Peer-to-Peer Networking and Applications (2023) 16:488–498
https://doi.org/10.1007/s12083-022-01414-4

Dynamic shielding to secure multi-hop communications in vehicular platoons

Yiran Yang[1] · Xiqing Liu[1] · Zhifeng Wang[1] · Yiliang Liu[2]

Received: 29 April 2022 / Accepted: 10 November 2022 / Published online: 23 November 2022

Abstract
Vehicular platoons are among the most advanced driving assistance systems that may generate considerable fuel savings and increase traffic efficiency. However, communication between vehicles in a platoon is always vulnerable to eavesdropping due to the broadcast nature of wireless channels. To address this issue, we investigate security issues from the physical layer perspective for multi-hop vehicular platooning. The dynamic shielding secured transmission scheme is proposed to guarantee the confidential transmission of private information. Specifically, the neighboring vehicles can alternately act as friendly shielders, which transmit jamming signals to interfere with the eavesdroppers without knowing the channel state information, and thus the secrecy capacity would increase. The mathematical derivation of secrecy capacity is obtained for performance analysis. Meanwhile, the numerical results verify the properties, efficiency, and adaptability of the proposed scheme.

Keywords Vehicular platoon · Physical layer security · Confidential communication · Secrecy capacity

1 Introduction

As 5G commercial applications become popular, autonomous driving, a key technology for ensuring road safety and alleviating traffic congestion, has received extensive attention and rapid development. Platooning is an important traffic strategy based on autonomous driving technology that can achieve improved traffic efficiency and reduced fuel consumption [1, 2]. Vehicular platoons operate a group of vehicles in a closely linked pattern, where vehicles communicate through a the multi-hop mechanism [3]. Driving status information and private information (e.g., location, speed, acceleration, and identity) are transmitted in real time between vehicles in the same platoon. Since these messages are crucial to driving safety and user privacy, they should be exchanged with confidentiality and be deciphered only by the vehicles within the platoon to ensure information security. However, vehicle-to-vehicle (V2V) communications are particularly vulnerable to eavesdropping due to the broadcast nature of wireless channels [4, 5].

Addressing security issues of vehicular platoons involves many challenges. First, in driving scenarios, a complex and changing surrounding environment can have an impact on the communication performance of the platoon. Various obstacles and multipath fading can make the wireless channel unstable, leading to difficulties for channel estimation. Second, data in vehicular platoon communication are time-sensitive; hence, vehicles should communicate using algorithms with high processing capability and low complexity. Third, since vehicles join or leave at any time during the driving of the platoon, the transmission scheme should be able to adapt to this dynamic system.

Many researchers focus on detecting and mitigating attacks at the network and application layers to address communication security issues [6–8]. Additionally, recent studies on physical layer security, which emerges as a promising means of protecting wireless communications against eavesdropping attacks, have received considerable attention.

✉ Xiqing Liu
liuxiqing@bupt.edu.cn

Yiran Yang
yiranyang@bupt.edu.cn

Zhifeng Wang
oscar_wang@bupt.edu.cn

Yiliang Liu
liuyiliang@xjtu.edu.cn

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China

[2] School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an, China

Existing studies on physical layer security can be divided into two types: key-based and keyless technologies.

Shannon [9] first introduced the theory of secure communication and the classic model of cryptosystems. It was pointed out that, when the key entropy is not less than the information entropy, the perfect secrecy of the one-time pad can be achieved. In key-based technologies, the characteristics of short-term reciprocity, space-time uniqueness, fast time-varying and unpredictability of wireless channels are used as random sources to generate the shared secret key. It is then used to encrypt the information through dynamic coordinate interleaving or constellation phase rotation.

Physical layer security achieves confidential communications without using keys, which was proposed by Wyner [10]. He introduced a discrete memoryless eavesdropping channel comprising the source, destination, and eavesdropper. He also proved that, provided the capacity of the legitimate link between the source and the target is higher than that of the eavesdropping link between the source and the eavesdropper, absolutely secure communication can be achieved through coding.

The condition of secure transmission in a Gaussian eavesdropping channel was further investigated in [11], and the authors proposed the concept of secrecy capacity, that is, the difference between the capacity of the legitimate link and the capacity of the eavesdropping link. Therefore, improving the secrecy capacity is one goal of designing a physical layer security scheme [12]. In keyless technologies, which mainly include beamforming and artificial noise (AN) technologies, the widely considered idea is to generate information signals that can only be decoded by a legitimate receiver or to generate jamming signals that can cause severe interference to the eavesdropper. However, most typical beamforming and AN technologies rely on accurate knowledge of channel state information (CSI) of the legitimate or the eavesdropping link. In fact, the transmitter has the difficulty in obtaining the perfect CSI of a wireless link, especially in a dynamic environment such as a vehicular platoon. Furthermore, the eavesdropper definitely not feeds back the CSI knowledge of the eavesdropping link to the transmitter.

In this work, we propose a keyless physical layer security scheme, called the dynamic shielding secured transmission (DSST) scheme; here, adjacent vehicles alternately function as legitimate transmitters and friendly shielders to ensure that critical messages can be transmitted confidentially within the platoon with a multi-hop mechanism. In this scheme, the jamming signal is not sent together with the information signal at the transmitter, but is sent by the legitimate receiver or the vehicle outside the communication range of the legitimate receiver. Hence, the jamming signal can be generated without resorting to the CSI of the eavesdropping and legitimate links and will not cause severe interference to the legitimate receiver. Additionally, a detailed derivation is conducted for the ergodic capacity of the legitimate and the eavesdropping links. On this basis, the secrecy capacity is carried out to evaluate the performance of the proposed scheme wherein its effectiveness is verified through numerical analysis.

The remainder of this paper is organized as follows. Section 2 presents the review of existing relevant literature on physical layer security issues is presented. In Sect. 3, we introduce a toy example of the DSST scheme for a multi-hop vehicular platoon and explain its basic principle. In Sect. 4, we provide the mathematical derivation of the ergodic capacity and the secrecy capacity for the confidential communication model of vehicular platoon. We also present the numerical results and conduct a detailed analysis in Sect. 5. Finally, the conclusion is made at the end of this paper.

2 Related work

2.1 Secret key technology

The authors in [13] proposed a physical layer key generation scheme based on channel estimation using zero-forcing (ZF) or minimum mean square error (MMSE) criteria. The scheme determines the optimal number of antennas for relays and legal nodes through algorithms and then selects the most suitable antenna for key generation to achieve a higher secret key rate than that of previous work. In [14], eavesdropping and message modification issues were considered in platoon-based V2V communications, and a security scheme was proposed where the vehicles generate a shared secret key according to the fading channel randomness. By recursively optimizing the quantization intervals of the channel quality indicator, the scheme can maximize the key agreement probability within a platoon, while the probability that eavesdroppers generate the same key is much lower. The key generation algorithms for multi-carrier systems were investigated in [15], where both the magnitudes of orthogonal frequency division multiplexing subcarriers and the indices/positions of subcarriers that correspond to the highest gains are used to generate secret bits. The proposed algorithms can provide extra dimensions for key generation and thereby enhance the overall key rate. The authors in [16] proposed a key-based algorithm that obscures information from eavesdroppers by mapping it to rotated reference signals. They further designed a key-based physical layer security protocol to connect the algorithm with modern cellular implementations.

