Hindawi Publishing Corporation
International Journal of Vehicular Technology
Volume 2011, Article ID 120194, 7 pages
doi:10.1155/2011/120194

Research Article

A New Distributed and Scalable Network Protocol Targeting Intelligent Transportation Systems

M. Meribout

Departmentof Electrical Engineering, The Petroleum Institute, Abu Dhabi, UAE

Correspondence should be addressed to M. Meribout, mmeribout@pi.ac.ae

Received 8 March 2011; Accepted 28 April 2011

Academic Editor: Mohsen Guizani

Vehicular networks are the major ingredients of the envisioned Intelligent Transportation Systems (ITS) concept. An important component of ITS which is currently attracting wider research focus is road traffic monitoring. The actual approaches for traffic road monitoring are characterized by longer response times and are also subject to higher processing requirements and possess high deployment costs. In this paper, we propose a completely distributed and scalable mechanism for wireless sensor network-based road traffic monitoring. The approach relies on the distributed and bidirectional exchange of traffic information between the vehicles traversing the routes and a miniature cluster head and takes into consideration both the security and reliability of data communication. In addition, the communication between nodes is collision-free since the underlined data link layer protocol relies on a heuristic time multiplexed-based protocol. The performance analysis shows that the proposed mechanism usually outperforms other algorithms for different traffic densities.

1. Introduction

Road traffic monitoring is important for the safety and well-being of passengers. The traditional ITS traffic information systems are based on a centralized structure in which radars and cameras along the roadside continuously monitor road traffic. The collected data is usually stored on a tape to be collected or transmitted to a remote control room via the Internet for further processing [1–3]. The results will then be communicated to road users. However, these systems require substantial public investment in sensing, processing, and communication equipments, which lead to their relatively weak deployment in the road network. Moreover, such systems are characterized by long reaction times and thus are not useable by all the applications requiring reliable decision making based on accurate and prompt road traffic awareness. In addition, the communication between these systems and the vehicles is usually performed in only one direction (i.e., from vehicle to ITS), preventing the car drivers to collect some useful information such as the actual upper speed limit of the road or various facilities and services surrounding the actual road. Thus, in order to overcome the disadvantages of centralized schemes, several initiatives using wireless sensor network began to appear. In the work described in [4], the authors propose a simple time-dependent solution for road congestion estimation. The solution is based on an opposite stream vehicle communication approach where each vehicle use its embedded wireless sensor network to exchange information about the average entry-exit times (travel times) of segments with their neighbors in the opposite streams. This updated traversal times, which are assumed to be stored at the street segments, could help the driver as descriptive network information to reevaluate current routes and to possibly produce new routes. Another wireless sensor network-based decentralized approach named as SOTIS (Self-Organizing Traffic Information System) was proposed in [5]. The traffic condition is evaluated in terms of average velocity for traffic segments. Then, the vehicles periodically exchange and update their current position and traffic information (e.g., average velocity), in order to inform the surrounding vehicles about the individual knowledge. Another wireless sensor network-based decentralized solution is proposed as part of the e-Road project [6], which aims to achieve a scalable communication infrastructure for

