Physical-Layer Security and Privacy for Vehicle-to-Everything

Article *in* IEEE Communications Magazine · June 2019

DOI: 10.1109/MCOM.001.1900141

CITATIONS
17

READS
979

3 authors:

Basem M. ElHalawany
Benha University
42 PUBLICATIONS **197** CITATIONS
SEE PROFILE

Ahmad elBanna
Benha University
22 PUBLICATIONS **39** CITATIONS
SEE PROFILE

Kaishun Wu
Shenzhen University
188 PUBLICATIONS **4,062** CITATIONS
SEE PROFILE

Physical-Layer Security and Privacy for Vehicle-to-Everything

Basem M. ElHalawany, Ahmad A.Aziz El-Banna, and Kaishun Wu

***Abstract*—Vehicular communications in intelligent transportation system (ITS) promise to improve traffic efficiency, road utilization, and safety. Achieving secure vehicular communications is vital for the deployment of vehicle-to-everything (V2X) applications. This article provides a comprehensive overview of physical-layer security (PLS) strategies employed for V2X. By exploiting the randomness and the physical characteristics of wireless channels, PLS offers reliable solutions against eavesdroppers attacks as complementary approaches to cryptographic techniques. We give a brief introduction to the architecture and characteristics of V2X networks. Then, the fundamental principles of PLS technology are proposed, followed by security threats in V2X. Additionally, we discuss some open issues and challenges for future research. Finally, we investigate a case study where different challenges and technologies coexistence in one V2X scenario.**

***Index Terms*—Vehicle-to-everything, physical layer security, NOMA based moving relay.**

I. Introduction: V2X Network Evolution

THE recent developments in communication technologies, smart sensors, and artificial intelligence have opened up a new era for the Intelligent Transportation Systems (ITS). Almost all modern vehicles are equipped with multiple sensors, which revolutionize the ability of vehicles to assess the environment. Additionally, the heterogeneous nature of the fifth generation (5G) and Beyond (B5G) communication systems is a key factor to facilitate vehicular communications. On the other hand, the promising capabilities of machine learning and deep neural network techniques to analyze data collected using crowed-sourcing provide another key factor for intelligent decisions to improve accidents prediction and traffic efficiency [1]. These advancements have led to various paradigms for ITS's information exchange including vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-network (V2N), vehicle-to-pedestrian (V2P), and eventually vehicle-to-everything (V2X) communication as shown in Fig.1. This in turns led to a plethora of applications including optimizing traffic efficiency, road safety, autonomous driving, efficient routing, reducing fuel consumption, and Internet access, etc. Both real-time and non real-time contents are expected to be carried through V2X networks, where the real-time contents include delay-sensitive sensory data, monitoring, and multimedia streams, while the non-real-time contents include web-browsing, messaging, and file transfers for vehicular users [2].

The authors are with Shenzhen University, Shenzhen, China (Emails: {basem.mamdoh, ahmad.elbanna, wu}@szu.edu.cn). Basem and Ahmad are also with Benha University, Egypt. kaishun Wu is also with PCL Research Center of Networks and Communications, Peng Cheng Laboratory, Shenzhen, China.

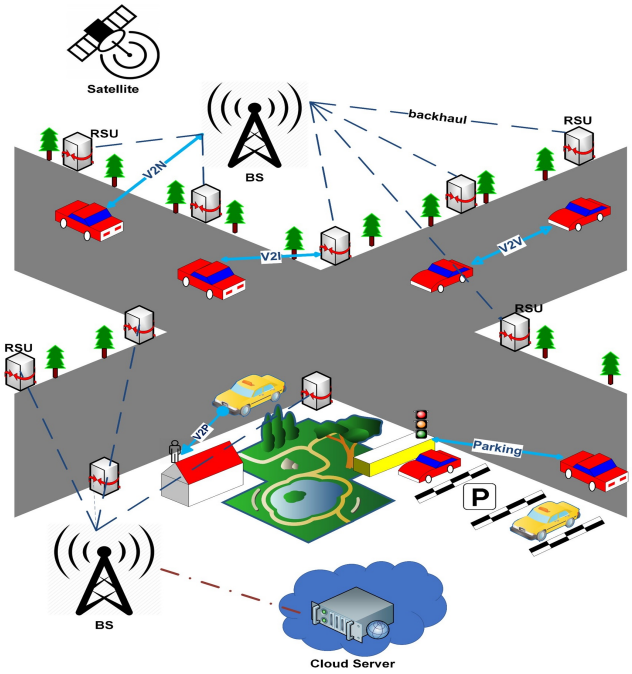

Fig. 1. Illustrative scenarios for V2X Network.

