Flexible Interval Intermittent Jamming Against Eavesdropping in WAVE Based Vehicular Networks

Hao Li[1] and Xiaoshuang Xing[2(✉)]

[1] The George Washington Univeristy, Washington, DC 20052, USA
haoli@gwu.edu
[2] Department of Computer Science and Engineering,
Changshu Institute of Technology, Changshu, Jiangsu, China
xing@cslg.edu.cn

Abstract. In this paper, we are focusing on the eavesdropping issue in Wireless Access in Vehicular Environments (WAVE) based vehicular networks. We proposed a flexible interval intermittent jamming (IJ) approach against the eavesdropper. This approach makes further improvement in reducing the energy cost of the existing IJ scheme while preventing eavesdropper sniffing acute information. We conducted a numerical analysis to explore and performed a simulation to compare the performance of our flexible interval IJ with the existing IJ scheme. The results show that our strategy is nearly saving 10% energy and guarantees the same security level as IJ can provide.

Keywords: WAVE · Friendly jamming · Vehicular networks · Physical layer security

1 Introduction

WAVE (Wireless Access in Vehicular Environments) based vehicular network has been considered as a promising way to improve the driving experience and safety with vehicular level information exchange playing the most critical role. Due to the broadcasting nature of wireless communication, the exchanged information, including vehicle identities, locations, speeds, and so on, are vulnerable to eavesdropping threats. To protect this private information from leakage, reliable eavesdropping defense mechanisms must be designed for WAVE based vehicular networks.

Friendly jamming is an effective approach to defense against eavesdropping [10,13,15,17,20]. Concurrent works are mainly focusing on continuous jamming (CJ) where the friendly jammer continuously sends jamming signals during the whole transmission of the legitimate transmitter. The eavesdropper is disabled while much energy is consumed by the jammer. Xing et al. argued in their recent work [24] that it is unnecessary to jam the whole transmission. A data packet can be protected from eavesdropping even if only part of the packet is jammed.

S. Chellappan et al. (Eds.): CSoNet 2020, LNCS 12575, pp. 48–58, 2020.
https://doi.org/10.1007/978-3-030-66046-8_5

Therefore, they proposed an intermittent jamming (IJ) scheme where the friendly jammer sends the jamming signal only in the jamming interval (JI) and keeps silent in the jamming-free interval (JF). This IJ scheme can keep the safety of the communication information while having a low energy cost. However, the length of JI and JF was fixed in their design (as shown in Fig. 1) without considering the length of the packet transmitted by the legitimate transmitter. The drawback of this fixed design comes from the following aspects. When the length of the transmitted packet is short, unnecessary energy will be consumed during a long JI. On the other hand, a combination of JI and JF will occur repeatedly for a long packet. The jammer should change between JI and JF frequently and energy will be wasted due to the switching loss. Therefore, the length of the transmitted packet should be considered when designing the length of JI and JF to achieve better energy efficiency.

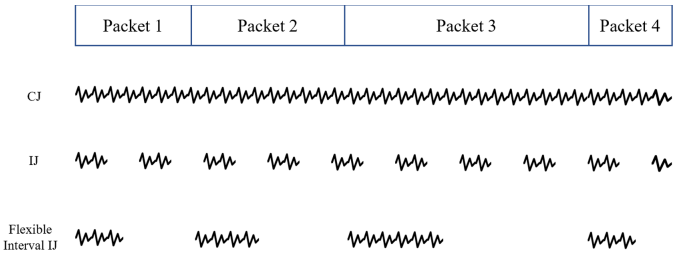


Fig. 1. Continuous jamming, intermittent jamming and flex interval intermittent jamming

In this paper, we aim at further reducing the energy cost of the IJ scheme by enabling the flexible length of JI and JF (as illustrated in Fig. 1). The following contributions are made in this paper.

- The physical packet structure in WAVE based vehicular networks is analyzed and the time length of the "Application Data", which contains the core information to be transmitted, is obtained.
- A flexible interval IJ scheme is designed where the length of JI varies with the length of the transmitted packet such that the friendly jammer disables the eavesdropper with less energy cost.
- The performance of our design is investigated through numerical study and an enhanced flexible interval IJ scheme is simulated to further reduce the energy cost.