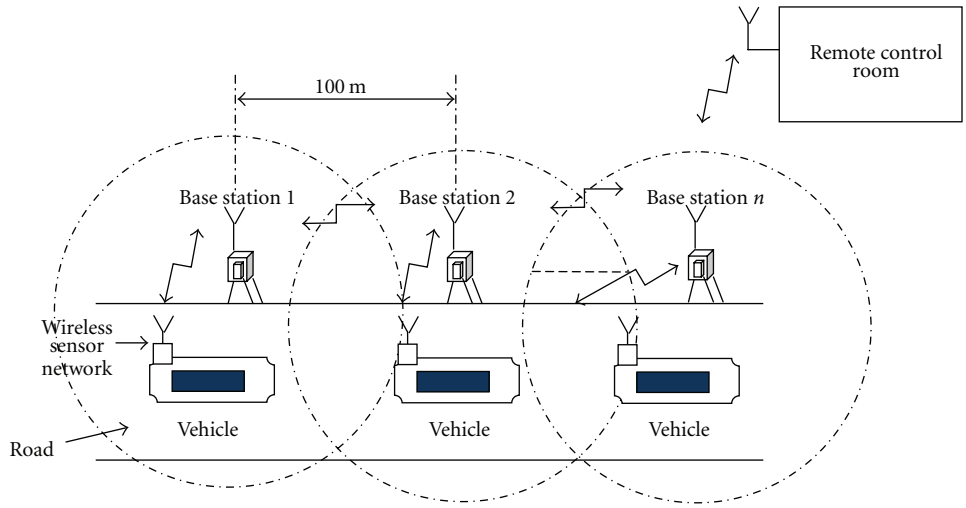

Figure 1: Wireless sensor network infrastructure for road traffic monitoring.

IVC (Intervehicle Communications). As part of this project, they propose a system called Traffic View [7], which aims at disseminating and gathering information about vehicles in the road. Using such a system, the vehicle driver will be aware of the road traffic, which helps in driving through foggy weather or in determining optimal route in a long distance trip. The system works based on frequent message broadcast based on the information provided by the GPS receiver (like location, speed, current time, and direction of the vehicle). The received neighborhood information is validated to avoid conflicting information and is then moved and merged with existing validated dataset. Periodically, the system displays the data from the validated set.

One of the major drawbacks of the above network architectures is the serious lack of security, where an intruder may attack the whole network by flooding false information about the actual status of the road or by detecting some confidential messages of the vehicles, such as the messages sent by these vehicles in case they exceed the speed limit or in case of a specific service enquiry. Instead, most of these approaches use the same constraints known in most other wireless sensor network applications: power consumption cost. However, since the sensor can be power-supplied by the car battery, this constraint is negligible. The other disadvantage of these approaches is that they rely on information exchanged between vehicles, and thus the performance of their underlined routing protocols may be weak in case of a low vehicles density in the road.

In this paper, a low cost and secure wireless network infrastructure for an effective car traffic management is proposed. It consists of a distributed cluster heads (e.g., miniature base stations) deployed along the side of the road which communicate with moving vehicles in a full duplex manner. The communication protocol for each cluster head uses a key refreshment algorithm, in order to securely exchange information with the neighboring vehicles within their corresponding cluster. Moreover, the communication within the network is performed in a time multiplexed manner, where each node of the network (for both moving vehicles and stationary cluster heads) is provided with dynamic and unique time slots which may vary depending on the status of the road. Hence, more than one time slot can be allocated for a vehicle by the cluster head of the corresponding cluster, depending on the traffic load in that cluster. Experimental results show that the proposed protocol might be a possible candidate in next generation network protocols for ITS applications.

2. Wireless Sensor Network Model

In the proposed architecture the wireless cluster heads (i.e., base stations) are deployed along the road every few dozens of meters, depending on the underline physical and data link network layers (e.g., 100 m for IEEE802.15.4) (Figure 1). Each cluster head comprises a wireless sensor network. One significant design factor for the routing protocol which handles the peer-to-peer communication between the vehicles and the base stations is that the power consumption of wireless nodes is not of primary importance since the power supply is provided to the base stations via the electrical wires which are usually available in the Poteau lights, whereas the wireless nodes of the vehicles are power supplied with the car's battery. On the other hand, reliability and security of real-time data transfer is an important factor. Unfortunately very few papers in the literature tackled this constraint for road traffic monitoring applications. This constitutes one of the contributions of this paper. The other contribution of this paper is the collision-free data link layer protocol since the peer-to-peer communication is performed in a time multiplexed manner.

