Masquerade Attacks. Sybil attack is considered as one of the most dangerous attacks in VANETs, where the malicious vehicle acts that it is more than a hundred vehicles by creating chaos and a large number of pseudonymous as shown in Figure 6. The goal of this behavior is to deceive other vehicles that there is congestion and force them to change their routes. On the contrary, as the name indicates, in a masquerade attack, a malicious vehicle changes its identity [41] to be another vehicle, trying to produce different messages, alter, and replay with information to deceive other vehicles. For example,

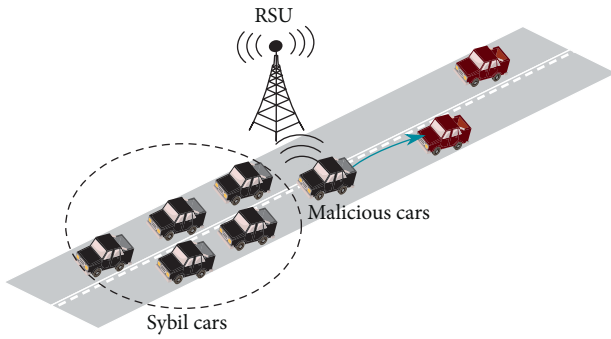


Figure 6: Sybil attack.

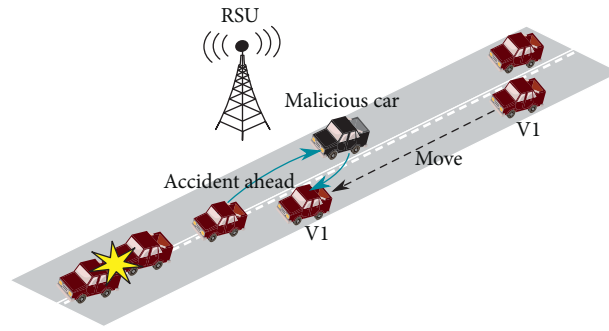


Figure 7: Timing attack.

a malicious vehicle can change its identity to be an ambulance and force other vehicles to slow down or change their routes. Works in [42, 43] propose a trust model based on NDN for autonomous vehicular applications in order to prevent bugs information and vehicle tracking. The authors designed a hierarchical naming scheme that composed of four levels: *autonomous vehicle*, *manufacturers*, *vehicles*, and *data*. Furthermore, they used a pseudonym and proxy-based scheme in order to make it difficult for attackers to track vehicles.

NDN binds content names using cryptography algorithms such as public-private keys that may secure the binding and outdo these issues. Furthermore, distributed solutions such as blockchain can be applied to enforce the content-name binding and preserve content and user privacy.

3.4.2. Timing Attack. In timing attacks, the malicious vehicles do not forward the emergency messages and information at the right time (Figure 7) they received it, by creating an explicit communication delay and adding time slots to the received messages. Their neighbor's vehicles receive these messages too late after the time they need it. The timing attack is a critical issue, especially when dealing with time-constraint applications.

3.4.3. Snooping Attack. Snooping is a passive attack, where the malicious vehicle accesses the content and information that traverse it, in order to use it for its benefits without modification. However, as the content is secure and signed, using cryptographic hashing techniques, when it has been created, only legitimate users can access it. Hence, snooping attack may not have an effect on VANET-based NDN.

3.4.4. Summary and Insight. Content and user privacy issues are presented in this part. Content privacy can be preserved using the content-name-binding mechanisms, and more investigation is required in such a context. Also, due to the illumination of host addresses, monitoring attacks can be decreased. The only issue that can occur because of NDN names is the caching-related attacks. Finally, serious solutions and secure forwarding schemes are required to overcome the timing attacks.

4. Future Research Directions

Based on the presented security attacks and issues and their relation with NDN, in the following section, we identify several NDN research directions that may enhance and improve the security of the NDN architecture. Table 2 summarizes this discussion.

4.1. Denial of Service. Solutions based on limiting Interest rate on the malicious interfaces or based on name-prefixes may end by punishing legitimate consumers and authorized requests. Hence, using the software-defined networking (SDN) approach [44] may detect DoS attack in the early stages using the global view of controllers and a per flow rate limiting that may yield highest fairness compared to interface/name-prefix-based solutions. Also, the core routers can collaborate to identify and filter the malicious name-prefixes and malicious traffic pattern using AI-based algorithms.

4.2. Content Poisoning. The purpose of this attacker is to fill the node's cache stores with fake contents. All the existing solutions require performing a data packet signature verification at the intermediate nodes level, that affects the content retrieval delay; comparing content hash with the hash taken from the corresponding Interest may reduce the network scalability, or ranking the content using consumers' feedback, where attackers also have the chance to send malicious feedbacks.

4.3. Naming and Content-Name Binding. Providing a secure naming scheme is still an open research challenge for ICN and NDN. A secure naming scheme should ensure an efficient and scalable binding between the name and the content that may avoid various types of attacks. All the existing binding schemes require signature verification for each and every data packet. This process is costly in terms of resources, as well as affects the data retrieval delay, where an intermediate node cannot perform it at the line speed rate.

4.4. Caching Pollution. The main objective of the caching pollution attack is to diminish the operation of in-network caching and augment content retrieval latency. The existing

Table 2: Summary of issues and research directions.

Category	Attacks	Compromised services	Target NDN aspects	Possible directions
Infrastructure protection	DOS	(1) Authentication (2) Availability	(1) Routing and forwarding plane	(1) Interface-based rate limit (2) Name-based rate limit (3) Statistical rate limit
	Black-hole and gray-hole	(1) Availability	(1) Routing and forwarding plane	(1) Securing the forwarding plane (2) Use of secure namespace
	Wormhole	(1) Confidentiality	(1) Data packets	(1) Use of content names instead of device identifications (2) Performing name-based forwarding
	Man-in-the-middle	(1) Authentication (2) Confidentiality (3) Integrity (4) Nonrepudiation	(1) Data packets (2) Forwarding plane	(1) Content-based security mechanism (2) Securing the content during the creation (3) Attaching access control policies with content
Content protection	Bogus information	(1) Authentication (2) Integrity	(1) Data plane	(1) Securing the content using cryptographic hashing techniques and public-private keys
	Replay	(1) Authentication (2) Integrity	(1) Data packet (2) Cache store	(1) Fetching content from the cache store based lifetime (2) Requesting only the fresh content
Content and user privacy	Sybil	(1) Authentication (2) Availability	(1) Routing and forwarding plane	(1) Securing content-name binding (2) Preserving blockchain-based identity
	Masquerade	(1) Authentication (2) Nonrepudiation (3) Integrity	(1) Routing and forwarding plane	(1) Preserving blockchain-based identity
	Timing attack	(1) Availability	(1) Data packets (2) Caching store	(1) Securing the forwarding plane (2) Trust-based forwarding scheme (3) Reputation-based caching and forwarding
	Snooping attack	(1) Authentication	(1) Data packets	(1) Applying content-based security mechanisms (2) Adding access rules within Data packets

solutions have a high computation overhead at intermediate nodes. We consider a collaborative caching scheme a suitable solution to help the core network to mitigate this attack by exchanging feedback between cache stores, keep only the popular content, and reduce the nonpopular ones.

4.5. Secrecy of Correspondence. Preserving the SoC and content copyrights is one of the most critical privacy topics in the whole networking domain and not only ICN [31]. From SoC perspectives, the content owner should state all privacy and content-use policies in the Data packet or in the content itself. We believe that the blockchain-like structure combined with the smart contract can be one of the promising solutions. The content owner specifies different smart contracts depending on the policies such as caching, providing, and consuming the content, that may be executed automatically when the action is triggered, to enforce SoC and content copyright.

4.6. Application Design Patterns. Several application-level security mechanisms have been proposed in ICN such as the following: (i) request filtering that intends to identify and remove the unwanted or forged content from untrusted providers, by using provider's information (e.g., public keys and name-prefix) and consumers' votes for content ranking. (ii) Anomaly detection aims to detect unwanted activities or network misbehavior, using statistical data analyses, fuzzy detection algorithms, and traffic clustering. However, there is no all-in-one scheme that deals with the existing application-level threats or discusses the design patterns for a secure application in ICN, which is a strong future research topic.

5. Conclusion

NDN architecture is a suitable candidate for the future Internet, including vehicular communication. Deploying NDN on top of VANET is still in the early phase. Security and privacy issues have a strong impact on the success of such merging. This article addresses the major networking security and privacy issues in VANET from the perspective of the NDN communication model. The nature of VANET communication and applications changes the way of seeing security; also, adding the NDN model on VANET makes the task more challenging. We categorized VANET security

challenges and discussed them from the NDN perspective. Also, we highlighted different NDN research directions and guidelines.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Hankuk University of Foreign Studies Research Fund of 2018 and National Research Foundation of Korea (2017R1C1B5017629).

References

[1] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of Network and Computer Applications*, vol. 37, pp. 380–392, 2014.

[2] F. Cunha, L. Villas, A. Boukerche et al., "Data communication in VANETs: protocols, applications and challenges," *Ad Hoc Networks*, vol. 44, pp. 90–103, 2016.

[3] T. Mekki, I. Jabri, A. Rachedi, and M. ben Jemaa, "Vehicular cloud networks: challenges, architectures, and future directions," *Vehicular Communications*, vol. 9, pp. 268–280, 2017.

[4] T. Mekki, I. Jabri, A. Rachedi, and M. B. Jemaa, "Proactive and hybrid wireless network access strategy for Vehicle Cloud networks: an evolutionary game approach," in *Proceedings of 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1108–1113, IEEE, Valencia, Spain, June 2017.

[5] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: a survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[6] J. Pan, S. Paul, and R. Jain, "A survey of the research on future internet architectures," *IEEE Communications Magazine*, vol. 49, no. 7, pp. 26–36, 2011.

[7] A. V. Vasilakos, Z. Li, G. Simon, and W. You, "Information centric network: research challenges and opportunities," *Journal of Network and Computer Applications*, vol. 52, pp. 1–10, 2015.

[8] L. Zhang, A. Afanasyev, J. Burke et al., "Named data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[9] Z. Su, Y. Hui, and Q. Yang, "The next generation vehicular networks: a content-centric framework," *IEEE Wireless Communications*, vol. 24, no. 1, pp. 60–66, 2017.

[10] M. A. Yaqub, S. H. Ahmed, S. H. Bouk, and D. Kim, "Interest forwarding in vehicular information centric networks: a survey," in *Proceedings of 31st Annual ACM Symposium on Applied Computing-SAC'16*, pp. 724–729, ACM, Pisa, Italy, April 2016.

[11] S. H. Bouk, S. H. Ahmed, D. Kim, K.-J. Park, Y. Eun, and J. Lloret, "LAPEL: hop limit based adaptive PIT entry lifetime for vehicular named data networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 5546–5557, 2018.

[12] S. Signorello, M. R. Palattella, and L. A. Grieco, "Security challenges in future NDN-enabled VANETs," in *Proceedings of 2016 IEEE Trustcom/BigDataSE/ISPA*, pp. 1771–1775, IEEE, Tianjin, China, August 2016.

[13] S. Boussoufa-Lahlah, F. Semchedine, and L. Bouallouche-Medjkoune, "Geographic routing protocols for Vehicular Ad hoc NETworks (VANETs): a survey," *Vehicular Communications*, vol. 11, pp. 20–31, 2018.

[14] D. Kim, Y. Velasco, W. Wang, R. Uma, R. Hussain, and S. Lee, "A new comprehensive RSU installation strategy for cost-efficient VANET deployment," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4200–4211, 2017.

[15] H. Sedjelmaci and S. M. Senouci, "Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution," *Journal of Supercomputing*, pp. 1–17, 2018.

[16] M. Laroui, A. Sellami, B. Nour, H. Moungla, H. Afifi, and S. Boukli-Hacéne, "Driving path stability in VANETs," in *IEEE Global Communications Conference*, Abu Dhabi, UAE, December 2018.

[17] L. Zhang, D. Estrin, J. Burke et al., *Named Data Networking (NDN) Project*, Relatório Técnico NDN-0001, Xerox Palo Alto Research Center-PARC, Palo Alto, CA, USA, 2010.

[18] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Communications Magazine*, vol. 50, no. 7, pp. 26–36, 2012.

[19] T. Chatterjee, S. Ruj, and S. D. Bit, "Security issues in named data networks," *Computer*, vol. 51, no. 1, pp. 66–75, 2018.

[20] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, privacy, and access control in information-centric networking: a survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 566–600, 2018.

[21] M. Amadeo, C. Campolo, and A. Molinaro, "Content-centric networking: is that a solution for upcoming vehicular networks?," in *Proceedings of Ninth ACM international Workshop on Vehicular inter-networking, systems, and applications*, pp. 99–102, ACM, New York, NY, USA, November 2012.

[22] S. H. Bouk, S. H. Ahmed, D. Kim, and H. Song, "Named-data-networking-based ITS for smart cities," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 105–111, 2017.

[23] S. H. Bouk, S. H. Ahmed, and D. Kim, "Hierarchical and hash based naming with compact trie name management scheme for vehicular content centric networks," *Computer Communications*, vol. 71, pp. 73–83, 2015.

[24] B. Nour, K. Sharif, F. Li, H. Moungla, and Y. Liu, "M2HAV: a standardized ICN naming scheme for wireless devices in internet of things," in *Proceedings of International Conference on Wireless Algorithms, Systems, and Applications*, pp. 289–301, Springer, Guilin, China, June 2017.

[25] X. Liu, Z. Li, P. Yang, and Y. Dong, "Information-centric mobile ad hoc networks and content routing: a survey," *Ad Hoc Networks*, vol. 58, pp. 255–268, 2017.

[26] M. F. Majeed, S. H. Ahmed, and M. N. Dailey, "Enabling push-based critical data forwarding in vehicular named data networks," *IEEE Communications Letters*, vol. 21, no. 4, pp. 873–876, 2017.

[27] S. H. Ahmed, S. H. Bouk, M. A. Yaqub, D. Kim, and H. Song, "DIFS: distributed interest forwarder selection in vehicular named data networks," *IEEE Transactions on Intelligent Transportation Systems*, 2017.

[28] M. A. Yaqub, S. H. Ahmed, and D. Kim, "Asking neighbors a favor: cooperative video retrieval using cellular networks in VANETs," *Vehicular Communications*, vol. 12, pp. 39–49, 2018.

[29] H. Khelifi, S. Luo, B. Nour, A. Sellami, H. Moungla, and F. Naït-Abdesselam, "An optimized proactive caching scheme based on mobility prediction for vehicular networks," in *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Abu Dhabi, UAE, December 2018.

[30] B. Nour, K. Sharif, F. Li, H. Moungla, A. E. Kamal, and H. Afifi, "NCP: a near ICN cache placement scheme for IoT-based traffic class," in *Proceedings of IEEE Global*

Communications Conference (GLOBECOM), pp. 1–6, Abu Dhabi, UAE, December 2018.

[31] C. Ghali, G. Tsudik, and C. A. Wood, "When encryption is not enough: privacy attacks in content-centric networking," in *Proceedings of 4th ACM Conference on Information-Centric Networking*, pp. 1–10, ACM, Berlin, Germany, January 2017.

[32] J. M. Duarte, T. Braun, and L. A. Villas, "Source Mobility in Vehicular Named-Data Networking: An Overview," in *Proceedings of 9th EAI International Conference on Ad Hoc Networks*, pp. 83–93, Springer, Niagara Falls, ON, USA, March 2018.

[33] S. M. Specht and R. B. Lee, "Distributed denial of service: taxonomies of attacks, tools, and countermeasures," in *Proceedings of 17th International Conference on Parallel and Distributed Computing Systems*, pp. 543–550, San Francisco, CA, USA, September2004.

[34] M. Aamir and S. M. A. Zaidi, "Denial-of-service in content centric (named data) networking: a tutorial and state-of-the-art survey," *Security and Communication Networks*, vol. 8, no. 11, pp. 2037–2059, 2015.

[35] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," in *Proceedings of 2013 IFIP Networking Conference*, pp. 1–9, IEEE, Brooklyn, NY, USA, May 2013.

[36] H. Dai, Y. Wang, J. Fan, and B. Liu, "Mitigate ddos attacks in NDN by interest traceback," in *Proceedings of 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 381–386, April 2013.

[37] K. Wang, J. Chen, H. Zhou, and Y. Qin, "Content-centric networking: effect of content caching on mitigating dos attack," *International Journal of Computer Science Issues*, vol. 9, no. 6, pp. 43–52, 2012.

[38] T. Nguyen, R. Cogranne, and G. Doyen, "An optimal statistical test for robust detection against interest flooding attacks in ccn," in *Proceedings of 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 252–260, IEEE, Ottawa, Canada, May 2015.

[39] F.-H. Tseng, H.-P. Chiang, and H.-C. Chao, "Black hole along with other attacks in MANETs: a survey," *Journal of Information Processing Systems*, vol. 14, no. 1, 2018.

[40] C. Ghali, A. Narayanan, D. Oran, G. Tsudik, and C. A. Wood, "Secure fragmentation for content-centric networks," in *Proceedings of IEEE 14th International Symposium on Network Computing and Applications (NCA)*, pp. 47–56, IEEE, Cambridge, MA, USA, 2015.

[41] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for Vehicular Ad-Hoc Networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2017.

[42] M. Chowdhury, A. Gawande, and L. Wang, "Anonymous authentication and pseudonym-renewal for VANET in NDN," in *Proceedings of 4th ACM Conference on Information-Centric Networking*, pp. 222-223, ACM, Berlin, Germany, January 2017.

[43] M. Chowdhury, A. Gawande, and L. Wang, "Secure information sharing among autonomous vehicles in NDN," in *Proceedings of Second International Conference on Internet-of-Things Design and Implementation*, pp. 15–25, ACM, Pittsburgh, PA, USA, April 2017.

[44] A. Alioua, S.-M. Senouci, S. Moussaoui, H. Sedjelmaci, and A. Boualouache, "Software-defined heterogeneous vehicular networks: taxonomy and architecture," in *Proceedings of Global Information Infrastructure and Networking Symposium (GIIS)*, pp. 50–55, IEEE, Saint Pierre, Reunion Island, France, October 2017.

Hindawi
Mobile Information Systems
Volume 2018, Article ID 6874158, 10 pages
https://doi.org/10.1155/2018/6874158

Research Article

Incentive Mechanism of Data Storage Based on Blockchain for Wireless Sensor Networks

Yongjun Ren[1,2], **Yepeng Liu**[1,2], **Sai Ji**[1,2], **Arun Kumar Sangaiah**[3] and **Jin Wang**[4]

[1]*School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing, China*
[2]*Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET), Nanjing University of Information Science & Technology, Nanjing, China*
[3]*School of Computing Science and Engineering, Vellore Institute of Technology (VIT), Vellore, India*
[4]*School of Computer & Communication Engineering, Changsha University of Science & Technology, Changsha, China*

Correspondence should be addressed to Jin Wang; jinwang@csust.edu.cn

Received 20 April 2018; Accepted 5 August 2018; Published 29 August 2018

Academic Editor: Yuh-Shyan Chen

In this paper, the blockchain technology is utilized to build the first incentive mechanism of nodes as per data storage for wireless sensor networks (WSNs). In our system, the nodes storing the data are rewarded with digital money. The more the data stored by the node, the more the reward it achieves. Moreover, two blockchains are constructed. One is utilized to store data of each node and another is to control the access of data. In addition, our proposal adopts the provable data possession to replace the proof of work (PoW) in original bitcoins to carry out the mining and storage of new data blocks, which greatly reduces the computing power comparing to the PoW mechanism. Furthermore, the preserving hash functions are used to compare the stored data and the new data block. The new data can be stored in the node which is closest to the existing data, and only the different subblocks are stored. Thus, it can greatly save the storage space of network nodes.

1. Introduction

Wireless sensor network (WSN) has become very hot research topic recently in the field of microelectronics, communication, network, database, etc., because of its broad application prospects. It combines multiple technologies, such as sensing, computing, and wireless communication. The physical targets are monitored in real time through various types of microsensors, producing a large number of perceptual data at an unprecedented rate. Although the application scenarios and the deployment of hardware are different, the ultimate goal is to collect, transmit, and process the perceived data. Finally, users can achieve interesting information from the data [1, 2].

The wireless sensor network is a data-centric network. Therefore, the data storage of nodes is the fundamental problem in WSN, which should be solved. For the users, what they concerned are the perception of the data, rather than the sensor node itself and the networks they make up. Furthermore, the wireless sensor networks support efficient and reliable data storage and access under the heterogeneous, unreliable environment. As the storage space and energy of each node are limited, how to effectively store data in the limited storage space has been an important research hot spot of data management in WSN.

The normal operations of WSN require the cooperation of network nodes. However, some network nodes may choose selfish behavior due to their limited resources, such as energy and storage space. If most network nodes take selfish behavior and do not forward packets, the entire network will not be able to provide normal service. Therefore, inciting selfish nodes to cooperate and ensuring the normal operation of the entire network are part of the important researches in WSN.

Traditionally, the solutions to the selfishness problem of nodes in WSN have based on the mechanisms of game theory and the mechanisms based on reputation. But the researches mainly focus on data transmission and packet

forwarding. Moreover, now there is no specific incentive mechanism of data storage for nodes in WSN.

The storage capacity of nodes in WSN is limited, and the data storage capacity is also an important resource. This paper focuses on the incentive of data storage in WSN. In this paper, the blockchain technology is adopted to construct the first incentive mechanism of nodes' data storage in WSN. In our system, the data set which is storing every node is considered as a block of the blockchain. If the nodes store the data, they will be rewarded with digital money (bitcoins, etc.). Additionally, if the nodes store more data, they will attain more rewards. When mining and storing new data blocks in progress, we apply the provable data possession instead of the proof of work (PoW) in original bitcoins. The method can greatly reduce the computing power of the miners. Apart from this, comparing the existing data in nodes with the new data block, we can take advantage of the preserving hash functions. The node stores the new data, which is closest to the existing data, and only the distinct subblocks need to be stored. So, it greatly saves the storage space of network nodes.

The rest of this paper is organized as follows. Section 2 introduces the related works of data storage strategy in WSN and incentive mechanism. In Section 3, we analyze the existing problem of data storage in WSN. Section 4 presents the building blocks of our scheme based on the blockchain. And in Section 5, the incentive mechanism of data storage based on blockchain in WSN is proposed. Finally, Sections 6 and 7 present the discussion and conclusions of this paper, respectively.

2. Related Work

2.1. Data Storage Strategy in WSN. At present, there are three main ways of data storage in WSN: external storage, local storage, and data-centric storage [3].

2.1.1. External Storage. Sink node is a special kind of storage node, and its storage space and energy are not restricted and do not need to consume another node energy. Other nodes will send the collected data to the sink node, which will consume a lot of energy. If all the nodes in the network send data to the sink node, it will cause the network block and the nearby sink nodes will be invalid.

The LEACH protocol is proposed to collect data from the hierarchical sensor network, in which a subset of nodes is randomly selected as cluster heads, and the other nodes added different cluster according to the calculated distances between the nodes and the cluster heads. During a period, the nodes transmit data to the cluster heads, and the cluster heads process the data and then sends them to the sink nodes. The PEGASIS protocol [4] improved the LEACH protocol, in which the sensor network was organized into a chain structure. Each node receives and forwards data by its neighboring nodes. The sink nodes only select one other node to communicate with it. The data are aggregated in the process of forwarding from a node to the next node and eventually reaching the sink node. Thus, the consumed energy in the PEGASIS protocol is less than that in LEACH. Wang et al. also proposed a new protocol [5], which is an improvement to the LEACH protocol. The protocol establishes the soft and hard threshold, which can dynamically adjust and compare the collected data to reduce unnecessary data transmission. When the node data are above the hard threshold, the data are transmitted and they are taken as a new hard threshold.

The storage strategy of external storage is mainly focused on data acquisition, ignoring the data storage ability of WSN and the demand of nodes for data.

2.1.2. Local Storage. In local storage, the data are stored in nodes of the network, which consumes little energy. The query commands are only sent to the other nodes. After the node receives the query and processes it, the result is passed to the sink node. So, queries consume longer delays.

The directed diffusion protocol stores the data collected by the nodes in the local nodes. The sink nodes achieve their information by broadcasting the "interest message" to the other network nodes. The node that received the message creates a gradient within the network, pointing to the sink node. The node establishes one or more paths to the sink nodes, doing flood search and performing data transmission. The geographic and energy-aware routing (GEAR) protocol [6] is the improvement of the directed diffusion protocol. In GEAR protocols, when a query message is sent in the target area, the propagation of the "interest message" is limited to the target area because of the geographical location, which avoids flooding in entire network and reduces the cost of routing.

The storage process of local storage strategy is simple. And the strategy focuses on data query processing and has less description of information, which leads to a lot of energy in the query process.

2.1.3. Data-Centric Storage. The data-centric storage is a hot research direction in recent years. It mainly studies how to store the perceived data of sensor nodes so as to ensure the high efficiency, stability, and real-time performance of the later query.

The concept of data-centric storage (DCS) is proposed by Meyfroyt et al., and the data storage algorithm GHT is designed based on the geographic information mapping table [7]. Its core idea is that data are stored according to their attributes, and a specific data are defined as an event. The sensor detects the data, hashes the event through a hash function, then achieves a geographic location, and saves the data to the nearest node based on the geographic information [8]. The algorithm is conducive to data query, which is only based on the query event attributes. And the use of mapping function can be found in the storage node, which avoids flooding. The disadvantage of the algorithm is the lack of efficient storage hot spot processing mechanism. When the data storage overloads, it cannot be transferred to another node. Moreover, accessing geographic information needs GPS and consumes system energy. In the data storage algorithm ARI [9], adaptive ring index structure is used to

solve the hot spot problem of the DCS algorithm. And hash functions are utilized to hash a certain type of event to the event storage node. A ring is created around the event storage node, and events are dispersed and stored in the index nodes. In general, it is difficult to define clear demarcation of a wireless sensor network, which is not ideal for hot spot problems. In data storage algorithm of Reference [10], two-tier data storage structure is used to track the moving target of the mobile multisink node in the WSN. Data are transferred and stored through the creation of virtual grids in the algorithm. When the data collected by the grid storage nodes are queried, it is just needed to flood the request within the grid, which will save energy. In addition, some scholars have proposed a distributed index structure algorithm (DIFS) [11]. DIFS is an improvement of the TTDD algorithm. In DIFS, multilevel quadtree is constructed based on spatial decomposition technique and hash function, and the geography hash method is used as the index of data [12, 13]. The corresponding node stores the observed data through hash functions, and it can determine the range of the minimum number of index nodes by the query range.

2.2. Incentive Mechanism. At present, there are two main incentive mechanisms. One is based on game theory. The other is based on external incentives [14–20].

2.2.1. Incentive Mechanism Based on Game Theory. In the paper [14], the concept of multidomain wireless sensor network was first proposed, and the game theory was used to evaluate the impact of cooperative behavior. In the system, the participants in game analysis are the various individual wireless sensor networks, and it is assumed that each wireless sensor network has to make decisions: whether to help other networks to carry out data transfer and whether to request other networks to help its data transmission, which is the strategy of each participant in game analysis. On the basis of the above mechanism, the problem was continued to study the cooperative behavior among networks in multidomain wireless sensor networks [15]. The main differences in the game analysis are as follows: (1) the income function of the game is mainly expressed by the whole life cycle number of the network [16], rather than the calculation of the accumulated revenue of nodes and (2) the strategy of the sensor node is more intelligent. The choice of actions will be limited after many unsuccessful data transfers so that the network has minimal QoS guarantee. References [17, 18] analyzed the impact of different cooperation strategies on the life cycle of multidomain wireless sensor networks. The author proposes a linear design framework and uses the corresponding one-dimensional and two-dimensional linear models to assess the performance of different strategies. Based on the ideal conditions, the author adds various restrictions to observe the influence on the cooperation strategy. Simulation experiments have confirmed that cooperation can significantly extend the life cycle of the network. And under some special circumstances, some cooperative strategies can increase the life cycle to an order of magnitude.

2.2.2. Incentive Mechanism Based on External Incentives. In addition to the use of game theory to analyze the multidomain wireless sensor network, there are some researches of external incentive mechanisms. The main external incentive methods include virtual currency mechanism and honor incentive mechanism. In [19–21], an economic model of dynamic prices and incentive methods is proposed to study the cooperation in multidomain wireless sensor networks. And the proposed economic model and the traditional routing protocol AODV protocol [22] are merged into a hybrid protocol for simulation experiments. In the simulation experiment, the author compared the proposed NES method with other EES methods and PDM [23]. The experimental results confirm that the cooperation between the sensor networks will be enhanced, and the overall energy consumption in the network will be significantly reduced.

3. Problem Statement

The development of wireless sensor networks originated from military applications, such as battlefield monitoring. Nowadays, wireless sensor networks have been applied to many civilian applications, such as environmental and ecological monitoring, healthcare, home automation, and traffic control.

In the sensor network, nodes are deployed in a variety of ways within or around a perceived object. These nodes form a wireless network through self-organization method. And they can sense, collect, and process specific information in a cooperative way within the coverage area. Finally, it can realize the collection, processing, and analysis of any location information at any time. Each node of the sensor network is not only equipped with a radio transceiver but also a small microcontroller and an energy source (usually a battery), in addition to multiple sensors. The size of a single sensor node is as large as a shoe box, as small as dust. The size and complexity of the restrictions for sensor nodes determine the constraints of energy, storage, computing speed, and bandwidth. In large sensor networks, the sensor and network structure are different. Thus, the integration of heterogeneous networks often occurs in sensor networks. At the same time, the heterogeneous network structure also brings difficulty to data storage and sharing in WSN.

