Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3884761, 8 pages
https://doi.org/10.1155/2022/3884761

Research Article

Jamming Attack in Vehicular Networks: Adaptively Probabilistic Channel Surfing Scheme

Anh Tuan Giang, Hoang Tung Tran, Huu Ton Le, Nhat Quang Doan, and Minh Huong Nguyen

University of Sciences and Technologies of Hanoi, Hanoi, Vietnam

Correspondence should be addressed to Anh Tuan Giang; giang-anh.tuan@usth.edu.vn

Received 8 April 2022; Accepted 29 June 2022; Published 11 July 2022

Academic Editor: Zahid Khan

Vehicular networks play a crucial role in Intelligent Transportation System (ITS), making transportation safer and more convenient. Most applications in ITS require information carried by basic safety messages (BSMs) to be exchanged periodically among vehicles. However, BSMs are vulnerable to different attacks, especially jamming attacks, due to their limited short message length and life span. In this paper, we analyze the impact of a jamming attack on BSMs and initially propose a random channel surfing scheme to attempt to react to the attack. We investigate the scheme by a simple extendible probabilistic model and simulation in NS-3. Obtained results provide a reference to design an optimal channel surfing scheme that adapts to its supported applications.

1. Introduction

Vehicular networks facilitate communication among vehicles (V2V) and between vehicles and roadside infrastructure (V2I) in the transportation network. Thanks to this communication, the network infrastructure can serve an extensive range of applications. Among these, safety applications that make transportation safer are one crucial type. They operate based on essential information included in basic safety messages (BSMs), such as position, velocity, acceleration of vehicles, and hazardous incident warnings. Due to the requirement of freshness and the compact of information, BSMs are exchanged periodically every 100ms [1, 2] and have short lengths. These characteristics make BSMs prone to be targets of many types of wireless attacks, especially attacks at the physical and medium access control layer, such as jamming attacks. Limited packet length does not allow complex cryptography. The short life span, in milliseconds, makes BSMs easily become victims of simple but effective attacks like jamming attacks, as no time is taken for the attacker to do complex computations.

Jamming is one kind of Denial-of-Service (DoS) attack. It broadcasts radio signals in the physical channel to block any communication in the same physical channel within its transmission range. Jamming can be either constant jamming or reactive jamming. In constant cases, the attacker continually emits radio signals not following any rule of communication protocol. In reactive jamming, the attacker (so-called the jammer) transmits radio signals upon sensing a transmission in the medium. Reactive jamming is more dangerous and harder to detect as it conforms to legitimate transmission [3]. The impact of jamming is graver to safety applications because of their time constraints. The consequence can be severe if the safety-related information is not delivered to the appropriate vehicles at the right time because of the interruption caused by jamming.

While the impact of a jamming attack is profound for safety applications, mitigation against them in vehicular networks encounters even more challenges. Indeed, characteristics of the vehicular environment have raised these challenges in VANETs. The main ones include issues of inherent properties of radio channels, highly dynamic operating environment, lack of centralized management, high-reliability requirements, and low latency communication and scalability.

In the case of BSMs, it becomes even more challenged because BSMs are supposed to be transmitted only in the control channel and renewed every short-time period (100 ms, as the suggestion in [1, 2]). It relates to a multichannel operation specified in the suit of standards IEEE 1609 for Wireless Ad hoc Vehicular Environments (WAVEs). According to the suit of standards, vehicles switch alternatively between one control channel (CCH) to any service channel (SCH), as illustrated in Figure 1. This working mechanism allows single-PHY devices, or vehicles in VANETs, to access high-prioritized data and management traffic in CCH during CCH intervals (CCHIs), as well as general traffic in SCH intervals (SCHI).

There are a considerable number of proposals dealing with jamming attacks, one of the most practical proposed approaches is channel surfing [4]. After detecting jamming [5] [6] (jamming detection are out of our scope), communication devices change from the current jammed channel to other available channels. The question is which channel should be chosen provided that the communication can be remained among as many devices as possible while other performance and security constraints should be satisfied. The concept of channel surfing is commonly studied in wireless and vehicular networks but is not dedicated to safety applications. This paper focuses on safety applications in vehicular networks, precisely the critical type of messages, the BSMs.

Our contributions are in both mathematical and networking aspects. Firstly, we study the integration of mitigation against jamming attacks from wireless networks into VANETs and propose an adapted channel surfing scheme to deal with jamming attacks on safety applications in VANETs. Secondly, we offer a probabilistic model in the evaluation of our works. Simulation results validated the model. Furthermore, the results allow us to choose appropriate parameters of the scheme for the delay requirement of safety applications.

The paper is organized as follows: the threat of jamming attacks on safety applications in vehicular networks is briefly described in this Section 1; Section 2 discusses related works on methods to deal with jamming attacks in wireless networks; our random channel surfing scheme is elaborated in Section 3; the analytical model to investigate our proposed scheme is defined in Section 4; the obtained numerical results are validated by simulation and also analyzed in details in Section 5; Section 6 concludes the paper.