In the above network, each cluster head node, i, is permanently provided with a unique and confidential physical address, A_i, and an initial confidential private key, Pk_i, which should be refreshed (i.e., modified) several times while the car is moving. This would allow a reinforcement of the security of the network, against intruders which may try to

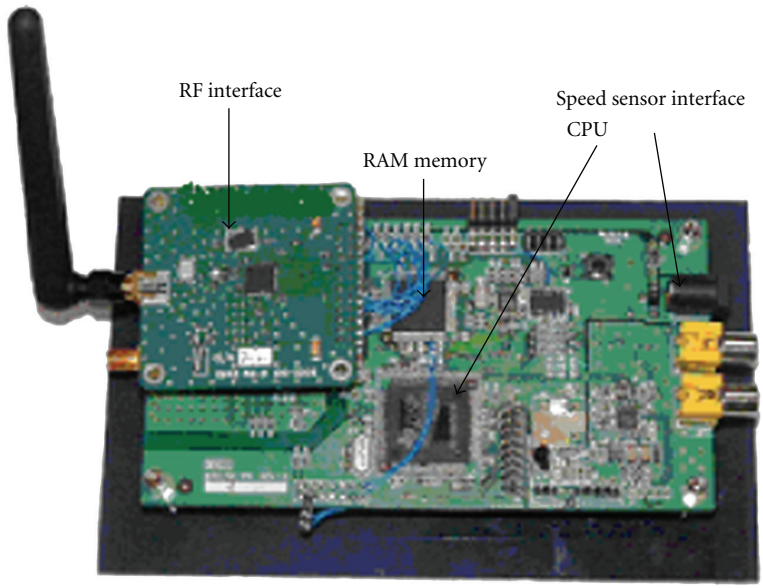

Figure 2: Development board.

capture the key of the actual vehicle. Hence, the communication between the vehicle and the cluster head (base station) is performed using a private key encryption algorithm (i.e., Data Encryption Standard, DES, algorithm). The cluster heads are assigned with a similar broadcast physical address, Br.

The wireless sensor network embedded into the vehicle is compact and comprises (Figure 2 shows the prototype board)

(i) a RISC processor to implement the network protocol,

(ii) a radio frequency module, to transfer/receive data in a wireless manner,

(iii) a speed sensor to continuously capture the actual speed of the car,

(iv) an LCD display interface to display some useful information to the driver.

As for the cluster head, in addition to the CPU and radio frequency module, it comprises a mass storage memory (i.e., flash) to store relatively longer messages such as the various services that can be provided in the area.

3. Communication Algorithm

In the proposed network infrastructure, the communication between the cluster heads and the vehicles within the same cluster is done in a full duplex manner to handle different situations. For instance, in case a vehicle exceeds the maximal speed limit, a corresponding message is immediately broadcasted by the vehicle to the nearby cluster heads, using the destination physical address, Br. The message will be then forwarded to the remote control room by the intermediary cluster heads. Moreover, in order to avoid sending duplicate packets to the remote control room (since a same message may be received by more than one cluster head), a base station checks if it has already transferred or not the same message by checking the sender's physical address and its time stamp. In addition, and in order not to penalize the same vehicle several times during a same trip, the received time stamp parameter, t_s, is compared against a threshold, th, to be set by the road traffic authorities. In another situation, a vehicle may enquire about a specific service such as the facilities surrounding the area (e.g., restaurants, hotels, and specific shops). Hence, the vehicle sends a corresponding request message to the neighboring cluster head. This scenario is straightforward for straight roads. However, in case of road intersections, the routing algorithm needs to switch from one road segment to another. For instance, in Figure 3, the vehicle which initiates an enquiry at time t_0, receives a first part of the answer (Ans no.1) from the base station A. The same message is also received by the base station B which would relay subsequent parts of the message to the same vehicle in case the vehicle would roam into its corresponding cluster. The vehicle then sends a corresponding acknowledgement message (Ack no. 1) to the same base station. At time t_1, however, the vehicle reaches the cross of the road and receives, together with the base stations C and D, the next message (Ans no. 2) from the base station B. Hence, both the base stations C and D send the third message (Ans no. 3). However, as only the base station D receives the corresponding acknowledgment message (Ack no. 3), the message relaying would switch from road segment A to road segment B.