Moreover, the data storage capacity is also an important resource. But the storage capacity of nodes in a wireless sensor network is limited. Some network nodes give up storing data in order to save their own storage and energy resources, which are called selfish behavior. If the most network nodes behave selfishly and do not store data, then the entire network will not be able to provide normal service.

To solve the problem, we use incentive mechanisms based on blockchain to encourage network nodes to store data. The data storage based on the blockchain technology can not only provide the corresponding data storage function but also reward the digital currency to the network node that stores data. Therefore, data storage based on the blockchain technology in WSN is very suitable.

4. Building Blocks

4.1. Blockchain Technology. The blockchain system contains the following important components: underlying transaction data, distributed ledgers, important consensus mechanism, complete and reliable distributed P2P network, and distributed application on the network. And the framework is shown in Figure 1. The underlying data are organized into blocks, and each block is chained into a chain in the chronological order, which is called blockchain [24–26]. Each node of a fully distributed network stores a distributed ledger, that is, blockchain. The P2P protocol is used in the network to communicate with each other. All parties will reach agreement through consensus mechanisms. Advanced applications are generated based on these foundations. In the architecture, the nontampering blockchain data structure, the consensus mechanism in distributed network, the proof of work mechanism, and the increasingly flexible smart contracts are representative innovations [27, 28].

The underlying data are not stored in the blockchain. The raw data need further processing so that they can be written into the block. The underlying data are the most fundamental transaction records; the other data are only intended to encapsulate the message records. The network layer encapsulates the networking mode of the blockchain system, the message propagation protocol, and the data authentication mechanism. Combining with the practical application requirements and designing the specific propagation protocol and data verification mechanism, each node in the blockchain system can participate in the checksum accounting process of the block data. Only when the block data are verified by most nodes in the whole network, the block is recorded in the blockchain [29–31].

The PoW mechanism is an important innovation that closely integrates the functions of currency issuance, transaction payment, and verification. And the safety and decentric of the blockchain system are ensured through the competition of computing force. The core idea is to ensure the consistency of data and the security of the consensus by the computing force competition of distributed nodes. In the bitcoin system, the miners work together to solve a complex but easy-to-valid SHA-256 mathematical problems (i.e., mining) based on their respective computer forces. The nodes that solve the problem the fastest will get the right to account the block and bitcoin reward. The mathematical problem can be expressed as follows. Based on the current difficulty value, a suitable random number (Nonce) is sought so that the double SHA-256 hash of the metadata of the block header is less than or equal to the target hash value. However, the PoW consensus mechanism has a significant flaw: the waste of resources (such as electricity), caused by their strong computing power, has always been criticized by researchers [32–34].

The consensus process of the blockchain system realizes the data validation and accounting of shared blockchain ledgers by aggregating the computational power resources of large-scale consensus nodes, so it is essentially a task crowdsourcing process of consensus nodes. In the decentralized system, the consensus nodes themselves are selfish, and maximizing its own revenue is the fundamental goal of its participation in data validation and accounting. Therefore, it is necessary to design a reasonable and well-conceived mechanism of incentive and compatibility so that the individual rational behavior of the consensus node maximizing its own income is consistent with the overall goal of guaranteeing the safety and effectiveness of the decentralized blockchain system. The blockchain system integrates large-scale nodes and forms a stable consensus on the history of the blockchain by designing a modest economic incentive mechanism and integrating with the consensus process.

The contract layer is business logic and algorithm based on the blockchain virtual machine, which is the basis for realizing the flexible programming and operation data of the blockchain system. The smart contract has important significance to the blockchain system, which not only provides the programmable capabilities to the underlying data of the blockchain but also encapsulates the complex behavior of each node in the blockchain network. And it provides a convenient interface for building an upper application based on blockchain technology. Thus, blockchain technology with smart contract is extremely broad prospects.

4.2. PDP Mechanism. Provable data possession (PDP) mechanism is used to determine whether the data on the remote node are damaged (Figure 2). The PDP mechanism was first used in grid computing and P2P networks. He et al. constructed the PDP mechanism using RSA-signed homomorphic properties, but this mechanism requires that the entire file is represented by a large number, which results in high computational costs. Wang et al. proposed a probabilistic strategy to complete the integrity verification, using the homomorphic properties of the RSA signature mechanism to aggregate the evidence into a small value, greatly reducing the communication overhead of the protocol [35–38]. Wang et al. realized another mechanism that supports full dynamic operation of the PDP mechanism. It considers the use of the Merkle hash tree in order to ensure the correctness of the data block in position, and data block value ensures its correctness through the BLS signature mechanism [39–42]. In order to reduce the burden on the user, the mechanism also introduces an independent third party instead of the user to verify the integrity of outsourced data. In this article, this algorithm is used to replace the PoW mechanism in the original blockchain.

The PDP scheme is as follows. At first, encode M into M' so that each data block m_i of M' contains s data segments, that is, $m_i = (m_{i,1}, m_{i,2}, \ldots, m_{i,s})$. The metadata σ_i are calculated for each data block m_i as follows:

$$\sigma_i = \left(H(\text{name}||i) \times \prod_{j=1}^{s} u_j^{m_{i,j}} \right)^{\alpha}, \tag{1}$$

where α is the private key of the user and $u_j\,(1 \le j \le s)$ is randomly selected from the bilinear group G. Similar to the

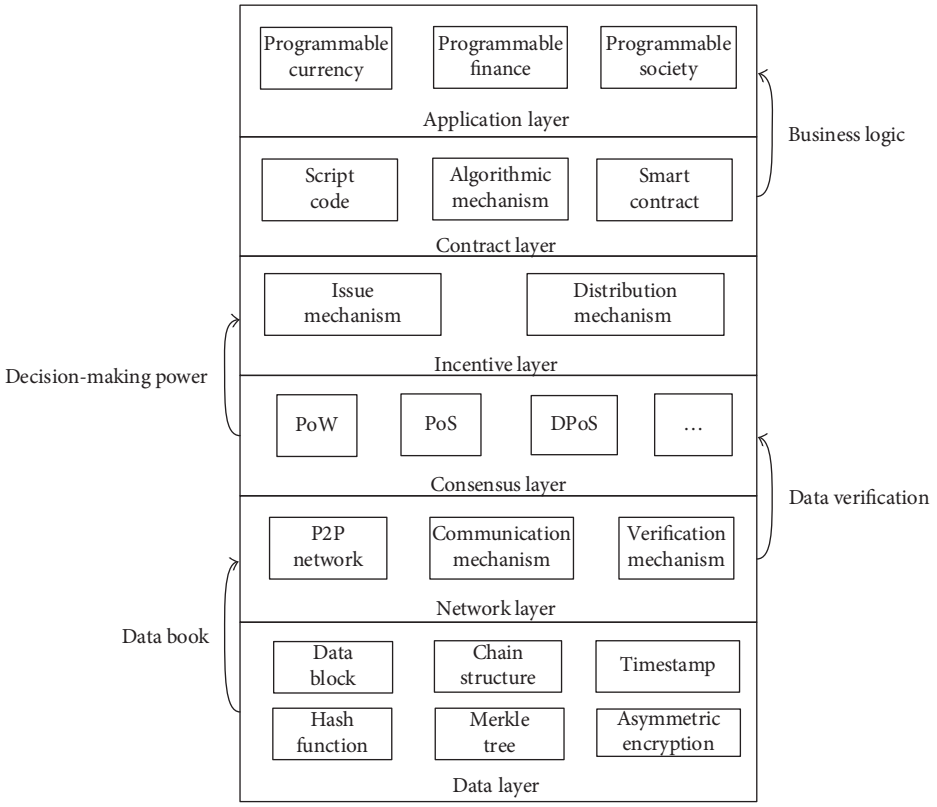


Figure 1: A basic framework of blockchain.

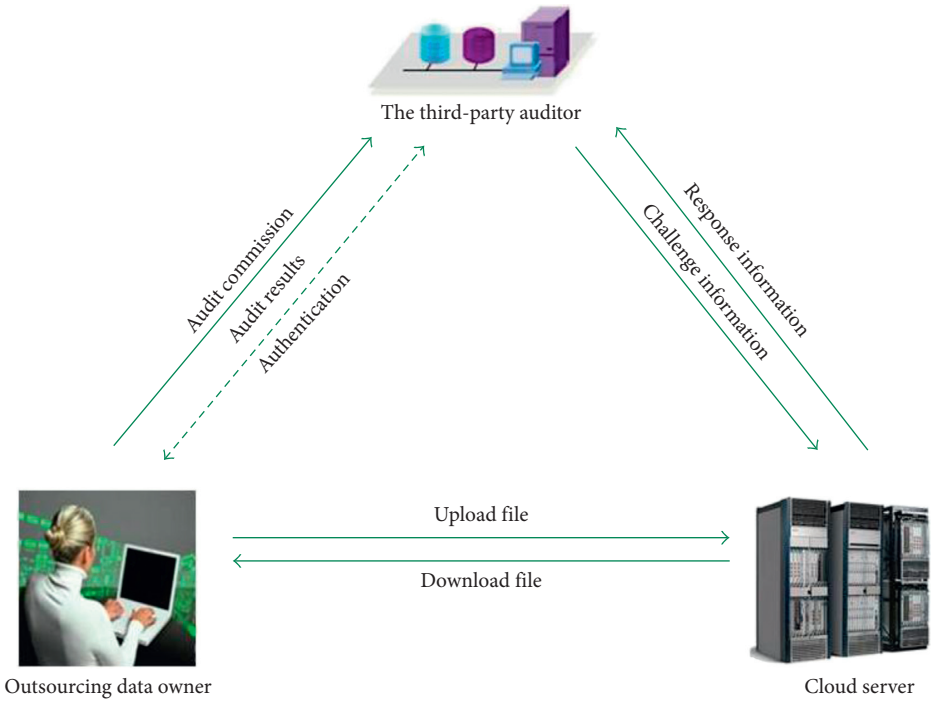


Figure 2: Provable data possession.

literature [4], the factor $(\prod_{j=1}^{s} u_j^{m_{i,j}})^{\alpha}$ contained in the metadata σ_i also supports the aggregation operation. So, the cloud storage server can generate the corresponding partial aggregation in the integrity verification phase. The algorithm also signs the data name, the number of data blocks, and the parameter u_j to obtain a tag of data r.

To verify the integrity of the outsourced data, a query challenge $C = \{(i, v_i)\}$ is submitted by the verifier, including the block number i which is randomly selected and the corresponding coefficient v_i. The cloud server calculates aggregated data blocks $\mu = (\mu_1, \mu_2, \ldots, \mu_n)$ and metadata σ as the proof, that is, (μ, σ), where $\prod_{(i,v_i)\in C} \sigma_i^{v_i}$ is the metadata, the aggregated data blocks is $\mu_i = \sum_{(i,v_i)\in C} v_i m_{i,j}$.

Verification is done by checking the following formula and performing two bilinear operations:

$$e(\sigma, g) = e\left(\prod_{(i,v_i)\in C} H(\text{name}||i)^{v_i} \times \prod_{j=1}^{s} u_j^{\mu_i}, v\right), \quad (2)$$

where v is the user's public key corresponding to α.

In the above scheme, Shacham and Waters double the data for the first time so that each data segment $m_{i,j}$ corresponds to a data block of the aforementioned scheme. This segmentation strategy has the obvious advantage that by generating metadata for a set of data segments, the size of the processed data can be reduced, thereby reducing the storage costs of the cloud server.

5. Incentive Mechanism of Data Storage Based on Blockchain in Wireless Sensor Network

In this paper, the blockchain technology is utilized to build the first incentive mechanisms of nodes' data storage in WSN. In our system, the data set stored by every node is treated as a block of the blockchain. The nodes storing the data are rewarded with digital money (bitcoin, etc.). Moreover, the more the data stored by the node, the more the reward it achieves. Our proposal adopts the provable data possession to replace the proof of work (PoW) in original bitcoin to carry out the mining and storage of new data blocks. The method can greatly reduce the computing power by PoW mechanism. Furthermore, the preserving hash functions are used to compare the stored data and the new data block. Thus, the new data can be stored in the node which is closest to the existing data, and only the different subblocks are stored. So, it can greatly save the storage space of network nodes.

5.1. Blockchain of Data Storage for Sensor Node. The sensor network is often composed of multiple heterogeneous subsystems, and various network nodes have different capabilities in computing, energy, communication, and storage. In addition, the network nodes which using different types of sensors make the types of collected data varied. Therefore, the shared data storage mechanism should be adopted to realize the storage and management of the data in wireless sensor network. The blockchain has the advantage of decentralization. Moreover, the data storage based on decentering credit can be realized in the WSN, where the node does not need to be trusted using the encryption algorithm, time stamp, tree structure, consensus mechanism, and reward mechanism. Each network node can use the Merkle tree in the blockchain to store its data. The data of the nodes are stored in the leaves of the Merkle tree. Each stored datum can be a block, and all the data stored by the nodes are linked to form the data blockchain (Figure 3).

5.2. Trust Management of Network Node. In the system, the trust of network nodes is managed. When the network node is found to be fraud and with other behaviors, it is removed from the WSN network. We use the reputation system to manage the nodes in WSN. Once the network node is found cheating, it will be immediately excluded from the WSN.

In the system, the trust of the data initiator (node i) in the network to the data store (node j) can be obtained by calculating the number of success and failure of the node data storage in a certain period of time. After the kth data storage is successful, d_{ij}^k indicates the trust evaluation value of the data initiator node i to the data store node j; $\delta\,(0 \le \delta \le 1)$ is the time attenuation coefficient of the trust, which is used to reflect the influence degree of trust for the network node in data storage procession. The larger the weight of the recent score record, the greater the weight of the calculation of the trust value, as shown in the following equation:

$$d_{ij}^k = \sum_{m=1}^{k} \delta_m d_{ij}^m. \quad (3)$$

In the system, the trust of data storage between node i and node j is divided into five levels according to the satisfaction degree, and 0, 0.25, 0.5, 0.75, and 1 are assigned in turn. The first level indicates that the data storage between the network node i and the network node j is failure, and the node i considers the node j is malicious. The second, third, fourth, and fifth levels of trusts are sequentially increased. The fifth level is the highest level, indicating that the data storage between the network node i and the network node j is successful, and that the node i fully trusts the node j. When there is a data storage relationship between the two nodes i and the node j, the degree of trust of node i to node j is calculated using Equation (1). When there is no direct transaction between the two nodes, use the following formula to calculate the average trust of the network as the recommended trust degree of node:

$$d_0 = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{k} d_{ij}^k}{n^2 \sum_{k=1}^{k} k}. \quad (4)$$

Most nodes in the network play dual role. One role is consumer, who is provided with storage service in the system. Another is the service provider, who provides storage service for other nodes. As a consumer, the trust evaluation of network nodes to other nodes is always considered accurate and deterministic. Therefore, the node modifies the data in the table with minimal possibility. Even if making a recommendation for a particular node, it does not make sense. In addition, it is safe to locally store the relevant calculated data of the trust value. As a service provider, it is the object to be evaluated. Any node i in the network cannot know the storage node which stores its reputation information, which avoids the possibility of the node to raise its reputation.

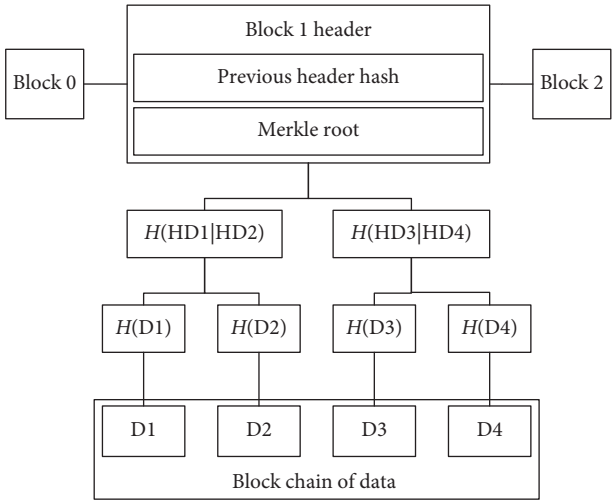


Figure 3: Data blockchain of the network node.

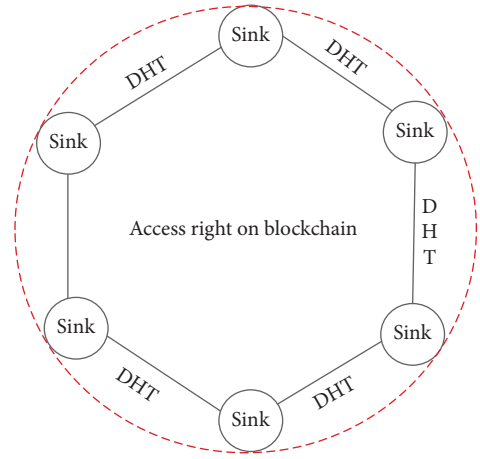


Figure 4: Access control based on blockchain.

5.3. Access Control Based on Blockchain. We use blockchain to securely store access right to the data stored in the sink nodes. The data owner, the data visitor, and some additional metadata are included in the signed storage transaction. Each data block is set to access rights and is restricted in time. The data owner can extend or revoke the right to access the data. For any data retrieval request, another node first checks the access rights record through the corresponding distributed hash table (DHT). Theoretically, malicious nodes can share data without permission. Since the access rights of the data are monitored, unauthorized data access will be detected. In addition, if the malicious node is detected, it will be removed out of the network. Therefore, the possibility of such insecure data access is very small. It is shown in Figure 4.

Below we build a block-based DHT for distributed storage and management of index data. DHT is a huge hash table, which is shared by a large number of nodes. Each sink node is assigned to a hash block that belongs to itself and becomes the manager of the hash block. Through the hash function, any data can be mapped to a 160-bit hash value, and the network nodes are mapped to a space. DHT can adapt to the dynamic join and exit sink nodes and has the characteristics of balance and query accuracy. We use the DHT algorithm based on Chord network; through the SHA series hash function, the data are mapped to 160-bit hash value. For chord structure, we use the predecessor list positioning to improve the positioning fault tolerance, by selecting the node to reduce the positioning delay. That is, in the positioning process to select the next jump, those nodes which are a small delay and closer to the other nodes are selected in the bottom of the logistics. Take the above predecessor's search function as an example. Assuming that a node m returns to the predecessor list of the node n, in addition to the node location information, there is a delay of each node to m. Based on these delays, the node n evaluates each node in the list and selects the node that it considers the most reasonable.

5.4. Mining and Incentive Mechanism Based on PDP for Data Storage of Node in WSN. There is a significant flaw of the PoW consensus mechanism in traditional blockchain technology, which requires a lot of computation and causes serious waste of resources (such as electricity). That has always been criticized by academics and industry. In order to solve the problem, the PDP mechanism is used to replace the PoW mechanism to construct the mining and incentive mechanism for data storage of node in the resource-constrained WSN.

5.4.1. Scheme Description. A new data block, which will be stored in the sensor network, is broadcast. And each network node then calculates the challenge of PDP for the data block. If the PDP is verified correctly, the new data block will be stored by the node, and the node will receive a reward for storing the data block as a result, that is, a unit of the digital currency. The proposed scheme is as follows.

(1) A new data block $M = \{m_1, m_2, \ldots, m_n\}$ which will be stored. The public key of the data publisher is $(g^x,\ u)$, and the private key is x; H_1 is a preserving hash function, and data publisher computes $\{H_1(m_i)\}$ and generates the authenticator $\sigma_i = (H(i)u^{m_i})^x$ for each subblock m_i; The request information for the data is broadcast in the sensor network.

(2) Each network node searches for the stored subblock m_i' closest to the value according to $\{H_1(m_i)\}$, that is, $|H_1(m_i) - H_1(m_i')| \le \text{dif}$. Then, the random number v_i will be selected for the subdata block i of the data block M, denoted as $Q = (i,\ v_i)$. The network node sends $\{H_1(m_i')\}$ and Q to the data publisher.

(3) The data issuer receives $\{H_1(m_i')\}$ from each network node and compares them with the $\{H_1(m_i)\}$ value, selecting the $H_1(m_i')$ value which is closest to each $H_1(m_i)$ value and adding the network node j that sent the $H_1(m_i')$ value to the node set J.

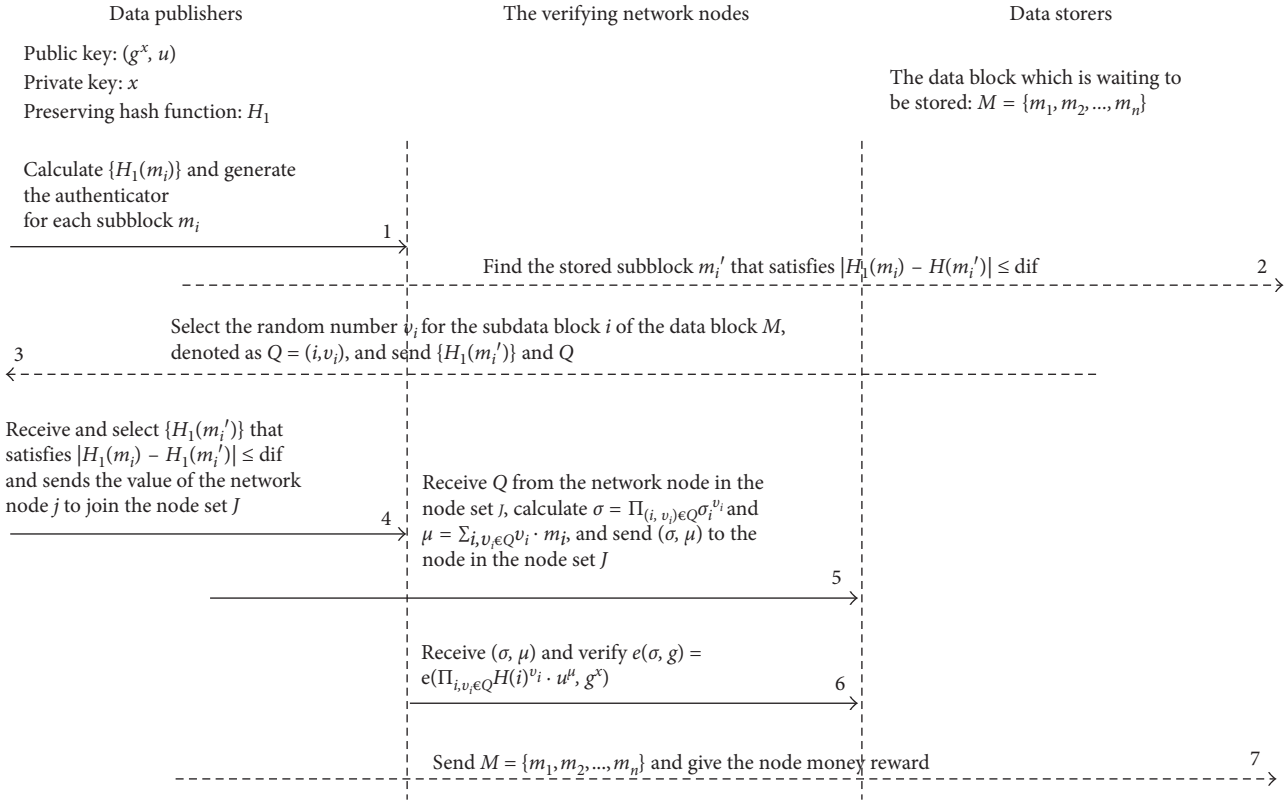


Figure 5: Incentive mechanism based on PDP.

Then, based on the Q received from the network node of the node set J, do the following calculation: $\sigma = \prod_{(i,v_i)\in Q} \sigma_i^{v_i}$ and $\mu = \sum_{(i,v_i)\in Q} v_i \cdot m_i$, and then send (σ, μ) to the network node of node set J.

(4) The network node of the node set J receives (σ, μ), verifying the following formula: $e(\sigma, g) = e(\prod_{(i,v_i\in Q)} H(i)^{v_i} \cdot u^{\mu}, g^x)$. If it is true, the data issuer will send the data block $M = \{m_1, m_2, \ldots, m_n\}$ to each network node of the set J for storage and give the node the digital currency reward.

(5) From the nature of the preserving hash function, it can be seen that the original data block of each network node in the set J contains data similar to the new data block $M = \{m_1, m_2, \ldots, m_n\}$. It only needs to store the part that is not the same as the original data. Therefore, through the strategy, it can greatly reduce the required storage space. The scheme is shown in Figure 5.

5.4.2. Parameters in Our Scheme. In our scheme, we take the pairing function $e : G_1 \times G_1 \to G_T$, where $|G_1| = |G_T|$ and g, u are generators of the group G_1. The practical constructions of pairings are done on hyperelliptic curves defined over a finite field. $E(F_q)$ is a set of points on an elliptic curve E defined over the finite field F_q. G_1 is taken as a subgroup of $E(F_q)$, and G_T is taken as a subgroup of $F^*_{q^{k'}}$, where k' is the embedding degree. The hash function H hashes a binary string of arbitrary length into G_1, and u is a random element of G_1. σ also is an element of G_1, and μ belongs to Z_p. The Barreto–Naehrig (BN) curves are suitable for our scheme.

5.4.3. Efficient Storage. In our scheme, the network node stores l data segments $\{(m_j, \sigma_j)\}$, $j \in I$ and $|I| = l$. I is the set of indices of M corresponding to these l segments, and σ_j is the tag of the segment m_j. If SHA-256 is used to compute these hash values, then the size of each σ_j becomes 256 bits. This generates a small storage requirement for each of the segments, though the number of segments in the data M is huge in general. Instead of the Merkle proof, the nodes store a small tag and authenticator of size 256 bits along with each segment. Therefore, a network node in our scheme enjoys around 256 bits less storage overhead per segment.

6. Discussion

Compared with the PDP mechanism, the POR (proofs of retrievability) mechanism can effectively identify whether a file is damaged, and at the same time, it can recover the errors that have occurred in the data file through fault tolerance technology to ensure that the file is available. The POR mechanism can be further adapted in our scheme to improve the fault tolerance of the system.

The PDP mechanism can quickly determine whether the data on the remote node are damaged or not and pay more attention to efficiency. POR mechanism can not only identify whether the data are damaged but also recover the

damaged data. POR mechanism can not only detect data integrity but also further ensure data integrity. The publicly authenticated POR mechanism allows any third-party alternative user to initiate the integrity detection of data on a remote node. When the damage of the data was found less than a certain threshold ε, the error is recovered through the fault tolerance mechanism; otherwise, the data returned to the user fail.

Before the POR performs the initialization phase, it is needed to increase the redundant coded data preprocessing process to make the data file fault-tolerant, that is, to divide M into n blocks and then group n blocks. Then, for each group of data blocks, the Reed–Solomon error correction code can be used for fault tolerance coding to form a new data file. The same verification technology as PDP mechanism is adopted. For the POR mechanism, the assumption is that it is within the allowed error range (an error occurs once in 1000000 but passes the verification of the POR mechanism). Define $Y\omega = 1/\#B + (\rho n)^c/(n-c+1)$, if $\varepsilon - \omega X$ is a negligible value, through $O(n/(\varepsilon-\omega))$ interactions, POR can recover the data with a failure rate of ρ. Here, B is the selection space of the random number when challenging the request, ρ is the data encoding rate, and c is the number of randomly selected data blocks.

7. Conclusions

In this paper, the first incentive mechanisms of nodes for data storage are built based on the blockchain technology in WSN. The data stored by every node are treated as a block of blockchain in our system. The reward for digital money will be obtained by the node who stored the data, and the reward for the node implementation increases as the data it store increases. In addition, it constructs two blockchains. One is to store data for each node, and the other for controlling the access of the data. Moreover, the provable data possession in the proposed scheme is used to substitute the proof of work (PoW) in primary bitcoins, which executes the mining and storage of the new data block. Compared with the PoW mechanism, it cuts down the computing power extremely. Furthermore, due to making use of the preserving hash functions, the new data can be stored in node which is nearest to the currently existing data. And only the different subblocks are stored. Therefore, the storage space of nodes in WSN can be highly saved.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Disclosure

The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; and in the decision to publish the results.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Authors' Contributions

All the authors wrote the paper.

Acknowledgments

This work was supported by the NSFC (61772280, 61772454, 61702236, and 6171101570), the PAPD fund from NUIST, and Changzhou Science and Technology Program (CJ20179027).

References

[1] J. Wang, Y. Cao, B. Li, H. Kim, and S. Lee, "Particle swarm optimization based clustering algorithm with mobile sink for WSNs," *Future Generation Computer Systems*, vol. 76, pp. 452–457, 2017.

[2] B. Wang, X. Gu, L. Ma, and S. Yan, "Temperature error correction based on BP neural network in meteorological WSN," *International Journal of Sensor Networks*, vol. 23, no. 4, pp. 265–278, 2017.

[3] L. Min, W. Fan, Z. Guo, and G. Fan, "Wireless sensor networks data storage strategy based on RCFile," *Computer Science*, vol. 42, pp. 76–80, 2015.

[4] S. C. Lindsey and S. P. Raghavendra, "Power efficient gathering in sensor information systems," in *Proceedings of IEEE Aerospace conference*, pp. 1125–1130, IEEE, Big Sky, MT, USA, March 2002.

[5] J. Wang, C. Ju, H. J. Kim, R. S. Sherratt, and S. Lee, "A mobile assisted coverage hole patching scheme based on particle swarm optimization for WSNs," *Cluster Computing*, vol. 3, pp. 1–9, 2017.

[6] N. Zaman, L. T. Jung, and M. M. Yasin, "Enhancing energy efficiency of wireless sensor network through the design of energy efficient routing protocol," *Journal of Sensors*, vol. 2016, Article ID 9278701, 16 pages, 2016.