2. Related Works

Many research efforts focus on designing defense strategies for vehicular networks, but the problem remains an open issue. Several approaches have been developed in wireless networks to defend against jamming attacks. We can classify these solutions into two types of strategies: competition strategy and retreat strategy. In the competition strategy, nodes reduce jamming effects by adjusting their physical-layer parameters such as transmit power, data rate, and carrier sensing threshold [3]. Because the radio channel substantially impacts communication in the vehicular environment, one should carefully consider the feasibility of competition strategy in vehicular networks. Besides, the retreat strategy seems more practical for communication in the vehicular environment. In retreat strategy, devices must coordinate to switch to the same new channel when jamming attacks block the current channel. However, channel coordination emerges as a problem for broadcasting, and BSM exchange has a broadcasting nature. This paper considers the feasibility of retreat strategy and channel surfing approach, particularly an attempt to deal with jamming attacks on BSMs.

In wireless networks, channel surfing approaches have been proposed [4, 7–9]. The crucial point making channel surfing feasible is how devices agree beforehand on the channel switching sequence. Based on how devices choose the channel switching sequence, channel surfing approaches can be classified into prior negotiation and without negotiation. In prior negotiation, devices must exchange information to make a channel agreement [10]. Considering Wi-Fi communication, Navda et al. [10] proposed a channel surfing scheme on which the access point generates a pseudorandom channel sequence, encrypts it, and exchanges it securely using the client's public key. In [8], the authors propose a coordinated channel-switching strategy. The devices, or nodes, detect themselves as jammed nodes, switch immediately to the orthogonal channel, and wait for chances to reconnect to the entire network. The boundary nodes who lose connectivity with their neighbors monitor available channels and connectivity to their neighbors in these channels. Finally, the boundary node selects the new channel and notifies all other nodes. Performance of channel surfing approaches also varies accordingly to the mobility of the networks because of the change in neighborhood leading to the variation of the number of neighbors [11, 12].

The prior negotiation may guarantee the channel agreement after jamming detection; however, it can be vulnerable to attackers. Negotiation data is exposed and possibly intercepted; thus, one can reveal the surfing sequence or information of the new channel. For this reason, Djuraev et al. propose a channel surfing scheme without prior negotiation. They use transmission power and received signal strength to determine the next channel in [4]. In [7], two entities, A and B, exchange packets, and B sends a data packet to A. Then, A acknowledges back to B in the following ACK. The next channel is determined based on the received signal strength indicator of the data packets and ACKs received at corresponding entities. Considering physical technology to deal with jamming, Strasser et al. propose a frequency hopping on which the two communication entities switch their channel at different rates [9]. There exist time slots that the two entities can encounter. The technique requires advanced transceivers and does not reach high channel utilization. The issue of effective coordination among vehicles to react to jamming attacks remains [3, 13].

The abovementioned approaches focus on communication between only two entities in wireless networks.

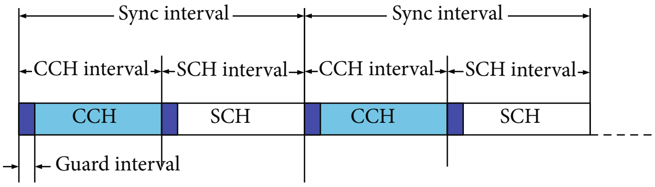

Figure 1: Multiple operation: alternating access.

Mitigating jamming attacks in vehicular networks for broadcast communication is still an open issue. There have been several works on broadcast in wireless networks. The authors in [14] utilize spreading code to cope with jamming in broadcast scenarios. The proposed protocol applies to the Code Division Multiple Access (CDMA) system. In [15], the authors propose a collaborative broadcast scheme using the uncoordinated frequency hopping technique. According to this scheme, nodes receiving a broadcast message will help forward it to other nodes. There are always opportunities for nodes to exchange messages through unjammed channels. As one of the limited number of works that consider broadcast in VANETs, [16] proposes a hideaway strategy. Vehicles stop all transmission until the jammer moves away. It means communication is interrupted for an undetermined period. Focusing on safety applications in vehicular networks, in this paper, we initially propose an adaptively probabilistic channel surfing scheme that adapts to their characteristics, such as broadcast manner, multiple channel operation, and short lifespan of BSMs. This scheme is an extended version of the one proposed in [17]. We study our scheme in a mathematical model and use simulation to validate the results. The mathematical model allows us to tune the scheme to achieve the time constraint requirements of safety applications in vehicular networks. We elaborate on the detail of the scheme in the following section.