In the above network architecture, the cluster heads are separated by a distance of 100 meters. Taking into consideration that the maximal speed limit of vehicles in all road segments is 120 km/hr, it takes around 180 s for a vehicle to roam from one cluster head to another. Hence, the routing algorithm needs to ensure that every vehicle can send

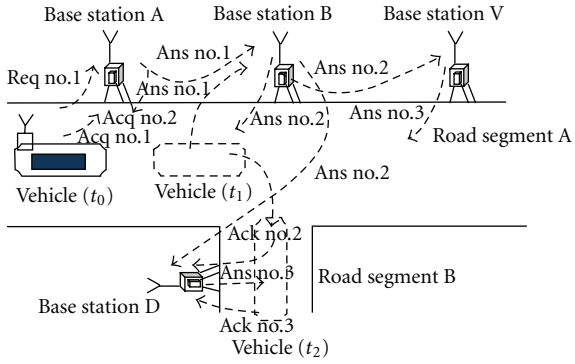

Figure 3: Handling network services in case of road intersection.

its message within this worst case frame period. In our case, each node is provided with a time slot, the time of which was set to be proportional to the number of bits to be sent. For instance, taking into consideration that each transmitted bit from the vehicle to the base station has a speed of 3×10^8 m/s, the transmission delay of N bits, in case the distance between the vehicle and the cluster head is 10 meters (upper limit in normal roads), would be less than $N \times 33$ ns. Therefore, in case of N bits messages, the maximal duration of one single time slot is $(180 \times 10^9)/(N \times 33)$ slots. The determination of the parameter N depends on the security protocol as well as on the type of messages to be transferred. Hence, in our algorithm, the time slots is divided into three types (Figure 4).

The vehicles messages are sent by the vehicles and include the enquiry and acknowledgement messages for general services, in addition to the information messages, in case of exceeding the speed limit. The services messages are sent by the base stations and are related to the various facilities surrounding the area. Finally, the emergency messages are sent by the base stations and are related to some emergency information for the vehicles, such as the speed limit in the actual road, the level of traffic congestion in nearby roads, or the existence of some ongoing road reparation works few hundred meters ahead. Note that the messages of the same type have the same duration (Ti, Ui, and Vi for the vehicles, services, and emergency messages, resp.) since they have the same size, whereas Ti, Ui, and Vi can be different. One important feature necessary for the successfulness of the above network protocol is the protection of the communication data against various types of security threats. For instance, an intruder may provide false advertisements to the vehicles. Also, an attacker may forward a speed limit exceed message of another vehicle. Therefore, various protocols need to be implemented in the proposed approach in both the base stations and the vehicles.

3.1. Initial Time Slot Allocation Algorithm. In the proposed infrastructure, a vehicle, i, before it moves, needs to request its nearest base station, u, for a unique and free time slot, $\mathrm{Ts}(i)$, that it can use for any eventual communication with the cluster corresponding to that base station. This would ensure a collision-free data link layer protocol, leading to a more effective usage of the physical medium by providing a fair load balance between the three various types of messages (Figure 4). However, while roaming from one cluster to another, a time slot refreshment algorithm is performed when a vehicle enters a new cluster as the same time slot may be already allocated for other vehicles. The two corresponding algorithms (i.e., initial time slots and time slot refreshment) are illustrated in Figures 5(a) and 5(b), respectively.

Following the execution of the function GetTimeSlot(Pki, Ai, Br) in the first algorithm, both neighboring base stations u and v are triggered to allow all the three devices to be aware on the time slot, $\mathrm{Ts}(i)$, and private key, Pki, allocated for the vehicle, i. The three and two ways handshaking between the vehicle i and the base station u and between the two base stations u and v, respectively, ensure a reliable communication as other communications may be simultaneously active since the node i is initially not aware about the free time slots which are available within the actual area. In the algorithm of Figure 5(b), each base station, v, afterwards knowing the presence of a vehicle, i, executes the function SendTimeSlot(Pki', Ai, $\mathrm{Ts}'(i)$) after a certain delay, estimated based on the actual congestion of the road and the speed of the vehicle, i, to send an eventual time slot to the vehicle, i. This latest needs to acknowledge the receipt of such packet to advertise its presence to both the base station, v, and the next one, w. In case the base station v does not receive this acknowledgement packet, the car is supposed to have taken another itinerary from the cross point heading the base station v.