The paper is organized as follows. The related works are discussed in Sect. 2. We illustrate the system model and formulate the problem in Sect. 3. The flexible interval IJ scheme is designed in Sect. 4. We display and analyze the numerical results in Sect. 5, and make a conclusion in Sect. 6.

2 Related Works

From the application layer to the link layer, the security threat has long been under concern [12,16,18,19]. The multimedia streaming scheme proposed in [3] aimed the security in the application layer. An authentication scheme [4,22,23] is frequently considered to ensure the confidentiality of communication in the transport layer security. The secured routing protocol proposed in [8] and [5] provide a safe transmission in the network layer. A new approach [9] is proposed to detect possible denial of service ahead of confirmation time in the link layer. A cooperative detection mechanism [7] was proposed and tested for reactive jamming.

According to the IEEE 802.11p standard, driving information is transmitted between vehicles and between vehicles and infrastructure. Sensitive information such as identity, location, speed, and direction is transmitted on the air. Due to the natural characteristics of wireless communication, despite numerous studies on a higher layer, eavesdropping attack in the physical layer is still a threat in securing sensitive information transmission. By eavesdropping this information, a malicious user may keep the track of driving information which could be used to possess and analyze driving route of legitimate user.

Friendly jamming is widely considered in defending eavesdropping attacks which is a threat to privacy and confidentiality. It can help to improve the security of vehicle localization [6], location verification [21] and secure communication [14]. In most existing friendly jamming schemes, friendly jammers keep sending signals. These schemes are known as CJ which are power consuming. In order to reduce power consumption, [2] proposes temporary jamming to provide information security when encryption is limited. A later research [24] advances an IJ scheme where the friendly jammer sends the jamming signal only in the jamming interval (JI) and keeps silent in the jamming-free interval (JF). The IJ scheme greatly decreases the power consumption while providing information security by ensuring the eavesdropper is always having a high package error rate (PER). However, this scheme fixes the length of JI and JF without considering the length of the packet transmitted by the legitimate transmitter. For a short physical packet, unnecessary energy will be consumed during a long JI. On the other hand, a combination of JI and JF will occur repeatedly for a long packet. Energy will be wasted during the frequent change between JI and JF. In order to further reduce the energy cost of the IJ scheme, this paper proposes to design flexible JI and JF depending on the length of the transmitted packet.

3 Problem Formulation

We are under a general vehicle communication scenario in vehicular network under WAVE protocol. As shown in Fig. 2, the legitimate user U_A is sending its driving information to U_B. Meanwhile, there is an eavesdropper U_E trying to overhear the packets being send. A cooperative jammer U_J located near U_A is sending jamming signals with power P_J to degrade the packets received by eavesdropper U_E.

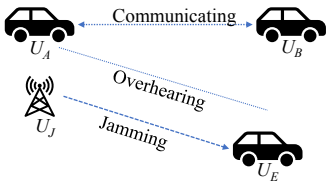


Fig. 2. General communication scenario

For a physical packet with time length T, U_J sends jamming signals in the JI with length T_J and keeps silence in the JF with length T_F. Here, $T_J \leq T$, $T_F \leq T$, and $T_J + T_F = T$. Let W_J indicate the energy cost of the cooperative jammer, B_J indicates the bit error rate (BER) of U_E during JI, B_F indicates the BER of U_E during JF, and B_E indicate U_E's average BER within T. It can be derived that