3. Adaptively Probabilistic Channel Surfing Scheme

3.1. Assumption. This paper assumes vehicles that participated in the network have been deployed with some safety applications, and these applications always have safety information that is needed to broadcast through BSMs. Second, the jammer will attack the network at a given time. According to the standard IEEE 1604.9, vehicles alternatively switch from one CCH to one of 6 available SCHs to accommodate corresponding services. BSMs are exchanged periodically every 100 ms at CCHIs. In case of being attacked, communication in CCH is blocked by a reactive jammer that emits a noninformation radio signal whenever it senses a transmission within its sensitivity range. After detecting the attack of the jammer, vehicles will trigger our proposed random channel surfing scheme. Vehicles change their operating channel to a random one of the 6 SCHs instead of CCH during each CCHI. For SCHIs, vehicles keep their original schedule to maintain non-safety services. Every vehicle is supposed to have one safety-related information included in several BSMs that should be sent repeatedly within a certain period, provided that the number of vehicles that received the information is as high as possible. In this work, vehicles continuously transmit the safety information till the transmission times reach 100, i.e., during 10 seconds.

3.2. Random Channel Surfing Scheme. When a vehicle detects a jamming attack, the channelSurfing() procedure implemented in this vehicle is triggered. First, the vehicle chose a set of predefined probability parameters for channel assignment. The values of those parameters represent the probabilities of which SCH channels will be assigned for the next CCHI. The applications that need to broadcast their safety information must choose which set of parameters. Criteria are selected based on their designs and requirements of time constrain. In this paper, we evaluate three different sets of predefined probability parameters (Table 1). The first set corresponds to when choosing one of the available SCHs is uniformly distributed between 1 and 6. In the second and third cases, the distribution of choosing SCH is linear and geometric. Figure 2 illustrates these distributions.

Once the channel number is assigned, the vehicle switches to that channel for the next CCHI. The SCH number follows the same distribution the vehicle chooses at the beginning. The channelSurfing() procedure is detailed in Algorithm 1. After the jamming attack is confirmed and the communication fails, this procedure first calls the channelGenerator() function. This function returns the number of SCH based on the type of safety application. Each application has a corresponding set of probability parameters. Next, the application stops communication on the current SCH, and a new SCH will be used in the next CCHI. The channelSurfing() procedure will be executed until the communication is recovered (receiving BSMs).

3.3. Evaluation Metric. We can evaluate the usefulness of this random channel surfing scheme by the mean number of vehicles that can recover the communication when suffering a jamming attack after a time interval t. It means that after t CCHIs (BSMs are exchanged periodically every CCHI), the larger the mean number of vehicles that receive BSMs is, the better the performance of the proposed scheme is. The evaluation of this proposed scheme thus boils down to finding out the average number of vehicles that receive the BSMs after t CCHIs.

4. Analytical Model

Proposition 1. *We consider the random channel surfing described in the previous section. Let N be the number of vehicles receiving BSMs from a sender. Let K_t be the random variable representing the number of vehicles able to receive*

Table 1: Different sets of probability parameters.

	p_1	p_2	p_3	p_4	p_5	p_6
Uniform distribution	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$
Linear distribution	$\frac{3}{10}$	$\frac{2.5}{10}$	$\frac{2}{10}$	$\frac{1.5}{10}$	$\frac{0.5}{10}$	$\frac{0.5}{10}$
Geometric distribution	$\frac{5}{10}$	$\frac{2}{10}$	$\frac{1.5}{10}$	$\frac{1}{10}$	$\frac{0.5}{10}$	$\frac{0.5}{10}$

BSMs after t CCHIs. Then, $K_t \sim Binomial(N, \sum_{i=1}^{t}(1-p)^{i-1} p)$ with its probability mass function:

$$\mathbb{P}(K_t = c) = \binom{N}{c}\left(\sum_{i=1}^{t}(1-p)^{i-1}p\right)^{c} \times \left(1 - \sum_{i=1}^{t}(1-p)^{i-1}p\right)^{N-c}, \quad (1)$$

where $p = \sum_{i=1}^{6} p_i^2$ is the matching probability for sender and receivers to stay in the same SCH number, p_i is the probability that SCH number i will be assigned. The mean number of vehicles that can receive BSMs after t timeslot is

$$\mathbb{E}[K_t] = N\sum_{i=1}^{t}(1-p)^{t-1}p = f(t,p). \quad (2)$$

Proof. Firstly, communication can only happen if the sender and receiver work in the same channel frequency. According to the assumption, the sender and receiver can randomly choose one of the six SCHs. The matching probability p for them to stay in the same SCH is given by:

$$\begin{aligned} p &= \mathbb{P}(\text{channel}_{\text{sender}} = \text{channel}_{\text{receiver}}) \\ &= \sum_{i=1}^{6}\mathbb{P}(\text{channel}_{\text{sender}} = i, \text{channel}_{\text{receiver}} = i) \\ &= \sum_{i=1}^{6}\mathbb{P}(\text{channel}_{\text{sender}} = i)\mathbb{P}(\text{channel}_{\text{receiver}} = i) = \sum_{i=1}^{6} p_i^2 \end{aligned} \quad (3)$$