3.2. Key Refreshment Algorithm. In the proposed network architecture, the peer-to-peer transmission of messages is protected by a private key encryption algorithm (i.e., DES algorithm). Hence, and in order to avoid the situation where the private key, Pki, may be caught by intruders, a key refreshment algorithm is performed periodically between all neighboring base stations and between a vehicle and its corresponding cluster head (Algorithm 1). Hence, each vehicle, i, generates a random counting number, $\mathrm{count}(i)$, which is then communicated to the neighboring cluster head, u. Next, both the vehicle, i, and the base station, u, update their key after exactly $\mathrm{count}(i)$ clock ticks. In case the vehicle leaves the area corresponding to the cluster head, u, to roam to a neighboring cluster with cluster head, v, then this latest enables its internal interrupt. In the algorithm, the function f depends on the hardware complexity of the wireless sensor in order to provide good security key in reasonable amount of time. In our case, because a 16 bits multiplication can be done in two clock cycles, the following function was implemented:

$$\mathrm{Pki} = \frac{\mathrm{Pk_i} \times \mathrm{Count}(i)}{N} \times \mathrm{code}, \tag{1}$$

where N is the number of times the key has been refreshed, and the code is the secret vehicle code.

3.3. Packets Formats. In Algorithm 1, various types of messages are used as described in Section 3 (Figure 4). Figure 6

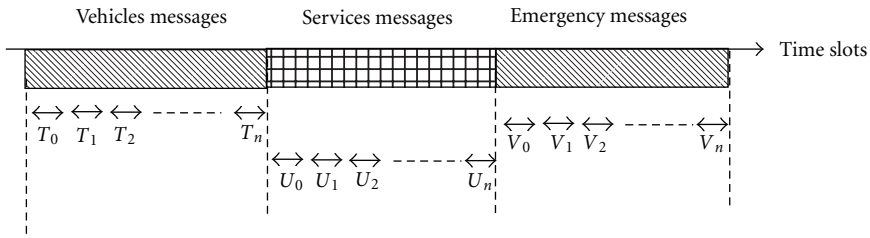

Figure 4: Time slots reservation in the proposed network architecture.