$$W_J = T_J \cdot P_J \tag{1}$$

$$B_E = \frac{T_J}{T} \cdot B_J + \frac{T_F}{T} \cdot B_F \tag{2}$$

The closed-form expressions of the BERs for different modulation schemes have been given in [11]. It can be found that BER is always an increasing function of the signal to noise plus interference ratio (SNIR), denoted by γ_b. During JF, no jamming signal is transmitted by the jammer. Therefore $\gamma_b^{JF} = \frac{E_b}{N_0}$ when calculating B_F with N_0 being the power spectral density of the noise. On the other hand, the receiving performance of U_E is degraged by the jammer during JI. Therefore, $\gamma_b^{JI} = \frac{E_b}{N_0+\phi_J}$ when calculating B_J. Here, $\phi_J = \frac{P_J|h_{JE}|^2}{B}$ is the received jamming signal power spectral density with $|h_{JE}|^2$ indicating the channel gain from U_J to U_E and B being the channel bandwidth. Obviously, $\gamma_b^{JI} \geq \gamma_b^{JF}$ and $B_J \geq B_F$. Therefore, B_E is an increasing function of T_J. According to (1), it can be found that W_J is also an increasing function of T_J. Recall that we want to disable the eavesdropping of U_E with low energy cost, we need to decide a proper T_J that can ensure a high enough BER at U_E while achieving a W_J as low as possible.

4 Design of Flexible Interval IJ Scheme

In order to obtain a high enough B_E while maintaining a low W_J, the jammer should transmit jamming signals only during the transmission time of the most significant part of the physical packet. Figure 3 shows the component of a physical packet. Intuitively, the "Application Data" contains the core information to be transmitted by U_A to U_B. Therefore, "Application Data" is the most significant part of the physical packet. If the jammer can identify the time duration within which the "Application Data" is transmitted and send jamming signals only during this time, U_E's eavesdropping will be disabled and U_J's energy cost

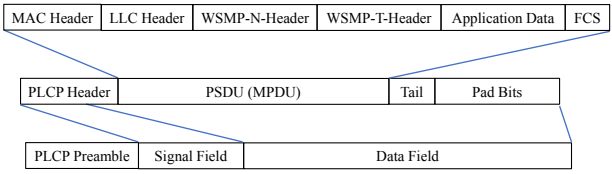


Fig. 3. Physical packet structure

will be reduced. Therefore, the main challenge to be solved in our design is to identify the time duration within which the "Application Data" is transmitted.

According to [1], a physical packet is consisting of a 16 µs PLCP preamble, a 4 µs Signal Field, and a variable-length Data Field. The Data Field is constructed by 16 bits of the PLCP Header, the WSMP-T-Header, the WSMP-N-Header, the LLC Header, the MAC Header, 32 bits FCS, 6 bits Tail, and variable-length Application Data. Moreover, n bits pad bits are also added in the Data Field to make the length of the Data Field divisible by N_{DBPS}. Therefore, n takes value between 0 to $N_{DBPS} - 1$. The value of N_{DBPS} depends on the modulation schemes and the coding rates. Typical values of N_{DBPS} in WAVE based vehicular networks are listed in Table 1.

Table 1. Values of N_{DBPS} for different modulation schemes and coding rates

Modulation	Coding Rate	N_{DBPS} (bits)	Modulation	Coding Rate	N_{DBPS} (bits)
BPSK	1/2	24	16-QAM	1/2	96
BPSK	3/4	36	16-QAM	3/4	144
QPSK	1/2	48	64-QAM	2/3	192
QPSK	3/4	72	64-QAM	3/4	216

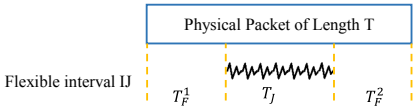


Fig. 4. Flexible interval IJ scheme for a physical packet of length T

When the Data Field is constructed, it will be divided into symbols. Each symbol consists of N_{DBPS} bits and is 4 µs long in time. According to [24], the minimum length of the WSMP-T-Header, the WSMP-N-Header, the LLC Header, and the MAC Header are 2 bytes, 2 bytes, 2 bytes, and 24 bytes respectively. There are a total of 30 bytes, which are 240 bits, in the physical packet before the Application Data in the Data Field. In time domain, the time length of these 240 bits will be $t_1 = \frac{240}{N_{DBPS}} \times 4\,\mu s$. As mentioned before, there are 6