[7] T. M. Meyfroyt, S. C. Borst, O. J. Boxma, and D. Denteneer, "Data dissemination performance in large-scale sensor networks," in *Proceedings of International Conference on Measurement and Modeling of Computer Systems*, pp. 395–406, Austin, Texas, USA, June 2014.

[8] X. Shen, W. Liu, I. W. Tsang, Q. S. Sun, and Y. S. Ong, "Multilabel prediction via cross-view search," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 99, pp. 1–15, 2018.

[9] R. Huang, X. Chu, J. Zhang, and Y. H. Hu, "Scale-free topology optimization for software-defined wireless sensor networks: a cyber-physical system," *International Journal of Distributed Sensor Networks*, vol. 13, no. 6, pp. 1–12, 2017.

[10] J. Wang, J. Cao, S. Ji, and J. H. Park, "Energy-efficient cluster-based dynamic routes adjustment approach for wireless sensor networks with mobile sinks," *Journal of Supercomputing*, vol. 73, no. 7, pp. 3277–3290, 2017.

[11] Y. Liu, Q. Zhang, and L. Ni, "Opportunity-based topology control in wireless sensor networks," *IEEE Transactions on Parallel and distributed systems*, vol. 21, no. 3, pp. 405–416, 2010.

[12] X. Shen, F. Shen, Q. S. Sun, Y. Yang, Y. H. Yuan, and H. T. Shen, "Semi-paired discrete hashing: learning latent hash codes for semi-paired cross-view retrieval," *IEEE Transactions on Cybernetics*, vol. 47, no. 12, pp. 4275–4288, 2018.

[13] X. Shen, F. Shen, L. Liu, Y. H. Yuan, W. Liu, and Q. S. Sun, "Multiview discrete hashing for scalable multimedia search," *ACM Transactions on Intelligent Systems and Technology*, vol. 9, no. 5, pp. 1–21, 2018.

[14] S. V. A. Jeba and R. S. Kumar, "Reliable anonymous secure packet forwarding scheme for wireless sensor networks," *Computers and Electrical Engineering*, vol. 48, pp. 405–416, 2015.

[15] J. R. M. Dios, K. Lferd, A. D. S. Bernabe, G. Nunez, A. Torres-Gonzalez, and A. Ollero, "Cooperation between UAS and wireless sensor networks for efficient data collection in large environments," *Journal of Intelligent and Robotic Systems*, vol. 70, pp. 491–508, 2013.

[16] D. Zeng, Y. Dai, F. Li, R. S. Sherratt, and J. Wang, "Adversarial learning for distant supervised relation extraction," *Computers, Materials and Continua (CMC)*, vol. 55, no. 1, pp. 243–254, 2018.

[17] H. Yetgin, K. T. K. Cheung, M. Ei-Hajjar, and L. Hanzo, "Network-lifetime maximization of wireless sensor networks," *IEEE Access*, vol. 3, pp. 2191–2226, 2015.

[18] R. I. Ogie, "Adopting incentive mechanisms for large-scale participation in mobile crowdsensing: from literature review to a conceptual framework," *Human-Centric Computing and Information Sciences*, vol. 6, no. 1, pp. 1–31, 2016.

[19] Z. M. Nezhad and S. Khorsandi, "Cooperation enforcement based on dynamic pricing in multi-domain sensor network," in *Proceedings of Consumer communications and networking conference 2011 (CCNC 2011)*, pp. 1055–1060, IEEE, Las Vegas, Nevada, USA, January 2011.

[20] S. Maity and J. Park, "Powering IoT devices: a novel design and analysis technique," *Journal of Convergence*, vol. 7, 2016.

[21] D. Yasmine, K. Bouabdellah, and F. K. Mohammed, "Using mobile data collectors to enhance energy efficiency and reliability in delay tolerant wireless sensor networks," *Journal of Information Processing Systems*, vol. 12, pp. 275–294, 2016.

[22] D. Goyal and M. R. Tripathy, "Routing protocols in wireless sensor networks: a survey," in *Proceedings of second international conference on advanced computing and communication technologies (ACCT 2012)*, pp. 256–275, IEEE, Rohtak, Haryana, India, January 2012.

[23] M. Li, E. Kamioka, and S. Yamada, "Pricing to simulate node cooperation in wireless Ad hoc networks," *IEICE Transactions on Communications*, vol. E90-B, no. 7, pp. 1640–1650, 2007.

[24] Y. Yuan and F. Wang, "Blockchain: the state of the art and future trends," *Acta Automatica Sinica*, vol. 42, no. 4, pp. 481–494, 2016.

[25] Q. Shao, C. Jin, Z. Zhang, W. Qian, and A. Zhou, "Blockchain: architecture and research progress," *Chinese Journal of Computers*, 2017, http://cjc.ict.ac.cn/online/cre/10xsqfs-2017127145754.pdf.

[26] Y. Ren, J. Shen, D. Liu, J. Wang, and J. Kim, "Evidential quality preserving of electronic record in cloud storage," *Journal of Internet Technology*, vol. 17, no. 6, pp. 1125–1132, 2016.

[27] B. Christian, M. Ueli, T. Daniel, and Z. Vassilis, "Bitcoin as a transaction ledger: a composable treatment," in *Proceedings of 36th annual international cryptology conference—Advances in Cryptology (CRYPTO 2017)*, pp. 324–356, Santa Barbara, CA, USA, August 2017.

[28] Y. Ren, J. Shen, Y. Zheng, J. Wang, and H. Chao, "Efficient data integrity auditing for storage security in mobile health cloud," *Peer-to-Peer Networking and Applications*, vol. 9, no. 5, pp. 854–863, 2016.

[29] W. Qian, Q. Shao, Y. Zhu, C. Jin, and A. Zhou, "Research problems and methods in blockchain and trusted data management," *Journal of Software*, vol. 29, pp. 150–159, 2018.

[30] Y. Tu, Y. Lin, J. Wang, and J. U. K. Kim, "Semi-supervised learning with generative adversarial networks on digital signal modulation classification," *Computers, Materials and Continua (CMC)*, vol. 55, no. 2, pp. 243–254, 2018.

[31] L. Xiang, Y. Li, W. Hao, P. Yang, and X. Shen, "Reversible natural language watermarking using synonym substitution and arithmetic coding," *Computers, Materials and Continua (CMC)*, vol. 55, no. 3, pp. 541–559, 2018.

[32] R. Qiao, S. Dong, Q. Wei, and Q. Wang, "Blockchain based secure storage scheme of dynamic data," *Computer Science*, vol. 45, pp. 57–62, 2018.

[33] R. Meng, S. Rice, J. Wang, and X. Sun, "A fusion steganographic algorithm based on faster R-CNN," *Computers, Materials and Continua (CMC)*, vol. 55, no. 1, pp. 1–16, 2018.

[34] P. He, G. Yu, Y. Zhang, and Y. Bao, "Survey on blockchain technology and its application prospect," *Computer Science*, vol. 44, pp. 1–8, 2017.

[35] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, "Mutual verifiable provable data auditing in public cloud Storage," *Journal of Internet Technology*, vol. 16, pp. 317–323, 2015.

[36] D. He, N. Kumar, S. Zeadally, and H. Wang, "Certificateless provable data possession scheme for cloud-based smart grid data management systems," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 3, pp. 232–242, 2018.

[37] H. Wang, K. Li, K. Ota, and J. Shen, "Remote data integrity checking and sharing in cloud-based health internet of things," *IEICE Transactions on Information and Systems*, vol. E99.D, no. 8, pp. 1966–1973, 2016.

[38] Q. Jiang, F. Wei, S. Fu, J. Ma, G. Li, and A. Alelaiwi, "Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy," *Nonlinear Dynamics*, vol. 83, no. 4, pp. 2085–2101, 2016.

[39] Z. Faheem, A. Khan, S. U. R. Malik et al., "A survey of cloud computing data integrity schemes: design challenges, taxonomy and future trends," *Computers and Security*, vol. 65, pp. 29–49, 2017.

[40] N. Gargn and S. Bawa, "Comparative analysis of cloud data integrity auditing protocols," *Journal of Network and Computer Applications*, vol. 66, pp. 17–32, 2016.

[41] K. Gu, W. Jia, and J. Zhang, "Identity-based multi-proxy signature scheme in the standard model," *Fundamenta Informaticae*, vol. 150, no. 2, pp. 179–210, 2017.

[42] Y. Wang and Q. Wu, "A survey on cryptographic technologies for data integrity checking in clouds," *Journal of Cyber Security*, vol. 2, pp. 23–35, 2017.

Hindawi
Mobile Information Systems
Volume 2018, Article ID 1710591, 7 pages
https://doi.org/10.1155/2018/1710591

Research Article

Cluster-Based Device Mobility Management in Named Data Networking for Vehicular Networks

Moneeb Gohar,[1] **Naveed Khan**,[1] **Awais Ahmad**,[1] **Muhammad Najam-Ul-Islam**,[1] **Shahzad Sarwar**,[2] **and Seok-Joo Koh**[3]

[1]*Department of Computer Science, Bahria University, Islamabad, Pakistan*
[2]*College of Information Technology, Punjab University, Lahore, Pakistan*
[3]*School of Computer Science and Engineering, Kyungpook National University, Republic of Korea*

Correspondence should be addressed to Seok-Joo Koh; sjkoh@knu.ac.kr

Received 4 April 2018; Revised 12 June 2018; Accepted 24 June 2018; Published 29 August 2018

Academic Editor: Mohamed Elhoseny

Named data networking (NDN) is an emerging technology. It was designed to eliminate the dependency of IP addresses in the hourglass model. Mobility is a key concern of the modern Internet architecture, even though the NDN architecture has solved the consumer mobility. That is, the consumer can rerequest the desired data contents, while the producer mobility remains as an issue in the NDN architecture. This paper focuses on the issue of producer mobility and proposes the cluster-based device mobility management scheme, which uses the cluster heads to solve the producer mobility issue in NDN. In the proposed scheme, a cluster head has all information of its attached devices. A cluster head updates the routes, when a device moves to the new access router by sending all the attachment information. The proposed scheme is evaluated and compared with the existing scheme by using the *ndnSIM* simulation. From the results, we see that the proposed scheme can decrease the numbers of interest packets in the network, compared with the existing scheme.

1. Introduction

NDN is a common networking model for all applications and network environment, and it is still under the developing phase. It has been designed as an alternative to the IP address-based network. IP was designed for conversation between endpoints, and it is used enormously for content distribution [1–3]. NDN uses data names instead of IP addresses. The NDN network removes the restriction of IP datagram which can only use both IP destination addresses and source addresses. NDN application removes middleware which causes inefficiency because middleware uses mapping application for interaction. In NDN, data looping is prevented via memory because every chunk of data has a unique name, while IP is used for single-path forwarding.

The NDN architecture uses the two types of packets [4], *interest packet* and *data packet*. A consumer uses the interest packet to request the desired contents, while a producer or NDN router uses the data packet to send the desired content to the consumer by using the reverse path. Each NDN router maintains the three tables for processing of interest packets and data packets [5]. These tables are content store (CS), pending interest table (PIT), and forwarding information base (FIB).

Initially, when an interest packet reaches the NDN router, the NDN router first checks the desired content in CS. If the content is found in the CS table, the NDN router will send the content back to the consumer. Otherwise, it is forwarded to PIT. When PIT waits for the same content from FIB, it only marks an entry in the PIT table. PIT forwards the desired content to the consumer upon reception. If PIT did not send the desired interest packet to FIB, it will forward it to FIB, and FIB will look for the desired content in the other NDN router. When the content is found, it will be delivered to the consumer by using the reverse path.

The producer mobility is a major issue in NDN. The consumer mobility is automatically solved by the NDN architecture since a consumer can rerequest the desired

contents. If the consumer nodes are interested in a desired data content, the producer nodes will offer the content to the consumers. Problems may occur when a consumer requests the desired content and the producer moves to the new access router by handover. One of the problems may occur when the interest packets reach the previous access router, and thus the interest packets cannot be delivered to the producer. Based on this, in this paper, we introduce a cluster-based device mobility management (CB-DMM) so as to locate the devices in NDN that may possibly move from the previous access router to a new access router.

The remaining parts of this paper are organized as follows. Section 2 will briefly review the related work. In Section 3, we will explain the existing scheme. The proposed CB-DMM model will be described in Section 4. We will evaluate the performance of the CB-DMM models in Section 5. Finally, Section 6 will give conclusions and future works.

2. Related Work

NDN is a new emerging networking model that can be applied in various networking areas. Specially, NDN provides a lot of advantages such as network caching, security, and efficient response time in the vehicular ad hoc networks (VANETs) [2, 3, 6–8]. There are two types of mobility considered in NDN: consumer mobility and producer mobility. A lot of studies have been done on consumer mobility. However, there are not many studies on producer mobility.

The producer mobility issue is often addressed by using the mobile IP [9]. However, it suffers from the problems, such as a single-point failure, nonoptimal routingand so on. In [1], a distributed scalable mobility management (SMM) mechanism is introduced to solve the issues of MIP-based solution for NDN mobility without changing the original NDN paradigm. SMM protocol separates the content locator and the identifier. The hierarchical MIP [10] is used to support the intradomain and interdomain handover. However, the use of mapping systems on a global scale brings latency and complexity in the network.

An anchor-based mobility support method was proposed in [5]. Mobility tracking node, called anchor, was used to redirect the consumer request to the producer from the old location to the new location. When the producer handover happens and the interest packet ends up with being undeliverable, the traveling interest packet is immediately redirected toward the anchor node instead of being dropped at the old point of attachment.

The content provider mobility is solved in [11] by providing the locator and the mapping system. The locator is used because we do not know where the information is located, and the mapping system is used to map an identifier to the locator. An identifier is used for matching in CS and PIT, and a locator is used for forwarding in FIB. The provider gets a locator when it joins the network. A locator represents the address of the provider in the access point. A mapping system, such as DNS, will resolve the query so as to map the name to the locator. These extra labels may cause more complexity and burden on the network.

In [12], the authors tested the named data network for mobility support in the wireless access network and provided the simulation-based results by using *ndnSIM*. This work focuses on delay-sensitive and delay-tolerant traffics by using different network topologies. These topologies are based on autonomous systems (ASs). The authors give the four scenarios. The first scenario is for a single mobile host and a single static host, which are assigned to the same AS. The second scenario is based on the first scenario with modification that allows both hosts to be mobile. The third scenario has a single mobile host and a single static host, and each host is assigned to different ASs. In the last scenario, the third scenario is modified, which allows both hosts to be mobile. In these scenarios, the application with delay-tolerant and delay-sensitive traffics may experience worse performance in the viewpoint of message overhead and throughput. NDN is not suitable for small size networks. The authors want to introduce the location-routing policies in NDN to satisfy the requirements of the different applications and to reduce the burden on network infrastructure.

In [13], the authors have divided the existing solutions for producer mobility in NDN into the three categories: routing, mapping, and tracking. A mobile node (MN) can keep its IP address while moving to another network, but MN must update the other routers in the routing-based approach. In mapping-based solution, whenever MN changes the network, it must update the current IP address at previous routers. The tracing-based approach is mainly used to reach the producer in the hop-by-hop manner by using the reverse path. The authors mainly concentrate on the producer mobility and give a detailed mechanism of the already available proposed solution. For producer mobility, the authors present the two chase mechanisms of the moving producer and also the two data-centric ways to find interest data.

In [14], a trace-based scheme is proposed for NDN mobility, called Kite. In Kite, a new forwarding mechanism is introduced for the producer mobility. A trade name field is used. Tracing flags are used to forward the tracking interest. The Kite is locator-free and based on application. The developer can make changes in its application to achieve better performance. But, the authors have not provided any simulation to validate the proposed approach. Trace-based solution also causes huge traffic in the network, and it is time-consuming.

In [15], the producer mobility problem is solved by data replication. The authors provided the two main strategies to handle the producer mobility. In the first strategy, they handle the producer mobility through data replication. Secondly, they evaluate when data replication improves the producer mobility in NDN. The producer mobility issue is divided into the two categories: unavailability period and reattachment to the network. In the unavailability period, they suggested replicating the content when the producer is unavailable. Through different parameters, they evaluate the performance for unavailability period and for reattachment to the network. But, the replication techniques can cause more storage and overhead in the network.

In [16], the authors minimize data loss in the real-time application which is caused by mobility in the NDN

network. They used the three approaches to minimize the loss which is caused by mobility. In the first approach, the point of access (PoA) is used, where a mobile node (MN) registers itself with a nearby PoA. This PoA sends interest packets and data packets to the MN. In the second approach, the rendezvous points are used. Rendezvous points represent the strategically located routers. The authors used the rendezvous point for seamless mobility. In the last approach, multipath interest and multipoint content are used to solve the mobility issue in NDN.

In [17], the producer mobility is solved by using the cache techniques. Before the producer handover occurs, data can be cached to offer seamless operation in NDN.

In [18], the authors built a prototype of NDN in the ns-3 simulation. A forwarding hint is used for the producer mobility. The forwarding hint was used in the previous IP mobility solution. The authors argue that this new element can be used for content-centric data transmission.

3. Existing SMM Scheme

Scalable mobility management (SMM) for content source in NDN is proposed in [1]. It solved the producer mobility issue in NDN. The authors used the mapping system on a global scale which may cause huge latency and bring more complexity to the network. The authors proposed the two handover models. In the first model shown in Figure 1, a producer is attached to a new access router, and it sends a special message to the mapping system by using a binding update (BU). The mapping system sends a binding acknowledgment (BA) to the producer. The mapping system also sends BU to the previous access router. The previous access router (PAR) sends data packets with BA, and the communication continues. In the second handover model, the producer sends the BU packet to both mapping system and PAR at the same time. The BA is sent from PAR to the producer. The second handover model introduced the mobility option (MO) packet which is a modification of NDN interest packets. The MO interest is sent from PAR to the new access router (NAR). We solve the mobility issue through the cluster-based device mobility in NDN. The device may be a producer or a consumer, which will further be discussed in Section 4.

4. Proposed CB-DMM Model

In this section, we will discuss the proposed CB-DMM model, including topology, handover procedure, selection of cluster heads, responsibilities of cluster heads, and NDN routers.

4.1. CB-DMM Topology Model. We have designed the cluster-based device mobility management (CB-DMM) to support the device mobility in NDN. In Figure 2, it is assumed that a consumer requests contents "contentsource/realtime/video1." The problem occurs when the interest packet reaches the previous access router and the producer moves to the new access router, and the interest packet cannot be delivered to the producer. To solve this problem, the cluster-based device mobility management scheme is used. Our model has the strength to solve other mobility issues such as consumer mobility. In CB-DMM, when the device moves from one access router to another, it will send its current location information to the cluster head, and the cluster head diverts the pending interest packets toward the intended device.

In Figure 2, a group of NDN routers selects cluster heads. There are different techniques available for selection of cluster heads based on the nature of network type. In a wireless network, we need more storage capacity, energy, and the location of the cluster head, while the situation is different for the wired network. Our topology is based on the mixed network. We use both wireless and wired networks in our model for simulation. The selection of cluster will be further discussed in Section 4.3.

4.2. CB-DMM Handover Procedure. A producer moves from PAR (previous access router) to NAR (new access router) in Figure 3. The moving device (producer) sends the attachment information to NAR. The NAR sends the attachment information to the cluster head and informs it about the producer. The cluster head updates its cached table and saves the current location of the producer. The cluster head sends the binding acknowledgment to NAR, and NAR sends BA to the content producer. The cluster heads exchange periodic updates with each other. When a request reaches the cluster head for producer, it simply checks its cache and sends a request to the current location of the producer. The producer sends the contents through the reverse path to the consumer.

4.3. Selection of Cluster Heads. Different approaches can be taken to select the cluster heads. The wired network is different from the wireless network. Selection of cluster heads in the wired network is easy, while selection in wireless is difficult. Our scenario is based on both wired and wireless networks. In our scenario, the consumer is connected to the wired network, and the producer is connected to the wireless network. The AP is connected to a cluster head via a wired link. Based on our approach, we select the cluster head on the following approaches. First, we use the existing algorithm [19] for the selection of cluster head, based on memory. Secondly, the cluster heads must provide easy connectivity to other cluster heads. Third, each cluster head knows the addresses of the other cluster head. Fourth, the cluster heads are connected with each other directly. In [19], the authors proposed an algorithm for selection of cluster heads. We will also use that algorithm for selection of cluster heads in a wireless network.

4.4. Operations of Cluster Head. In our scenario, different operations are possible for each cluster head. The different routers can be connected to the same cluster head. Now, User A is connected to router R1, and User B is connected to R2, and both (i.e., R1 and R2) are connected to the same cluster head R. User A requests the contents "contentsource/realtime/video1" and sends the interest packet for content toward R1. Then, R1 will forward the interest packet to the cluster head R.

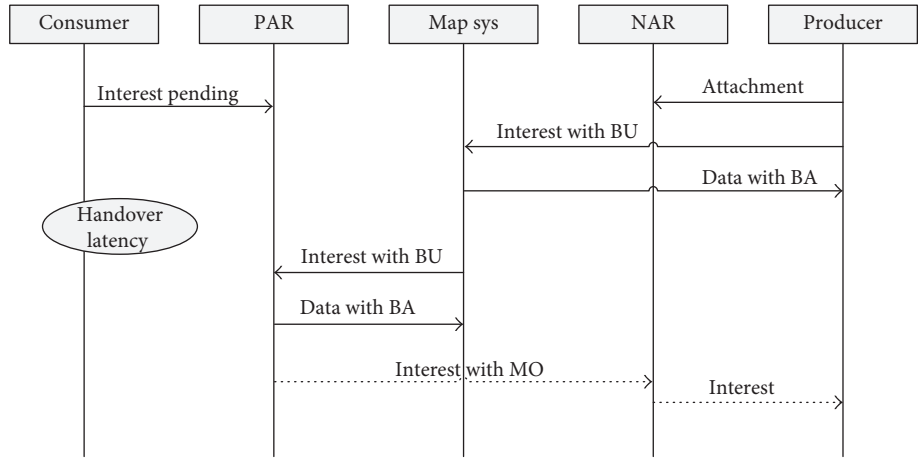


Figure 1: SMM handover model.

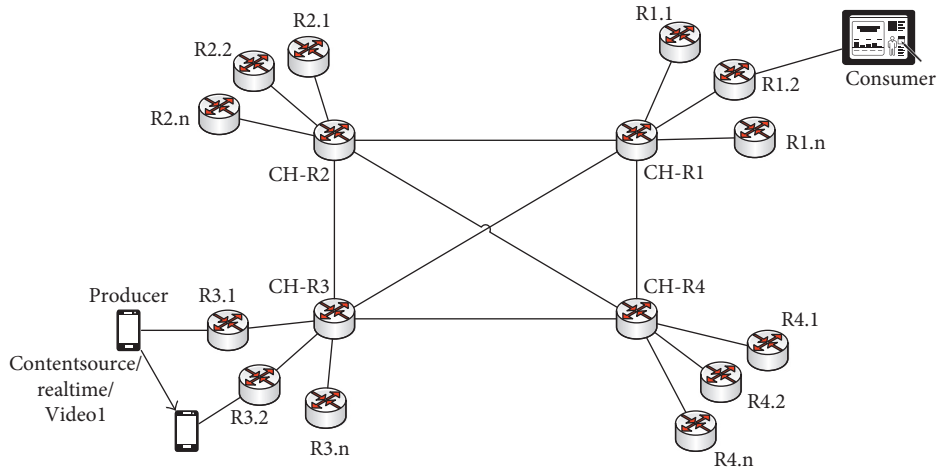


Figure 2: CB-DMM network topology model.

The "contentsource/realtime/video1" is sent through the data packet using the reverse path to User A. Now, User B sends interest packets for the same data through different router R2, when the interest reaches the cluster head. The cluster head simply sends data packets to User B from it CS table. Through this process, a lot of network resources can be saved, and overhead can be decreased from the network. Our model can also solve the consumer mobility because whenever a device moves to a new access router, it will send its current location information to cluster heads. Now, for both cases, the data packets will be sent to a new location. In case of a producer, the interest packets will be sent to the new location. The cluster heads in our scenario also send a periodic update about connected devices to each other. Through this process, the contents can be easily found in the network. The mobility problem can also be solved through periodic updates, which the cluster heads share with each other.

5. Performance Analysis

We simulate the CB-DMM model in *ndnSIM* [20] and compare our results with the SMM model. The SMM model is an existing scheme that is presented in Section 3. We used the two scenarios to simulate CB-DMM and SMM models in *ndnSIM*.

Figure 4 shows the basic network topology for CB-DMM and SMM models. For scenarios 1 and 2 in CB-DMM, the producer is initially connected to AP1. Both APs are connected to cluster heads, and the cluster heads are connected with each other through a direct link. The consumer is connected to an NDN router, and the NDN router is connected to a cluster head. For the SMM model, the mapping system is placed three hops away from the producer node for scenario 1. While for scenario 2, the mapping system is six hops away from the producer. In the SMM model, the mapping system is used to locate the desired contents in the NDN network. We placed the mapping system in a different position because according to [1], the mapping system can be placed globally in the NDN Network.

Table 1 shows the basic network parameters for both CB-DMM and SMM models. The SMM model uses the mapping system to locate the producer. The location of the mapping system in the network is a big challenge for the SMM model.

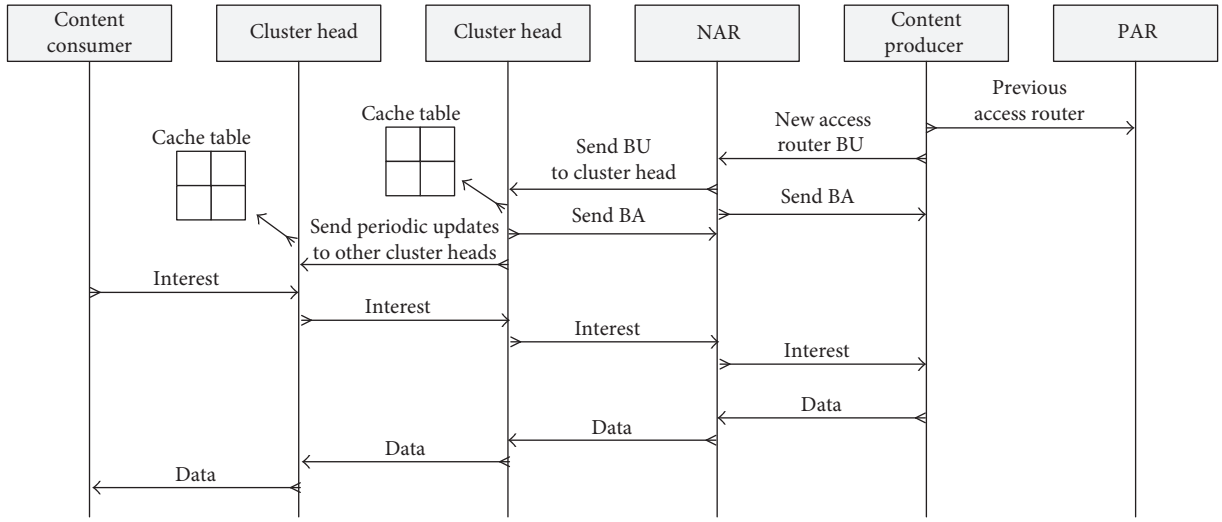


Figure 3: CB-SMM handover procedure.

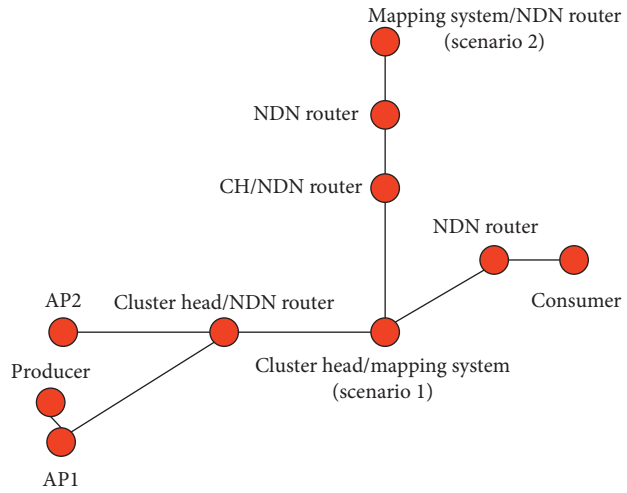


Figure 4: Models for CB-DMM and SMM network simulation: scenarios 1 and 2.

We use the two scenarios for the SMM model, where the mapping system is located 3 and 6 hops away from the producer. According to the SMM model, the mapping system is placed on a global scale in the network. The topology of Figure 4 is used for simulation of CB-DMM and SMM models. The difference occurs in the node functionality. That is, when we simulate the SMM model, the node has the functionality of the mapping system; whereas for the CB-DMM model, some nodes have the functionality of cluster heads. The number of nodes in the networks is 11. The capacity of the link is set to 100, 50, and 10 Mbps, and the link delay is set to 1, 10, and 20 ms, respectively. The *RandomWalk2Mobility* model is used as a mobility model. The Wi-Fi bandwidth is set to 24 Mbps, and the simulation time is 15 seconds.

Figure 5 shows the performance of CB-DMM and SMM models. We used two scenarios for the SMM model and compared the results with the CB-DMM model. The performance measurement is based on the interest satisfied ratio. At the start of simulation for the CB-DMM model, the interest satisfied ratio was 30 percent at 0.2 seconds, and the interest satisfied ratio reached 100 percent at 1 second. For the SMM model (scenario 1), the communication started at 1 second, and the interest satisfied ratio was 20 percent; whereas for scenario 2, the communication started at 2 seconds, and the interest satisfied ratio was 20 percent. The SMM scenario 1 reached 100 percent approximately in 2.2 seconds, and the SMM scenario 2 reached 100 percent in 4 seconds.