Despite the remarkable advantages and promising applications of V2X, several critical challenges such as mobility, establishment of constant connectivity, stringent reliability, low-latency guarantee, efficient resource allocation and security issues for information exchange need to be addressed. The expected huge increase in data traffic of V2X over the next few years encourages researchers to propose several solutions to these challenges. In this paper, we shed light on the existence of Physical-Layer Security (PLS) in highly-mobile V2X environments.

A. V2X Network Architecture

Figure 1 shows illustrative scenarios for a V2X network, at which the vehicular users' equipment (VUEs) are communicating with infrastructure objects (i.e., roadside units (RSUs), traffic lights, parking areas, road signs, and smart roadblocks, etc.) to form the V2I portion of the network. The infrastructure objects are in turns connected to the eNodeB (eNB) via high-speed links for backhauling. On the other hand, each VUE is capable of communicating to other close VUEs and pedestrians nodes, which forms sidelinks for V2V

and V2P networking. Additionally, VUEs can be connected directly to the eNBs or the associated cloud service for V2N. The heterogeneous architecture offered in V2X allows VUEs to exchange real-time information about traffic, routes, road situation, direction, speed, location, braking status, steering wheel position, and sensory data of each VUE in order to bring a global view for appropriate decisions better than on-board counterparts. Different V2X architectures have been proposed in literature to meet ITS's requirements, where some are integrated with 5G mobile communication technologies, software defined networking, and visible light communication [3].

This heterogeneous and dynamic architecture introduces design challenges to keep the QoS and security constraints. The careful study of V2X network architecture helps to identify QoS requirements and security threats for specific ITS services in different applications. One interesting insight about such dynamic and decentralized architecture is that VUEs may randomly access or leave the network at any time which leads to difficulties for cryptographic key management and distribution.

B. V2X Standards

Recently, several V2X standards have been launched by different standardization bodies such as the dedicated short-range communications (DSRC) of the Society of Automotive Engineers (SAE), the cellular intelligent transportation system (C-ITS) of the European Telecommunications Standards Institute (ETSI), wireless access for vehicular environment (WAVE) of IEEE, communications access for land mobiles (CLAIM) of ISO, and the long-term evolution (LTE) cellular-V2X (C-V2X) of the 3rd Generation Partnership Project (3GPP) [1]. In the following, we briefly highlight the fundamental characteristics of the four major standard.

1) DSRC: SAE has proposed DSRC, which relies on IEEE 802.11a WLAN standard that defines the physical transmission (PHY) and medium access control (MAC). DSRC adapted IEEE 802.11a to V2X communication requirements. DSRC subdivided the 5.825 GHz to 5.925 GHz frequency band into 10 MHz channels.

2) C-ITS: C-ITS is the IEEE 802.11p equivalent proposed by ETSI. C-ITS includes communication architecture and protocol stacks, where the stack covering the PHY and MAC layers is termed ITS-G5, and "G5" refers to the 5 GHz frequency band. Similar to DSRC, it uses the 5.9 GHz band, whereas the spectrum is portioned into 5 parts (A to D).

Notice that the key features of IEEE-802.11p for both DSCR and ITS-G5 are the same, which are based on IEEE 802.11p technology that suffers from unbounded delay and lack of QoS guarantee as consequences of using PHY and MAC that have been optimized for low-mobility wireless LAN [1]. At the PHY layer, both adopt orthogonal frequency division multiple access (OFDM) technology with half clock compared to IEEE 802.11a to cope with inter-carrier interference caused by the Doppler spread of fast moving VUEs. At the MAC layer, both employ a contention-based enhanced distributed channel access, which applies Carrier Sense Multiple Access with Collision Avoidance and access categories that allow traffic prioritization.

3) WAVE: IEEE has proposed WAVE in US, where it is also known as IEEE 1609 standard family. WAVE defines protocol stack on top of the IEEE 802.11 PHY and MAC layers, in addition to V2X message sets and related performance requirements. The WAVE short-message protocol defined by IEEE 1609.3 is the main protocol stack that fulfills the role of the transport protocol, while the IEEE 1609.4 standard defines a management extension for multi-channel operation MAC that allows a system with several transceivers to efficiently switch between the channels.