bits tail bits, 32 bits FCS, and 0 to $N_{DBPS} - 1$ bits pad bits after the Application Data. These are total 38 to $37 + N_{DBPS}$ bits and the time length of these bits is denoted by t_2. t_2 takes value from $\frac{38}{N_{DBPS}} \times 4\,\mu s$ to $\frac{37+N_{DBPS}}{N_{DBPS}} \times 4\,\mu s$. Since the PLCP preamble, the Signal Field, and the headers are transmitted before the Application Data. The time length before transmitting the Application Data in the physical packet, which is denoted by T_F^1, can be calculated as $T_F^1 = 16\,\mu s + 4\,\mu s + t_1$. On the other hand, the FCS, the tail bits, and the pad bits are transmitted after the Application Data. Therefore, the time length after transmitting the Application Data in the physical packet, which is denoted by T_F^2, can be calculated as $T_F^2 = t_2$. Then, for a physical packet of length T, the flexible interval IJ scheme will be designed as shown in Fig. 4. According to the value of N_{DBPS} given Table 1, the value of T_F^1, T_F^2 can be easily obtained. For example, $T_F^1 = 60\,\mu s$ and $6.3\,\mu s \leq T_F^2 \leq 10.17\,\mu s$ when the physical packet is BPSK modulated with coding rate being $\frac{1}{2}$. Then, we have $T_J = T - T_F = T - T_F^1 - T_F^2$. Theoretically, the best anti-eavesdropping performance can be achieved when T_F^2 takes the lower bound value, which is $T_F^2 = 6.3\,\mu s$ in the aforementioned example. While most energy can be saved when T_F^2 takes the upper bound value, that is $T_F^2 = 10.17\,\mu s$ in the example.

5 Numerical Results

In this section, we validate the performance of our design for securing the transmission of the physical packets with varying lengths. The length of the physical packet is indicated by the length of the PSDU part shown in Fig. 3. The performance of the proposed flexible interval IJ scheme is compared with the IJ scheme proposed in [24]. Besides, the performance of our design when T_F^2 takes the lower bound value (referred to as FIJ-shortest TF in the following) and the upper bound value (referred to as FIJ-longest TF in the following) is also investigated. The simulation is performed in MATLAB 2018b and using the WLAN toolbox. We use function 'wlanNonHTConfig' to generate non-HT packets transmitted in WAVE based vehicular network. The channel bandwidth is set to 10 MHz and we are using the default sampling rate for 10 MHz. We set the delay profile as 'Urban NLOS' because most of the V2V communication happens in an urban area and do not have a line of sight. BPSK modulation is used and the coding rate r is set to be $\frac{1}{2}$ and $\frac{3}{4}$.

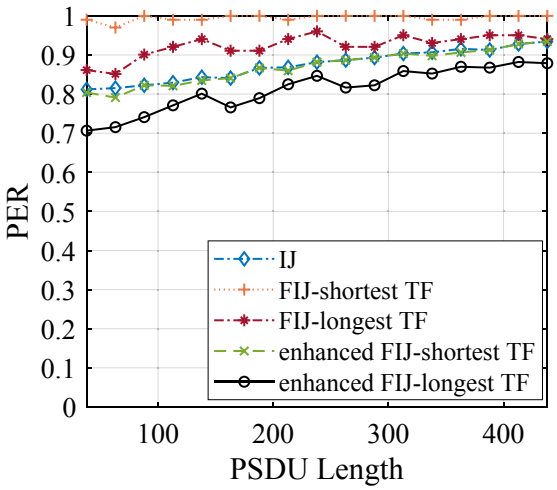
The performance comparison is conducted from two aspects. To validate the anti-eavesdropping performance of our design, the packet error rate (PER) of U_E, which is the ratio of the number of physical packets not successfully decoded by U_E to the number of the physical packets sent by the transmitter U_A, is adopted. The function 'V2VPERSimulator' from MATLAB is utilized to simulate the PER. The energy cost for sending jamming signals referred to as the jamming energy cost in the following is used to investigate the energy efficiency of our design.