Table 1: Network parameters.

Parameters	Values
Number of nodes	11
Link capacity	100, 50, 10 Mbps
Link delay	1,10, 20 ms
Mobility model	*RandomWalk2Mobility*
Wi-Fi AP bandwidth	24 Mbps
Simulation time	15 seconds

At 7 seconds, in the CB-DMM and SMM model, the producer moves to another network. Both models use their handover procedures to locate the producer node. The CB-DMM model locates the producer in 0.2 seconds, whereas the SMM model scenario 1 takes 1 second, and the SMM scenario 2 takes 2 seconds.

In Figure 6, we reduce the link speed to 50 Mbps and increase the link delay to 10 ms, and then compare the CB-DMM model with the SMM scenarios. The CB-DMM model starts communication at 0.2 seconds, and the interest satisfied ratio is 20 percent. Compared to Figure 5, the interest satisfied ratio was less at 0.2 seconds. For SMM scenario 1, the communication started at 1 second, and the interest satisfied ratio was around 8 percent; whereas for scenario 2, the interest satisfied ratio was the same but the communication started at 2 seconds. The CB-DMM model reached 100 percent of the interest satisfied ratio at 0.8 seconds, while the SMM model reached 100 percent at 2 seconds and 3.6 seconds, respectively. When a handover happened again at 7 seconds,

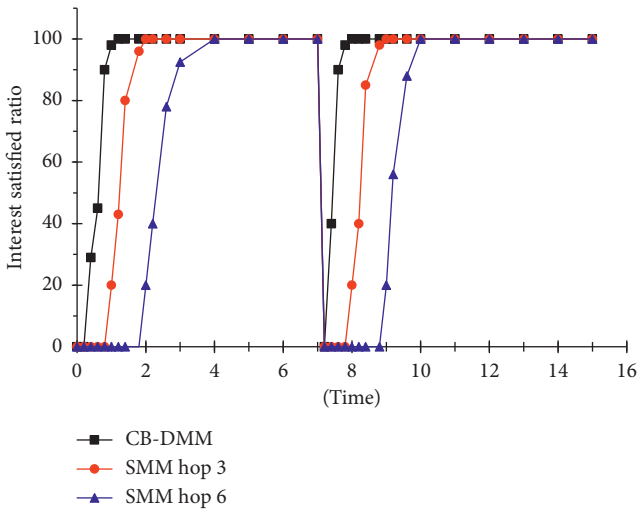


Figure 5: Comparison of CB-DMM and SMM (3 and 6 hops) with 100 Mbps and 1 ms.

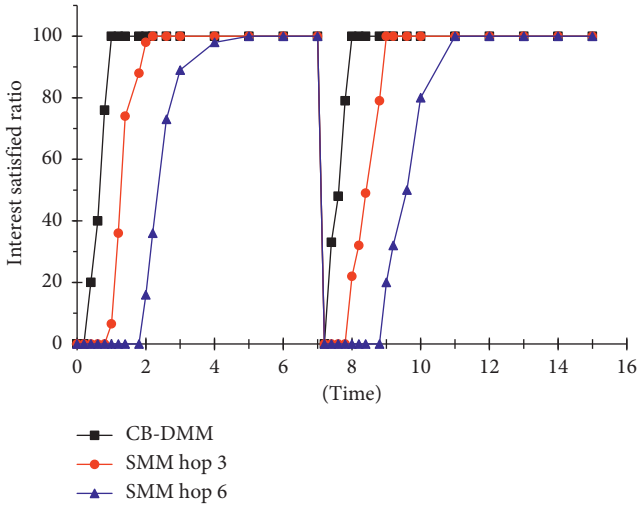


Figure 6: Comparison of CB-DMM and SMM (3 and 6 hops) with 50 Mbps and 10 ms.

both models went down to 0 percent. The CB-DMM model started communication again at around 7.2 seconds, while the SMM model started the communication at 8 seconds and 9 seconds, respectively.

In Figure 7, we reduce the link speed to 10 Mbps and increase the link delay to 20 ms, and then compare the CB-DMM model with both the SMM scenarios. Initially, the interest satisfied ratio for the CB-DMM model was around 10 percent; whereas for the SMM model scenario 1, the interest satisfied ratio was approximately 7 percent, and for scenario 2, the ratio was around 5 percent. In the CB-DMM model, the interest satisfied ratio was good, and after around 1 second, the ratio reached 100 percent; whereas for the SMM model, the interest satisfied ratio for scenario 1 reached 100 percent in 1.8 seconds, and for scenario 2, the ratio reached 100 percent in 4 seconds. When the producer changed the network, both models started searching for the producer node to get data contents. After around 7 seconds,

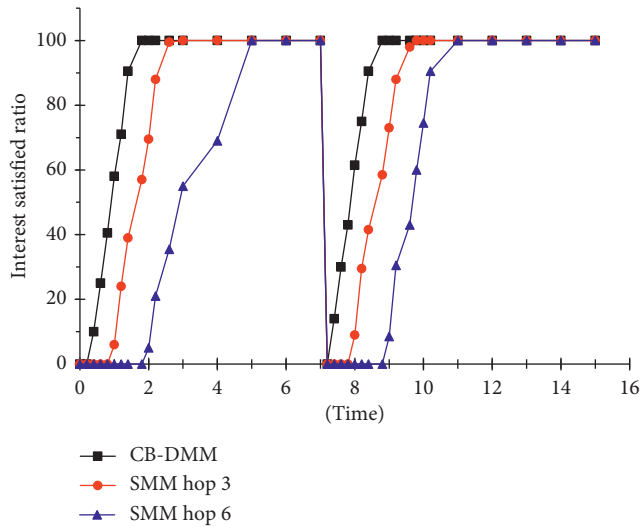


Figure 7: Comparison of CB-DMM and SMM (3 and 6 hops) with 10 Mbps and 20 ms.

the producer moved to another network. The CB-DMM model started communication again after 7.2 seconds, and the interest satisfied ratio was 12 percent. In the SMM model, for scenario 1, the communication started again in around 8 seconds, and for scenario 2 the producer started communication approximately in 9 seconds. After around 8 seconds, the CB-DMM model reached 100 percent, and in the SMM model, the first scenario reached 100 percent in approximately 8.4 seconds, while scenario 2 reached 100 percent after around 10.2 seconds. We can see that the CB-DMM model is better than the SMM Model in terms of the interest satisfied ratio and time.

6. Conclusions and Future Work

This paper proposes the solutions to locate the producer in the NDN network. In the proposed CB-DMM model, devices send their information to a cluster head after handover. The cluster head keeps that information for future use. We have compared our results with the existing SMM model. In the SMM model, the producer sends the new location information to the mapping system. Then, the mapping system sends the information to the previous access router to divert the interest packets toward the new access router. In our solution, we send the device information to the cluster head, and the cluster head is responsible for diverting the interest packets toward the new access router. There is no need to tell the previous access router to divert the interest packets.

The proposed scheme provides better performance than the existing SMM model in terms of diversion of interest packets toward producer and the interest satisfied ratio. The diversion of interest packets toward producer is quicker in our proposed model, compared with the existing scheme. The interest packet satisfied ratio is also good in our proposed scheme.

The future work will be made to reduce the overhead of the cluster head in the network and to use the cluster head for other purposes, which can solve the network query very

quickly. We also plan to move the producer into different cluster heads in the network.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the BK21 Plus project funded by the Ministry of Education, School of Computer Science and Engineering, Kyungpook National University, Korea (21A20131600005).

References

[1] S. Gao and H. Zhang, "Scalable mobility management for content sources in Named Data Networking," in *Proceedings of IEEE Annual Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, USA, January 2016.

[2] M. F. Majeed, S. Ahmed, S. Muhammad, H. Song, and D. B. Rawat, "Multimedia streaming in information-centric networking: a survey and future perspectives," *Computer Networks*, vol. 125, pp. 103–121, 2017.

[3] S. Isa and P. Kadam, "Named data networking in VANET: a survey," *International Journal of Scientific Engineering and Science*, vol. 1, no. 11, pp. 45–49, 2017.

[4] X. Jiang, J. Bi, and Y. Wang, "What benefits does NDN have in supporting mobility," in *Proceedings of IEEE Symposium on Computers and Communication (ISCC)*, Messina, Italy, June 2014.

[5] X. Jiang, J. Bi, Y. Wang, P. Lin, and Z. Li, "A content provider mobility solution of named data networking," in *Proceedings of IEEE International Conference on Network Protocols (ICNP)*, Austin, TX, USA, October 2012.

[6] S. Ahmed, D. Mu, and D. Kim, "Improving bivious relay selection in vehicular delay tolerant networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 3, pp. 987–995, 2018.

[7] S. H. Bouk, S. Ahmed, D. Kim, K. J. Park, Y. Eun, and J. Lloret, "LAPEL: hop limit based adaptive PIT entry lifetime for vehicular named data networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 5546–5557, 2018.

[8] S. Ahmed, S. Hussain Bouk, M. A. Yaqub, D. Kim, and H. Song, "DIFS: distributed interest forwarder selection in vehicular named data networks," *IEEE Transactions on Intelligent Transportation Systems*, 2018.

[9] IETF RFC 6275, *Mobile IPv6*, IETF, Fremont, CA, USA, 2011.

[10] IETF RFC 5380, *Hierarchal Mobile IPv6*, IETF, Fremont, CA, USA, 2008.

[11] J. Su, X. Tan, Z. Zhao, and P. Yan, "MDP-based forwarding in named data networking," in *Proceedings of Chinese Control Conference (CCC)*, Chengdu, China, July 2016.

[12] Y. Zhang, H. Zhang, and L. Zhang, "Kite: a mobility support scheme for ndn," in *Proceedings of International Conference on Information-Centric Networking*, Paris, France, September 2014.

[13] D. Kim and Y. Ko, "On-demand anchor-based mobility support method for named data networking," in *Proceedings of International Conference on Advanced Communication Technology (ICACT)*, Pyeongchang, Republic of Korea, 2017.

[14] A. Aytac, R. Ravindran, and G. Wang, "Mobility study for named data networking in wireless access networks," in *Proceedings of IEEE International Conference on Communications (ICC)*, Sydney, Australia, June 2014.

[15] M. Lehmann, M. Barcellos, and A. U. Mauthe, "Providing producer mobility support in NDN through proactive data replication," in *Proceedings of Conference on Network Operations and Management Symposium (NOMS)*, Istanbul, Turkey, April 2016.

[16] R. Ravishankar, S. Lo, X. Zhang, and G. Wang, "Supporting seamless mobility in named data networking," in *Proceedings of IEEE International Conference on Communications (ICC)*, Ottawa, ON, Canada, June 2012.

[17] F. Hesham and H. Hassanein, "Optimal caching for producer mobility support in named data networks," in *Proceedings of IEEE International Conference on Communications (ICC)*, Kuala Lumpur, Malaysia, May 2016.

[18] Z. Liu, Y. Wu, E. Yuepeng, J. Ge, and T. Li, "Experimental evaluation of consumer mobility on named data networking," in *Proceedings of International Conference on Ubiquitous and Future Networks (ICUFN)*, Shanghai, China, July 2014.

[19] S. Muhammad, "Cluster-based mobility support in content-centric networking," *Research Notes in Information Science (RNIS)*, vol. 14, pp. 441–444, 2013.

[20] A. Alexander, I. Moiseenko, and L. Zhang, "ndnSIM: NDN simulator for NS-3," Technical Report, University of California, San Francisco, CA, USA, 2012.

Hindawi
Mobile Information Systems
Volume 2018, Article ID 5107024, 14 pages
https://doi.org/10.1155/2018/5107024

Research Article

Smartwatch-Based Legitimate User Identification for Cloud-Based Secure Services

Muhammad Ahmad[1,2] **Mohammed A. Alqarni,**[3] **Asad Khan,**[4] **Adil Khan,**[1] **Sajjad Hussain Chauhdary,**[3] **Manuel Mazzara,**[5] **Tariq Umer**[6] **and Salvatore Distefano**[2]

[1]*Institute of Robotics, Innopolis University, Innopolis, 420500 Kazan, Tatarstan, Russia*
[2]*University of Messina, Messina, Italy*
[3]*Faculty of Computing and Information Technology, University of Jeddah, Saudi Arabia*
[4]*Graphic and Computing Lab, School of Computer Science, South China Normal University, Guangzhou, China*
[5]*Director of Institute of Technologies and Software Development, Head of Service Science and Engineering Lab, Innopolis University, Innopolis, 420500 Kazan, Tatarstan, Russia*
[6]*Department of Computer Science, COMSATS University, Wah Campus, Islamabad, Pakistan*

Correspondence should be addressed to Muhammad Ahmad; mahmad00@gmail.com

Received 15 May 2018; Accepted 5 July 2018; Published 14 August 2018

Academic Editor: Syed Hassan Ahmed

Smartphones are ubiquitously integrated into our home and work environment and users frequently use them as the portal to cloud-based secure services. Since smartphones can easily be stolen or coopted, the advent of smartwatches provides an intriguing platform legitimate user identification for applications like online banking and many other cloud-based services. However, to access security-critical online services, it is highly desirable to accurately identifying the legitimate user accessing such services and data whether coming from the cloud or any other source. Such identification must be done in an automatic and non-bypassable way. For such applications, this work proposes a two-fold feasibility study; (1) activity recognition and (2) gait-based legitimate user identification based on individual activity. To achieve the above-said goals, the first aim of this work was to propose a semicontrolled environment system which overcomes the limitations of users' age, gender, and smartwatch wearing style. The second aim of this work was to investigate the ambulatory activity performed by any user. Thus, this paper proposes a novel system for implicit and continuous legitimate user identification based on their behavioral characteristics by leveraging the sensors already ubiquitously built into smartwatches. The design system gives legitimate user identification using machine learning techniques and multiple sensory data with 98.68% accuracy.

1. Introduction

We are living in an era of context-aware systems whose aim is to acquire a user's context and reason on it to change a system's behavior to match the user's changing situation [1]. Making user's context information available to such systems is a critical task, and one such information is the identity of the user. Furthermore, today's era is an era of smart devices such as smartphones (SP), smartwatches (SW), smart TVs, and even smarthomes (SHs). The modern SWs consist of extensive computing power, different sensors, and the ability to communicate with other smart devices, for example, SH and SP via Bluetooth or the WIFI. SWs are a comparatively new expansion and probably the first SW to be truly modern and smart "The Pebble" became available in early 2013 [2].

In 2014, many other SWs were released, and almost all of these operate with Android phones and run the Android Wear subsystem. These SWs include the Moto 360, Sony SW 3, LG G, and Samsung Gear. While the sale of these SWs has recently been modest, the introduction of the Apple watch in 2015 greatly increased interest in such devices. It is now clear

that SWs have become as ubiquitous as SPs, and current market projections indicate that nearly 400 million SWs will ship by 2020 which is 25 times greater than 2014 sales [2, 3].

Modern SWs are equipped with a variety of motion sensors that are useful for monitoring device movements like tilt, rotate, and shake. Some of these sensors are the ambient light sensor, accelerometer, compass, gyroscope, magnetometer, and GPS sensors. These sensors support similar capabilities and applications of smartphones such as healthcare applications that require physical activity recognition (PAR). The accelerometer, linear accelerometer, magnetometer, and gyroscope sensors are ideal for PAR and gait-based legitimate user identification over SPs [4–7]. This work will show that SWs are equally capable of performing PAR and gait-based legitimate user identification.

The proposed legitimate user identification model uses a personal (single predictive) model to identify a user within a group of users. Finally, the identification model uses a predictive model to determine if an unknown user is a legitimate user or is an impostor. This work utilizes SWs and SPs to collect and store sensor data from three different sensors. These sensors include accelerometer, magnetometer, and gyroscope sensors. The data collected by these sensors were ultimately sent to the computer for further processing. This work utilizes the Android-based SPs and SWs because these devices are easily available in the market at low price.

Gait-based legitimate user identification on SWs has several advantages over the SPs, for example, portability, location, and orientation that almost remain stable which are quite important advantages over SPs. Both the location and orientation of SP may diverge, depending on the user's style of wearing and on the activity that the user is performing. Change in any of the above-discussed issues will reduce the effectiveness. Furthermore, some locations and positions simply do not generate the appropriate signatures for legitimate identification. Explicitly, the issue of orientation and location occurs with females because they frequently bring their SPs off the body, but in case of SW, the device will be carried in a fix position such as on the wrist almost all the time. Above all, a SW can easily transmit the data to other paired devices using Internet or Bluetooth which is evident that the SWs are superior for user identification for cloud-based secure applications like Internet banking or to access SHs.

To support the above-said discussion, we found that recently a South Korean telecommunication company named SK Telecommunication started working towards a system meant to use SW to provide legitimate user identification, in order to access a secure online banking application [8]. However, banking applications normally use security similar to that of most other applications, where accessing your bank online requires a special randomized key from your bank or a special USB drive or any other secure identification means. A custom-designed user identification application will simply allow customers to tap on their registered SW to access their online banking system without much effort. In addition to this, the online system is subject to powerful encryption at both ends to secure the user personal information.

Keeping in mind the computational sources of SWs, the proposed system will be fairly simple as the user only needs to register the SW to use it in conjunction with any digital banking portals to authorize legitimate user access. Once a user is registered, it presumably involves some sort of verification and identification or the user's SW can be given a tap while running the correct software for identification as a legitimate user. If the SW is lost or stolen, the user can pass a kill command to nullify the online access by SW. This system has a number of different possible ways in which it could pair up and identified a legitimate user on SW, and our proposed solution can be a foundation for such secure applications.

In addition to the above, SW-based legitimate user identification can support many other real-life applications, for example, acting as the foundation for a delegated identification system for SH. More specifically, while a legitimate user is approaching their SH, their SW transmits its sensor signal to the SH which would compare it with the previously sent signals, and if sensor signal matched, then it would open the door. The proposed solution can also be used for such kind of secure systems to identify a legitimate user with an acceptable accuracy with least computational power and time.

The rest of the paper is organized as follows: Section 2 describes the related work. Section 3 presents the procedure for collecting the raw signals from the six users performing five different activities and how the raw signal is transformed into a suitable format for machine learning algorithms. The results of these experiments are presented in Section 4. Section 5 discusses the immediate future extensions to the current research. Finally, Section 6 concludes the work.

2. Related Work

Recently, wearable devices like SWs have emerged in our daily lives. However, limited research has been done on legitimate user identification by these wearable devices. Besides, these several traditional legitimate user identification approaches have been proposed based on passwords such as secret information possession and physiological biometrics such as iris patterns and fingerprints. More recently, behavior-based legitimate user identification utilizes the distinct behavior of users such as gestures and gaits [5, 7].

Different physiological biometrics for legitimate user identification systems are out there, such as iris patterns [9], fingerprints [10], and face patterns. However, such legitimate user identification requires user interactions. For example, fingerprint identification needs users to put their finger on the scanner. Hence, these approaches requiring user compliance cannot achieve continuous and implicit identification [11] which was an ultimate goal of our proposed system to overcome.

In contrast to above-discussed solutions, behavior-based legitimate user identification assumes that the people have distinct but stable patterns for a certain behavior such as gait [5, 7, 12], handwriting patterns [13, 14], and GPS patterns [15]. Such legitimate user identification exploits users' behavioral patterns to identify a legitimate user. Some

important and classical works from the literature in the area that specifically use built-in sensors for legitimate user identification are discussed below.

Kayacik et al. [16] proposed a temporally and spatially aware user behavioral lightweight model based on hard and soft sensors. For some reason, they did not quantitatively show the legitimate identification performance, but they have shown that the attackers can be detected in 717 seconds. Buthpitiya et al. [15] proposed a GPS sensor-based system that could detect abnormal activities by analyzing legitimate users' location history. Trojahn and Ortmeier [14] and Shahzad et al. [13] have developed a mixture of a handwriting and keystroke-based method to achieve legitimate user identification through the screen sensor. Zhu et al. [17] proposed a system which constantly collects the data from three different built-in sensors namely the gyroscope, magnetometer, and accelerometer to construct gesture models while a legitimate user is using the device. Nickel et al. [12] proposed an accelerometer-based behavior recognition system for legitimate user identification using a k-nearest neighbor-based classification algorithm. Lee et al. [18, 19] empirically proved that using more sensors can improve legitimate user identification performance by using a support vector machine (SVM) as a final classification algorithm. Li et al. [20] proposed five basic movements, namely, sliding up, sliding down, sliding right, sliding left, and tapping and their related combinations as legitimate user behavioral patterns with which to perform legitimate user identification.

In regards to the works discussed above, Riva et al. [21] proposed a prototype using voice recognition, phone placement, and face recognition proximity to progressively identify a legitimate user. However, their objectives were just to decide when to identify the legitimate user and thus not match to the proposed framework. Furthermore, their scheme requires access to sensors that need users' permissions, which limiting their application for implicit legitimate user identification in a real-time environment. Mare et al. [22] proposed a two-fold legitimate user identification model in which the signals sent from a bracelet worn on the user's wrist are correlated with the operations of the terminal to confirm the continued presence of the user if the two movements correlate according to a few coarse-grained actions. Lee and Lee [11] proposed a legitimate user identification system named iAuth for implicit but continuous user identification in which the end user is identified based on their behavioral characteristics by leveraging the built-in sensors. They have built a system which gives better identification than previously possible using sensor data from multiple devices and machine learning techniques. Their system was able to consume only 2% of the battery to produce 92.1% accuracy.

To the best of our knowledge, there is no SW gait-based legitimate user identification research proposed in the literature that works in the way this one does including the ones discussed above. This study takes the advantage of the idea of identifying a legitimate user on SW by employing different activity patterns. Data on different activities are recorded using the embedded triaxial without limiting the scope only to a controlled environment. The aim of this work is to propose a semicontrolled environment system in which the proposed system overcomes the limitations of users' age, gender, SW wearing style (left or right hand), and regular activity style while wearing a SW. The user was enforced to perform daily activity differently at different times because the goal was to investigate the ambulatory activity performed by any user towards legitimate user identification in real-time scenarios.

Thus, this work introduces a novel two-fold legitimate user identification system in which the proposed system first recognizes the activity and then the identification process comes in to decide whether the recognized activity has been performed by a legitimate user or imposture. Additionally, this work experiments with a single-subject-cross-validation process to further validate a legitimate user identification. The proposed system is a semicontrolled environment-based activity recognition and legitimate user identification system.

3. System Modeling

This section describes the process for collecting the raw signals from different users performing different physical activities under study. This section also explains the process for extracting the meaningful features. Furthermore, we will explain the process of transforming the time series raw sensor signals into examples that can be handled by different classifiers from machine learning literature, for example, Decision Tree (DT), K-Nearest Neighbor (KNN), Support Vector Machine (SVM), and Naive Bayes (NB).

3.1. Data Collection. The raw signals were collected for five different activities from six users (three female and three male) having a mean age of twenty-five years old. The criterion for selecting the subjects was based on gender because different genders exhibit different patterns when performing the same activity. These activities include walking, walking upstairs, walking downstairs, running, and jogging. All subjects performed these activities twice each day for more than a month. Therefore, the proposed system utilizes the collected raw data from the same users for the same activity but performed on different days.

The participants enrolled in this study were approved by the laboratory head. This is a formal prerequisite because the experiments involved human subjects although there was a negligible risk of injury. The involved subjects were asked to answer a few nontechnical questions about their gender, age, height, weight, left-or-right handedness, and so on, which were used as characteristics in the proposed study. Then the subjects were asked to fasten the SW on their wrist and place a Bluetooth paired SP in their pocket. Both devices run a simple custom-designed application that controls the data collection process and instructs the participant to add their name and select the activity from the list of five different activities and the sensor from three different sensors. Once the initial instructions have been completed, the SP screen is turned off and placed into the pants pocket. The SP

instructs the SW running the paired data collection application to collect the raw signal at a rate of 20 Hz. Each of these sensors generates 3-dimensional signals and appends a timestamp to the values. After every five minutes, the SW sends the data to the SP, and after a successful transmission, the SP vibrates to notify the user that the data collection process has been successfully completed and they can stop the current activity.

3.2. Feature Extraction. SW sensor measurements are of the form (X, Y, Z) where X, Y, and Z are, respectively, the X, Y, and Z components of the acceleration relative to the smartwatch. The proposed system systematically removes the gravity component from each of the X, Y, and Z measurements. Raw accelerometer measurements are quite noisy since even a SW in a fixed position could return sensor measurements depicting bursts of acceleration. To minimize the effect of noise, the proposed system used a simple moving average based on a window of 3 points for each of the X, Y, and Z components. For each component, the smoothed time series was then broken into windows.

There are plenty of ways to prepare the raw sensor signals prior to using them for legitimate user identification. Some gait-based works utilized the data within the time domain [23–25] but other systems map the time series sensor data onto examples using a sliding window approach. This technique permits the use of traditional machine learning classification approaches to handling the time series data. Our proposed study also utilizes the same sliding window approach employed in the prior work [2, 5–7].

The discussed windowing process initially partitions the time series raw signal into 30 seconds non-overlapping windows. Then, from each window, the system generates relatively simple features (together with time and frequency) for each sensor individually but uses the same encoding technique [2]. Each feature is calculated from each axis of the raw signal. Since the data are sampled at 20 Hz and the window size is 30 seconds (which includes 25 samples within each iteration), there are 600 time series values per axis per window and 1800 values per window for three sensors. During the feature extraction process, the proposed system changes the window size from 25 samples per window to up to 400 samples per window in different experiments to further validate the behavior of window size for legitimate user identification.

The said process holds for all three sensors' data, and each of these time series values is transformed into 72 features using the feature encoding. The extracted features are average acceleration, average absolute difference, standard deviation, and average resultant acceleration, in which 1 feature for each axis is obtained (in total 4 features per axis), the average difference between peaks (10 features for each axis). Our system also calculates the binned distribution in which the proposed system determines what fraction of readings fall within a 10 equal-sized bins, and this function generates 10 features for each axis individually.

3.3. Classifiers. This work leverages the different classifiers available in Matlab. The literature has highlighted that each classifier will have varying results depending on what the proposed system is predicting. The training process involves learning in relation to the label user wants to predict [26]. For experimental setup, the proposed system involved four different types of classifiers, for example, DT, KNN, SVM, and NB in order to compare the performance.

3.3.1. Decision Tree (DT). In DTs, the input space is first separated by class regions to determine the DTs. Nodes are generated with decision functions that branch depending on the output of a decision. As one traverses from root to leaf, the classifier effectively narrows the prediction space until it reaches its final prediction at the leaf. Decision trees bring scalable and fast implementation with the need to tune many parameters [26].

3.3.2. K-Nearest Neighbors (KNN). When classifying a given unseen feature vector, KNN will find the k-nearest points given a distance function, look at all k training labels, and predict the label as the majority of the k labels. An advantage of KNN is its robustness against noisy data, and there is only the number of nearest neighbors which needs to carefully tune [26]. It is an instance-based classifier which is also one of the most popular classifiers used for SP-based PAR and is found to be the best in terms of performance and computational complexity as compared to the decision trees [27].

3.3.3. Support Vector Machine (SVM). SVM recognizes a diverse set of physical activities using motion and other sensors, and the literature has highlighted that their performance is superior to that of the other classifiers [28].

3.3.4. Naive Bayes (NB). NB is a simple and well-known classification method. NB is a probabilistic classifier [30], and Bayes' rule contains probabilistic models. Bayes' rule relies on the statistical properties of data and the accuracy of data. To begin with, it finds the solution from statistics as well as by data mining [29]. All of these classification methods are suitable for real-time legitimate user identification because they can be generated and evaluated rapidly.

The values used for the different parameters of the classification methods are as follows: SVM is used with a quadratic kernel function; KNN is used with a Euclidean distance function, and nearest neighbors are set to 10; DT is used with 85 as the number of trees. All the said parameters are carefully tuned and optimized prior to the final experimental setups. All the experiments are carried out using Matlab R2014b and installed on core i5 and 8 GB of RAM machine.

4. System Setup

The output of each classifier result is a strong indicator of the system's ability to predict the legitimate user of the SW. 10-fold-cross-validation has been performed to extract the meaningful information for each legitimate user. In each experiment, the user's data are split into 10 subsets in which

a single subset is chosen as a validation set towards legitimate user identification and the rest of the 9 subsets are used as training data to be fed into each classifier individually. Classifier results are generated with the given setup with every instance in the validation set being classified against the training sets. This entire process is repeated for every activity and each user and for all three sensors by picking each subsequent subset as a validation set with the reaming as the training set. Leading to a total of 30 experiments for a single sensor's data, 90 experiments for all 3 sensors and 360 experiments for all four classifiers which are weighted for the final results to identify either a legitimate user or imposture.

4.1. Experimental Setup. The first experimental setup compared the performance of four different classifiers for three different sensors data for a fixed number of samples per window, after which each classifier was chosen and tested multiple times while changing the number of samples per window, that is, 25, 50, 75, 100, 125, 150, 175, 200, 225, 250, 275, 300, 325, 350, 375, and 400 samples. The main goal of our second experiment was to measure the effect of changing the window size on the performance of each classifier. In both experimental setups, the training and testing data are randomly divided, and classification results are obtained using a 10-fold-cross-validation process.