Secondly, call T the number of CCHIs until a receiver receives the BSM message. The best scenario is $T = 1$, meaning that the receiver gets the message immediately. The worst scenario occurs when $T \longrightarrow \infty$, meaning this receiver always selects the channel differently from the sender. Indeed, T is a discrete random variable that could take any value from 1 to ∞. For instance, consider the case $T = 9$, which means that in 8 previous timeslots, this receiver did not receive the message. As mentioned above, at any given timeslot, the probability that the receiver gets the message is p, and the probability of not receiving the message is $1 - p$. Thus, the probability of $T = 9$ is given by

$$\mathbb{P}(T = 9) = (1 - p(1-p)^8 p. \quad (4)$$

Specifically, the random variable T follows the Geometric distribution with parameter p: $T \sim \text{Geometric}(p)$ and its probability mass function (PMF) is

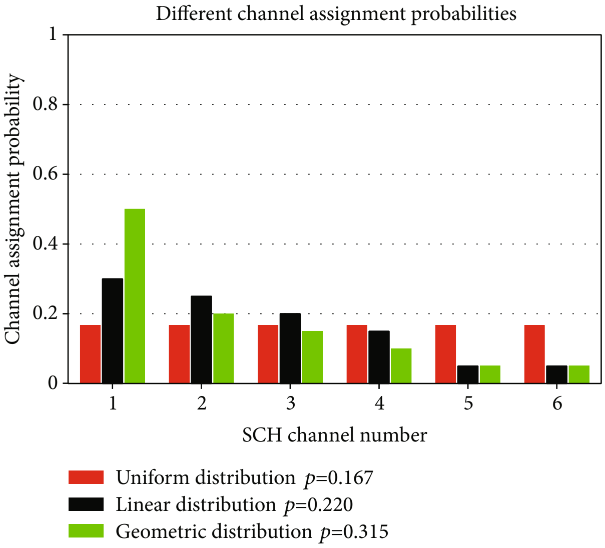

Figure 2: SCH assignment probability distributions.

$$\mathbb{P}(T = t) = (1-p)^{t-1}p. \quad (5)$$

So, the probability for the receiver to receive the message at a given timeslot $T = t$ is given by

$$\mathbb{P}(T \le t) = \sum_{i=1}^{t}\mathbb{P}(T = i) = \sum_{i=1}^{t}(1-p)^{i-1}p. \quad (6)$$

Finally, consider the number of receiver that got the message after t timeslots, K_t. Each receiver has $\sum_{i=1}^{t}(1-p)^{i-1}p$ chance to receive the message independently from other receiver, and K_t is fundamentally a Binomial random variable $K_t \sim \text{Binomial}(N, \sum_{i=1}^{t}(1-p)^{i-1}p) + .$ □

4.1. Application of Random Channel Surfing Model. One direct application of our analytical model for this random channel surfing scheme is to optimize the design of safety applications in vehicular networks. Indeed, safety applications are sensitive to time constrain. A natural way to improve the communication of safety applications when suffering jamming attacks is to adjust the matching probability. From (2), we can write

$$p = f^{-1}(t, \mathbb{E}[K_t]). \quad (7)$$

Thus, p can be computed as a function of t and $\mathbb{E}[K_t]$.

Figure 3 depicts the mean number of vehicles that can recover communication as regards time (computed from the number of CCHIs). As the analytical model showed, when p is uniformly distributed, we need almost 1 second for 80% of vehicles to recover. In case p is geometrically distributed ($p = 0.315$), only 0.5 seconds is required for 80% of vehicles to reestablish the communication. Thus, by adjusting the channel assignment probabilities, a safety application

```
Input: jamming alert signal
Output: new communication channel
begin
    ifa jamming attack is detectedthen
      whilecommunication is falsedo
          Choose a new channel for the appropriate application;
          Stop communication on the current channel;
          Start communication on the new selected channel;
```

Algorithm 1: ChannelSurfing() procedure.

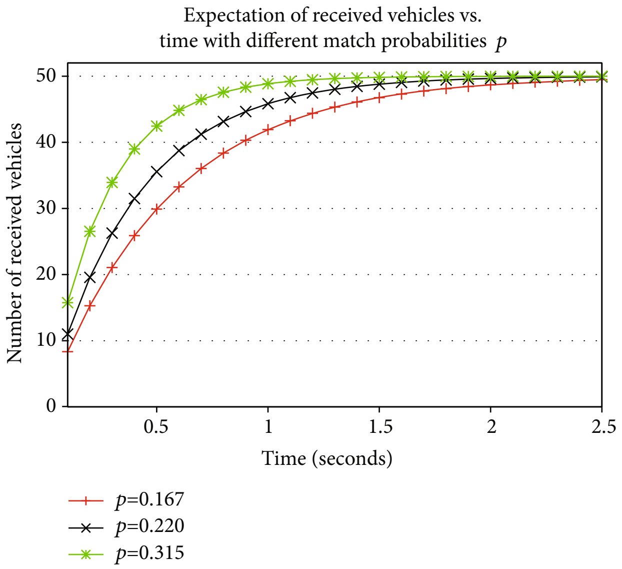

Figure 3: Comparison between theoretical results in case the choosing of SCHs is uniformly ($p = 0.167$), linearly ($p = 0.220$), and geometrically ($p = 0.315$) distributed.

can easily achieve its target of how many vehicles can be notified about safety information within a certain time slot.