According to [24], the optimal transmission power of U_J is set to be $P_J = 760\,\text{mW}$ for BPSK modulation with coding rate r being $\frac{1}{2}$. The corresponding T_J and T_F are 47.12 us, and 28.88 us respectively in the IJ scheme. While for BPSK modulation with $r = \frac{3}{4}$, the IJ scheme is set as $P_J = 760\,\text{mW}$, $T_J = 37.2\,\text{us}$, and $T_F = 22.8\,\text{us}$. The setting of the IJ scheme is fixed regardless of the length of the transmitted physical packet. On the other hand, the length of T_J and $T_F = T_F^1 + T_F^2$ in our design are flexible which can be calculated as given in Sect. 4. U_J's transmission power in our flexible interval IJ scheme is set to be the same as that in the IJ scheme, which is $P_J = 760\,\text{mW}$.

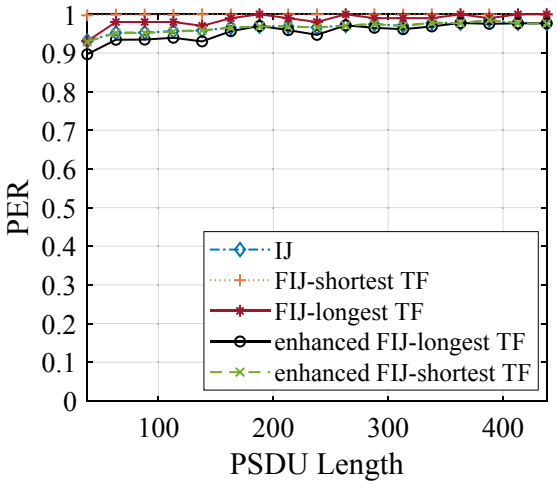
We change the length of the PSDU from 38 Octets to 438 Octets and the PER of U_E is shown in Fig. 5. It can be found that U_E's PER increases with the increasing of the PSDU length for schemes other than FIJ-shortest TF. With the increase of the PSDU length, more information bits are enclosed in a physical packet. The probability of information bits within a physical packet being incorrectly decoded will increase resulting in an increased PER. For the FIJ-shortest TF scheme, U_E's SNR keeps low since U_J sends jamming signals during the whole transmission time of the "Application Data". Therefore, U_E's PER is always close to 100% regardless of the PSDU length. Small performance fluctuations occur for the FIJ-longest TF scheme. In the FIJ-longest TF scheme, the length of TF_2 is fixed to be $\frac{37+N_{DBPS}}{N_{DBPS}} \times 4\,\mu\text{s}$ by assuming that there are always $N_{DBPS} - 1$ pad bits in the physical packet. However, the length of the pad bits varies with the PSDU length leading to insufficient jamming of the "Application Data" for some PSDU length and thus performance fluctuations on U_E's PER. Moreover, one can see that a higher coding rate r causes a higher PER. A higher r implies more information bits and less redundant bits are enclosed in a physical packet, which means that more information is transmitted in a physical packet and the transmission efficiency is improved. However, the redundant bits play an important role in error correction, and less redundant bits can decrease U_E's error correction capability and lead to a higher PER.

The results regarding the jamming energy cost are given in Fig. 6. We found that our flexible interval IJ scheme consumes less energy when the physical packet is short (for example when the PSDU is 100 bytes long). While for long physical packets, the IJ scheme performs better in terms of energy cost. This is because the length of T_J and T_F is fixed in IJ. In other words, $\frac{T_J}{T}$ is fixed for any PSDU length (i,e, any physical packet length). In the flexible interval IJ scheme, the length of $T_F = T_F^1 + T_F^2$ is fixed, while the length of $T_J = T - T_F$ increases with the length of the physical packet. Therefore, $\frac{T_J}{T}$ increases with the increasing of the PSDU length leading to more jamming energy cost compared with the IJ scheme propose in [24].