4.2. Experimental Results. The SW gait-based legitimate user identification task is first to identify a user from a pool of users and then to verify that specific user can access the device based on a sample of the user's performed activities taken from the selected sensor. This process requires the training data from all the users and their performed activities. Such experiments seem fairly simple, such as the transformed data associated with the sensor data are individually used to train and evaluate using 10-cross-validation. In the identification process, each user has its own classification model, and when a sample is provided, the model determines whether the sample belongs to the legitimate user or to an imposter. This identification experiments and evaluates a model for each of the 6 participants in the study, and in each case, each activity is considered independently.

Here, we turn to the first experimental results, in which we used a fixed sample size in each window. Table 1 shows the raw accuracy for legitimate user identification for three different sensors and four classifiers based on the performed activities. Straight walking activity-based legitimate user identification using the accelerometer sensor performed better than the other activity-based methods over a DT classifier with an accuracy of 98.68%.

These results show that even 400 samples per window are sufficient to identify a user most of the time especially if one uses the accelerometer data with a classifier other than NB. Here, one can note that the accelerometer sensor data are clearly more informative and helpful in identifying a legitimate user than the magnetometer and gyroscope data.

The gait-based legitimate user identification process explained above involves building a single predictive model to first identify a specific user from a set of users and then deciding whether the identified user is legitimate or an impostor. At the lowest level, the results are based on identifying an individual user based on 400 samples per window of data for different activities performed at different times. However, one can improve the proposed model by using more data and then employing a majority voting scheme to identify a legitimate user from the pool of different users.

In order to demonstrate how this scheme works and to provide greater insight into the results, confusion matrices are generated for each user which is presented in the following tables. Due to space limitations, Table 1 shows the overall results only for legitimate user identification based on different activities performed by the legitimate user or impostor. The results shown in the tables are based on an identification model generated from three sensors' data and four different classifiers.

The columns in Tables 2 and 3 correspond to the predicted users and the rows correspond to the actual users. Thus, the values in the diagonal in boldface correspond to correct identification of the legitimate user while the rest of the values correspond to identification of an impostor as a legitimate user or vice versa. The obtained results clearly indicate the ability of the proposed model to correctly identify the legitimate user. Based on the stated results, one can compute the accuracy for identifying a legitimate user or accuracy for aggregated overall six users. For example, the accuracy for correctly identifying the legitimate user 1 is almost 97.81% while the accuracy for identifying the legitimate user 2 is 98.26%. Whereas, the overall accuracy would be simply the total number of correct predictions divided by the total number of predictions in the case of a DT classifier using accelerometer sensor data.

The corresponding results interpreted with the most predicted legitimate user strategy are shown in Tables 1–3 within a fixed size of the window for each activity. This strategy always leads to perfect results except for the case of NB classifier. Based on a visual inspection of the confusion matrices and based on the fact that there is usually no second user who gets nearly as many votes as the actual user. We believe that for the population used in this experiment, one could get perfect legitimate user identification accuracy using fairly small samples of data.

For trusted external judgments and for statistical analysis of any legitimate user identification system, true positive, true negative, false positive, and false negative are usually compared. The terms true and false refer to whether the prediction corresponds to the external judgment or not and the terms positive and negative refer to the classifier's prediction. The test names in Tables 4 and 5 are abbreviated as TPR = true positive rate, TNR = true negative rate, FPR = false positive rate, FNR = false negative rate, PPV = positive predictive values, NPV = negative predictive values, SEN = sensitivity, SEP = specificity, FDR = false discovery rate, FOR = false omission rate, and ACC = individual user identification accuracy.

Table 1: Average accuracy for legitimate user identification with 400 samples per window.

Sensor	Activities	Classifiers			
		DT	SVM	KNN	NB
Acc.	Walking	**0.9868 ± 0.0094**	0.9391 ± 0.0181	0.9375 ± 0.0171	0.7616 ± 0.0201
	Walking up	**0.8753 ± 0.0327**	0.8005 ± 0.0422	0.7874 ± 0.0388	0.5876 ± 0.0540
	Walking down	**0.8835 ± 0.0383**	0.8447 ± 0.0534	0.7831 ± 0.0598	0.5619 ± 0.0909
	Running	**0.8168 ± 0.0363**	0.6381 ± 0.0554	0.5969 ± 0.0477	0.5311 ± 0.0325
	Jogging	**0.9572 ± 0.0147**	0.8816 ± 0.0163	0.9260 ± 0.0236	0.6234 ± 0.0384
Gyr.	Walking	**0.9638 ± 0.0115**	0.9177 ± 0.0268	0.9504 ± 0.0066	0.5149 ± 0.0367
	Walking up	**0.8575 ± 0.0389**	0.8362 ± 0.0333	0.8313 ± 0.0181	0.5423 ± 0.0683
	Walking down	**0.8983 ± 0.0453**	0.8062 ± 0.0339	0.8126 ± 0.0225	0.5476 ± 0.0595
	Running	**0.8521 ± 0.0651**	0.6737 ± 0.0390	0.7359 ± 0.0220	0.5866 ± 0.0483
	Jogging	**0.9424 ± 0.0163**	0.8964 ± 0.0272	0.8903 ± 0.0095	0.6629 ± 0.0376
Mag.	Walking	**0.9193 ± 0.0208**	0.7699 ± 0.0259	0.8551 ± 0.0339	0.6777 ± 0.0339
	Walking up	**0.7600 ± 0.0549**	0.5951 ± 0.0486	0.7107 ± 0.0405	0.5907 ± 0.0674
	Walking down	**0.8298 ± 0.0543**	0.7233 ± 0.0486	0.7055 ± 0.0671	0.5826 ± 0.0716
	Running	**0.6384 ± 0.0611**	0.5768 ± 0.0339	0.5916 ± 0.0481	0.3524 ± 0.0589
	Jogging	**0.7056 ± 0.0461**	0.4637 ± 0.0419	0.5873 ± 0.0361	0.3340 ± 0.0287

Table 2: Confusion matrix according to the users using 400 samples per window with accelerometer and gyroscope sensors.

Users	Accelerometer sensor						Gyroscope sensor					
	User 1	User 2	User 3	User 4	User 5	User 6	User 1	User 2	User 3	User 4	User 5	User 6
DT classifier												
User 1	**1710**	2	6	40	1	42	**1246**	1	0	12	3	44
User 2	0	**1796**	48	9	35	6	29	**1889**	42	1	78	17
User 3	0	40	**1774**	31	125	0	1	19	**1772**	30	123	15
User 4	12	13	11	**1695**	18	45	32	7	19	**1699**	7	31
User 5	18	24	40	2	**1457**	0	0	21	69	0	**1476**	4
User 6	121	16	3	49	1	**1880**	140	2	4	30	0	**1895**
SVM classifier												
User 1	**1473**	16	27	76	28	135	**1511**	32	9	63	1	100
User 2	9	**1597**	91	40	84	9	53	**1787**	51	10	110	40
User 3	14	165	**1568**	51	163	0	18	36	**1576**	26	181	20
User 4	26	81	75	**1644**	22	68	69	3	37	**1627**	1	33
User 5	50	48	134	9	**1346**	0	4	39	119	0	**1344**	29
User 6	152	0	8	53	16	**1781**	185	4	4	69	5	**1862**
KNN classifier												
User 1	**1514**	11	15	59	19	113	**1428**	13	18	17	0	79
User 2	1	**1679**	131	24	132	23	52	**1779**	109	29	238	88
User 3	10	113	**1616**	12	111	7	0	12	**1638**	37	184	36
User 4	41	56	11	**1575**	5	83	97	16	27	**1680**	8	87
User 5	15	46	89	3	**1332**	0	4	37	53	21	**1282**	3
User 6	238	13	10	68	7	**1888**	183	4	6	43	0	**1749**
NB classifier												
User 1	**1008**	49	108	178	24	205	**593**	83	4	12	62	102
User 2	1	**1370**	112	35	169	2	79	**1264**	28	12	244	68
User 3	40	230	**1069**	32	218	35	131	94	**974**	191	96	44
User 4	221	211	157	**1079**	29	127	364	50	561	**1104**	601	106
User 5	190	83	350	28	**1472**	119	74	177	193	41	**611**	23
User 6	338	10	58	438	52	**1566**	487	202	132	485	82	**1693**

PPVs are the scores of the positive statistical results based on true positive and true negative values. PPV shows the performance of a statistical measure and in the proposed model it has been used to confirm the probability of positive and negative results. A higher value of PPV indicates that fewer positive results are false. False Omission Rate and False Discovery Rate is a statistical method used in multiple hypothesis testing to correct for multiple comparisons. It measures the proportion of false negatives which are incorrectly rejected. FOR is computed by using false negative and true positive and it can also be computed by taking the complement of NPVs. FDR measures the proportion of actual positives that are incorrectly identified. FDR is also one way to abstracting the rate of type I errors in null

Table 3: Confusion matrix according to the users using 400 samples per window and magnetometer sensor.

Users	User 1	User 2	User 3	User 4	User 5	User 6
DT classifier						
User 1	**1230**	48	17	151	21	184
User 2	39	**1499**	63	49	89	43
User 3	29	136	**1551**	110	282	9
User 4	160	101	125	**1476**	84	79
User 5	51	63	188	17	**1138**	1
User 6	263	22	3	37	3	**1696**
SVM classifier						
User 1	**1005**	73	19	168	52	302
User 2	137	**1244**	292	69	72	110
User 3	56	284	**1124**	167	511	15
User 4	147	220	184	**1166**	107	94
User 5	48	68	238	24	**914**	29
User 6	343	28	23	178	26	**1521**
KNN classifier						
User 1	**1300**	41	21	233	45	318
User 2	78	**1423**	168	93	132	47
User 3	34	182	**1311**	134	353	48
User 4	198	103	167	**1248**	87	178
User 5	45	79	226	45	**998**	4
User 6	168	24	29	64	2	**1425**
NB classifier						
User 1	**763**	99	49	201	72	354
User 2	149	**1047**	224	103	75	200
User 3	135	339	**1003**	190	511	65
User 4	343	258	269	**1050**	298	368
User 5	109	44	186	54	**594**	0
User 6	879	108	139	175	121	**1078**

hypothesis testing when conducting multiple comparisons between classes. FDR is computed by using FP and TP.

The second experimental study is based on varying the window size for the legitimate user identification process. The window size is an important system parameter which determines the time that the system needs to perform an identification, that is, window size directly determines the system's identification frequency. In this experiment, the system varies the window size from 25 samples per window to 400 samples per window with 25 sample blocks within each window. Given a fix window size for each targeted user, the model is learned using 10-fold-cross-validation for training, validation, and testing. Here, we utilize the average accuracy across all activities stated before. In these experiments, we investigate the influence of the window size on average accuracy in choosing a proper window size. Within each window, another important system parameter is the total number of samples from the 3-dimensional signal which affects the average and overall accuracy because a larger training set provides the system more information but allows more chances for the system to be overwhelmed and degrades the classifier's generalization performance. According to the observations; the largest number of samples per window produces the maximum accuracy in almost all cases and for each activity, particularly, when the number of samples per window exceeds 200 samples or more. The accuracy decreases when the training set size is lower than 200 because a larger training set is likely to cause over-fitting so that the constructed training model would introduce more errors than expected. The detailed results over a different number of samples per windows with a 99% confidence interval are shown in Figures 1–3.

5. Discussion

The outcomes of the activity recognition and identification experiments described above provide the overall results for the proposed identification model. Recall that the results presented in Tables 1–3 have been aggregated over all identification models, that is, one per subject and all identification decisions presented here are based on multiple instances, that is, 25–400 samples per window of data. The results in Figures 1–3 indicate that SW-based identification can be relatively accurate when using only 400 samples per window of data from different activities performed by each user. Form the identification results, one can confirm that the accelerometer sensor data performs slightly better than the gyroscope sensor data and together the accelerometer and gyroscope sensors produce much higher identification results than the magnetometer sensor. In terms of classifiers, DT outperforms the KNN, SVM, and NB classifiers. In this sequence, KNN outperforms the SVM and NB but performs less well than Dts. SVM slightly underperforms against KNN but performs much better than NB classifier.

Activity recognition-based user identification models perform much better for almost all activities except for running. The overall accuracy for the proposed activity recognition-based identification is almost 98% for walking

Table 4: Statistical results for four different classifiers using accelerometer and gyroscope sensors data.

Metric	Method	Accelerometer sensor						Gyroscope sensor					
		User 1	User 2	User 3	User 4	User 5	User 6	User 1	User 2	User 3	User 4	User 5	User 6
TPR	DT	0.9495	0.9483	0.9005	0.9448	0.9455	0.9083	0.9540	0.9188	0.9041	0.9465	0.9401	0.9150
	SVM	0.8393	0.8727	0.7996	0.8580	0.8481	0.8861	0.8805	0.8713	0.8487	0.9192	0.8756	0.8746
	KNN	0.8746	0.8437	0.8646	0.8893	0.8969	0.8489	0.9183	0.7752	0.8589	0.8773	0.9157	0.8811
	NB	0.6412	0.8111	0.6583	0.5917	0.6566	0.6361	0.6927	0.7457	0.6366	0.3963	0.5460	0.5495
TNR	DT	0.9837	0.9897	0.9882	0.9859	0.9811	0.9897	0.9786	0.9942	0.9848	0.9919	0.9770	0.9872
	SVM	0.9730	0.9664	0.9632	0.9749	0.9669	0.9766	0.9648	0.9873	0.9761	0.9819	0.9687	0.9751
	KNN	0.9673	0.9736	0.9722	0.9821	0.9714	0.9745	0.9646	0.9906	0.9767	0.9839	0.9555	0.9677
	NB	0.9197	0.9400	0.9198	0.9258	0.9464	0.9455	0.8888	0.9354	0.9037	0.9105	0.8909	0.9570
FPR	DT	0.0505	0.0517	0.0995	0.0552	0.0546	0.0918	0.0459	0.0812	0.0959	0.0535	0.0599	0.0849
	SVM	0.1607	0.1273	0.2004	0.1419	0.1519	0.1139	0.1195	0.1287	0.1513	0.0808	0.1244	0.1254
	KNN	0.1254	0.1563	0.1354	0.1107	0.1030	0.1511	0.0817	0.2248	0.1411	0.1227	0.0843	0.1189
	NB	0.3588	0.1889	0.3417	0.4084	0.3434	0.3639	0.3072	0.2543	0.3634	0.6037	0.4539	0.4505
FNR	DT	0.0164	0.0104	0.0119	0.0141	0.0189	0.0103	0.0214	0.0057	0.0152	0.0081	0.0229	0.0128
	SVM	0.0269	0.0336	0.0368	0.0250	0.0330	0.0234	0.0352	0.0127	0.0239	0.0181	0.0313	0.0248
	KNN	0.0326	0.0263	0.0278	0.0178	0.0286	0.0255	0.0354	0.0094	0.0234	0.0161	0.0445	0.0323
	NB	0.0803	0.0599	0.0802	0.0741	0.0536	0.0545	0.1112	0.0647	0.0963	0.0895	0.1091	0.0429
PPV	DT	0.9495	0.9483	0.9005	0.9448	0.9455	0.9082	0.9541	0.9188	0.9041	0.9465	0.9401	0.9150
	SVM	0.8393	0.8727	0.7996	0.8580	0.8481	0.8861	0.8805	0.8713	0.8487	0.9192	0.8756	0.8746
	KNN	0.8746	0.8437	0.8646	0.8893	0.8969	0.8489	0.9183	0.7752	0.8589	0.8773	0.9157	0.8811
	NB	0.6412	0.8111	0.6582	0.5916	0.6566	0.6361	0.6928	0.7457	0.6366	0.3963	0.5460	0.5495
NPV	DT	0.9837	0.9896	0.9881	0.9859	0.9811	0.9897	0.9786	0.9942	0.9848	0.9919	0.9770	0.9872
	SVM	0.9730	0.9664	0.9632	0.9749	0.9669	0.9765	0.9648	0.9873	0.9761	0.9819	0.9687	0.9751
	KNN	0.9673	0.9737	0.9722	0.9821	0.9714	0.9745	0.9646	0.9906	0.9767	0.9839	0.9555	0.9677
	NB	0.91975	0.9400	0.9198	0.9259	0.94643	0.9455	0.8888	0.9353	0.9037	0.9105	0.8909	0.9570
SEN	DT	0.9189	0.9498	0.9426	0.9283	0.8900	0.9529	0.8605	0.9742	0.9297	0.9588	0.8749	0.9447
	SVM	0.8544	0.8374	0.8239	0.8777	0.8113	0.8936	0.8212	0.9400	0.8775	0.9064	0.8185	0.8935
	KNN	0.8323	0.8754	0.8632	0.9047	0.8293	0.8931	0.8095	0.9559	0.8849	0.9195	0.7488	0.8565
	NB	0.5606	0.7015	0.5766	0.6028	0.7495	0.7624	0.3432	0.6759	0.5148	0.5984	0.3603	0.8315
SPE	DT	0.9901	0.9893	0.9787	0.9893	0.9911	0.9791	0.9936	0.9811	0.9788	0.9893	0.9896	0.9799
	SVM	0.9698	0.9745	0.9571	0.9704	0.9744	0.9747	0.9778	0.9712	0.9697	0.9846	0.9797	0.9702
	KNN	0.9765	0.9660	0.9725	0.9789	0.9838	0.9625	0.9863	0.9439	0.9708	0.9745	0.9874	0.9738
	NB	0.9413	0.9662	0.9419	0.9226	0.9185	0.9043	0.9718	0.9531	0.9394	0.8176	0.9458	0.8463
FDR	DT	0.0505	0.0517	0.0995	0.0552	0.0545	0.0918	0.0459	0.0812	0.0959	0.05349	0.0599	0.0849
	SVM	0.1607	0.1273	0.2004	0.1419	0.1519	0.1139	0.1195	0.1287	0.1513	0.0808	0.1244	0.1254
	KNN	0.1254	0.1563	0.1354	0.1107	0.1030	0.1511	0.0817	0.2248	0.1411	0.1227	0.0843	0.1189
	NB	0.3588	0.1889	0.3417	0.4084	0.3434	0.3639	0.3072	0.2543	0.3634	0.6037	0.4539	0.4505
FOR	DT	0.0163	0.0104	0.0119	0.0142	0.0189	0.0103	0.0214	0.0057	0.0152	0.0081	0.0229	0.0128
	SVM	0.0269	0.0336	0.0368	0.0250	0.0330	0.0234	0.0352	0.0127	0.0239	0.0181	0.0313	0.02486
	KNN	0.0327	0.0263	0.0278	0.0179	0.0286	0.0255	0.0354	0.0094	0.0233	0.0161	0.0445	0.0323
	NB	0.0803	0.0599	0.0802	0.0741	0.0536	0.0545	0.1112	0.0647	0.0963	0.0895	0.1091	0.0429
ACC	DT	0.9781	0.9826	0.9725	0.9792	0.9762	0.9744	0.9756	0.9798	0.97007	0.9843	0.9716	0.9733
	SVM	0.9518	0.9509	0.9342	0.9547	0.9499	0.9601	0.9517	0.9658	0.9547	0.9719	0.9558	0.9558
	KNN	0.9528	0.9503	0.9540	0.9672	0.9614	0.9492	0.9581	0.9459	0.9564	0.9655	0.9504	0.9522
	NB	0.8814	0.9209	0.8826	0.8724	0.8894	0.8787	0.8737	0.9063	0.8668	0.7811	0.8561	0.8436

activity and 93% accuracy for jogging and 82% to 86% for the rest of the activities-based user identification model. The results of the proposed two-fold activity recognition and legitimate user identification model are presented in Figures 1–3 and Tables 1–5 which show the ability to efficiently recognize the individual activity and identification based on the recognized activity of the individual user.

As we earlier explained, there is no research in the literature as similar to the work presented in this paper. However, we found two closely related works, and their comparison results are presented in Table 6. These methods have exactly been tested as the settings mentioned in their respective works. Based on the results, one can conclude that the activity recognition-based legitimate user identification framework performed better because we used a single predictive model and ambiguity activity recognition analysis that significantly help the model to perform better in the identification process.

We also measured the time for doing activity recognition and user identification in the proposed system which is less than 5 seconds in extreme case of 400 samples per window as shown in Figure 4. One can also observe that as we decrease

Table 5: Statistical results for four different classifiers using magnetometer sensor data.

Metric	Method	User 1	User 2	User 3	User 4	User 5	User 6
TPR	DT	0.7450	0.8412	0.7326	0.7289	0.7805	0.8379
	SVM	0.6206	0.6465	0.5211	0.6079	0.6919	0.7178
	KNN	0.6639	0.7331	0.6358	0.6299	0.7144	0.8324
	NB	0.4961	0.582	0.4472	0.4060	0.6018	0.4312
TNR	DT	0.9424	0.9601	0.9557	0.9597	0.9501	0.9650
	SVM	0.9226	0.9263	0.9151	0.9337	0.9211	0.9385
	KNN	0.9425	0.9529	0.9320	0.9373	0.9359	0.9363
	NB	0.8403	0.9139	0.9079	0.9203	0.8990	0.8922
FPR	DT	0.2549	0.1588	0.2674	0.2711	0.2195	0.1621
	SVM	0.3793	0.3534	0.4789	0.3921	0.3081	0.2822
	KNN	0.3361	0.2669	0.3642	0.3700	0.2856	0.1676
	NB	0.5039	0.4177	0.5528	0.5939	0.3982	0.5688
FNR	DT	0.0576	0.0399	0.0443	0.0403	0.0499	0.0349
	SVM	0.0774	0.0737	0.0849	0.0663	0.0789	0.0615
	KNN	0.0575	0.0471	0.0679	0.0627	0.064	0.0637
	NB	0.1597	0.0861	0.0921	0.0797	0.1009	0.1078
PPV	DT	0.7450	0.8411	0.7326	0.7289	0.7805	0.8379
	SVM	0.6208	0.6466	0.5211	0.6079	0.6919	0.7178
	KNN	0.6639	0.7331	0.6358	0.6299	0.7144	0.8324
	NB	0.4961	0.5823	0.4472	0.4060	0.6018	0.4312
NPV	DT	0.9424	0.9601	0.9557	0.9597	0.9501	0.9650
	SVM	0.9226	0.9263	0.9151	0.9337	0.9211	0.93847
	KNN	0.9425	0.9529	0.9320	0.9373	0.9359	0.9363
	NB	0.8403	0.9139	0.9078	0.9203	0.8990	0.8922
SEN	DT	0.6941	0.8020	0.7966	0.8022	0.7038	0.8429
	SVM	0.5789	0.6489	0.5979	0.6580	0.5434	0.7344
	KNN	0.7131	0.7684	0.6821	0.6868	0.6172	0.70545
	NB	0.3209	0.5525	0.5364	0.5922	0.3555	0.5220
SPE	DT	0.9547	0.9692	0.9379	0.9404	0.9661	0.9637
	SVM	0.9341	0.9256	0.8874	0.9190	0.9566	0.9335
	KNN	0.9287	0.9437	0.9177	0.9206	0.9577	0.9682
	NB	0.9164	0.9230	0.8732	0.8445	0.9606	0.8517
FDR	DT	0.2549	0.1588	0.2674	0.2711	0.2195	0.1621
	SVM	0.3792	0.3534	0.4789	0.3921	0.3081	0.2822
	KNN	0.3361	0.2669	0.3642	0.3700	0.2856	0.1676
	NB	0.5039	0.4177	0.5528	0.5939	0.3982	0.5688
FOR	DT	0.0576	0.0399	0.0443	0.0403	0.0499	0.0349
	SVM	0.0774	0.0737	0.0849	0.0663	0.0789	0.0615
	KNN	0.0575	0.04709	0.0679	0.0627	0.064	0.0637
	NB	0.1597	0.0861	0.0921	0.0797	0.1009	0.1078
ACC	DT	0.9129	0.9409	0.9129	0.9174	0.9277	0.9418
	SVM	0.8784	0.8777	0.8382	0.8772	0.8937	0.8962
	KNN	0.8931	0.9143	0.8768	0.8822	0.9079	0.9202
	NB	0.7949	0.8628	0.8192	0.8061	0.8738	0.7933

the size of the window (i.e., we increase the number of samples for training model), the time for doing an implicit activity recognition and user identification increases slowly at first and then sharply increases when the size of the window decreases from 150 samples per window. One can also observe from identification results that the higher the window size, the better the identification results. Therefore, the proposed system can achieve acceptable performance in terms of accuracy and computational time which makes the proposed system efficient and applicable in real-world scenarios.

We have also analyzed the model's ability to defend against impostures such as masquerading attacks. Recall that the goal of the proposed model was to prevent an imposture from getting access to the secure and sensitive information or services against the stored passwords. The obtained results also show that the proposed model is secure against the masquerading attacks. The term "secure" means that the imposture cannot cheat the system by performing these attacks in a short time. Therefore, the proposed system performed well in recognizing the adversary who is launching the masquerading attack. Thus, within several windows, the probability for imposture escaping detection is 0.038% only. Therefore, the proposed system shows good performance in defending against masquerading attacks too.

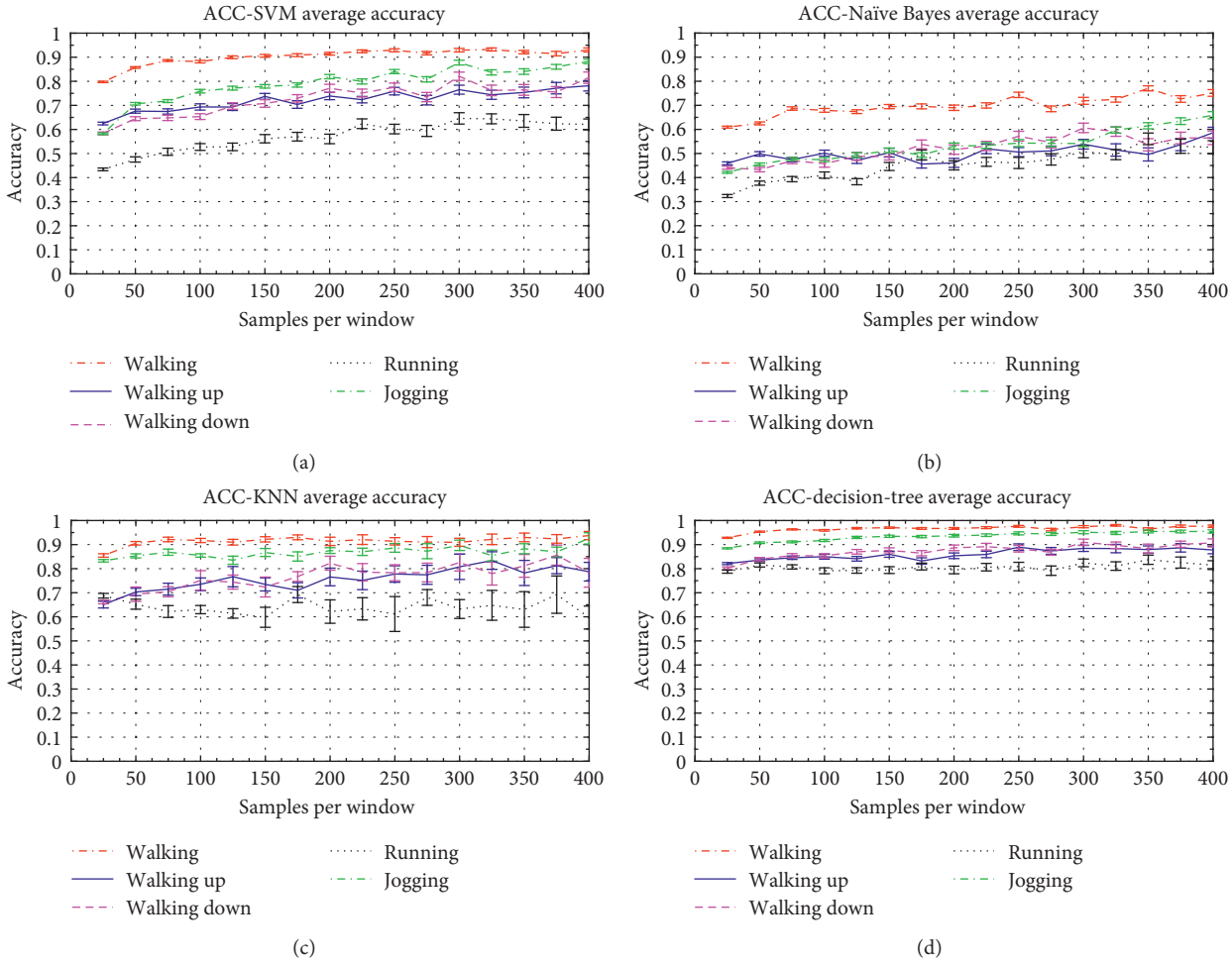


Figure 1: Accelerometer sensor-based accuracy for SVM, NB, KNN, and DT classifiers (a–d).

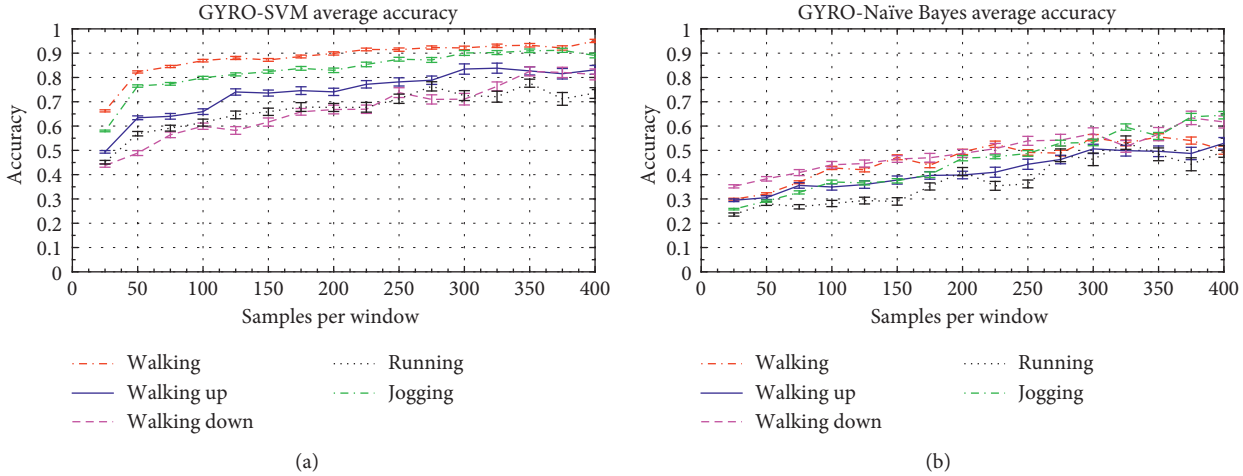


Figure 2: Continued.