2.2 Keyless technology

The authors in [17] proposed a secure precoding algorithm based on the concept of constructive interference (CI), which

takes advantage of the constructive nature of multiuser interference to improve the signal power at the legitimate receiver and utilizes its destructive effects to degrade the performance of the eavesdropper. The algorithm can strike a better tradeoff between energy overhead and security. However, additional transmit power is required to prevent eavesdropping when the CSI of the eavesdropper is unavailable. A strategy of relay selection and cooperative jammer beamforming was proposed in [18], wherein one node is selected from the intermediate nodes as the relay, while the rest of the nodes as friendly jammers to maximize the secrecy rate. The scheme was proved to have a better performance than the conventional schemes under the same power constraint. For the MIMO-non-orthogonal multiple-access-based cognitive radio network, a transmit-zero-forcing beamforming technique with signal alignment was proposed in [19] for communication security when perfect CSI can be obtained. Additionally, for practical scenarios with partial CSI knowledge, the authors proposed an eigen beamforming technique, which can mitigate the impact of imperfect CSI and ensure that users at the center of the cell maintain a positive secrecy capacity. An AN-based secure transmission scheme for a multi-input single-output eavesdropping system was also proposed, wherein an optimal power allocation and an optimal transmission rate algorithm based on cyclic iteration were used to maximize the system security [20]. The authors in [21] investigated the AN scheme for coordinated multipoint transmission in frequency division duplex multi-cell systems with imperfect CSI. The secrecy performance analysis that is mathematically rigorous was conducted in detail, and an algorithm with low complexity was introduced to optimize the allocation of CSI feedback bits for the channels of the target signal link and inter-cell interference links.

3 System model

Some assumptions should be given initially before introducing the system model. The power constraint for each vehicle member in a platoon should be seriously considered to avoid severe interference to the surrounding traffic.

Moreover, the communication distance for each vehicle is limited locally within its neighboring vehicles. Under this premise, for a platoon with its length to be N, there will be $N-1$ hop links to complete after transmission from the head vehicle to the tail vehicle. The store-and-forward mode is used for the relay transceiver; that is, the messages containing driving status and commands are generated at the head vehicle and forwarded to the following vehicle all the way toward the tail vehicle [22].

Fig. 1 presents the system model of the proposed scheme, where the private messages are exchanged within the platoon according to the multi-hop mechanism, with each vehicle broadcasting the information to its neighboring vehicles. An eavesdropping vehicle, denoted by V_e, appears next to the $(n-1)$th hop. Here V_{n-1}, V_n and V_{n+1} refer to the $(n-1)$th vehicle, the nth vehicle and the $(n+1)$th vehicle, respectively. For the $(n-1)$th hop, V_{n-1} broadcasts the information signal to the surroundings, and V_n, serving as both the legitimate receiver and friendly shielder, broadcasts the jamming signal to protect the information from eavesdropping. Under this case, V_e will receive the signal from V_{n-1} and V_n

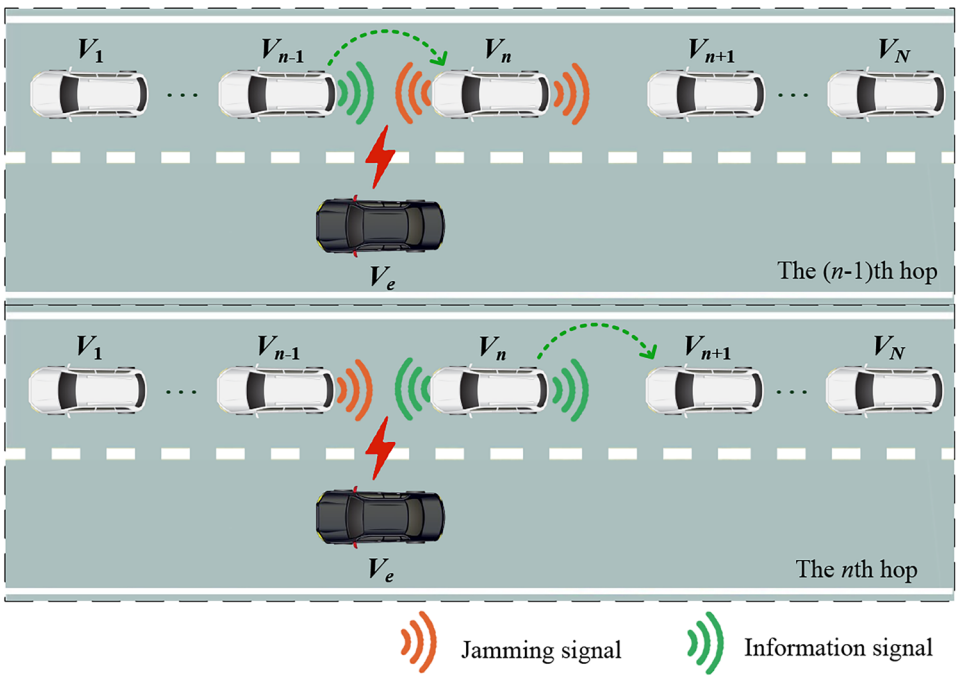

Fig. 1 DSST scheme in the multi-hop vehicular platoon. Assume that the eavesdropper V_e is attempting to eavesdrop on the private messages from the $(n-1)$th and the nth hops, where $n\,(n=1,\cdots,N-1)$ refers to the index of the nth vehicle

simultaneously and will be unable to decode the information signal due to the existence of the jamming signal. Then, for the nth hop, V_n will become a relay to extend the communication link to V_{n+1}, with V_{n-1} serving as a friendly shielder to broadcast the jamming signal. In this hop, V_{n+1} is out of the communication range of V_{n-1}, and thus it can avoid interference from the shielding action taken by V_{n-1}. For convenience, the symbol definitions used in this paper are given in Table 1.

4 Performance derivation

This section presents the mathematical derivations associated with the ergodic capacity of the legitimate link, ergodic capacity of the eavesdropping link, and secrecy capacity, respectively, to illustrate the proposed scheme in detail. Not all of the $N-1$ hop links are taken into our design; instead, we only address the vulnerable links allocated within an eavesdropper's range. For illustration purposes, the communication process of the $(n-1)$th hop and the nth hop is considered without loss of generality.