4) C-V2X: 3GPP has extended the Device-to-Device (D2D) communications Proximity Services (ProSe) functionality in release 12 to include two new modes (i.e., Modes 3 and 4, which are also known as LTE-V-Cell mode and LTE-V-Direct mode) in release 14 for C-V2X communication. The addition of those modes is a direct consequence of the constraints on packets delays and losses in V2X networks which are certainly different from static or slowly-moving D2D nodes with the severe impact on time-sensitive operations. Mode 3 supports V2I and V2N communication by relying on the eNodeB, while Mode 4 supports V2V and V2P communications where short-range sidelinks are used similar to D2D communication for safety applications and content exchange [4]. Consequently, C-V2X is based on a modification of the LTE which is highly reliable, with higher bandwidth.

The rest of the paper is organized as follows: In section II, We introduce PLS types, metrics, and threats in V2X networks. In section III, we provide the PLS challenges and future research directions over V2X. A case study that sheds light on the coexistence of different challenges and technologies in one V2X scenario is introduced in section IV. Finally, the paper is concluded in section V.

II. Physical-Layer Security (PLS)

A huge percentage of fatal car accidents are caused by humans' mistakes. In order to improve road safety, autonomous or non/semi-autonomous cars need to be connected in a reliable and timely manner, where the confidentiality and security of messages are vital [5], [6]. Confidentiality and security issues are usually handled in the upper layers of the protocol stack using key-based security encryption techniques. These cryptographic techniques are based on computational mathematical operations, which are hard to be performed by a limited-computational power attacker.

A. Motivations Behind PLS

The computational security paradigm has been proven to be effective; however, this is not the case in all scenarios. The following main concerns have been raised in literature for encryption techniques in emerging networking architectures like V2X and ad hoc networks:

- The computational security may be compromised if the eavesdropper has sufficient computational-power to solve mathematical models in cryptographic techniques.

- The management and exchange of secret keys to legitimate parties are challenging under mobility in V2X.
- In order to improve security, longer security keys are desirable; although they represent waste of resources and incur more delay in delay-sensitive V2X applications.

For these and other reasons, there has been considerable interest to find complementary types of security that can work on top of the conventional cryptography. Information-theoretic results show a potential of hiding messages from eavesdropper or authenticating devices without a shared secret key by designing solutions based on the physical characteristics of the radio channel (it is known as wireless physical layer security). The main characteristics of the physical layer are the noise and the fading of wireless channel, which are usually treated as impairments; however, they can be exploited to hide messages. Consequently, PLS can be defined as the study of different methods and algorithms that aim to improve the security of networks by exploiting the properties of the physical layer.

Wyner in his seminal work [7] laid the foundations of PLS based on the assumption of a much noisier eavesdropper's channel with respect to the legitimate receiver. Notice that Wyner's wiretap channel model captures the confidentiality assuming authentication is already in place. However, the physical-layer based authentication is also possible and will be discussed in subsection II.C. as the second category of PLS.

B. Key-less PLS

The most famous type is the key-less PLS, which is built to exploit the difference in wireless channels between legitimate user and eavesdroppers to securely transmit a message from a source to an intended legitimate receiver. Wyner showed that a positive rate can be achieved in perfect secrecy which is known as the secrecy rate. In other words, it is possible to secretly communicate if we can ensure that the wireless channel between the transmitter and the legitimate receiver is better than the channel to any eavesdropper. Recently, considerable research efforts have been dedicated to improve the wireless secrecy rate over different fading channels and system models by employing different technologies such as MIMO, artificial noise, millimeter waves beamforming, non-orthogonal multiple access, and relaying [8], [9], [10].

C. Physical-Layer Authentication (PLA)

PLA is the key-based category of PLS techniques, which exploits the random nature of the channels between different transceivers pairs to generate security key [11]. PLA encrypts each message bits with the generated random secret key as alternative to public key cryptography. The possibility to exploit channel features (i.e., channel state information and the received signal strength indicator) of a specific transceiver pair as a mean of physical-layer authentication that differentiates signals received from a legitimate transmitter and those from spoofing transmitters is a promising approach in wireless network.