5. Performance Evaluation

We evaluate our random channel surfing scheme by the number of vehicles receiving one information sent by a vehicle, called the sender, after a given time which is computed in a number of CCHIs. The analytical model and simulation allow us to study many scenarios with a different number of vehicles in the network. Due to lack of space, we present only the result for the scenario of $N + 1 = 51$ vehicles in a communication range. Among $N + 1$ vehicles, one vehicle plays the sender role. It retransmits its information in messages broadcast every CCHI. Every vehicle switches randomly to one of 6 service channels every CCHI when the jamming attack is detected. The numerical result obtained from the analytical model allows us to determine $\mathbb{E}[K_t]$, the expectation or the average number of vehicles that received the information after t CCHIs. To validate the analytical model, we run simulations in NS-3 [18] with the channelSurfing() procedure being implemented in all vehicles (nodes) and using the WAVE model that is specified for the vehicular environment. The IEEE standard 802.11p and the 1609 standard set are implemented in the simulations. All simulation results are computed at 95% confidence intervals. We evaluate our scheme with three different sets of probabilities parameters (p_1, p_2, p_3) given in Table 1 and consider two cases of mobility: constant mobility where vehicle pattern has been fixed and traffic mobility where a traffic simulator generates vehicle pattern. Parameters used in the simulation are listed in Table 2.

5.1. Constant Mobility. Firstly, we analyze our scheme by studying the average number of received vehicles after a given time. Analytical and simulation results are compared in all figures. Figures 4–6 show the increase in the average number of vehicles that receive the information; in another words, the expectation of random variable K_t as defined in the previous section. This figure also displays its corresponding standard deviation, which expresses how the real value differs from the average one. The simulation results validate the analytical results: they closely match the analytical results. At early CCHIs, the number of received vehicles increases dramatically and reaches 80%, i.e., nearly 40 vehicles at 9th CCHI in case $p = 0.167$ (5th and 7th in case $p = 0.220$ and $p = 0.315$, respectively). After that, the number increases insignificantly. Almost vehicles, up to 48 among 49 vehicles, received information after 25 CCHIs (2.5 seconds). Matching the time requirement of ITS safety application specified in [19], approximately 80% of vehicles using our scheme can satisfy the maximum latency of a given safety application of 1 second. Depending on the use cases of applications, this performance can probably be acceptable. Thus, it raises the question of which cases this performance is reasonable. Then, in these cases, the information should be more critical to some vehicles than others. For example, vehicles close to the origin of the information about an incident may be much more impacted than vehicles at a far distance. Therefore, it is potential to extend our channel surfing scheme with the idea of prioritizing the receivers. It means that the scheme should somehow manage groups of vehicles provided that higher prioritized vehicles must be acknowledged of the safety information early, while others can loosen the time constraint.

Secondly, our analytical model also allows us to figure out the likely number of received vehicles after a certain time. Figure 7 depicts the probability distribution of the obtained value of K_t at 10th CCHIs in the analytical model and so in simulation. The number of received vehicles

Table 2: Parameters used in simulations.

Parameters	Value
Number of vehicles	51
CCHI	50ms
Frequencies of channels	DSRC allocated spectrum [3]
Samples per point	100
Jamming attack event	At 2.0 seconds
SCH assignment probabilities	Uniform, linear and geometric Distribution
Message size	100 bytes
Number of retransmissions	100
Simulation time	12 seconds

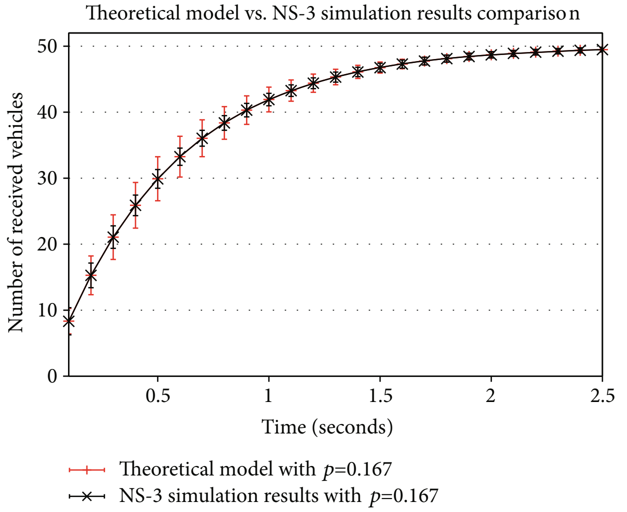

Figure 4: Comparison between simulation and theoretical results in case SCH is uniformly distributed.