4.1 Ergodic capacity of the legitimate link

In the system model presented in Fig. 1, let the transmit power of V_{n-1} and V_n, yielding the information signal and jamming signal, be $\mathcal{P}_{n-1}$ and $\mathcal{P}'_n$, respectively. Specifically, the signal to interference plus noise ratio (SINR) at the side of V_n can be calculated as

$$\gamma_{n-1} = \frac{\mathcal{P}_{n-1}|h_{n-1}|^2}{\xi\mathcal{P}'_n|h_\xi|^2 + N_0}, \tag{1}$$

where the complex gain of the $(n-1)$th hop link, between V_{n-1} and V_n, is defined as $h_{n-1} \triangleq |h_{n-1}|e^{j\phi_{n-1}}$ $(n = 2, \cdots, N)$, where $|h_{n-1}|$ follows the Rayleigh distribution and ϕ_{n-1} follows the uniform distribution in $[-\pi, \pi]$. Each vehicle is equipped with a full-duplex transceiver. Self-interference is defined as $\mathcal{I}_n$, and ξ is used to denote the self-interference factor, defined as $\xi \triangleq \mathcal{I}_n/\mathcal{P}'_n$ [23]. The channel gain of the self-to-self loop for a full-duplex transceiver is represented by h_ξ.

Consequently, the transmit power involved in each hop, denoted by P_n, should be taken comprehensively to utilize the power generated both by V_{n-1} and by V_n. In addition, the transmit power regarding each hop is assumed as a constant; that is, $P_1 = \cdots = P_n = \cdots = P_{N-1} = P$. Take the constraint here; we have

$$\begin{cases} \mathcal{P}_{n-1} + \mathcal{P}'_n = P; \\ \alpha \triangleq \mathcal{P}_{n-1}/\mathcal{P}'_n,\ 0 \le \alpha \le 1, \end{cases} \tag{2}$$

where α is the power ratio in terms of $\mathcal{P}_{n-1}$ and $\mathcal{P}'_n$. The ergodic capacity for the $(n-1)$th hop can be calculated using

Table 1 Definitions of the symbols used in this paper

Symbols	Definitions	Remarks
N	Length of the platoon	
V_n	The nth vehicle in the platoon	$n = 1, \cdots, N$
V_e	Eavesdropper	
ξ	Self-interference factor for a full-duplex transceiver	$\xi \in (0, 1)$
σ_n^2	Variation of h_n; that is, $\sigma_n^2 = \mathbb{E}(h_n h_n^*)$	$\sigma_1^2 = \cdots = \sigma_n^2 = \sigma_{N-1}^2 \triangleq \sigma^2$
σ_ξ^2	Variation of h_ξ; that is, $\sigma_\xi^2 \triangleq \mathbb{E}(h_\xi h_\xi^*)$	
σ'^2_n	Variation of $\hbar_n$; that is, $\sigma'^2_n \triangleq \mathbb{E}(\hbar_n \hbar_n^*)$	
N_0	Power of the Gaussian noise	
P_n	Constraint of the transmit power in the nth hop	$P_1 = \cdots P_n = P_{N-1} = P$
$\mathcal{P}'_{n-1}$	Power of the jamming signal transmitted by V_{n-1} in the nth hop	
$\mathcal{P}'_{n-1}$	Transmit power of V_{n-1} in the $(n-1)$th hop	$\mathcal{P}_{n-1} + \mathcal{P}'_n = P_n$
$\mathcal{P}'_n$	Power of the jamming signal transmitted by V_n in the $(n-1)$th hop	
$\mathcal{P}_n$	Transmit power of V_n in the nth hop	$\mathcal{P}_n + \mathcal{P}'_{n-1} = P_n$
h_n	Channel gain of the legitimate link in the nth hop	From V_n to V_{n+1}
h_ξ	Channel gain of the self-to-self loop for a full-duplex transceiver	
$\hbar_n$	Channel gain of the eavesdropping link in the nth hop	
C_n	Ergodic capacity of the legitimate link in the nth hop	$n = 1, \cdots, N-1$
C'_n	Ergodic capacity of the eavesdropping link in the nth hop	$n = 1, \cdots, N-1$
$\mathcal{C}_n$	Secrecy capacity of the nth hop	$\mathcal{C}_n \triangleq \left[C_n - C'_n\right]^+$
$\mathrm{Ei}(t)$	Exponential integral function	$\mathrm{Ei}(t) = \int_t^\infty e^{-x}x^{-1}\,\mathrm{d}x$

$$
\begin{aligned}
C_{n-1} &= \mathbb{E}\left[\log_2\left(1+\gamma_{n-1}\right)\right] \\
&= \iint \log_2\left(1+\gamma_{n-1}\right) p(|h_{n-1}|) p(|h_\xi|)\,\mathrm{d}|h_{n-1}|\mathrm{d}|h_\xi| \\
&= \iint \log_2\left(1+\frac{\mathcal{P}_{n-1}|h_{n-1}|^2}{\xi\mathcal{P}'_n|h_\xi|^2+N_0}\right)\frac{|h_{n-1}|}{\sigma^2}e^{-\frac{|h_{n-1}|^2}{2\sigma^2}}\times \\
&\quad \frac{|h_\xi|}{\sigma_\xi{}^2}e^{-\frac{|h_\xi|^2}{2\sigma_\xi{}^2}}\,\mathrm{d}|h_{n-1}|\mathrm{d}|h_\xi| \\
&= \frac{1}{\ln 2}\frac{\alpha}{\xi-\alpha}\left\{\mathrm{Ei}\left[\frac{(1+\alpha)N_0}{\xi 2\sigma_\xi^2 P}\right]e^{\frac{(1+\alpha)N_0}{\xi 2\sigma_\xi^2 P}} - \right. \\
&\quad \left.\mathrm{Ei}\left[\frac{(1+\alpha)N_0}{2\alpha\sigma^2 P}\right]e^{\frac{(1+\alpha)N_0}{2\alpha\sigma^2 P}}\right\},
\end{aligned}
\tag{3}
$$

in which $p(|h_{n-1}|)$ and $p(|h_\xi|)$ denote the probability density function of h_{n-1} and h_ξ, respectively. Assume that the channel qualities of all links involved in this platoon are equal; that is, $\sigma_1^2 = \cdots = \sigma_n^2 = \cdots = \sigma_N^2 = \sigma^2$, where σ_n^2 is defined as $\sigma_n^2 \triangleq \mathbb{E}(|h_n|^2)$. Further, the exponential integral function is employed in (3) for derivation purposes, which is mathematically defined as $\mathrm{Ei}(t) = \int_t^\infty e^{-x}x^{-1}\,\mathrm{d}x$.