In order to further improve the jamming energy cost of the flexible interval IJ scheme. We conduct enhanced-FIJ in our simulation study. The enhanced-FIJ is designed by taking the same TF_1 and TF_2 as that of the FIJ scheme. While for the "Application Data" transmitted within T_J, the IJ scheme proposed in [24] is applied. That is, T_J is further divided into sub-jamming intervals and sub-jamming-free intervals according to the IJ scheme proposed in [24]. The



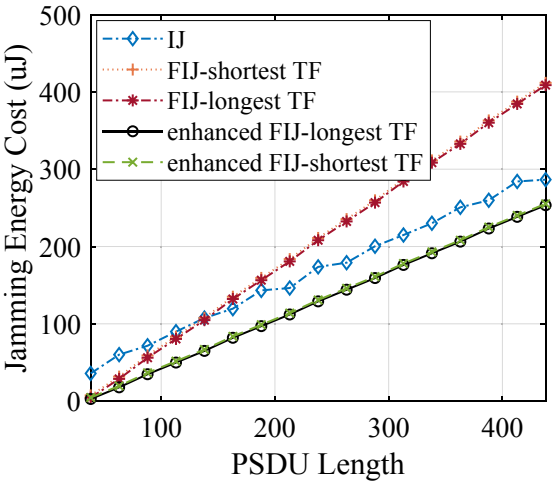
(a) BPSK, $r = \frac{1}{2}$



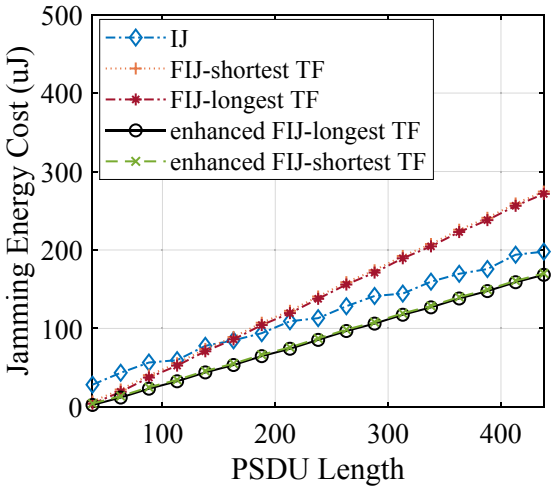
(b) BPSK, $r = \frac{3}{4}$

Fig. 5. Packet Error Rate comparison with different PSDU length

performance of enhanced FIJ-shortest TF and enhanced FIJ-longest TF are shown by green dashed lines and black solid lines in Fig. 5 and Fig. 6. We found that enhanced FIJ-shortest TF can achieve PER performance almost the same as the IJ scheme while saving 10% energy.



(a) BPSK, $r = \frac{1}{2}$



(b) BPSK, $r = \frac{3}{4}$

Fig. 6. Jamming energy cost comparison with different PSDU length

6 Conclusion

In conclusion, our contribution is providing a method to save more energy when dealing with eavesdropping attacks in WAVE based vehicular networks. The proposed flexible interval IJ approach can further save more energy than the existing IJ approach. Simulation results confirm our design is capable of defense against the eavesdropping attacks while enhancing the performance in energy saving.