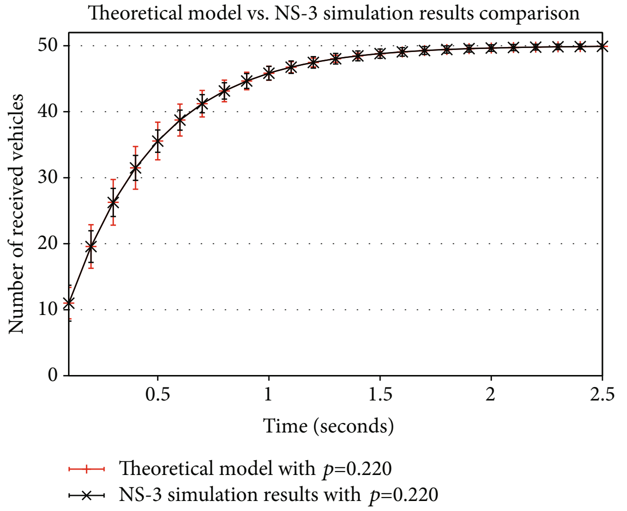

Figure 5: Comparison between simulation and theoretical results in case SCH is linearly distributed.

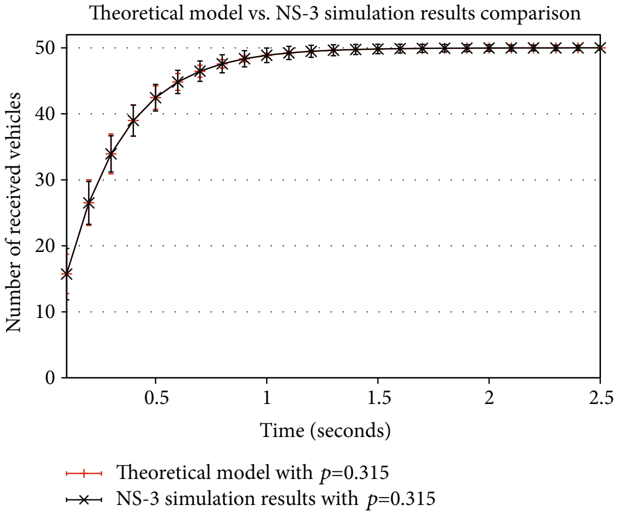

Figure 6: Comparison between simulation and theoretical results in case SCH is geometrically distributed.

approximately ranges from 34 to 46. It means that about 70% to 93% of vehicles are warned about the information after 1 second. The value has the highest probability at 41(83%) in theory and 43(88%) in simulation. The probability distribution of K_t after 5 CCHIs is illustrated in Figure 8. After 5 CCHIs, 19(39%) to 23(47%) vehicles receive the information. The results indicate the list of possible values of the number of received vehicles after a given time. It can be a reference to select the proposed scheme for suitable applications in terms of the freshness of exchanged information, expected informing scale of information, and network parameters such as the number of vehicles, density, available frequencies.

5.2. Traffic Mobility. To evaluate the impact of realistic traffic patterns, we generate vehicle locations from a traffic simulator in this scenario. This traffic simulator allows us to emulate driver behavior faithfully. On a highway, driver behavior is limited to accelerating, braking, and changing lanes. We assume that there is no off-ramp on the section of the highway. The desired speed is associated with each vehicle. It corresponds to the speed that the driver would reach if he was alone in his lane. If the driver is alone (the downstream vehicle is sufficiently far), he adapts his acceleration to reach his desired speed (free-flow regime). If he is not alone, he adapts his acceleration to the vehicles around him (car following regime). He can also change lanes if the conditions of another lane seem better. All these decisions are functions of traffic conditions (speed and distance) and random variables used to introduce a different behavior for each vehicle. This kind of simulation is called microsimulation [20], and the model we used, which has been tuned and validated with regard to real data collected on a highway, is presented in detail in [21, 22]. We simulated a road/highway with this traffic simulator with three lanes, and the simulation time was 60 minutes. The vehicle positions are then injected into NS-3 for simulation. In this

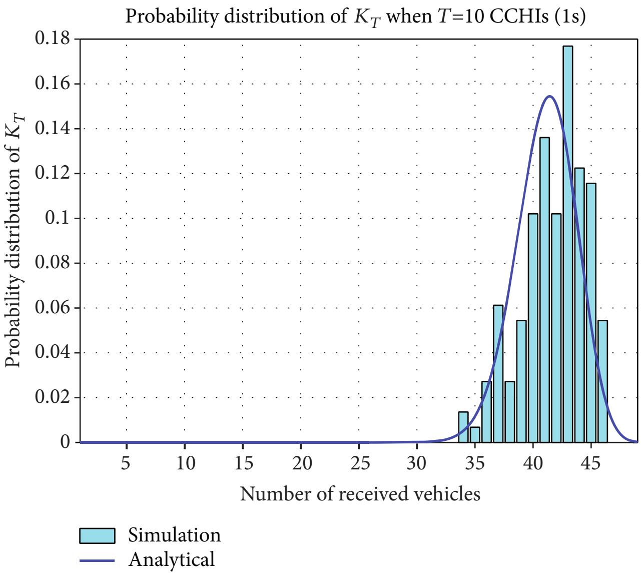

FIGURE 7: Probability distribution of the number of received vehicles after $t = 10$ CCHIs $(1\,\text{s.})$