For the next hop shown in Fig. 1, V_n broadcasts the information signal to surrounding vehicles, and hence both V_{n+1} and V_e are within the communication range. To protect the information from eavesdropping, V_{n-1} takes its turn to perform the shielding task. The SINR at the side of V_{n+1} can be obtained as

$$
\gamma_n = \frac{\mathcal{P}_n|h_n|^2}{N_0},
\tag{4}
$$

in which $\mathcal{P}_n$ denotes the transmit power of V_n. Hold the power constraint of the nth hop link here; that is,

$$
\begin{cases}
\mathcal{P}_n + \mathcal{P}'_{n-1} = P; \\
\beta \triangleq \mathcal{P}_n/\mathcal{P}'_{n-1},\ 0 \le \beta \le 1,
\end{cases}
\tag{5}
$$

where $\mathcal{P}'_{n-1}$ is defined as the transmit power of V_{n-1} in the nth hop, and β is the power ratio between $\mathcal{P}_n$ and $\mathcal{P}'_{n-1}$. The ergodic capacity for the nth hop can be expressed by

$$
\begin{aligned}
C_n &= \mathbb{E}\left[\log_2\left(1+\gamma_n\right)\right] \\
&= \int \log_2\left(1+\gamma_n\right) p(|h_n|)\mathrm{d}|h_n| \\
&= \int \log_2\left(1+\frac{\mathcal{P}_n|h_n|^2}{N_0}\right)\frac{|h_n|}{\sigma^2}e^{-\frac{|h_n|^2}{2\sigma^2}}\,\mathrm{d}|h_n| \\
&= \frac{1}{\ln 2}e^{\frac{N_0(1+\beta)}{2\sigma^2\beta P}}\mathrm{Ei}\left[\frac{N_0(1+\beta)}{2\sigma^2\beta P}\right].
\end{aligned}
\tag{6}
$$

4.2 Ergodic capacity of the eavesdropping link and secrecy capacity

The $(n-1)$th hop and the nth hop, which are both exposed to the eavesdropper, broadcast the same information through two separate time slots, respectively. Thus the eavesdropper can obtain the time diversity gain when decoding the data. Here we investigate the capacity obtained by the eavesdropper according to the selective combination. At the eavesdropper side, the SINR can be expressed as

$$
\gamma_e = \begin{cases}
\gamma_{e,n-1}, & \mathbb{E}[\gamma_{e,n-1}] > \mathbb{E}[\gamma_{e,n}]; \\
\gamma_{e,n}, & \mathbb{E}[\gamma_{e,n}] \ge \mathbb{E}[\gamma_{e,n-1}],
\end{cases}
\tag{7}
$$

in which $\gamma_{e,n-1}$ and $\gamma_{e,n}$ are defined as

$$
\begin{cases}
\gamma_{e,n-1} \triangleq \dfrac{\mathcal{P}_{n-1}|\hbar_{n-1}|^2}{\mathcal{P}'_n|\hbar_n|^2+N_0}; \\
\gamma_{e,n} \triangleq \dfrac{\mathcal{P}_n|\hbar_n|^2}{\mathcal{P}'_{n-1}|\hbar_{n-1}|^2+N_0},
\end{cases}
\tag{8}
$$

where $\hbar_{n-1}$ and $\hbar_n$ denote the channel gains of the eavesdropping links with respect to the $(n-1)$th hop and the nth hop. Subsequently, the capacity at the eavesdropper side for the $(n-1)$th hop can be obtained as

$$
\begin{aligned}
C'_{n-1} &= \mathbb{E}\left[\log_2\left(1+\gamma_{e,n-1}\right)\right] \\
&= \frac{1}{\ln 2}\frac{\alpha\sigma'^2_{n-1}}{\sigma'^2_n - \alpha\sigma'^2_{n-1}}\left\{\mathrm{Ei}\left[\frac{(1+\alpha)N_0}{2\sigma'^2_n P}\right]e^{\frac{(1+\alpha)N_0}{2\sigma'^2_n P}} - \right. \\
&\quad \left.\mathrm{Ei}\left[\frac{(1+\alpha)N_0}{2\alpha\sigma'^2_{n-1}P}\right]e^{\frac{(1+\alpha)N_0}{2\alpha\sigma'^2_{n-1}P}}\right\},
\end{aligned}
\tag{9}
$$

in which σ'^2_n and σ'^2_{n-1} stand for the variations of $\hbar_n$ and $\hbar_{n-1}$, respectively. Similarly, the capacity of the eavesdropping link in the nth hop can be derived as

$$
\begin{aligned}
C'_n &= \mathbb{E}\left[\log_2\left(1+\gamma_{e,n}\right)\right] \\
&= \frac{1}{\ln 2}\frac{\beta\sigma'^2_n}{\sigma'^2_{n-1} - \beta\sigma'^2_n}\left\{\mathrm{Ei}\left[\frac{(1+\beta)N_0}{2\sigma'^2_{n-1}P}\right]e^{\frac{(1+\beta)N_0}{2\sigma'^2_{n-1}P}} - \right. \\
&\quad \left.\mathrm{Ei}\left[\frac{(1+\beta)N_0}{2\beta\sigma'^2_n P}\right]e^{\frac{(1+\beta)N_0}{2\beta\sigma'^2_n P}}\right\}.
\end{aligned}
\tag{10}
$$

Therefore, according to the definition of secrecy capacity [11], secrecy capacities of the $(n-1)$th hop and the nth hop can be achieved as

$$\begin{cases} \mathcal{C}_{n-1} \triangleq \left[C_{n-1} - C'_{n-1}\right]^+; \\ \mathcal{C}_n \triangleq \left[C_n - C'_n\right]^+, \end{cases} \tag{11}$$

$$\begin{aligned} \mathcal{C}_{n-1} = \Bigg\{ & \frac{1}{\ln 2}\frac{\alpha}{\xi-\alpha}\Bigg\{ \mathrm{Ei}\left[\frac{(1+\alpha)N_0}{\xi 2\sigma_\xi^2 P}\right] e^{\frac{(1+\alpha)N_0}{\xi 2\sigma_\xi^2 P}} \\ & - \mathrm{Ei}\left[\frac{(1+\alpha)N_0}{2\alpha\sigma^2 P}\right] e^{\frac{(1+\alpha)N_0}{2\alpha\sigma^2 P}} \Bigg\} \\ & - \frac{1}{\ln 2}\frac{\alpha\sigma'^2_{n-1}}{\sigma'^2_n - \alpha\sigma'^2_{n-1}}\Bigg\{ \mathrm{Ei}\left[\frac{(1+\alpha)N_0}{2\sigma'^2_n P}\right] e^{\frac{(1+\alpha)N_0}{2\sigma'^2_n P}} \\ & - \mathrm{Ei}\left[\frac{(1+\alpha)N_0}{2\alpha\sigma'^2_{n-1} P}\right] e^{\frac{(1+\alpha)N_0}{2\alpha\sigma'^2_{n-1} P}} \Bigg\} \Bigg\}^+ \end{aligned} \tag{12}$$

$$\begin{aligned} \mathcal{C}_n = \Bigg\{ & \frac{1}{\ln 2} e^{\frac{(1+\beta)N_0}{2\sigma^2\beta P}} \mathrm{Ei}\left[\frac{(1+\beta)N_0}{2\sigma^2\beta P}\right] \\ & - \frac{1}{\ln 2}\frac{\beta\sigma'^2_n}{\sigma'^2_{n-1} - \beta\sigma'^2_n}\Bigg\{ \mathrm{Ei}\left[\frac{(1+\beta)N_0}{2\sigma'^2_{n-1} P}\right] e^{\frac{(1+\beta)N_0}{2\sigma'^2_{n-1} P}} \\ & - \mathrm{Ei}\left[\frac{(1+\beta)N_0}{2\beta\sigma'^2_n P}\right] e^{\frac{(1+\beta)N_0}{2\beta\sigma'^2_n P}} \Bigg\} \Bigg\}^+ \end{aligned} \tag{13}$$

where $[x]^+ \triangleq \max\{0, x\}$. These two equations can be specifically written into Eqs. (12) and (13), respectively. As the eavesdropper employs the selective combination scheme, it obtains the capacity $C_e \triangleq \max\{C'_{n-1}, C'_n\}$, while the overall capacity in this study of the two hops is defined as $C \triangleq \min\{C_{n-1}, C_n\}$. Thus, the overall secrecy capacity of this two-hop local system can be calculated using

$$\mathcal{C} \triangleq \left[C - C_e\right]^+. \tag{14}$$

5 Numerical results and analysis

In this section, the numerical results based on Eqs. (11) and (14) are presented to verify the proposed scheme.