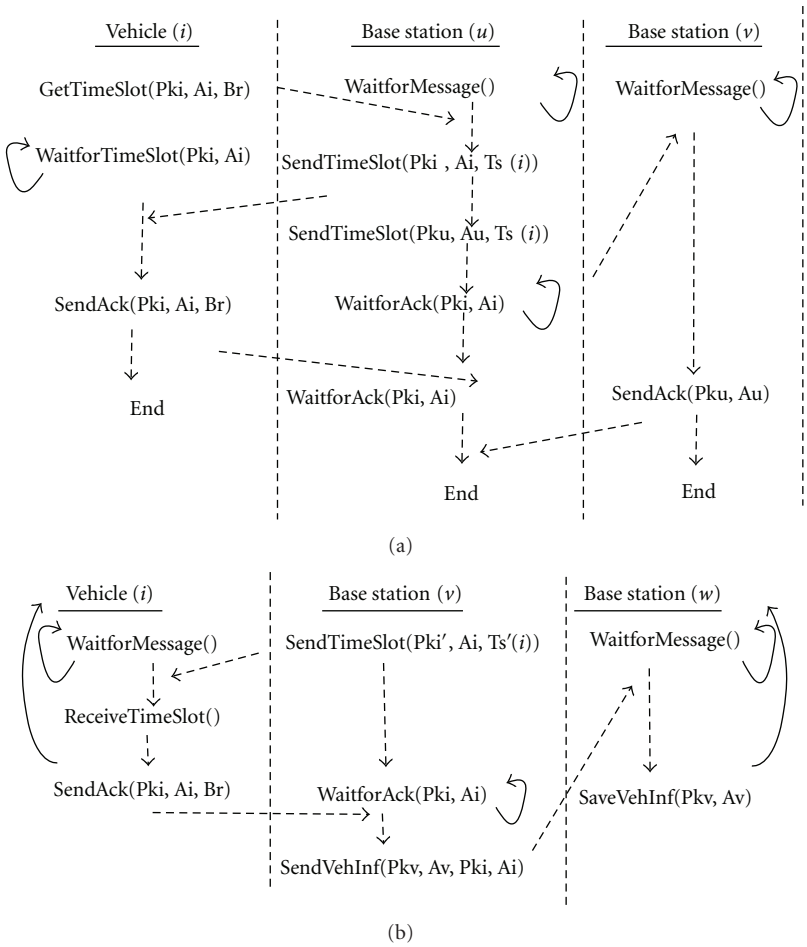

Figure 5: Initial time slot allocation (a) and time slot refreshment algorithms (b).

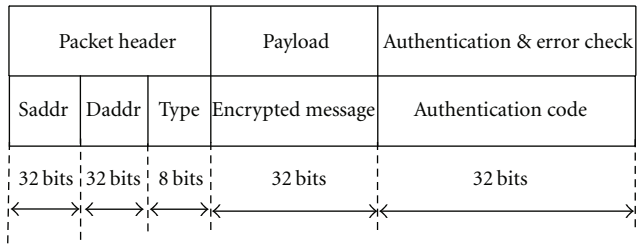

Figure 6: Packet format of vehicles messages.

```
1    while (CarEngineisOn()){
2      Count(i) = random();
3      SetTimer(count(i));
4      SendMsg(Pki, Ai, count(i), Br)
5      WaitforTimerInterrupt();    // Loop here
6      Pki = f(Pki, count(i), code);
7    }// end while;
```

Algorithm 1: Key refreshment algorithm.

shows the formats of the packets related to vehicles messages. Hence, the source address, Saddr, is the actual address of the car which is uniquely provided by the traffic road authority. The destination address, Daddr, is the broadcast address (Br) for the cluster heads only in order for the packet to be only explored by the cluster head, not by other vehicles. Both of these two fields have been assigned with 32 bits. The message contains various types of information such as the secret key, Pki, of the sender, i, its confidential physical address, Ai, and the count value, count(i), for private key refreshment (used by the function keSendMsg(Pki, Ai, count(i), Br) in Algorithm 1). As for the authentication code field, it is used to ensure that the message has not been sent by intruders and is performed by the sender according to the following equation:

$$\text{Authentication Code} = \sum_{i=0}^{M} \frac{(\text{DecryptedMessage}[i] \oplus \text{EncryptedMessage}[i]) \times \text{Count}(i)}{\text{Pki}}, \quad (2)$$

where M is the message size. Hence, in order for the intruder to produce the same authentication code, it has to know the private key to correctly decrypt the message field, in addition of knowing the actual value of count(i).

The type field has been assigned with 8 bits, whereas the encrypted message is assigned with 32 bits since only one of the parameters: The value of count(i), type of services, and actual speed of the are sent. In addition, each of these parameters is less than 32 bits.

As for the base stations, the structure of the packets of the emergency messages is similar to those corresponding to the vehicles messages (Figure 4). However, the services messages are longer and are assigned with 100 bits since their length usually exceeds this amount. In case the service message exceeds this amount, then a packet segmentation is performed to split it into smaller segments.