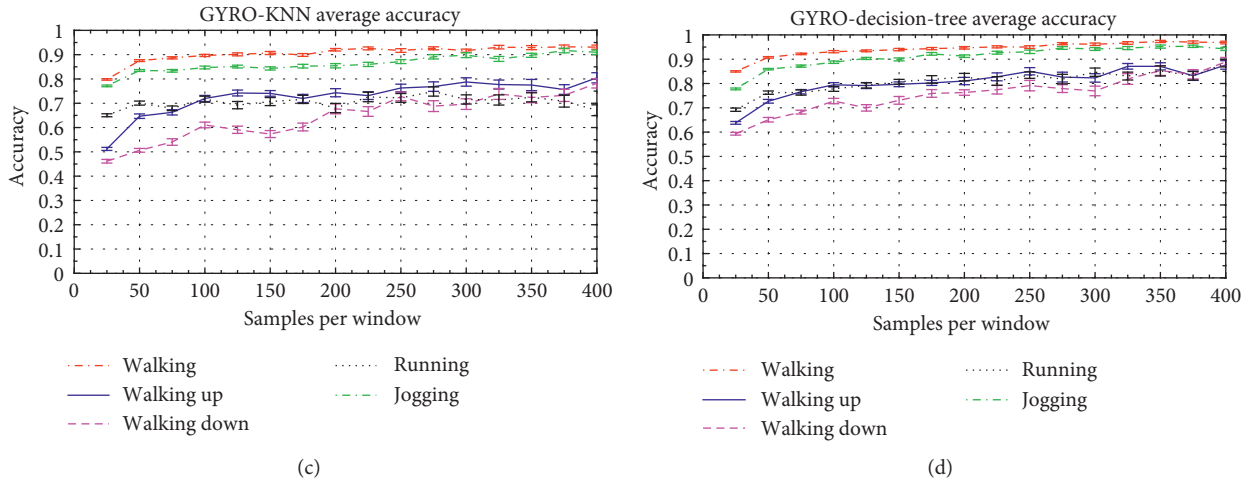


Figure 2: Gyroscope sensor-based accuracy for SVM, NB, KNN, and DT classifiers (a–d).

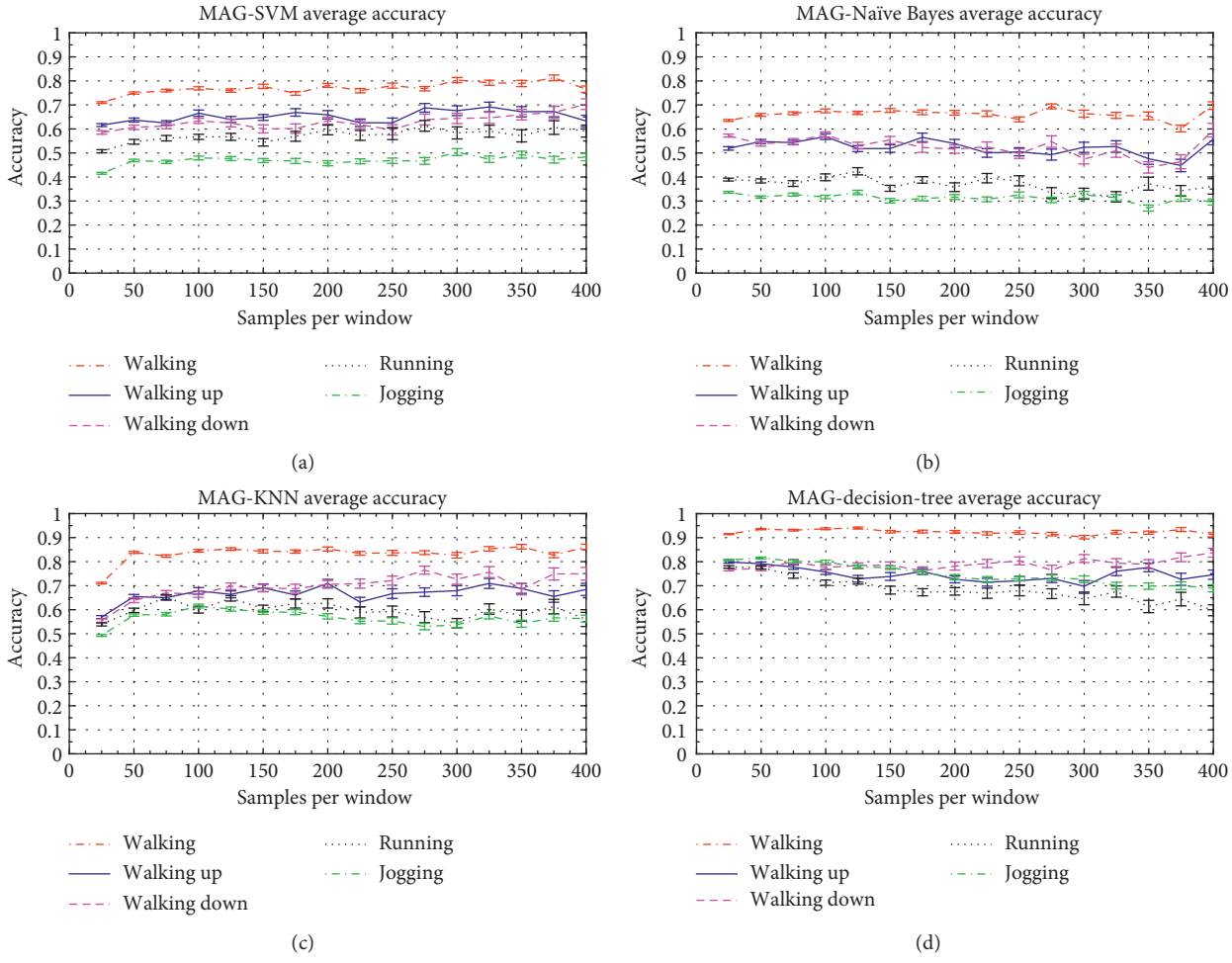


Figure 3: Magnetometer sensor-based accuracy for SVM, NB, KNN, and DT classifiers (a–d).

6. Future Work

The goal of this research was to show that activity recognition-based legitimate user identification is an effective approach in gait-based identification domain. As we have shown, it is possible to distinguish between both individuals performing the same activity. An immediate question we have for future work is to determine how identification time can be improved

Table 6: Comparison with state-of-the-art work.

Reference	Sensor		
	Accelerometer	Gyroscope	Magnetometer
[1]	97.2%	93.8%	—
[9]	92.1% combined		—
Proposed work	98.7%	96.4%	91.9%

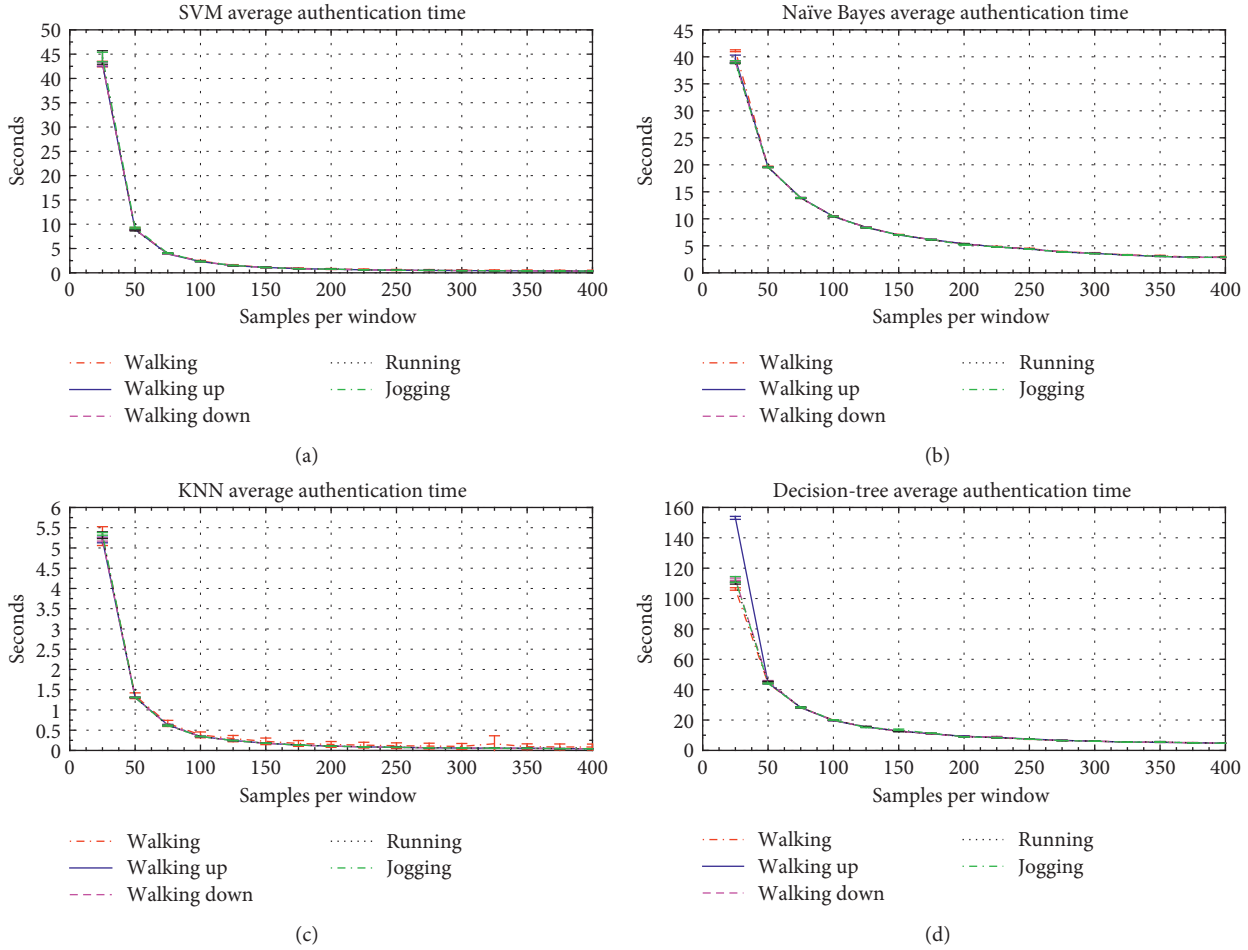


Figure 4: Identification time for SVM, NB, KNN, and DT classifiers (a–d).

within different activities as a first step. For this, the immediate solution is to use any lightweight feature selection method which somehow will help to improve the discriminative power and reduce the dimensions at the same time. To the best of our knowledge, this idea is relatively new in SW-based activity recognition and identification. The preliminary results indicate that this is indeed a promising area of research.

Additionally, as discussed above, a key limitation to activity recognition-based user identification is the variability of the signal. Our future work will focus on studying the potential of a further windowing process and feature selection. We will then use simple DT, KNN, and SVM classifiers. However, from the current results, one can observe that the DT classifier outperformed all other classifiers. When using the DT classifier, the results are promising for both activity recognition and user identification. However, this study was conducted on a relatively small set of users. The experimental dataset includes 5 activities performed by 6 six users per activity but the advantage is this dataset does not distribute classes uniformly. This has led to a set of results in line with other state-of-the-art works.

In addition to the above, future work would entail bulking out the experimental dataset with more users (*more than 15*), activities (*more than 10*), and training runs. Finally, our experimental dataset was collected using Android SWs running in Android Wear OS. It would be useful to use different SWs running different operating systems. We believe it is useful to measure PAR-based user identification on a wide verity of SWs. One final goal of this study was to incorporate this technology into a real-time system.

7. Conclusion

Smartwatches are becoming increasingly popular. This popularity has forced the community to study the security implications of these small and powerful devices. It has been suggested that activity recognition and gait-based identification combined with SWs are possible. This study described an effective two-fold system for performing SW-based activity recognition and user identification. This study demonstrates that gait as measured by the commercial grade SW sensor is sufficient to identify an individual with modest accuracy. Furthermore, a simple sliding window approach is shown to be sufficient for representing the time series sensor data. Experimental results demonstrate the advantage of combining the time and frequency domain information. The proposed system can achieve user identification average accuracy up to 98.68% with negligible system overhead, minimum time, and power consumption. We hope that the proposed system can act as a key technique for implicit activity recognition-based legitimate user identification in real-world scenarios.

Data Availability

The experimental datasets will be provided upon reasonable requests to mahmad00@gmail.com.

Conflicts of Interest

The authors have no conflicts of interest to declare.

Authors' Contributions

The authors Mohammed A. Alqarni, Asad Khan, Adil Khan, Sajjad Hussain Chauhdary, Manuel Mazzara, Tariq Umer, and Salvatore Distefano contributed equally to this work.

References

[1] A. M. Khattak, N. Akbar, M. Aazam et al., "Context representation and fusion: advancements and opportunities," *Sensors*, vol. 14, no. 6, pp. 9628–9668, 2014.

[2] A. H. Johnston and G. M. Weiss, "Smartwatch-based biometric gait recognition," in *Proceedings of 7th IEEE International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–6, Washington, DC, USA, September 2015.

[3] J. Siegal, "Smartwatch sales set to explode, expected to top 100m within four years," September 2013, http://bgr.com/2013/09/27/smartwatch-sales-forecast-2020/.

[4] J. A. Hughes, J. A. Brown, and A. M. Khan, "Smartphone gait fingerprinting models via genetic programming," in *Proceedings of IEEE International Joint Conference on Neural Networks (IEEE IJCNN) in conjunction with IEEE World Congress on Computational Intelligence (IEEE WCCI)*, pp. 408–415, Vancouver, BC, Canada, July 2016.

[5] M. Ahmad, A. M. Khan, J. A. Brown, S. Protasov, and A. M. Khattak, "Gait fingerprinting-based user identification on smartphones," in *Proceedings of IEEE International Joint Conference on Neural Networks (IEEE IJCNN) in conjunction with IEEE World Congress on Computational Intelligence (IEEE WCCI)*, pp. 3060–3067, Vancouver, BC, Canada, July 2016.

[6] M. Ahmad and A. M. Khan, *Seeking Optimum System Settings for Physical Activity Recognition on Smartwatches* CoRR abs/1706.01720, Cornell University Library, Ithaca, NY, USA, 2017.

[7] M. Ahmad and A. M. Khan, *Extended Sammon Projection and Wavelet Kernel Extreme Learning Machine for Gait Based Legitimate User Identification on Smartphones (GUI)*, CoRR abs/1706.01720, Cornell University Library, Ithaca, NY, USA, 2017.

[8] April 2017 https://www.androidheadlines.com/2017/01/sk-telecom-outs-smartwatch-based-identification-system.html.

[9] M. Qi, "User-specific iris authentication based on feature selection," in *Proceedings of IEEE International Conference on Computer Science and Software Engineering*, pp. 1040–1043, Washington, DC, USA, 2008.

[10] L. Hong and A. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 12, pp. 1295–1307, 1998.

[11] W.-H. Lee and R. Lee, "Implicit sensor-based authentication of smartphone users with smartwatch," in *Proceedings of the Hardware and Architectural Support for Security and Privacy*, pp. 1–9, Seoul, Republic of Korea, June 2016.

[12] C. Nickel, T. Wirtl, and C. Busch, "Authentication of smartphone users based on the way they walk using k-NN algorithm," in *Proceedings of IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pp. 16–20, Piraeus-Athens, Greece, July 2012.

[13] M. Shahzad, A. X. Liu, and A. Samuel, "Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it," in *Proceedings of 19th Annual International Conference on Mobile Computing and Networking (MobiCom)*, pp. 39–50, Miami, FL, USA, January 2013.

[14] M. Trojahn and F. Ortmeier, "Toward mobile authentication with keystroke dynamics on mobile phones and tablets," in *Proceedings of IEEE Advanced Information Networking and Applications Workshops*, pp. 697–702, Barcelona, Spain, March 2013.

[15] S. Buthpitiya, Y. Zhang, A. K. Dey, and M. Griss, "n-gram geo-trace Modeling," in *Proceedings of 9th International Conference on Pervasive Computing*, pp. 97–114, San Francisco, CA, USA, June 2011.

[16] H. G. Kayacik, M. Just, L. Baillie, D. Aspinall, and N. Micallef, "Data-driven authentication: on the effectiveness of user behavior modeling with mobile device sensors," in *Proceedings of the 3rd Workshop on Mobile Security Technologies (MoST)*, San Jose, CA, USA, May 2014.

[17] J. Zhu, P. Wu, X. Wang, and J. Zhang, "SenSec: mobile security through passive sensing," in *Proceedings of IEEE International Conference on Computing, Networking and Communications (IEEE ICNC)*, pp. 1128–1133, San Diego, CA, USA, January 2013.

[18] W.-H. Lee and R. B. Lee, "Multi-sensor authentication to improve smartphone security," in *Proceedings of Conference on Information Systems Security and Privacy (IEEE ICISSP)*, pp. 1–11, Angers, France, February 2015.

[19] W.-H. Lee and R. B. Lee, "Implicit authentication for smartphone security," in *Proceedings of International Conference on Information Systems Security and Privacy*, vol. 576, pp. 160–176, Angers, France, February 2015.

[20] L. Li, X. Zhao, and G. Xue, "Unobservable re-authentication for smartphones," in *Proceedings of IEEE NDSS Symposium (NDSS)*, San Diego, CA, USA, February 2013.

[21] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos, "Progressive authentication: deciding when to authenticate on mobile phones," in *Proceedings of 21st USENIX Security Symposium (USENIX 12)*, pp. 301–316, Bellevue, WA, USA, August 2012.

[22] S. Mare, A. M. Markham, C. Cornelius, R. Peterson, and D. Kotz, "Zebra: zero-effort bilateral recurring authentication," in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 705–720, San Jose, CA, USA, May 2014.

[23] C. Nickel, H. Brandt, and C. Busch, "Classification of acceleration data for biometric gait recognition on mobile devices," *BIOSIG*, vol. 11, pp. 57–66, 2011.

[24] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user authentication on mobile phones using biometric gait recognition," in *Proceedings of 6th IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pp. 306–311, Darmstadt, Germany, October 2010.

[25] H. M. Thang, V. Q. Viet, T. D. Nguyen, and D. Choi, "Gait identification using accelerometer on a mobile phone," in *Proceedings of IEEE International Conference on Control, Automation and Information Sciences (ICCAIS)*, pp. 344–348, Ho Chi Minh City, Vietnam, November 2012.

[26] S. Davidson, D. Smith, C. Yang, and S. Cheah, "Smartwatch user identification as a means of authentication," 2016, https://cseweb.ucsd.edu/classes/wi16/cse227-a/report4.pdf.

[27] X. Su, H. Tong, and P. Ji, "Activity recognition with smartphone sensors," *Tsinghua Science and Technology*, vol. 19, no. 3, pp. 235–249, 2014.

[28] A. M. Khan, Y.-K. Lee, S. Y. Lee, and T.-S. Kim, "A triaxial accelerometer-based physical activity recognition via augmented-signal features and a hierarchical recognizer," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 5, pp. 1166–1172, 2010.

[29] A. Parnandi, "Coarse in-building localization with smartphones," in *Proceedings of International Conference on Mobile Computing, Applications, and Services (MobiCASE)*, pp. 343–354, San Diego, CA, USA, October 2009.

[30] I. Rish, "An empirical study of the naive Bayes classifier," in *Proceedings of Workshop on Empirical Methods in Artificial Intelligence (IJCAI-01)*, vol. 335, Seattle, WA, USA, August 2001.

Hindawi
Mobile Information Systems
Volume 2018, Article ID 9728328, 13 pages
https://doi.org/10.1155/2018/9728328

Research Article

A Novel Method for Predicting Vehicle State in Internet of Vehicles

Yanting Liu,[1] **Ding Cheng**,[2] **Yirui Wang**,[1] **Jiujun Cheng**,[3] **and Shangce Gao**[1]

[1]*Faculty of Engineering, University of Toyama, Toyama 930-8555, Japan*
[2]*College of Computer Science and Technology, Anhui University, Hefei 230601, China*
[3]*Key Laboratory of Embedded System and Service Computing, Ministry of Education, Tongji University, Shanghai 201804, China*

Correspondence should be addressed to Shangce Gao; gaosc@eng.u-toyama.ac.jp

Received 23 January 2018; Accepted 12 April 2018; Published 21 May 2018

Academic Editor: Mohamed Elhoseny

In the fields of advanced driver assistance systems (ADAS) and Internet of Vehicles (IoV), predicting the vehicle state is essential, including the ego vehicle's position, velocity, and acceleration. In ADAS, an early position prediction helps to avoid traffic accidents. In IoV, the vehicle state prediction is essential for the required calculation of the expected reliable communication time between two vehicles. Many approaches have emerged to perform this vehicle state prediction. However, such approaches consider limited information of the ego vehicle and its surroundings, and they may not be very effective in practice because the real situation is highly complex and complicated. Moreover, some of the approaches often lead to a delayed prediction time due to collecting and calculating the substantial history information. By assuming that the driver is a robot driver, which eliminates distinct driving behaviors of different persons when facing the same situation, this paper creates a decision tree as a new quick and reliable method adapted to all road segments, and it proposes a new method to perform the vehicle state prediction based on this decision tree.

1. Introduction

Advanced driver assistance systems (ADAS) installed in vehicles use sensing and computing technologies to assist drivers in avoiding traffic accidents. Predicting the positions of surrounding vehicles is a crucial problem, and it facilitates the early detection of potential collisions. In Internet of Vehicles (IoV), one of the most important foundations for the network connectivity is the vehicle state, including its position, velocity, and acceleration. This importance is because the vehicle state is a deterministic characteristic for communicating among vehicles and infrastructures. Therefore, a common requirement is to calculate the expected reliable communication time quickly in various road segments when two vehicles are to communicate with each other. The vehicle state can influence the network topology of IoV where the location between two vehicles determines the communication range and their velocities and accelerations affect the stability of network topology [1–3]. The routing protocol based on location is particularly important due to its adaptability for frequently changing IoV [4]. Alsaqour et al. found that the inaccurate location obviously decreased the efficiency of the routing protocol [5]. Thus, a neighbor wireless link break prediction was proposed to predict the neighbor node's location so as to detect the ineffective node by using their velocities and accelerations [6]. However, this method is just suitable for short-time and short-distance prediction because the accelerations of vehicles may significantly change according to changing environments. Consequently, the vehicle state prediction is necessary and essential for IoV.

A decision tree is an effective method for evaluating the behaviors of vehicle drivers; some studies include a decision tree to predict or monitor vehicle drivers [7, 8]. Ahmed presented a method to predict the vehicle state, in which a decision tree was used to determine whether the vehicle changed its lane and to obtain the lane after the vehicle changed lanes [9]. Kedowide et al. used a decision tree to monitor the vehicle driver and log the driving activities, such as to evaluate whether the driver was performing the blind spot check, integrated with the behaviors of the driver [10].

The aforementioned methods are primarily used in advanced driver assistance systems (ADAS) to avoid collisions

on the planned trajectories of vehicles and considering limited information about the ego vehicle and its surroundings. Moreover, a delayed prediction time will arise when history data need to be collected. Although some studies have employed a decision tree to quickly make judgments, the decision tree does not use much road and environment information and does not perform predictions across all road segments.

This paper proposes a new approach based on a decision tree that considers more information about the ego vehicle, its surroundings, and driver behaviors in varieties of road segments and without a delayed prediction time because no history data are collected as in some previous methods. This approach saves time and reduces the precious prediction time. According to information of the ego vehicle, roads, traffic lights, other surrounding vehicles, and so forth, our approach prejudges the driving behaviors of the ego vehicle, and then a decision tree is adapted to all road segments. Thus, the state of the ego vehicle, including its position, velocity, and acceleration, can be predicted based on a previously created decision tree. Such a decision tree with considerable useful information including more road surrounding cases helps to predict the vehicle state more accurately in some complex and complicated environments and without a delayed prediction time. The decision tree has advantages such as quick situation judgment and easy extension to more complicated problems with more determination conditions to be adapted to all road segments.

The contributions of this paper can be summarized as follows: (1) This paper defines three varieties of road segments: section, intersection, and transition. Based on the definitions in System Representation, this work extracts different behaviors in distinct road segments. These defined behaviors are introduced in Driving Behavior Modeling. (2) To predict the vehicle state from the behavior, we use a decision tree in all road segments, which is illustrated in State Prediction. The decision tree includes the predefined road segment situations and has advantages such as fast situation judgment and easy extension to more complicated problems with more determination conditions to be adapted to more road segments. We discuss the state prediction by taking advantage of the decision tree, which allows our work to predict the vehicle state through the decision tree.

The remainder of this paper is organized as follows. Section 2 gives the past works in vehicle state. Section 3 presents an overview of the system. Section 4 delineates several models of driving behaviors. Our prediction approach is described in Section 5. The numerical results are presented in Section 6. Finally, the conclusions of this paper are drawn in Section 7.

2. Related Works

Researches about vehicle state can be classified as three parts, that is, environments, maneuvers, and trajectories [11]. Environments are components of conducting vehicle behaviors. Various approaches have been done to discuss vehicle behaviors in different driving environments. In [12], a detection-by-tracking method was used to detect vehicles in a spatio-temporal environment. In [13], intersection driving and nonintersection driving were distinguished by histograms of scene flow vectors. In [14], a dynamic driving environment was established for detecting the vehicle motion. Maneuvers such as overtaking [15], turning [16], and changing lanes [17] are investigated to analyze the vehicle motion on the path. Overtaking behavior is implemented generally by using some devices to detect vehicles in front of the ego vehicle [15, 18, 19]. When overtaking conditions are satisfied in search space, vehicles will realize an overtaking maneuver. Turning behavior is another usual maneuver for vehicles. Detecting the yaw rate can judge the vehicle turning behavior [20]. Adopting a clustering of 3D points to analyze vehicle's shape can also handle a turning behavior [21]. In [17], changing lanes was achieved by establishing a dynamic Bayesian network based on practical data. Trajectories composed of a set of sequences of positions and velocities with a time window are used to extract vehicle behaviors in the past few years. In [22], a Gaussian mixture model was utilized to predict long-term trajectories of vehicles. On the highway, trajectories were constructed using a stereo vision and clustering method [23].

Besides the study of practical vehicle state, many approaches have emerged to obtain a credible vehicle state prediction. Hermes et al. predicted the position of a vehicle after several seconds using the history information of the vehicles [24]. Hermes et al. extracted a large number of vehicle trajectories to perform data training based on trajectory classification technology, in which trajectories were classified into several behaviors, such as left-handed rotation and right-handed rotation, and then they classified the existing trajectories [25]. In addition to objectivities, some researches added drivers' subjective purposes such as left turn, right turn, and changing lanes into the prediction models [26, 27]. A prediction technology for a motorcade formed by several vehicles was proposed by Pandita and Caveney, and in their approach, how a car follows was simulated using the smart driver model [28]. Additionally, a technology that combined the motion model and maneuver recognition was validated, in which probabilistic finite-state machines, fuzzy logics, and driving context recognitions were involved to predict a vehicle trajectory [29–31]. Petrich et al. used additional information from a digital map to enable a stochastic filter to select a representative set of reasonable trajectories [32]. Kumar et al. predicted the lane change intention online using a support vector machine and Bayesian filtering [33]. Yao et al. learned a simplified trajectory set using a collection of lane change trajectories from real driving data [34]. By introducing essential maneuver recognition, Houenou et al. predicted the vehicle trajectory using the constant yaw rate and acceleration motion model [31], which was widely and importantly used in [35–37]. These prediction technologies need more history information of vehicles; meanwhile, the impact of lane and traffic light on trajectories of vehicles is ignored. The trajectories of vehicles are restricted by lanes; however, a digital map based on the routing protocol can offer information of lanes to improve routing efficiency of IoV. Vehicle state prediction can also use the digital map and traffic light to enhance the accuracy of location prediction of vehicles [32, 38].

3. System Overview

3.1. Motivation. Vehicle state prediction is suitable for IoV in city scenario, integrating the digital map, traffic light, and surrounding vehicles. It models the driver's behavior in different traffic environments. In this paper, according to the driver's behavior, a decision tree is established to describe vehicle state in diverse conditions. Vehicle state prediction is an important part of the connectivity model in IoV, which is proper for predicting the positions of vehicles and dynamic changes of links. Taking advantage of information IoV provides, vehicle state can be predicted to further guide the driver to adopt several operations in order to implement a better trajectory of vehicle and save time. Nevertheless, the primary purpose of the vehicle state prediction is not to find an optimal route but to predict the vehicle state in next seconds. The vehicle state contains the position, velocity, and acceleration of vehicle. The change of vehicle state can influence the topology of IoV. For example, position can determine whether two vehicles are accessible to communicate with each other, whereas velocity and acceleration influence the stability of network topology. These factors could finally affect the survival time of links among vehicles. Hence, vehicle state prediction is mainly to calculate the survival time of links so as to guarantee to achieve a better communication among several vehicles and maintain a steady structure of IoV. Meanwhile, it also offers an effective method to construct a reasonable route.