In Fig. 2, the influence of the self-interference factor, defined as ξ, on the secrecy capacity of the $(n-1)$th hop is investigated. It can be observed in Fig. 2 that the secrecy capacity increases with an increase in the signal-to-noise ratio (SNR), and a larger self-interference factor leads to a smaller secrecy capacity, which can be also known from Eqs. (3) and (12). This is because full-duplex transceivers suffer from the self-loop interference caused by signal leakage

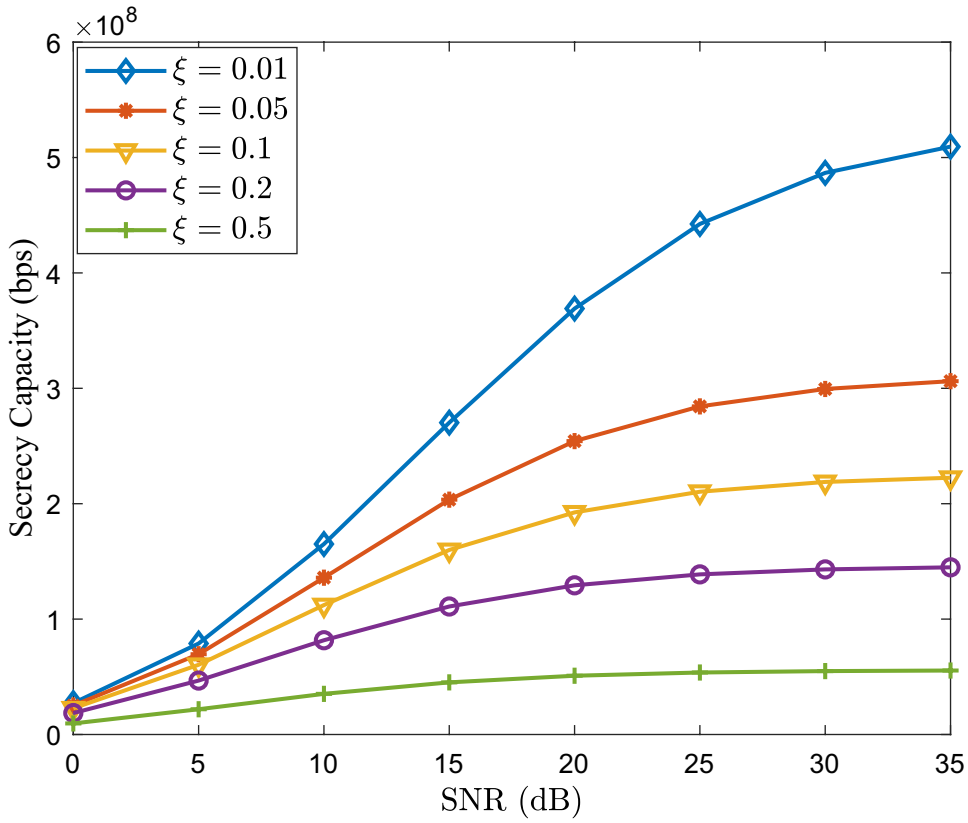

Fig. 2 Secrecy capacity versus SNR in the $(n-1)$th hop under different self-interference factors. Assume that the standard deviations of the different channels are equal (i.e., $\sigma'_{n-1} = \sigma'_n = \sigma = \sigma_\xi$), and the power ratio is set to be $\alpha = 1$

between the transmitter and receiver, which is a drawback of the full-duplex relay system. Larger self-interference factor indicates larger self-interference on the legitimate receiver V_n, resulting in a smaller ergodic capacity of the legitimate link and secrecy capacity of the $(n-1)$th hop. In the following numerical analyses, the self-interference factor is set to 0.01, which is practically reasonable [24].

In Fig. 3, the performance of the overall secrecy capacity of the two-hop local system concerning the power ratio α and β is investigated. Here it is assumed that the qualities of all the communication links are the same. As shown in Fig. 2(a), the peak area of the surface can be reached under the condition that both α and β are approximately equal to one. The fundamental reasons can be summarized as follows. For the $(n-1)$th hop, a low secrecy capacity under the case of small ratio α is obtained due to the small transmit power of V_{n-1}. However, as α becomes larger than one, the jamming signal power transmitted from V_n to V_e decreases with the continuous increase of α, leading to a high capacity at the eavesdropper side, as described in (9). For the nth hop, a similar principle can be delivered, which has been discussed in (10). Additionally, since V_{n+1} does not require to transmit jamming signals in the nth hop, and hence there is no self-interference stepping in. It indicates that a higher channel capacity can be obtained under the same power ratio between information and jamming signals if compared with the $(n-1)$th hop. Therefore, clearly to obtain the maximum overall secrecy capacity, β can be set slightly larger than α. The results also indicate that, with the identical link qualities, the powers of the information and the jamming signals should be averaged out to achieve an excellent secrecy performance.

In Fig. 4, the secrecy capacity for the $(n-1)$th hop is compared under different ratios among σ'_{n-1}, σ'_n, and σ, which denote the standard deviations of the eavesdropping, the jamming and the legitimate links, respectively. Evidently, larger SNRs always provide higher secrecy capacities. When the qualities of both the jamming and legitimate links are better than that of the eavesdropping link (i.e., $\sigma'_n : \sigma'_{n-1} : \sigma = \sqrt{2} : 1 : \sqrt{2}$), the capacity obtained by V_e is much smaller than that at the V_n side. Therefore, it exhibits the highest secrecy capacity among the six cases. As the eavesdropping link is relatively weak, the received information signal power by V_e is small, whereas that of the jamming link is relatively strong. Thus, V_{n-1} poses significant interference to V_e. Conversely, the case that the eavesdropping link is more robust than the legitimate link and the jamming link exhibits the lowest secrecy capacity. It can also be found that, for the cases with the ratios $\sqrt{2} : 1 : 1$ and $1 : \sqrt{2} : \sqrt{2}$, the curves completely overlap. For the former, the friendly shielder plays a crucial role in protecting the information from eavesdropping attacks, as the legitimate and eavesdropping links are relatively weak. Conversely, for the latter, the eavesdropping link is relatively powerful. Thus, V_e can efficiently take eavesdropping although the legitimate link is not quite poor.