References

1. IEEE standard for information technology-telecommunications and information exchange between systems local and metropolitan area networks-specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007), pp. 1–2793 (2012)
2. Allouche, Y., Arkin, E.M., Cassuto, Y., Efrat, A., Grebla, G., Mitchell, J.S., Sankararaman, S., Segal, M.: Secure communication through jammers jointly optimized in geography and time. Perv. Mob. Comput. **41**, 83–105 (2017)
3. Challita, U., Ferdowsi, A., Chen, M., Saad, W.: Machine learning for wireless connectivity and security of cellular-connected UAVs. IEEE Wirel. Commun. **26**(1), 28–35 (2019)
4. Cui, J., Zhang, J., Zhong, H., Xu, Y.: SPACF: a secure privacy-preserving authentication scheme for VANET with cuckoo filter. IEEE Trans. Veh. Technol. **66**(11), 10283–10295 (2017)
5. DasGupta, S., Chaki, R., Choudhury, S.: SBRPV: Security based routing protocol for vehicular ad hoc networks. In: 2019 4th International Conference on Computer Science and Engineering (UBMK), pp. 745–750. IEEE (2019)
6. Deka, B., Gerdes, R.M., Li, M., Heaslip, K.: Friendly jamming for secure localization in vehicular transportation. In: Tian, J., Jing, J., Srivatsa, M. (eds.) SecureComm 2014. LNICST, vol. 152, pp. 212–221. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-23829-6_16
7. Del-Valle-Soto, C., Mex-Perera, C., Aldaya, I., Lezama, F., Nolazco-Flores, J.A., Monroy, R.: New detection paradigms to improve wireless sensor network performance under jamming attacks. Sensors **19**(11), 2489 (2019)
8. Feng, L., Xiu-Ping, Y., Jie, W.: Security transmission routing protocol for MIMO-VANET. In: Proceedings of 2014 International Conference on Cloud Computing and Internet of Things, pp. 152–156. IEEE (2014)
9. Fotohi, R., Ebazadeh, Y., Geshlag, M.S.: A new approach for improvement security against DOS attacks in vehicular ad-hoc network (2020). arXiv preprint: arXiv:2002.10333
10. Gao, Q., Huo, Y., Ma, L., Xing, X., Cheng, X., Jing, T., Liu, H.: Joint design of jammer selection and beamforming for securing MIMO cooperative cognitive radio networks. IET Commun. **11**(8), 1264–1274 (2017)
11. Goldsmith, A.: Wireless Communications. Stanford University, California (2004)
12. Hasrouny, H., Samhat, A.E., Bassil, C., Laouiti, A.: VANET security challenges and solutions: a survey. Veh. Commun. **7**, 7–20 (2017)
13. Huo, Y., Fan, X., Ma, L., Cheng, X., Tian, Z., Chen, D.: Secure communications in tiered 5G wireless networks with cooperative jamming. IEEE Trans. Wirel. Commun. **18**(6), 3265–3280 (2019)
14. Lee, H., Eom, S., Park, J., Lee, I.: UAV-aided secure communications with cooperative jamming. IEEE Trans. Veh. Technol. **67**(10), 9385–9392 (2018)
15. Li, Y., Zhang, R., Zhang, J., Gao, S., Yang, L.: Cooperative jamming for secure UAV communications with partial eavesdropper information. IEEE Access **7**, 94593–94603 (2019)
16. Mejri, M.N., Ben-Othman, J., Hamdi, M.: Survey on VANET security challenges and possible cryptographic solutions. Veh. Commun. **1**(2), 53–66 (2014)
17. Mobini, Z., Mohammadi, M., Tellambura, C.: Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications. IEEE Trans. Inform. Forens. Secur. **14**(3), 621–634 (2018)

18. Mokhtar, B., Azab, M.: Survey on security issues in vehicular ad hoc networks. Alex. Eng. J. **54**(4), 1115–1126 (2015)
19. Raya, M., Hubaux, J.P.: Securing vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)
20. Siyari, P., Krunz, M., Nguyen, D.N.: Distributed power control in single-stream MIMO wiretap interference networks with full-duplex jamming receivers. IEEE Trans. Signal Process. **67**(3), 594–608 (2018)
21. Tithi, T., Deka, B., Gerdes, R.M., Winstead, C., Li, M., Heaslip, K.: Analysis of friendly jamming for secure location verification of vehicles for intelligent highways. IEEE Trans. Veh. Technol. **67**(8), 7437–7449 (2018)
22. Wang, X., Li, S., Zhao, S., Xia, Z.: A VANET privacy protection scheme based on fair blind signature and secret sharing algorithm. Automatika **58**(3), 287–294 (2017)
23. Wei, Z., Li, J., Wang, X., Gao, C.Z.: A lightweight privacy-preserving protocol for VANETS based on secure outsourcing computing. IEEE Access **7**, 62785–62793 (2019)
24. Xing, X., Sun, G., Qian, J.: Intermittent Jamming for Eavesdropping Defence in WAVE based Vehicular Networks, pp. 1–10 (2019)