3.2. System Architecture. The vehicle state prediction proposed in this paper is designed specifically to be used in Internet of Vehicles (IoV). It is assumed that the state prediction is hosted by the server that maintains the states of vehicles on the Internet. This assumption is often considered to be a reasonable assumption. Each vehicle manages its state prediction via a virtual object. Nowadays, the virtual object plays an important role in Internet of Things to implement its virtualness and service [39]. For IoV, virtual objects implement the communication among vehicles and provide a practical application for managing vehicles. Position-based and map-based routing protocols in the previous literature are widely accepted routing protocols in IoV based on position and path. Cheng et al. [40] classify notable routing protocols into routing categories for performing routing. Both position-based and map-based routing protocols require vehicles to send their state information to the server, which is generally distributed, when a source vehicle needs to communicate with other vehicles periodically. The server destination node first queries the state information of the destination from the server and then sends data toward the vehicle at the position. The position of the destination will often change during data forwarding; thus, if the position of the destination could be predicted, it would improve the routing performance. Moreover, by predicting vehicle states in a forward routing path, the server has the ability to calculate the expected reliable communication time between two vehicles and then calculate the connectivity of the path, which helps to select a stable path from multiple paths. When a source queries for the position of a destination, the server could send the predicted state and the optimal forward routing to the source, which will also improve the routing performance.

3.3. System Representation. The following describes the vehicle information that will be used in this work:

(i) The position of a certain vehicle at a certain time can be represented using a two-dimensional column vector:

$$\mathbf{p}(t) = (x(t), y(t))^T. \tag{1}$$

(ii) The velocity of a certain vehicle at a certain time can be represented as follows:

$$\mathbf{v}(t) = \left(v_x(t), v_y(t)\right)^T. \tag{2}$$

(iii) The acceleration of a certain vehicle at a certain time can be expressed as follows:

$$\mathbf{a}(t) = \left(a_x(t), a_y(t)\right)^T. \tag{3}$$

(iv) The length of a certain vehicle is l. Specifically, the length of the ego vehicle is l_α.

(v) The number of vehicles in front of a certain vehicle at a certain time is $n(t)$.

(vi) α refers to the ego vehicle, and $\alpha - k$ refers to the kth vehicle that is in front of the ego vehicle. For example, the directly previous vehicle is $\alpha - 1$.

(vii) $d_{\alpha-k}$ refers to the distance between the ego vehicle and the kth vehicle in front of the ego vehicle. For example, the distance between the ego vehicle and the directly previous vehicle $\alpha - 1$ is $d_{\alpha-1}$.

Hence, the vehicle state in this work is defined as a triple:

$$\mathbf{state}(t) = \langle \mathbf{p}(t), \mathbf{v}(t), \mathbf{a}(t) \rangle, \tag{4}$$

where $\mathbf{p}(t)$, $\mathbf{v}(t)$, and $\mathbf{a}(t)$ are all mentioned above.

Additionally, the road information and vehicle surroundings should also be extracted and represented. Before extracting and representing the road information and vehicle surroundings, this work introduces a new concept of a transition between a section and an intersection. The road is divided into three segments, as shown in Figure 1. All predictions in the three segments are integrated into one decision tree. A transition is a special part of a section with information of the intersection that needs to be considered. In other words, when a vehicle is at a transition, the driver faces the intersection and is able to obtain information such as traffic lights.

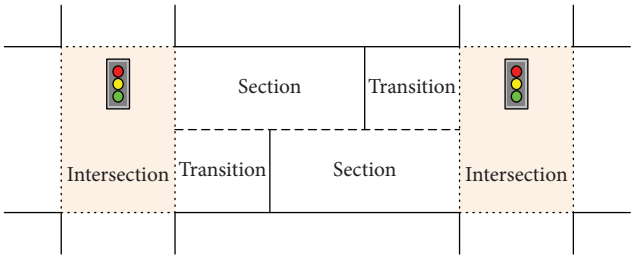


Figure 1: Road components.

(i) A certain intersection is defined as a two-dimensional point:

$$\mathbf{intersec} = (x_0, y_0), \tag{5}$$

where (x_0, y_0) is its position. On an intersection, we just consider three behaviors of each vehicle, that is, left turn, right turn, and pass through. Therefore, the intersection is expressed by a point.

(ii) A certain section between two consecutive intersections $\mathbf{intersec}_1$ and $\mathbf{intersec}_2$ that are the ends of the certain section is defined as follows:

$$\mathbf{sec} = \langle \mathbf{intersec}_1, \mathbf{intersec}_2, 0 \rangle, \tag{6}$$

where the direction of the vehicle is from intersection $\mathbf{intersec}_1$ to intersection $\mathbf{intersec}_2$.

(iii) Consequently, a certain lane is

$$\mathbf{lane} = \langle \mathbf{sec}, n \rangle, \tag{7}$$

where **sec** is the section to which the certain lane belongs and n is the number of the lane. In this work, the width of every lane is the same, and it is a known constant. When a vehicle faces an intersection, the driver can see three directions. Additionally, this work defines three directions: $\mathbf{lane}_N$ is the direction of the lane in which the driver faces straight forward, $\mathbf{lane}_W$ is the direction of the lane that the driver turns right into, and $\mathbf{lane}_E$ is the direction of the lane that the driver turns left into.

(iv) A certain transition between a certain section and a certain intersection that is an end of the certain section is

$$\mathbf{trans} = \langle \mathbf{intersec}_1, \mathbf{intersec}_2, 1 \rangle, \tag{8}$$

where **trans** is very similar to **sec** because a transition is a special part of a section, and when the vehicle is in the transition, the driver is facing intersection $\mathbf{intersec}_2$ and sees the traffic lights in the intersection. The purpose of 0 and 1 in **sec** and **trans** is to distinguish their mathematical definition.

Table 1 presents a summary of the aforementioned variables, including the definitions of the position, velocity, acceleration, and vehicle state of a vehicle and of several elementary road environments, such as an intersection, a section, a lane, and a transition.

Table 1: Variable summary.

Variable	Explanation
$\mathbf{p}(t)$	The position of a vehicle at time t
$\mathbf{v}(t)$	The velocity of a vehicle at time t
$\mathbf{a}(t)$	The acceleration of a vehicle at time t
$\mathbf{state}(t)$	The vehicle state of a vehicle, including its position, velocity, and acceleration
intersec	An intersection, which is defined by a point
sec	A section, which is defined by two **intersec**s
lane	A lane, which is defined by **intersec** and its lane number
trans	A transition, whose definition is similar to **sec**

Note that in this work, the number of lanes is based on zero, and the lane number starts from the central line of the section to which the lane belongs.

4. Driving Behavior Modeling

In this work, the driving behaviors of a vehicle are considered as the mean motions of the vehicle, such as some sudden changes including accelerating, decelerating, changing lanes, and turning at an intersection. These driving behaviors lead to discontinuous acceleration, which causes the acceleration, velocity, and position of the vehicle to be difficult to predict using their history states. The early detection of sudden changes is necessary for predicting the vehicle state. Driving behaviors can be defined as elements in a set, and each behavior is an element of the set. To create the decision tree in all road segments in this work, it is necessary to model the driving behaviors of a vehicle. The driving behavior is divided into three cases: section prediction, intersection prediction, and transition prediction. At sections, vehicles accelerate or decelerate, which is caused by the influence of the front vehicles. Additionally, vehicles may change lanes to leave an upcoming jam or to avoid a slow vehicle that is directly in front. Only when adjacent lanes have spacing can lane changes occur. A transition, with some specific characteristics, is a certain area between a section and its intersection. Vehicles at a transition are forbidden from changing lanes, and their behaviors are mainly dependent on the traffic lights. At intersections, vehicles may turn left or right or pass through, depending on the out direction of the lane that the vehicle is in and on the traffic light.

According to the aforementioned road in various situations, this paper classifies driving behaviors into three models: section behaviors, intersection behaviors, and transition behaviors. Section behaviors occur in the section, which are relatively simple without considerations of orientation changing. Considerations of intersection behaviors include changing direction. Transition behaviors are relatively complicated. The transition situation is between section and intersection, and it contains possibilities of section's and intersection's behaviors; thus, it is difficult to predict the coming driving behavior due to various possibilities.

4.1. Section Behaviors. Section behaviors are always when the vehicle is far away from the front intersection and the traffic light is out of the range of the driver.

4.1.1. Jam Leaving Intent. When a driver realizes that a jam has occurred in the front of his current lane, he will attempt to enter adjacent lanes to avoid the jam. Lane-changing behavior is an important intent and has already been considered in the previous literature, such as by Ahmed [9]. In this work, α refers to the ego vehicle and $\alpha - m$ refers to the mth vehicle in front of the ego vehicle; for example, the vehicle directly in front of the ego vehicle is $\alpha - 1$. Here, r_α is the range of the driver in the ego vehicle α. The driver could see τ_α vehicles $\alpha - 1, \alpha - 2, \ldots, \alpha - \tau_\alpha$ in the driver's range r_α, but the vehicle $\alpha - \tau_\alpha - 1$ is out of the driver's range. Thus, τ could be represented mathematically by

$$\tau_\alpha = \max_i d_{\alpha-i} < r_\alpha, \tag{9}$$

where $d_{\alpha-i}$ is the distance between the vehicle α and the ith front vehicle $\alpha - i$. The jam density ρ_α, which defines an indicator to quantify the congestion level, is as follows:

$$\rho_\alpha = \frac{\tau_\alpha}{r_\alpha}. \tag{10}$$

The driver will have a jam leaving intent if the driver cannot tolerate such a jam that $\rho_\alpha > \rho_\alpha^*$, where ρ_α^* is a tolerance threshold for the driver. In this paper, the length of vehicle is 4.3–4.7 meters; we set one vehicle within 5 meters as a tolerance threshold. Thus, this paper uses $\rho_\alpha^* = 0.2$ and $r_\alpha = 400$ m in our later numerical experiments. Then, the driver will change lanes if the condition for changing lanes is satisfied. The driver always prefers to change to the right lane, and when the condition for changing to the right lane is not satisfied, the driver considers changing to the left lane.

4.1.2. Overtaking Intent. For this intent, this work considers two aspects: the sizes of and the velocities between the front vehicle and the ego vehicle.

When the front vehicle, such as a truck, is considerably larger than the ego vehicle, the driver always tends to avoid following it. This work simply assumes that the width of every vehicle is the same; thus, this case is simply to compare the lengths and is presented by

$$l_{\alpha-1} > \lambda_{\text{length}} l_\alpha, \tag{11}$$

where $\lambda_{\text{length}} > 1$ is the tolerance threshold for the ratio of the length of the directly previous vehicle to the length of the ego vehicle.

In the other case, if the speed of the vehicle ahead is too slow, the driver often attempts to change lanes and overtakes the slow vehicle. Mathematically,

$$v_{\alpha-1} < \lambda_{\text{velocity}} v_\alpha, \tag{12}$$

where $\lambda_{\text{velocity}} < 1$ is the tolerance threshold. This paper uses $\lambda_{\text{length}} = 1.5$ and $\lambda_{\text{velocity}} = 0.8$.

4.1.3. Following Intent. In general, the driver of the ego vehicle will follow the front vehicle. However, when the driver follows the front vehicle, the driver will also adapt the ego vehicle such that it will be more comfortable and safe. For example, when the ego vehicle is too close to the front vehicle, the driver tends to brake to avoid driving into it. Mathematically,

$$t_{\text{brake}} = \frac{d_{\alpha-1}}{v_\alpha - v_{\alpha-1}}. \tag{13}$$

Here, we select a safety braking time t_{safety} as a threshold for the ratio of the velocity of the directly previous vehicle to the velocity of the ego vehicle. When $t_{\text{brake}} \le t_{\text{safety}}$ is satisfied, the driver will decelerate with an acceleration value. In this paper, $t_{\text{safety}} = 1.5$s and $\delta = 2$ is a correlation coefficient:

$$a = -\delta \frac{v_\alpha - v_{\alpha-1}}{d_{\alpha-1}}. \tag{14}$$

4.1.4. Free Driving Intent. Otherwise, the state of the driver will be maintained. This case is called *free driving intent*. For free driving, this work will consider that if the velocity of a vehicle is less than the speed limit, then the driver tends to accelerate with a constant acceleration to reach the speed limit.

4.2. Intersection Behaviors. Intersection behaviors are to predict the motions when the vehicle is close to or facing the front intersection. In such cases, the driver should consider the information of the front intersection, such as traffic lights. Behaviors at intersections are difficult to detect without information, including the out directions of the lane where the ego vehicle is located and the traffic lights. Existing studies always use history trajectories to recognize vehicle behavior using pattern classifications, fuzzy logics, probabilistic finite-state machines, or other technologies [29]. However, these technologies all require sufficiently long trajectories, which lead to delayed time, and these technologies have considerable computational requirements, which make them unsuitable for performing recognition of behaviors at a server with a massive number of vehicles. According to the out direction of the driving lane and traffic light, it is simple and accurate to achieve early detection of whether the vehicle is going to turn left, right, or pass through. However, there is a case in which the motion cannot be detected only using the out direction and traffic lights. This situation arises because the traffic light may occasionally allow the three directions simultaneously. In this case, the motion cannot be determined only by the directions of the lane and the traffic light. As shown in Figure 2, the $\mathbf{lane}_S$ has three out directions: S/E, S/W, and S/N. Here, S is marked as the directing lane toward the south, E is marked as the left lanes of the intersection toward the east, W is marked as the right lanes of the intersection toward the west, and N is marked as the lanes across the north. Hence, S/E means that the driver turns left from the current lane to the east lanes, and S/W and S/N have similar

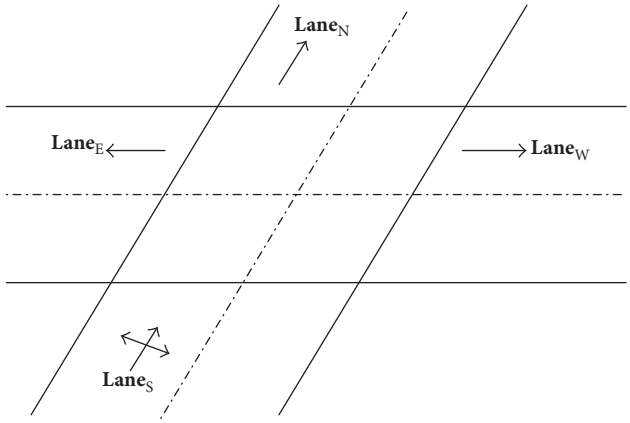


Figure 2: Intersection.

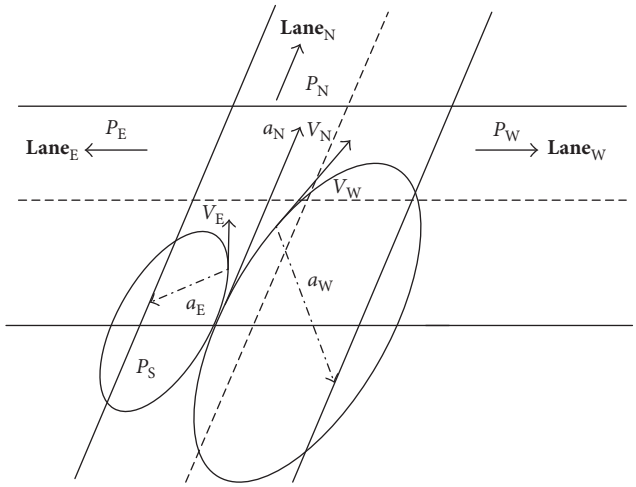


Figure 3: Behaviors at intersection.

meanings. The motion may be to turn left or right or pass through with the trajectories $P_S\widehat{P}_E$, $P_S\widehat{P}_W$, and $P_S\widehat{P}_N$, as shown in Figure 3. Here, P_E, P_S, P_W, and P_N are four positions standing for positions to the east, south, west, and north, respectively, of the certain transition. For simplicity, this work considers the curve trajectory of the motion from the ego vehicle, which is similar to 1/4 part of an ellipse, as illustrated in Figure 3, due to two accelerations changing, in which one's direction is the original direction and the other's direction is the terminal one. The details of the calculation of the two accelerations and corresponding velocity and position will be discussed in Section 4. When a vehicle is arriving from the south, it will have three probabilities: to turn left (go $\mathbf{trans}_E$ in Figure 3), to turn right (go $\mathbf{trans}_W$ in Figure 3), and to go straight (go $\mathbf{trans}_N$ in Figure 3). We will discuss these three cases in the following. If

$$\left|\frac{\mathbf{a}^T \cdot \mathbf{v}}{|\mathbf{a}||\mathbf{v}|}\right| > 1 - \epsilon, \tag{15}$$

the motion is to pass through. If

$$\mathbf{a}^T \cdot \mathbf{lane}_E > \epsilon \text{ or } \mathbf{a}^T \cdot \mathbf{lane}_W < -\epsilon, \tag{16}$$

the motion is to turn left. If

$$\mathbf{a}^T \cdot \mathbf{lane}_W > \epsilon \text{ or } \mathbf{a}^T \cdot \mathbf{lane}_E < -\epsilon, \tag{17}$$

the motion is to turn right. $\mathbf{lane}_E$ and $\mathbf{lane}_W$ are column vectors. The aforementioned ϵ is a positive value close to zero, indicating that it is sufficiently small. In this paper, $\epsilon = 0.01$.

4.3. Transition Behavior. When a vehicle is in a transition, the driver can see the traffic light. Different traffic lights can lead to distinct behaviors of the vehicle. Here, we consider that when a driver faces a red or yellow traffic light, the driver will give the vehicle a constant acceleration $\mathbf{a}_\delta$. We also provide a vector $\mathbf{e}$ to represent the traffic light information:

$$\mathbf{e} = \begin{cases} (1,0,0)^T, & \text{if the traffic light is red} \\ (0,1,0)^T, & \text{if the traffic light is yellow} \\ (0,0,1)^T, & \text{if the traffic light is green.} \end{cases} \tag{18}$$

Thus, the constant acceleration vector can be represented as

$$\delta_a = (\mathbf{a}_\delta, \mathbf{a}_\delta, 0)^T, \tag{19}$$

where each dimension indicates the acceleration of the vehicle in corresponding traffic light.

Hence, when the driver faces the traffic light, the acceleration that the driver will provide is

$$\mathbf{a}_\Delta = \delta_a^T \cdot \mathbf{e}. \tag{20}$$

5. State Prediction

Now, driving behaviors are modeled, and a decision tree can be created based on the surroundings and driving behaviors in varieties of road segments. Our decision tree is illustrated in Figure 4. The decision tree in Figure 4 represents the aforementioned situations in various road segments and their judgment conditions, and it will help provide quick and easy determination and extension. First, it will be considered that the ego vehicle is in a section, an intersection, or a transition, and these cases will be discussed individually. Note that in this work, when the ego vehicle is in the intersection, it means that the ego vehicle has passed the beginning line and will no longer consider traffic lights.

5.1. Prediction in Section. When the ego vehicle is in a section, it is considered whether the vehicle is changing lanes. This is because if the vehicle is changing lanes, its velocity and acceleration are not in the same direction, which will lead to a different trajectory. If the ego vehicle is not changing lanes, it is considered whether the vehicle will change lanes based on the aforementioned *jam leaving intent* and *overtaking intent*. These two intents are very common in reality. If the ego vehicle does not choose to change lanes, then there are two intents for the driver of the ego vehicle: *free driving intent* and *following intent*. To summarize, the prediction in a section could have four cases, A, B, C, and D, as indicated in Figure 4.

(1) A: When a vehicle is in a section **sec** and it is changing lanes, it has a velocity $\mathbf{v}_\perp(t)$ and an

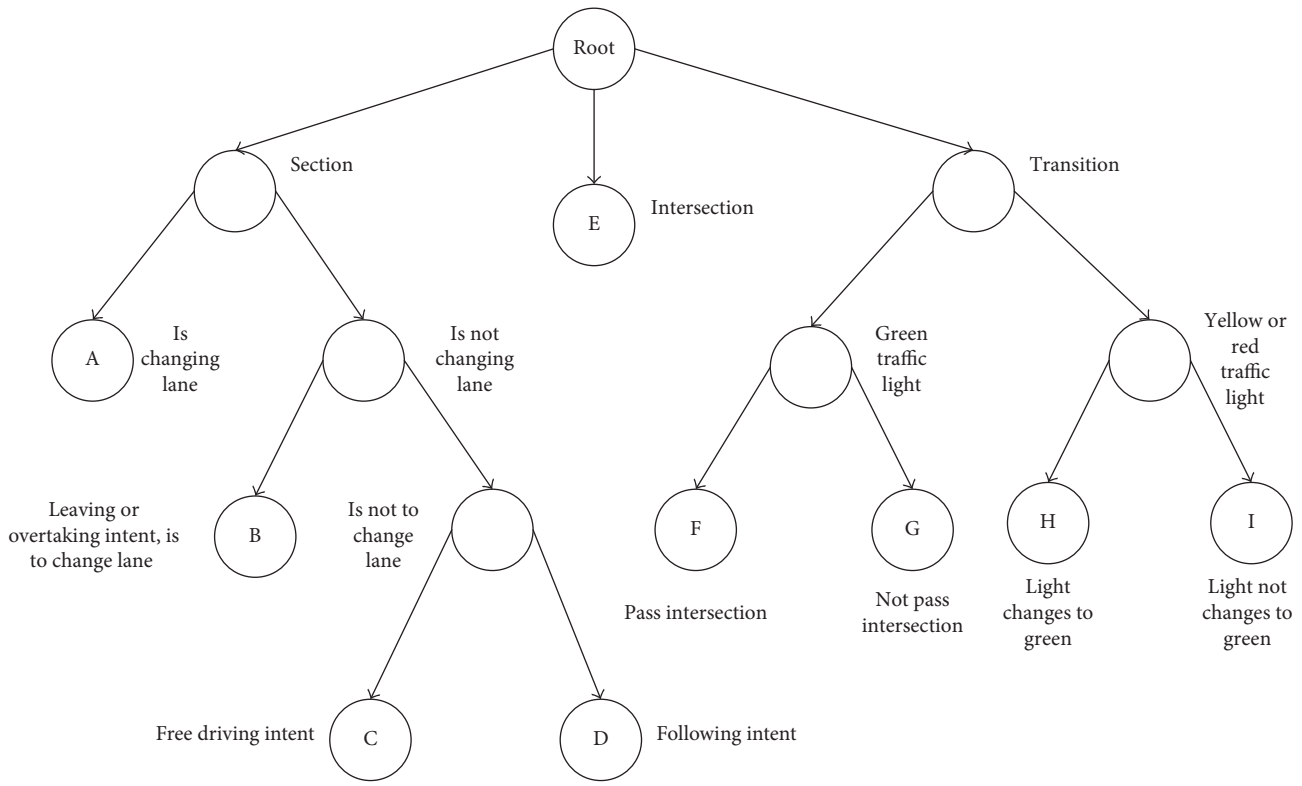


Figure 4: Decision tree based on driving behaviors.

acceleration $\mathbf{a}_\perp(t)$ whose directions are both perpendicular to **sec**. During the lane change, the vehicle is supposed to have an acceleration $\mathbf{a}_\perp$ to first accelerate and then $-\mathbf{a}_\perp$ to decelerate, where $|\mathbf{a}_\perp| > 0$ could be calculated from the data set. Therefore,

$$\mathbf{a}_\perp(t) = \begin{cases} \mathbf{a}_\perp, & t < t_0 \\ -\mathbf{a}_\perp, & t > t_0, \end{cases} \tag{21}$$

where t_0 is the time point between accelerating and decelerating and t is during the lane change. Moreover, $\mathbf{v}(t) = \mathbf{v}_\perp$ could be calculated from the data set, and the distance of changing the lane equals the lane width, which is also a known constant mentioned in the previous discussion. Hence, the $\mathbf{p}(t)$ during the lane change and the current time point could both be calculated. Then, the position after t_Δ can be determined as follows:

$$\mathbf{p}_\Delta = \begin{cases} \mathbf{p}(t + t_\Delta), & \text{if still changing} \\ \mathbf{p}(t + t') + \int_{t+t'}^{t+t_\Delta} \mathbf{v}(t)dt, & \text{if changing is done,} \end{cases} \tag{22}$$

where $\mathbf{p}_\Delta$ is the position at time point $t + t_\Delta$ and $t + t'$ is the time point when the vehicle completes the lane change.

(2) B: This case is very similar to Case A, but the time point t is not during the lane change but rather when starting to change lanes. Moreover, in Case A, the acceleration could be calculated from the data set, whereas in this case, the acceleration $\mathbf{a}_\perp(t)$ cannot be calculated from the data set. In this case, this work assumes that the time for changing lanes is a known constant; then, the $\mathbf{a}_\perp(t)$ could be calculated according to the distance of changing the lane, which equals the lane width. Thus, the position after t_Δ could be predicted by the method in Case A.

(3) C: When a vehicle faces this case, the driver will choose *free driving intent*, which was previously mentioned.

(4) D: When a vehicle faces this case, the driver will choose *following intent*, which was previously mentioned.

5.2. Prediction in Intersection

(1) E: When a vehicle is in an intersection **intersec**, the driver could have three options: to drive straight forward, to turn left, and to turn right. The velocity $\mathbf{v}_t$ at the current time point can be calculated from the data set, and it will be compared with $\mathbf{lane}_\mathrm{N}$, $\mathbf{lane}_\mathrm{W}$, and $\mathbf{lane}_\mathrm{E}$ to determine which direction the vehicle will go. Mathematically, the direction that the vehicle will go is given by the following equation:

$$\mathbf{direction} = \begin{cases} \mathbf{lane}_\mathrm{W}, & \mathbf{v}(t) \cdot \mathbf{lane}_\mathrm{W} > \epsilon \\ \mathbf{lane}_\mathrm{E}, & \mathbf{v}(t) \cdot \mathbf{lane}_\mathrm{E} > \epsilon \\ \mathbf{lane}_\mathrm{N}, & \text{otherwise,} \end{cases} \tag{23}$$

where $\epsilon > 0$ is a positive value that is sufficiently small, as previously mentioned. $\epsilon = 0.01$ in this paper. If **direction** = $\mathbf{lane}_{\mathrm{N}}$, then the intersection **intersec** could be considered as a section. If **direction** = $\mathbf{lane}_{\mathrm{W}}$ or **direction** = $\mathbf{lane}_{\mathrm{E}}$, then the vehicle has two accelerations that have the straight forward direction and the direction same as $\mathbf{lane}_{\mathrm{W}}$ or $\mathbf{lane}_{\mathrm{E}}$, respectively. This work denotes the first mentioned acceleration as $\mathbf{a}_{\mathrm{o}}(t)$ and the second mentioned acceleration as $\mathbf{a}_{\mathrm{l}}(t)$. This work assumes that in the intersection **intersec**, $\mathbf{a}_{\mathrm{o}}(t)$ is linearly increasing from zero and $\mathbf{a}_{\mathrm{l}}(t)$ is linearly decreasing to zero. That is, $|\mathbf{a}_{\mathrm{o}}(t)| + |\mathbf{a}_{\mathrm{l}}(t)|$ is a constant during turning. At some certain time point t_0, $\mathbf{a}_{\mathrm{o}}(t_0)$ and $\mathbf{a}_{\mathrm{l}}(t_0)$ could be calculated from the data set; thus, we let

$$a_{\Sigma} = \left|\mathbf{a}_{\mathrm{o}}(t_0)\right| + \left|\mathbf{a}_{\mathrm{l}}(t_0)\right|. \tag{24}$$

From the data set of the map, the distance between the current time point and the time point when the vehicle completes turning can be calculated. Hence, the time t_{s} remaining for turning can be obtained. Therefore,

$$\begin{aligned} \mathbf{a}_{\mathrm{o}}(t_0 + t) &= \left(\left|\mathbf{a}_{\mathrm{o}}(t_0)\right| - \frac{\left|\mathbf{a}_{\mathrm{o}}(t_0)\right|}{t_{\mathrm{s}}} t\right)\mathbf{e}_{\mathrm{o}}, \qquad t < t_{\mathrm{s}}, \\ \mathbf{a}_{\mathrm{l}}(t_0 + t) &= \left(\left|\mathbf{a}_{\mathrm{l}}(t_0)\right| + \frac{\left|a_{\Sigma} - \mathbf{a}_{\mathrm{l}}(t_0)\right|}{t_{\mathrm{s}}} t\right)\mathbf{e}_{\mathrm{l}}, \quad t < t_{\mathrm{s}}, \end{aligned} \tag{25}$$

where $\mathbf{e}_{\mathrm{o}}$ is the direction of the original direction and $\mathbf{e}_{\mathrm{l}}$ is the direction of **direction**. The position after t_Δ is

$$\mathbf{p}(t_0 + t_\Delta) = \begin{cases} \mathbf{p}(t_0) + \int_0^{t_\Delta} v_0 + \mathbf{a}(t_0 + t)dt, & t < t_{\mathrm{s}} \\ \mathbf{p}(t_0 + t_{\mathrm{s}}) + (t_\Delta - t_{\mathrm{s}})v', & t > t_{\mathrm{s}}, \end{cases} \tag{26}$$

where $\mathbf{v}'$ is the velocity when the vehicle completes turning.

5.3. Prediction in Transition

(1) F: When the driver faces a green traffic light and the vehicle could pass in time, the case could be in a section (when the requested time point is not sufficient to pass) or in an intersection (when the requested time point is sufficient to pass).