The AN scheme based on the MIMO system [25] is adopted here for comparison purposes, wherein the case with restricted transmit antennas is considered. The scheme requires the accurate CSI of the legitimate channel to generate AN that the receiver can eliminate while the eavesdropper cannot. Here, we compare its secrecy capacity under three cases. The first case is based on an ideal assumption that the CSI is estimated accurately, and the

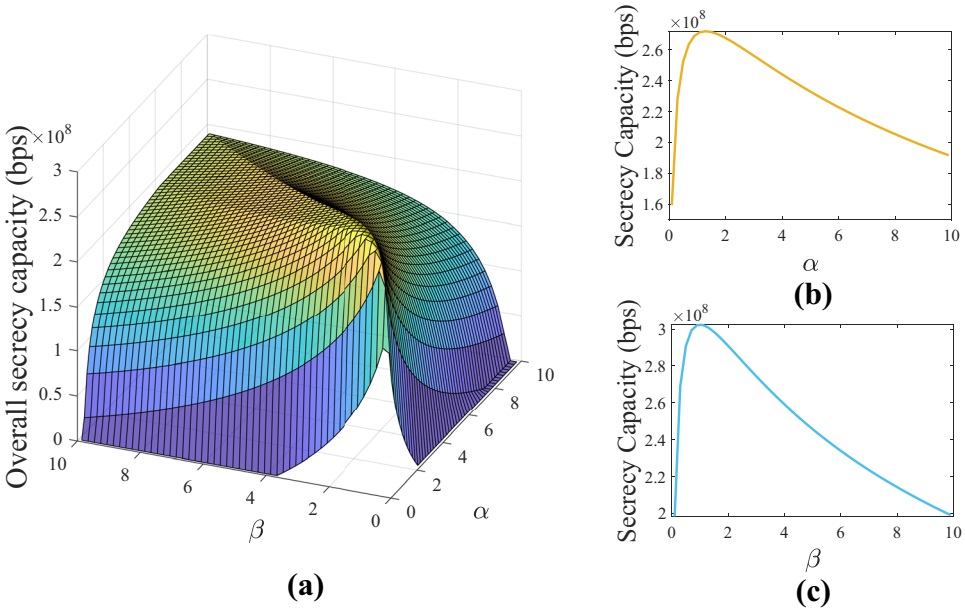

Fig. 3 Secrecy capacity versus power ratios α and β. **a** Joint impacts of both α and β on the overall secrecy capacity for the two hops. **b** Impact of α on the secrecy capacity for the $(n-1)$th hop. **c** Impact of β on the secrecy capacity for the nth hop. Assume that the standard deviations of the different channels are equal (i.e. $\sigma'_{n-1} = \sigma'_n = \sigma = \sigma_\xi$) and the self-interference factor ξ equals to 0.01. The SNR is set to 15 dB

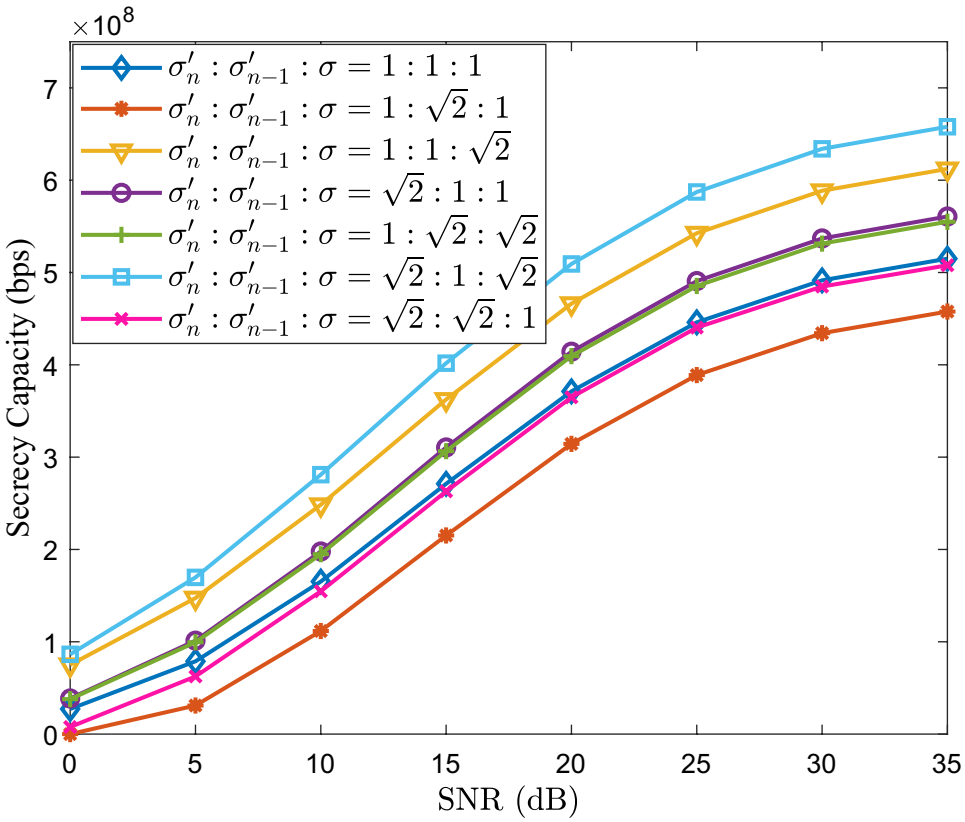

Fig. 4 Secrecy capacity versus SNR in the $(n-1)$th hop under different channel qualities. Assume that the self-interference factor ξ equals to 0.01. The power ratio is set to be $\alpha = 1$

number of antennas equipped on the transmitter is larger than that of the eavesdropper and legitimate receiver; that is, $N_t = 4 > N_r = N_e = 3$. Second, the secrecy capacity under the condition that 10% error occurs in the CSI estimation is studied. In the third case, the number of antennas equipped on the eavesdropper is equal to the number of transmit antennas; that is, $N_t = N_e = 4 > N_r = 3$. As shown in Fig. 5, as the SNR increases, the secrecy capacities achieved by the DSST and the MIMO-based AN schemes for the first case are both increasing as well. When the transmitter employs more antennas than the eavesdropper and the receiver on the premise that the perfect CSI is available, the MIMO-based AN scheme outperforms the DSST scheme.