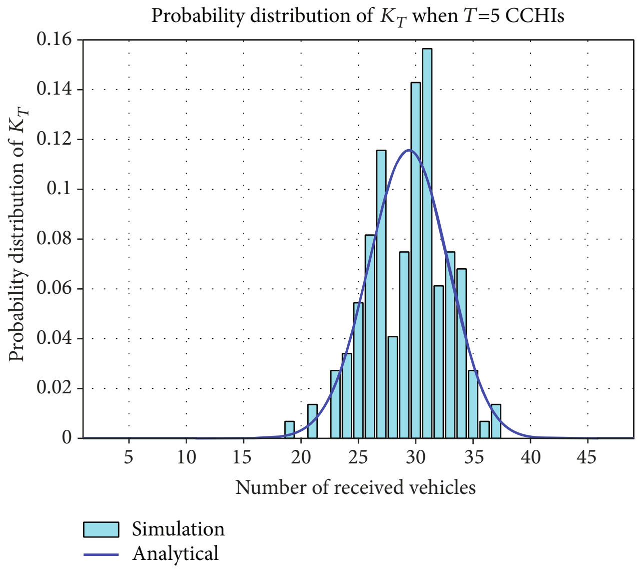

FIGURE 8: Probability distribution of the number of received vehicles after $t = 5$ CCHIs $(0.5\,\text{s})$

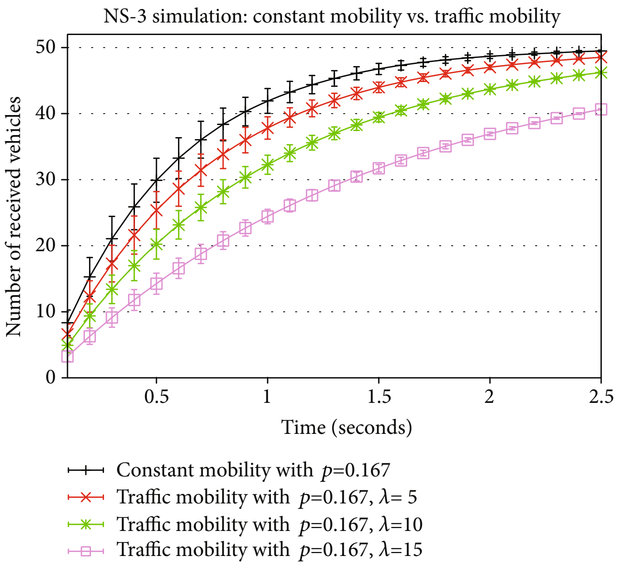

FIGURE 9: Comparison between constant mobility and different traffic mobility scenarios.

scenario, we also consider 50 receivers in the communication range of the sender as in the constant mobility case.

In Figure 9, we compare the simulation results performed with different traffic intensities (λ) in traffic mobility and constant mobility scenarios. For both scenarios (constant and traffic mobility), the channel assignment probability is the same and uniformly distributed $(p = 0.167)$. As shown, the traffic pattern has an important impact on the performance of our proposed scheme. When the traffic intensity is high ($\lambda = 5$, the mean distance between two consecutive vehicles is 5 meters), the average number of vehicles that can be acknowledged of the information is about 10% lower than the constant mobility case at $t = 1$ s. Moreover, we can observe a significant decrease (30% and 60%, respectively, at $t = 1$ s) in the performance of the traffic mobility scenario when considering low traffic intensities $(\lambda = 10, \lambda = 15)$. This may happen due to the high frame error rate in the traffic mobility scenario. The traffic simulator mimics the real traffic pattern where vehicles are likely to form clusters. Consequently, vehicles that belong to a far cluster could not receive any message even when they chose the same SCH as the sender.