(2) G: When the driver faces a green traffic light and the vehicle cannot pass in time, the driver will stop the vehicle. The vehicle knows if some vehicle is in front of it. If some vehicle is in front of it, the driver will have *following intent*. If no vehicle is in front of it, the vehicle will calculate the distance between the current position and the final stopped position, which is denoted as d_{s}. This work assumes that the vehicle will be stopped by a constant acceleration. The constant acceleration can be calculated as

$$\mathbf{a} = -\frac{\left|\mathbf{v}(t_0)\right|^2}{2d_{\mathrm{s}}}\mathbf{e}, \tag{27}$$

where $\mathbf{e}$ is the direction of the vehicle. Thus, the velocity and position are

$$\begin{aligned} \mathbf{v}(t_0 + t_\Delta) &= \mathbf{v}(t_0) + \mathbf{a} \cdot t_\Delta, \\ \mathbf{p}(t_0 + t_\Delta) &= \mathbf{p}(t_0) + \int_0^{t_\Delta} \mathbf{v}(t_0 + t)dt. \end{aligned} \tag{28}$$

(3) H: This case could be separated into two time intervals: before and after the traffic light turns green. Before the traffic light turns green, the driver would choose *following intent*, while after the traffic light turns red, the case would be Case F.

(4) I: Because the vehicle will stop as Case G, irrespective of whether some vehicle is in front of it, the vehicle has the same intent as Case G.

5.4. Prediction Summary. We call the above proposed method as driver behavior decision tree (DBDT), which obtains the relatively accurate trajectories of vehicles in a long term according to the sudden changes such as acceleration, deceleration, and turn. Moreover, to prevent the prediction from going too far, this work includes the constant yaw rate and acceleration (CYRA) [31] into our approach. CYRA is a physical kinematic-based prediction method. It assumes that within a very short term, the force on a vehicle remains unchanged and the vehicle would keep a constant accelerate vector, including its accelerate direction and value. Thus, the CYRA model regards the acceleration and direction of vehicle as a constant to predict the vehicle state. Its constant acceleration $\mathbf{a}_t$ is formulated as follows:

$$\mathbf{a}_t = \mathbf{a}_0, \tag{29}$$

where $\mathbf{a}_0$ is a constant value. Next, its velocity and position are calculated as follows:

$$\begin{aligned} \mathbf{v}_t &= \int_0^t \mathbf{a}_t\, dt, \\ \mathbf{p}_t &= \int_0^t \mathbf{v}_t\, dt. \end{aligned} \tag{30}$$

The linearity of its state equation achieves a transmission of state probability distribution. The next vehicle state could be predicted based on this kind of constant accelerate vector.

For a short term, the acceleration of vehicle can be considered as a constant, CYRA can effectually adapt to this situation according to its constant acceleration characteristics. Hence, CYRA can effectively handle the vehicle state prediction in a short term so as to obtain more accurate results. However, it could result in a great error for predicting the vehicle state in a long term because the acceleration of vehicle continually changes. On the contrary, DBDT can detect the sudden change of acceleration of vehicle to instantly adapt to the current state so as to obtain better results and avoid a great error, suggesting that it is more suitable for predicting the vehicle state in a long term. On the basis of both characteristics, this work finally adopts the following formula to evaluate their performances.

$$T_{\mathrm{DBDT}}(t) = f(t)T_{\mathrm{DBDT}'}(t) + (1 - f(t))T_{\mathrm{CYRA}}(t), \quad (31)$$

where $T_{\mathrm{DBDT}'}(t)$ is the result of our approach and $T_{\mathrm{CYRA}}(t)$ is the result of another approach. $f(t)$ is an increasing function, which means driving behavior recognition is more suitable for long-term prediction and CYRA is more accurate for short-term prediction. In this paper, $f(t) = 1/4t$.

5.5. Time Complexity. A time complexity comparison between DBDT and CYRA is discussed in this subsection. For DBDT, we set C to be the number of vehicles in the same lane. The time complexity regarding prediction in section, intersection, and transition is calculated as follows:

5.5.1. Prediction in Section

(i) Motion prediction

(1) Jam Leaving Intent: scanning vehicles in front of itself in the same lane needs the time complexity $C_{\mathrm{m1}} = O(c)$.
(2) Overtaking Intent: considering the vehicle in front of itself requires $C_{\mathrm{m2}} = O(1)$.
(3) Following Intent: calculating the vehicle in front of itself needs $C_{\mathrm{m3}} = O(1)$.
(4) Free Driving Intent: this situation takes $C_{\mathrm{m4}} = O(1)$.

(ii) Vehicle state prediction

(A) Computing the location data of the lane and state of itself costs $C_{\mathrm{s1}} = O(1)$.
(B) Computing the location data of the lane and vehicle states in front of itself needs $C_{\mathrm{s2}} = O(c)$.
(C) Computing the vehicle state in front of itself requires $C_{\mathrm{s3}} = O(1)$.
(D) Computing the state of itself takes $C_{\mathrm{s4}} = O(1)$.

Thus, the time complexity of prediction in section is

$$C_{\mathrm{sec}} = (C_{\mathrm{m1}} + C_{\mathrm{m2}} + C_{\mathrm{m3}} + C_{\mathrm{m4}}) + \max(C_{\mathrm{s1}}, C_{\mathrm{s2}}, C_{\mathrm{s3}}, C_{\mathrm{s4}}) = O(c). \quad (32)$$

5.5.2. Prediction in Intersection

(i) Motion prediction

Predicting the vehicle motions by the traffic light data and the location data of intersection lanes costs the time complexity $C_{\mathrm{m}} = O(1)$.

(ii) Vehicle state prediction

(E) Computing the vehicle state of itself and intersection lanes data needs $C_{\mathrm{s}} = O(1)$.

Therefore, the time complexity of prediction in intersection is

$$C_{\mathrm{intersec}} = C_{\mathrm{m}} + C_{\mathrm{s}} = O(1). \quad (33)$$

5.5.3. Prediction in Transition

(i) Motion prediction

When a vehicle is in a transition, its motion is predicted by the traffic light. This operation needs $C_{\mathrm{m}} = O(1)$.

(ii) Vehicle state prediction

(F) When the driver faces the green traffic light and the vehicle could pass in time, computing the state of itself needs $C_{\mathrm{s1}} = O(1)$.
(G) When the driver faces the green traffic light and the vehicle could not pass in time, computing the vehicle state and traffic light time requires $C_{\mathrm{s2}} = O(1)$.
(H) When the driver faces the red traffic light and the traffic light turns to green before it passes the transition, computing the vehicle state and traffic light time requires $C_{\mathrm{s3}} = O(1)$.
(I) When the driver faces the red traffic light and the traffic light keeps red before it passes the transition, computing the vehicle state and traffic light time costs $C_{\mathrm{s4}} = O(1)$.

Thus, the time complexity of prediction in transition is

$$C_{\mathrm{trans}} = C_{\mathrm{m}} + \max(C_{\mathrm{s1}}, C_{\mathrm{s2}}, C_{\mathrm{s3}}, C_{\mathrm{s4}}) = O(1). \quad (34)$$

The number of vehicles is set to be n for prediction. Consequently, the whole time complexity about DBDT is $C = \max(C_{\mathrm{sec}}, C_{\mathrm{intersec}}, C_{\mathrm{trans}}) = n * O(c) = O(n)$. For CYRA, each vehicle is predicted by the data of itself. Hence, its time complexity is $O(n)$ [31]. According to both time complexity, we can find that DBDT and CYRA have the same time complexity, suggesting they possess the same efficiency.

6. Results and Analysis

To test whether our work is valid, experiments are conducted in a real environment, which is based on the Lankershim Boulevard Dataset of the Next Generation Simulation (NGSIM) program [41]. The Lankershim Boulevard Dataset collects detailed vehicle trajectory data from Lankershim Boulevard in the Universal City neighborhood of Los Angeles. It provides the map of an area of Lankershim Boulevard, including three to four lane segments and covering three signalized intersections. Moreover, the traffic light data and the precise vehicle position, velocity, and acceleration in the periods of 8:30 am and 8:45 am on June 16, 2005, are available. The Lankershim Boulevard Dataset covers the driver behavior of lane changing on congested segments, overtaking, and behavior at traffic lights, which fits the experimental requirements of this work. The details of the Lankershim Boulevard Dataset are listed in Table 2. This work creates a model for the provided map in the

Table 2: Data set parameters.

Lankershim Boulevard Dataset	Parameters
Address	Lankershim Boulevard in Los Angeles
Time	8:28–8:45 am and 8:45–9:00 am on June 16, 2005
Road length	490 m
Intersection number	4
Sampling time	1/10 s
Lane number (same direction)	1–6
Provides traffic light data	Yes
8:28–8:45 am data amount	705294 records
8:28–8:45 am vehicle number	1375
8:45–9:00 am data amount	902025 records
8:45–9:00 am vehicle number	1601

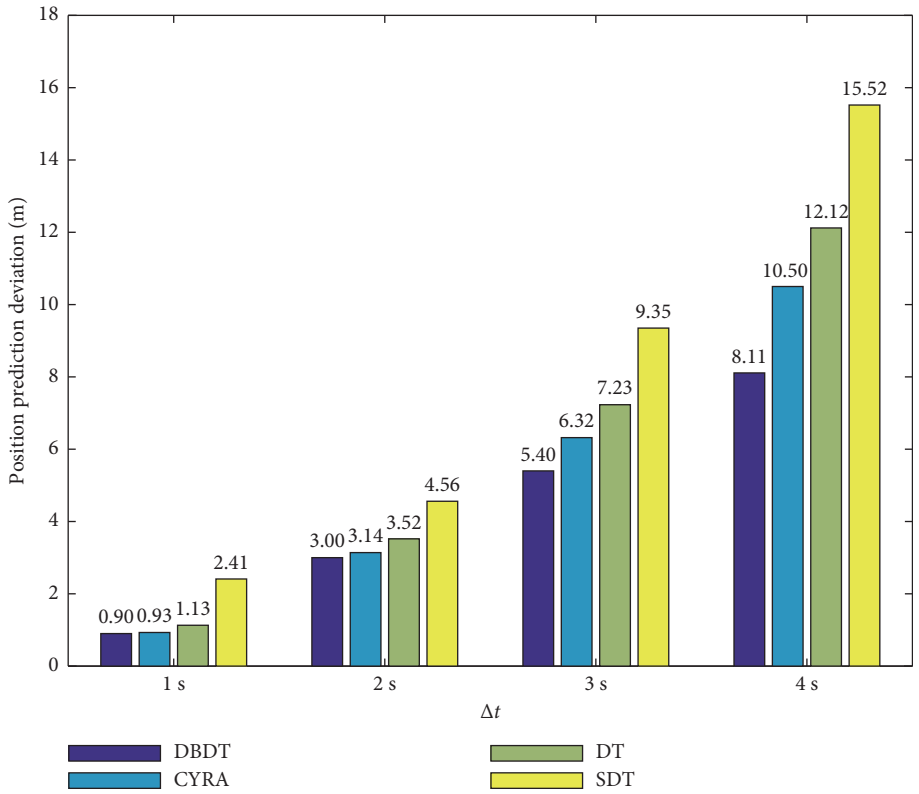


Figure 5: Accuracy of position prediction.

Lankershim Boulevard Dataset to extract location data of sections, intersections, and transitions. Then, this work extracts traffic light information, and thus, it obtains all road information. By inputting trajectory information of vehicles, this work will compare our approach (DBDT for short) to CYRA [31], DT which is a variant of DBDT by setting $f(t) = 1$ in (31), and SDT [7, 8] which is a self-selection threshold decision algorithm based on decision tree in four cases: $t_\Delta = 1$ s, $t_\Delta = 2$ s, $t_\Delta = 3$ s, and $t_\Delta = 4$ s, respectively.

The results for the accuracy of position prediction are shown in Figure 5, those for the accuracy of velocity prediction are shown in Figure 6, and those for the accuracy of acceleration prediction are shown in Figure 7. The results show that although the state predicted by our approach is not very accurate at the beginning, the state is more accurate than that of CYRA as time passes. This is because our approach provides early detection of the driving behavior, which leads to changing the state at the very beginning of the prediction time point. Moreover, the vehicle state includes the ego vehicle's position, velocity, and acceleration, for which the importances are decreasing in many fields. For example, to avoid traffic accidents, the vehicle position prediction is the most essential. Considering the discontinuous acceleration, the three vehicle state components, which are the position, the velocity, and the acceleration, are becoming more difficult. Thus, it is expected that from the numerical results, the position prediction is the best, the velocity prediction is not good when $\Delta t = 1$ s, and the acceleration prediction is not good when $\Delta t = 1$ s or $\Delta t = 2$ s. As time passes, the numerical results become better. From the results, the difference value between the previous one second and the next one second becomes increasingly

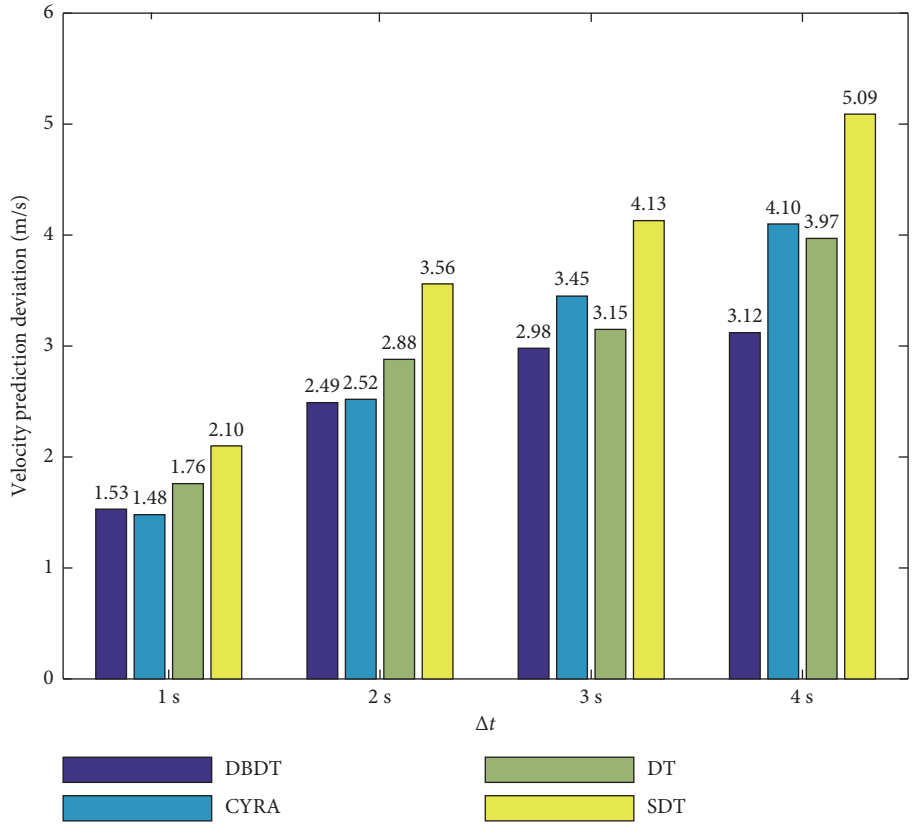


Figure 6: Accuracy of velocity prediction.

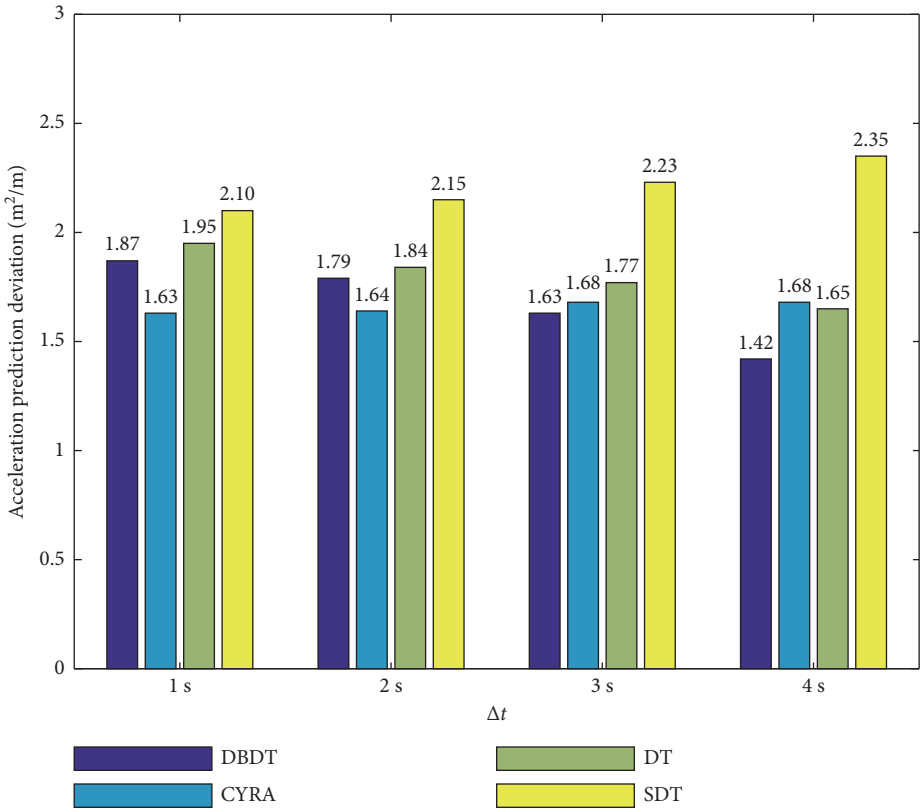


Figure 7: Accuracy of acceleration prediction.

smaller. Thus, as time lasts past a certain range, the state prediction will be more accurate than that of CYRA.

Additionally, the results of DBDT are better than those of DT, suggesting that the key to the good performance of our proposal is the incorporation and extension of the decision tree and CYRA. In comparison with SDT which generally utilizes thresholds to determine the state selection in a decision tree, our proposal performs better with the aid of accurate modeling of the driving behaviors. Moreover, in light of the results, we believe that more research on how to use driving behaviors of vehicle in the varieties of the all road segments to predict or monitor vehicle drivers by decision trees is warranted.

7. Conclusion

This paper highlights that the previous approaches for predicting the vehicle states using the substantial history information have a delayed prediction time. Some trajectory prediction methods based on lane changing recognition are proposed. Although a validation method for complicated environments such as multilanes and intersections is not currently available, this paper proposes a new method for the prediction by using a decision tree in varieties of road segments generated by the driving behaviors. This decision tree helps to detect driving behaviors and predict the vehicle state in all road segments, including sections with multilanes, transition segments, and intersections. The driving behavior recognition improves the accuracy of vehicle state prediction in long-term cases. Our approach shows advantages in the provided real environments.

Social Internet of Vehicles is an important and intelligent transport network [42]. It has more characteristics and more complicated circumstances. Thus, to predict this kind of IoV is more meaningful and challenging in the future work. Furthermore, the proposed technique might lead to the development of vehicle networking and intelligentialization [43], as well as to provide effective methods to solve vehicle routing problems in dynamic environments [44].

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research was partially supported by the JSPS KAKENHI Grant no. JP17K12751 and the National Natural Science Foundation of China (Grant no. 61472284).

References

[1] T. Taleb, M. Ochi, A. Jamalipour, N. Kato, and Y. Nemoto, "An efficient vehicle-heading based routing protocol for VANET networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2006)*, vol. 4, pp. 2199–2204, Las Vegas, NV, USA, April 2006.

[2] T. Taleb, E. Sakhaee, A. Jamalipour, K. Hashimoto, N. Kato, and Y. Nemoto, "A stable routing protocol to support ITS services in VANET networks," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3337–3347, 2007.

[3] M. Dixit, R. Kumar, and A. K. Sagar, "VANET: architectures, research issues, routing protocols, and its applications," in *Proceedings of the IEEE 2016 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 555–561, Greater Noida, India, April 2016.

[4] J. Liu, J. Wan, Q. Wang, P. Deng, K. Zhou, and Y. Qiao, "A survey on position-based routing for vehicular ad hoc networks," *Telecommunication Systems*, vol. 62, no. 1, pp. 15–30, 2016.

[5] R. Alsaqour, M. Abdelhaq, and T. Abdullah, "Modeling the position information inaccuracy in MANET position-based routing protocols," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 3, no. 9, pp. 971–976, 2011.

[6] R. A. Alsaqour, M. S. Abdelhaq, and O. A. Alsukour, "Effect of network parameters on neighbor wireless link breaks in GPSR protocol and enhancement using mobility prediction model," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, p. 171, 2012.

[7] S. Wang, C. Fan, C. H. Hsu, Q. Sun, and F. Yang, "A vertical handoff method via self-selection decision tree for internet of vehicles," *IEEE Systems Journal*, vol. 10, no. 3, pp. 1183–1192, 2016.

[8] B. Ma, D. Wang, S. Cheng, and X. Xie, "Modeling and analysis for vertical handoff based on the decision tree in a heterogeneous vehicle network," *IEEE Access*, vol. 5, pp. 8812–8824, 2017.

[9] K. I. Ahmed, *Modeling Drivers' Acceleration and Lane Changing Behavior*, Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, MA, USA, 1999.

[10] C. Kedowide, C. Gouin-Vallerand, and É. Vallières, "Recognizing blind spot check activity with car drivers based on decision tree classifier approach," in *Workshops at the Twenty-Eighth AAAI Conference on Artificial Intelligence*, pp. 22–26, Québec City, QC, Canada, July 2014.

[11] S. Sivaraman and M. M. Trivedi, "Looking at vehicles on the road: a survey of vision-based vehicle detection, tracking, and behavior analysis," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 4, pp. 1773–1795, 2013.

[12] A. Jazayeri, H. Cai, J. Y. Zheng, and M. Tuceryan, "Vehicle detection and tracking in car video based on motion model," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 2, pp. 583–595, 2011.

[13] A. Geiger and B. Kitt, "Object flow: a descriptor for classifying traffic motion," in *Proceedings of the 2010 IEEE Intelligent Vehicles Symposium (IV)*, pp. 287–293, La Jolla, CA, USA, June 2010.

[14] S. Cherng, C. Y. Fang, C. P. Chen, and S. W. Chen, "Critical motion detection of nearby moving vehicles in a vision-based driver-assistance system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 10, no. 1, pp. 70–82, 2009.

[15] F. Garcia, P. Cerri, A. Broggi, A. de la Escalera, and J. M. Armingol, "Data fusion for overtaking vehicle detection based on radar and optical flow," in *Proceedings of the 2012 IEEE Intelligent Vehicles Symposium (IV)*, pp. 494–499, Alcala de Henares, Madrid, Spain, June 2012.

[16] A. Barth and U. Franke, "Tracking oncoming and turning vehicles at intersections," in *Proceedings of the 2010 13th*

International IEEE Conference on Intelligent Transportation Systems (ITSC), pp. 861–868, Funchal, Madeira Island, Portugal, September 2010.

[17] D. Kasper, G. Weidl, T. Dang et al., "Object-oriented Bayesian networks for detection of lane change maneuvers," *IEEE Intelligent Transportation Systems Magazine*, vol. 4, no. 3, pp. 19–31, 2012.

[18] Y. Zhu, D. Comaniciu, M. Pellkofer, and T. Koehler, "Reliable detection of overtaking vehicles using robust information fusion," *IEEE Transactions on Intelligent Transportation Systems*, vol. 7, no. 4, pp. 401–414, 2006.

[19] J. Wang, G. Bebis, and R. Miller, "Overtaking vehicle detection using dynamic and quasi-static background modeling," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition-Workshops (CVPR'2005)*, p. 64, San Diego, CA, USA, June 2005.

[20] A. Barth and U. Franke, "Estimating the driving state of oncoming vehicles from a moving platform using stereo vision," *IEEE Transactions on Intelligent Transportation Systems*, vol. 10, no. 4, pp. 560–571, 2009.

[21] B. Barrois and C. Wöhler, "3D pose estimation of vehicles using stereo camera," in *Encyclopedia of Sustainability Science and Technology*, pp. 10589–10612, Springer, Berlin, Germany, 2012.

[22] J. Wiest, M. Höffken, U. Kresel, and K. Dietmayer, "Probabilistic trajectory prediction with Gaussian mixture models," in *Proceedings of the 2012 IEEE Intelligent Vehicles Symposium (IV)*, pp. 141–146, Alcala de Henares, Madrid, Spain, June 2012.

[23] S. Sivaraman, B. Morris, and M. Trivedi, "Learning multi-lane trajectories using vehicle-based vision," in *Proceedings of the 2011 IEEE International Conference on Computer Vision Workshops (ICCV Workshops)*, pp. 2070–2076, Barcelona, Spain, November 2011.

[24] C. Hermes, J. Einhaus, M. Hahn, C. Wöhler, and F. Kummert, "Vehicle tracking and motion prediction in complex urban scenarios," in *Proceedings of the 2010 IEEE Intelligent Vehicles Symposium (IV)*, pp. 26–33, La Jolla, CA, USA, June 2010.

[25] C. Hermes, C. Wohler, K. Schenk, and F. Kummert, "Long-term vehicle motion prediction," in *Proceedings of the 2009 IEEE Intelligent Vehicles Symposium*, pp. 652–657, Xi'an, China, June 2009.

[26] M. Dagdelen, G. Reymond, A. Kemeny, M. Bordier, and N. Maïzi, "Model-based predictive motion cueing strategy for vehicle driving simulators," *Control Engineering Practice*, vol. 17, no. 9, pp. 995–1003, 2009.

[27] J. Sorstedt, L. Svensson, F. Sandblom, and L. Hammarstrand, "A new vehicle motion model for improved predictions and situation assessment," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1209–1219, 2011.

[28] R. Pandita and D. Caveney, "Preceding vehicle state prediction," in *Proceedings of the 2013 IEEE Intelligent Vehicles Symposium (IV)*, pp. 1000–1006, Gold Coast City, Australia, June 2013.

[29] T. Hülnhagen, I. Dengler, A. Tamke, T. Dang, and G. Breuel, "Maneuver recognition using probabilistic finite-state machines and fuzzy logic," in *Proceedings of the 2010 IEEE Intelligent Vehicles Symposium (IV)*, pp. 65–70, La Jolla, CA, USA, June 2010.

[30] B. Morris, A. Doshi, and M. Trivedi, "Lane change intent prediction for driver assistance: on-road design and evaluation," in *Proceedings of the 2011 IEEE Intelligent Vehicles Symposium (IV)*, pp. 895–901, Baden-Baden, Germany, June 2011.

[31] A. Houenou, P. Bonnifait, V. Cherfaoui, and W. Yao, "Vehicle trajectory prediction based on motion model and maneuver recognition," in *Proceedings of the 2013 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 4363–4369, Tokyo, Japan, November 2013.

[32] D. Petrich, T. Dang, D. Kasper, G. Breuel, and C. Stiller, "Map-based long term motion prediction for vehicles in traffic environments," in *Proceedings of the 2013 16th International IEEE Conference on Intelligent Transportation Systems-(ITSC 2013)*, pp. 2166–2172, The Hague, Netherlands, October 2013.

[33] P. Kumar, M. Perrollaz, S. Lefevre, and C. Laugier, "Learning-based approach for online lane change intention prediction," in *Proceedings of the 2013 IEEE Intelligent Vehicles Symposium (IV)*, pp. 797–802, Gold Coast City, Australia, June 2013.

[34] W. Yao, H. Zhao, F. Davoine, and H. Zha, "Learning lane change trajectories from on-road driving data," in *Proceedings of the 2012 IEEE Vehicles Symposium (IV)*, pp. 885–890, Alcala de Henares, Madrid, Spain, June 2012.

[35] R. Schubert, E. Richter, and G. Wanielik, "Comparison and evaluation of advanced motion models for vehicle tracking," in *Proceedings of the IEEE 2008 11th International Conference on Information Fusion*, pp. 1–6, Cologne, Germany, June-July 2008.

[36] A. Berthelot, A. Tamke, T. Dang, and G. Breuel, "Handling uncertainties in criticality assessment," in *Proceedings of the 2011 IEEE Intelligent Vehicles Symposium (IV)*, pp. 571–576, Baden-Baden, Germany, June 2011.

[37] A. Tamke, T. Dang, and G. Breuel, "A flexible method for criticality assessment in driver assistance systems," in *Proceedings of the 2011 IEEE Intelligent Vehicles Symposium (IV)*, pp. 697–702, Baden-Baden, Germany, June 2011.

[38] N. Mattern, R. Schubert, and G. Wanielik, "High-accurate vehicle localization using digital maps and coherency images," in *Proceedings of the 2010 IEEE Intelligent Vehicles Symposium (IV)*, pp. 462–469, La Jolla, CA, USA, June 2010.

[39] M. Nitti, V. Pilloni, G. Colistra, and L. Atzori, "The virtual object as a major element of the internet of things: a survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1228–1240, 2016.

[40] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in internet of vehicles: a review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2339–2352, 2015.

[41] V. Punzo, M. T. Borzacchiello, and B. Ciuffo, "Estimation of vehicle trajectories from observed discrete positions and next-generation simulation program (ngsim) data," in *Proceedings of the TRB 2009 Annual Meeting*, Washington, DC, USA, January 2009.

[42] K. M. Alam, M. Saini, and A. El Saddik, "Toward social internet of vehicles: concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, 2015.

[43] F. Wang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of internet of vehicles," *China Communications*, vol. 11, no. 10, pp. 1–15, 2014.

[44] S. Gao, Y. Wang, J. Cheng, Y. Inazumi, and Z. Tang, "Ant colony optimization with clustering for solving the dynamic location routing problem," *Applied Mathematics and Computation*, vol. 285, pp. 149–173, 2016.