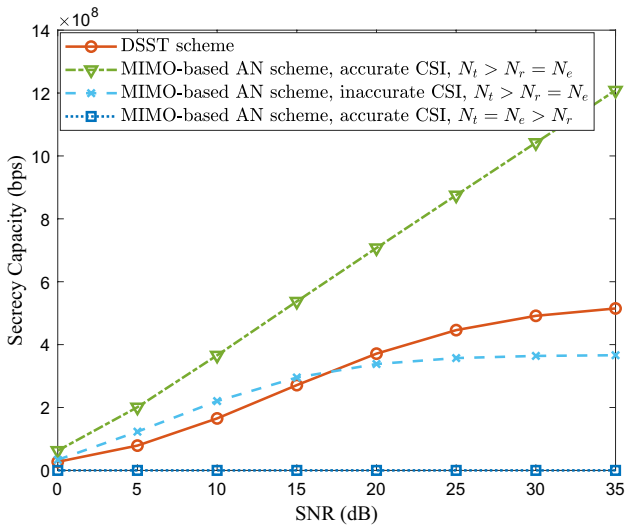

Fig. 5 Secrecy capacity versus SNR in the $(n-1)$th hop. Assume that the standard deviations of the different channels are equal (i.e., $\sigma'_{n-1} = \sigma'_n = \sigma = \sigma_\xi$), and the self-interference factor ξ equals to 0.01. The power ratio is set to be $\alpha = 1$

For the second case, it is observed that the MIMO-based AN scheme exhibits better performance than the proposed scheme in the low SNR region. The reason is that the self-interference is considered in the proposed scheme, which decreases the secrecy capacity. As the CSI estimation error occurs, the AN signal is generated to interfere with the eavesdropper but inevitably affects the receiver. This effect is particularly significant when the transmit power is high and thus severely degrades the performance. Therefore, with an increase of the SNR, the DSST scheme gradually provides a higher secrecy capacity. Furthermore, once the eavesdropper owns as many antennas as the vehicles in the platoon, the eavesdropper is able to eliminate the AN signal with the help of the eavesdropping channel matrix [25]. In such a case, the MIMO scheme completely fails to secure communication.

In addition, the DSST and MIMO-based AN schemes are compared in the case where the desired SINR is imposed at the legitimate receiver to ensure the quality of service (QoS).

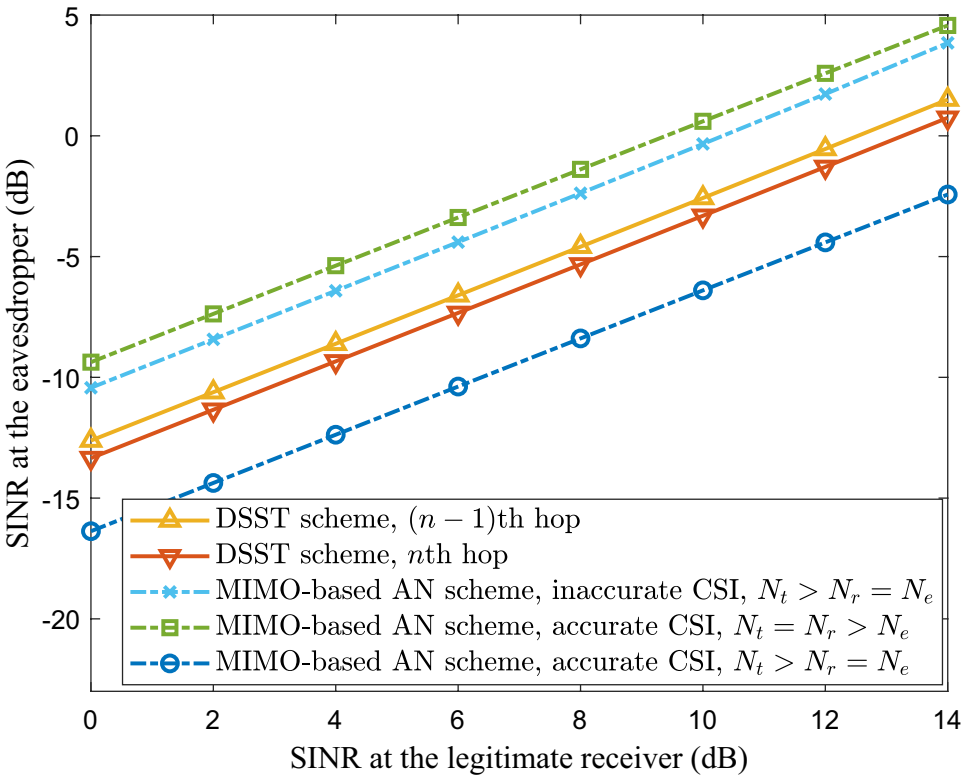

Fig. 6 SINR at the eavesdropper versus SINR at the legitimate receiver, with a total power constraint $P = 30$ dB. Assume that the standard deviations of the different channels are equal (i.e., $\sigma'_{n-1} = \sigma'_n = \sigma = \sigma_\xi$) and the self-interference factor is set to 0.01

The noise power is assumed to be one (i.e., $N_0 = 1$), and the transmit power P can be expressed in decibels relative to the noise power. A power constraint $P = 30$ dB is considered in both schemes. In Fig. 6, the SINR at the eavesdropper with an increasing desired SINR at the legitimate receiver is exhibited. Evidently, with the SINR at the legitimate receiver increasing, an increased SINR can be also obtained by the eavesdropper. This is because, when more power is used on the information signal, less power will be available for the jamming signal with a transmit power constraint. The results show that, in the MIMO-based AN scheme, when the number of receive antennas is not less than the number of transmit antennas or the CSI is inaccurately estimated, the AN signal cannot be completely eliminated at the legitimate receiver and severely reduces its SINR. Conversely, the proposed DSST scheme achieves a better performance without CSI knowledge. This finding reveals that the DSST scheme has good adaptability and is not limited by various realization conditions. Further, under the same QoS requirement, the DSST scheme is more energy-efficient. This is because the DSST scheme fully uses the multi-hop mechanism in the vehicle platoon to minimize the negative impact of jamming signals on the legitimate receiver. It is also noticed that the performance of the $(n-1)$th hop is slightly worse than that of the nth hop due to the existence of self-interference when the legitimate receiver transmits the jamming signal itself. When the jamming signal does not affect the legitimate receiver (i.e., the nth hop of the DSST and MIMO-based AN schemes with accurate CSI as well as $N_t > N_r = N_e$), the comparison scheme performs better than the proposed scheme. An advantage of the MIMO-based AN scheme is its ability to improve the SINR of the legitimate receiver through precoding. Fortunately, the proposed scheme does not contradict the MIMO-based scheme, as the MIMO technique can be equipped in vehicles to achieve improved performance. From the analysis, we believe that the proposed DSST scheme can exhibit superiority in adaptability, especially due to the dynamics of the platoon and uncertainty of eavesdroppers.

6 Conclusion

In this work, we proposed a secure transmission scheme, called DSST, to protect the vehicular platoon communication against eavesdropping attacks. Considering a multi-hop communication mechanism in the vehicular platoon, the scheme used a similar concept to cooperative jamming and consequently makes the neighboring vehicles function as relays and shielders; hence, the impact of jamming signals on the legitimate receiver can be effectively minimized. Unlike typical technologies of physical layer security, the proposed DSST scheme does not require the transmitter to know the CSI of the eavesdropping or the legitimate link. We used the vulnerable link to derive the security performance of the local system under the DSST scheme. The performance of various scenarios was evaluated based on the numerical

results, and comparisons with the MIMO-based AN scheme were presented. Specifically, numerical results verified the feasibility and effectiveness of the proposed scheme. When CSI cannot be accurately acquired, the proposed scheme can achieve higher secrecy capacity than the compared scheme. In our future research, we will focus on considering the specific design of jamming signals and attempt to enhance the DSST scheme by incorporating the MIMO technique to further improve the system performance.