6. Conclusion

This paper investigated the feasibility of a channel surfing approach against jamming attacks in vehicular networks, especially for safety applications with strict time constraints and a broadcast nature. We initialize and implement a random channel surfing scheme in vehicular networks. A simple, extensible probabilistic model is proposed to evaluate and study the favorable use case of our scheme. This model provides the key to designing safety applications sensitive to time constrain by adjusting SCH assignment probabilities. We validate the analytical model by NS-3 simulations. The simulation results have shown that a large number of vehicles can recover their communication within an acceptable time. The real traffic pattern has an essential effect on the performance of this random channel surfing scheme. We are currently working on an extension of this model that takes into account the frame error rate to model the real testbed scenarios accurately reported in this manuscript.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank the University of Sciences and Technologies of Vietnam, Vietnam Academy of Science and Technology (VAST), for funding this research in the scope of project USTH.ICT.01/21-22. The original idea about the random channel surfing scheme was partially published at the 2020 RIVF International Conference on Computing and Communication Technologies (RIVF) [17]. We would like to thank Professor Anthony BUSSON (LIP, ENS Lyon) and Professor Yacine Ghamri-Doudane (L3I, University of La Rochelle) for their enthusiastic discussions that allowed us to extend our previous work to this version.

References

[1] SAE International, *Dsrc Implementation Guide. A Guide of Users of sae j2735 Message Sets Over dsrc*, 2010.

[2] A. T. Giang, A. Lambert, A. Busson, and D. Gruyer, "Topology control in VANET and capacity estimation," in *2013 IEEE Vehicular Networking Conference*, pp. 135–142, Boston, MA, USA, December 2013.

[3] H. Nguyen-Minh, *Contribution to the Intelligent Transportation System: Security of Safety Applications in Vehicle Ad Hoc Networks*, PhD thesis, University of Avignon, 2016.

[4] S. Djuraev, J.-G. Choi, K.-S. Sohn, and S. Y. Nam, "Channel hopping scheme to mitigate jamming attacks in wireless LANS," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, no. 1, 2017.

[5] A. Benslimane and H. Nguyen-Minh, "Jamming attack model and detection method for beacons under multichannel operation in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 7, pp. 6475–6488, 2017.

[6] L. Wang and A. M. Wyglinski, "A combined approach for distinguishing different types of jamming attacks against wireless networks," in *Proceedings of 2011 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, pp. 809–814, Victoria, BC, Canada, August 2011.

[7] S. Chen, K. Zeng, and P. Mohapatra, "Jamming-resistant communication: channel surfing without negotiation," in *2010 IEEE International Conference on Communications*, pp. 1–6, Cape Town, South Africa, May 2010.

[8] X. Wenyuan, W. Trappe, and Y. Zhang, "Channel surfing: defending wireless sensor networks from interference," in *2007 6th International Symposium on Information Processing in Sensor Networks*, pp. 499–508, Cambridge, MA, USA, April 2007.

[9] M. Strasser, C. Pöpper, and S. Čapkun, "Efficient uncoordinated fhss anti-jamming communication," in *Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing - MobiHoc '09*, pp. 207–218, New Orlean, LA, USA, 2009.

[10] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, pp. 2526–2530, Anchorage, AK, USA, May 2007.

[11] H. Nguyen-Minh, A. Benslimane, and M. Radenkovic, *Social Delay Tolerant Protocol for Safety Services in Vehicular Networks*.

[12] H. N. Minh, A. M. Vegni, V. Loscrí, and A. Benslimane, "Connectivity management in an integrated heterogeneous social networks framework in vehicular environments," in *Proceedings of the Conference on Information Technology for Social Good*, pp. 25–30, New York, NY, USA, September 2021.

[13] N. Lyamin, D. Kleyko, Q. Delooz, and A. Vinel, "Ai-based malicious network traffic detection in VANETs," *IEEE Network*, vol. 32, no. 6, pp. 15–21, 2018.

[14] J. T. Chiang and H. Yih-Chun, "Cross-layer jamming detection and mitigation in wireless broadcast networks," *IEEE/ACM Transactions on Networking*, vol. 19, no. 1, pp. 286–298, 2011.

[15] L. Xiao, H. Dai, and P. Ning, "Jamming-resistant collaborative broadcast using uncoordinated frequency hopping," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 297–309, 2012.

[16] I. K. Azogu, M. T. Ferreira, J. A. Larcom, and H. Liu, "A new anti-jamming strategy for VANET metrics-directed security defense," in *2013 IEEE Globecom workshops (GC Wkshps)*, pp. 1344–1349, Atlanta, GA, USA, December 2013.

[17] N.-M. Huong, T. Hoang Tung, G. Anh Tuan, and H. Thanh Tung, "Channel surfing to mitigate against jamming attacks on safety applications in vehicular networks," in *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*, pp. 1–5, Ho Chi Minh City, Vietnam, October 2020.

[18] "Network simulator 3 - ns3," http://www.nsnam.org.

[19] ETSI TS 102 637-2 V1.1.1, "Intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service," 2010.

[20] S. Druitt, "Introduction to microsimulation," *Traffic Engineering & Control*, vol. 39, no. 9, 1998.

[21] K. I. Ahmed, *Modeling Drivers' Acceleration and Lane Changing Behavior*, PhD thesis, Massachusetts Institute of Technology, 1999.

[22] A. T. Giang and A. Busson, "Modeling CSMA/CA in VANET," in *ASMTA*, Springer, 2012.