4. Experimental Results and Discussions

The proposed scheme was implemented in TinyOS and evaluated using the build-in simulator in TinyOS, TOSSIM [8]. Several experiments under various scenarios have been conducted and compared with tinysec [8] and the standard Public Key Infrastructure (PKI) signature scheme in [9]. In all these experiments, the cluster heads were separated by a distance of 100 meters to cover the maximal number of vehicles while reducing the overlaps between the clusters. A group of several vehicles, running at different speeds, were initially associated to each cluster. The overall length of the road was set to 2 Km. Figures 7 and 8 show the number of packets lost function of the number of communicating nodes for the vehicles messages (sent by vehicles) and services messages (sent by the cluster head), respectively, when the nodes move at a same constant speed (i.e., 100 km/hr). In

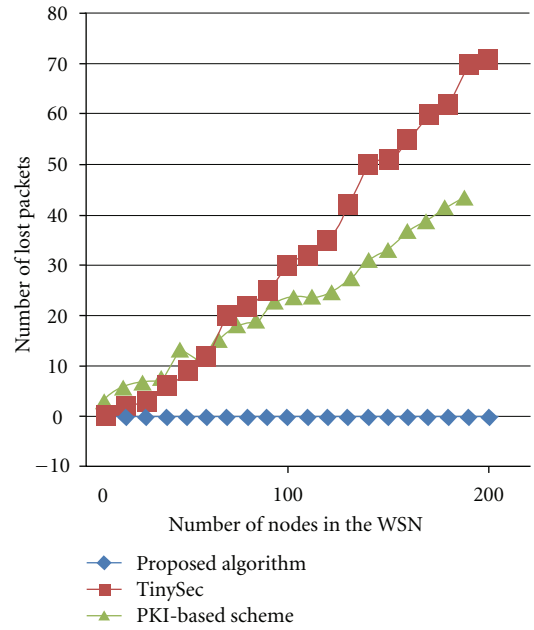

Figure 7: Algorithm performance: number of packets lost versus the number of communicating nodes moving at speed of 100 km/hr for vehicles messages.

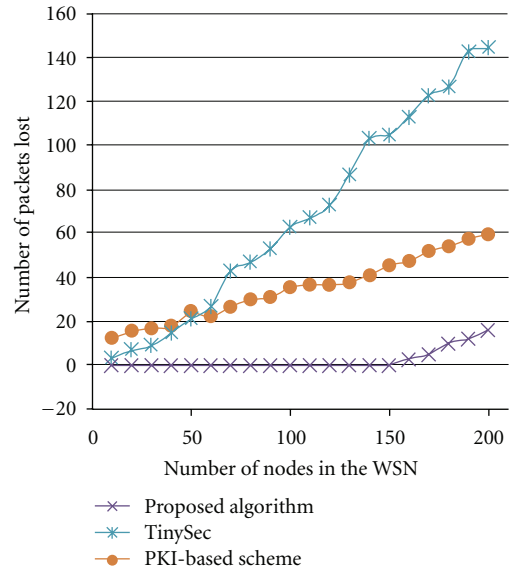

Figure 8: Algorithm performance: number of packets lost versus the number of communicating nodes moving at speed of 100 km/hr for services messages.

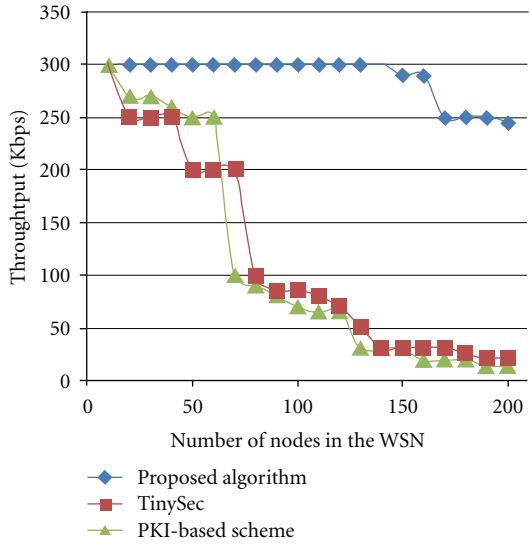

Figure 9: Algorithm performance: throughput versus the number of communicating nodes moving at speed of 100 km/hr for services messages.