Acknowledgements This work was supported in part by the National Key R &D Program of China (Grant No. 2020YFB1806703), and in part by the National Natural Science Foundation of China (Grant Nos. 61901315 and 62101429).

Author contributions All authors contributed to the study equally. All authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding This work was supported in part by the National Key R &D Program of China (Grant No. 2020YFB1806703), and in part by the National Natural Science Foundation of China (Grant Nos. 61901315 and 62101429).

Availability of supporting data Not applicable.

Declarations

Ethical approval and consent to participate Not applicable.

Human and animal ethics Not applicable.

Consent for publication All authors unanimously agree to publish the paper.

Competing interests The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Jia D, Lu K, Wang J (2014) A disturbance-adaptive design for VANET-enabled vehicle platoon. IEEE Trans Veh Technol 63(2):527–539
2. Michael P, Lammert Kevin et al (2014) Effect of platooning on fuel consumption of class 8 vehicles over a range of speeds, following distances, and mass. SAE Int J Commer Veh 7(2):626–639
3. Jia D, Lu K, Wang J, Zhang X el al (2015) A survey on platoon-based vehicular cyber-physical systems. IEEE Commun Surv Tutorials 18(1):263–284
4. Mishra R, Singh A, Kumar R (2016) VANET security: Issues, challenges and solutions. International Conference on Electrical. IEEE 1050–1055
5. Li K, Voicu RC, Kanhere SS et al (2019) Energy efficient legitimate wireless surveillance of UAV communications. IEEE Trans Veh Technol 68(3):2283–2293
6. Lai C, Lu R, Zheng D et al (2020) Security and privacy challenges in 5G-enabled vehicular networks. IEEE Netw 34(2):37–45
7. Xiong J, Ma R, Chen L et al (2019) A personalized privacy protection framework for mobile crowdsensing in IIoT. IEEE Trans Industr Inf 16(6):4231–4241
8. Petrillo A, Pescape A, Santini S et al (2020) A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks. IEEE Transactions on Cybernetics 51(3):1134–1149
9. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Tech J 28(4):656–715
10. Wyner AD (1975) The wire-tap channel. Bell Syst Tech J 54(8):1355–1387
11. Leung-Yan-Cheong S, Hellman M (1978) The Gaussian wire-tap channel. IEEE Trans Inf Theory 24(4):451–456
12. Zou Y, Wang X, Shen W (2013) Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack. IEEE International Conference on Communications. IEEE 2183–2187
13. Thai CDT, Lee J, Quek TQ (2015) Physical-layer secret key generation with colluding untrusted relays. IEEE Trans Wirel Commun 15(2):1517–1530
14. Li K, Lu L, Ni W et al (2019) Cooperative secret key generation for platoon-based vehicular communications. IEEE International Conference on Communications. IEEE 1–6
15. Furqan HM, Hamamreh JM, Arslan H (2020) New physical layer key generation dimensions: Subcarrier indices/positions-based key generation. IEEE Commun Lett 25(1):59–63
16. Yerrapragada AK, Eisman T, Kelley B et al (2021) Physical layer security for beyond 5G: Ultra secure low latency communications. IEEE Open Journal of the Communications Society 2:2232–2242
17. Xu Q, Ren P, Swindlehurst AL (2020) Rethinking secure precoding via interference exploitation: A smart eavesdropper perspective. IEEE Trans Inf Forensics Secur 16:585–600
18. Zhang M, Shang Y, Zhao Y (2020) Strategy of relay selection and cooperative jammer beamforming in physical layer security. IEEE Vehicular Technology Conference. IEEE 1–6
19. Nandan N, Majhi S, Wu HC (2021) Beamforming and power optimization for physical layer security of MIMO-NOMA based CRN over imperfect CSI. IEEE Trans Veh Technol 70(6):5990–6001
20. Lin S, Han R, Yu G et al (2020) A secure transmission scheme based on artificial noise in a MISO eavesdropping system. IEEE International Conference on Communication Technology. IEEE 1134–1138
21. Tang Z, Sun L, Tian X et al (2021) Artificial-Noise-Aided Coordinated Secure Transmission Design in Multi-Cell Multi-Antenna Networks With Limited Feedback. IEEE Trans Veh Technol 71(2):1750–1765
22. Li K, Ni W, Tovar E et al (2018) LCD: Low latency command dissemination for a platoon of vehicles. IEEE International Conference on Communications. IEEE 1–6
23. Yang K, Cui H, Song L et al (2015) Efficient full-duplex relaying with joint antenna-relay selection and self-interference suppression. IEEE Trans Wirel Commun 14(7):3991–4005
24. Zhang X, Xia XG, He Z et al (2019) Phased-array transmission for secure mmWave wireless communication via polygon construction. IEEE Trans Signal Process 68:327–342
25. Liu Y, Chen HH, Wang L (2016) Secrecy capacity analysis of artificial noisy MIMO channels-An approach based on ordered eigenvalues of Wishart matrices. IEEE Trans Inf Forensics Secur 12(3):617–630

Yiran Yang received the B.E. degree in telecommunications engineering from the Beijing University of Posts and Telecommunications, China in 2021. He is currently working toward the Ph.D. degree with the State Key Laboratory of Networking and Switching Technology, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China. His main research interest is multiple access technologies.

Xiqing Liu received the M.S. and Ph.D. degrees from the Harbin University of Science and Technology and Harbin Institute of Technology, Harbin, China in 2012 and 2017, respectively. Currently, he is an associate research fellow at the State Key Laboratory of Networking and Switching Technology, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications. His current research interests include interference suppression in multicarrier systems, non-orthogonal multiple access, and MIMO technologies.

Zhifeng Wang received the B.S. degree from Shanghai University, Shanghai, China, in 2015 and the M.S. degree from Hainan University, Haikou, China, in 2018. He is currently working toward the Ph.D. degree with the State Key Laboratory of Networking and Switching Technology, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include channel estimation, coding, and multiple access technologies.

Yiliang Liu received the B.E. and M.Sc. degrees in computer science and communication engineering from Jiangsu University, Zhejiang, China, in 2012 and 2015, respectively. He is currently pursuing the Ph.D. degree withthe Communication Research Centre, Harbin Institute of Technology, China. He was a Visiting Research Student with the Department of Engineering Science, National Cheng Kung University, Tainan, Taiwan, from 2014 to 2015, and the Department of Electrical and Computer Engineering, University of Waterloo, Canada, from 2018 to 2019. His research interests include security of wireless communications, physical-layer security, and intelligent connected vehicles.