the simulator, both the wireless sensor nodes and the cluster heads perform the data encryption algorithm (DES-based encryption algorithm) before actually accepting any received data. It can be seen that, overall, the proposed algorithm achieves a linear scalability since no packet loss occurred even for high number of vehicles (i.e., 200 vehicles). This can be justified from the statements outlined in Sections 3 and 4 where the vehicles messages need a time slot of 136 bits $\times$ 33 ns $=$ 4.5 ms. Hence, in case the three types of messages are assigned with similar durations (e.g., 60 s for each type in Figure 4), a total of 13,300 vehicles can intercommunicate within the same cluster without having collisions which is much higher than the maximal number of cars which should not exceed 200 meters within a road segment of 100 meters length. On the other hand, using TOSSIM routing algorithm, the packet loss increases with the number of simultaneous packet because of the increasing congestion in the network. In case of services messages, the proposed algorithm clearly outperforms the other two algorithms; however, some packets lost occurred when more than 150 vehicles are available in the same road segment. The performance of the algorithm in terms of packets throughputs (in bits/s), function of the number of communicating nodes, is shown in Figure 9. Hence, the proposed algorithm outperforms other algorithms as well. However, for a large number of nodes (i.e., number of nodes greater than 170), the throughput tends to decrease because of the overhead caused by the symmetric encryption algorithm.

5. Conclusion

In this paper, a new distributed wireless sensor network for secure traffic road monitoring is provided. The architecture features a full duplex and deterministic communication between the vehicles and the stationary cluster heads which are distributed along the side of the road. It allows a seamless monitoring of the speed of vehicles, while providing various types of services to the drivers such as the available facilities surrounding the actual cluster. Simulation results indicate that the algorithm clearly outperforms other available routing algorithms in terms of packet lost and throughput. As a possible future work, a deeper analysis of the effect of the packets sent by the intruders on the overall performance of the network will be investigated. Hence, a primary idea is to trigger an alarm whenever an intruder is detected in the road. This can be done by counting the number of times the authentication code does not match the message, which when it exceeds a predefined threshold, a security threat is most likely to be occurring.

Acknowledgment

The author would like to thank the Petroleum Institute (UAE) for supporting the present work.

References

[1] D. Schrank and T. Lomax, "The 2003 annual urban mobility report," Tech. Rep., Texas Transportation Institute, Texas A&M University, 2003.

[2] D. Schrank and T. Lomax, "The 2001 annual urban mobility report," Tech. Rep., Texas Transportation Institute, Texas A&M University, 2001.

[3] ITS America, "Ten-Year National Program Plan and Research Agenda for Intelligent Transportation Systems in the US 2001".

[4] A. K. Ziliaskopoulos and J. Zhang, "A zero public infrastructure vehicle based traffic information system," in *Proceedings of the Transportation Research Board Meeting (TRB '03)*, July 2003.

[5] L. Wischhof, A. Ebner, H. Rohling, M. Lott, and R. Halfmann, "SOTIS—A self-organizing traffic information system," in *Proceedings of the 57th IEEE Semiannual Vehicular Technology Conference (VTC '03)*, pp. 2442–2446, April 2003.

[6] E-Road Project, http://discolab.rutgers.edu/traffic/.

[7] T. Nadeem, S. Dashtinezhad, C. Liao, and L. Iftode, "TrafficView: traffic data dissemination using car-to-car communication," in *Proceedings of the ACM Mobile Computing and Communications Review (MC2R '04)*, July 2004.

[8] P. Levis, N. Lee, M. Welsh, and D. Culler, "TOSSIM: accurate and scalable simulation of entire TinyOS applications," in *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys '03)*, pp. 126–137, ACM Press, New York, NY, USA, November 2003.

[9] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages, IEEE Std. 1609.2-2006, Jul. 2006.