D. PLS Performance Metrics

Recently, four main security metrics have been used for evaluating the performance in PLS-based systems, namely the secrecy rate, secrecy capacity, ergodic secrecy rate, and secrecy connection probability [10], which are defined as follows

- The secrecy rate (R) is the positive transmission rate at which information can be communicated securely in the presence of an eavesdropper, which can be mathematically formulated as the non-negative difference between the achievable rates of the legitimate receiver and the eavesdropper.
- The secrecy capacity is the maximum secrecy rate.
- The ergodic secrecy capacity is the statistical average of the secrecy rate over channel distribution.
- The secrecy connection probability is the probability that the secrecy rate is larger than a certain threshold value.

E. PLS Threats in V2X

V2X may suffer from different attacks [5], where the most famous types are listed as follows

- Emulating Attacker (EA): refers to an eavesdropper that emulate a legitimate party by sending radio signals with similar characteristics.
- Jamming Attacker (JA): refers to an eavesdropper that attempts to transmit an interfering radio signal with sufficiently high power that disrupts the communications between legitimate parties.
- Eavesdropping Attacker (EvA): intercepts the confidential transmissions of legitimate parties.

III. PLS Challenges and Future Directions over V2X

In spite of the progress in understanding how PLS can support confidentiality, it is vital to recognize the existence of different issues and challenges that must be addressed if PLS is to be adopted in practical security systems. In this section, we present how PLS affects and be affected by various challenges in V2X. Fig. 2 shows four major categories of challenges and open research directions for enabling PLS for V2X, which are summarized in the following subsections.

A. Mobility and Speed Challenges

Due to the high-speed mobility of VUEs, different challenges need to be addressed to fully understand and analyze the performance of V2X in general and the PLS aspects in V2X networks.

1) Channel Modeling: The traditional channel models of stationary communication links, such as Rayleigh, Rician, and Nakagami, do not fit well in evaluating different performance metrics including the secrecy capacity and the secrecy connection probability. Recently, other channel models have been theoretically and empirically investigated to give a higher precision for characterizing the dynamic non line-of-sight (NLOS) communication links in V2X such as the double

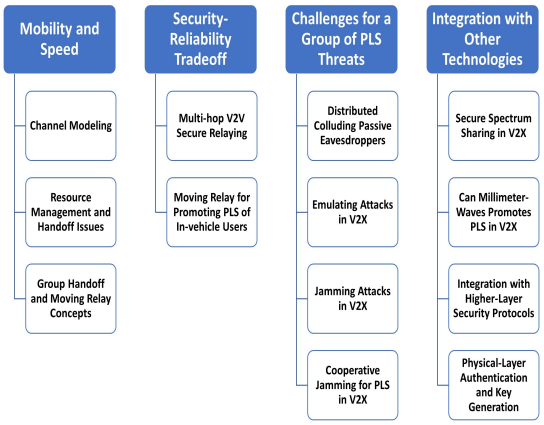

Fig. 2. Challenges and open research directions for enabling PLS in V2X networks.

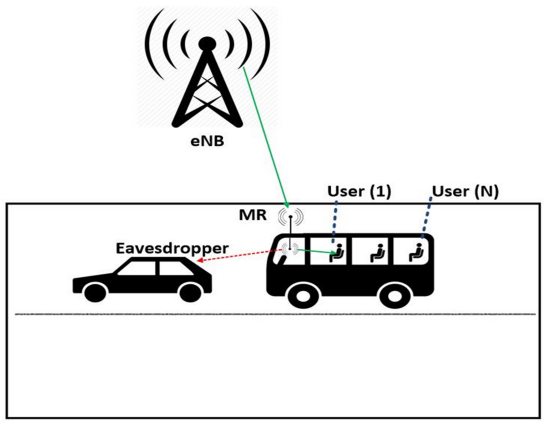

Fig. 3. Illustrative scenario of the vehicle penetration loss (VPL) in a bus with moving relay.

Rayleigh, Weibul, and $\kappa-\mu$ shadowed fading. However, V2X performance still needs deeper investigations.

Additionally, the adaptive cruise control (ACC) is one of the most important features for adjusting speed and safe distances for autonomous self-driving vehicles to avoid collision. In [12], the authors have investigated the secrecy capacity for ACC between two vehicles in the presence of an eavesdropper. The results show that secrecy capacity is inversely proportional to the speed of the transmitting vehicles; however, the study needs to be extended, validated with theoretical analysis, and consider the speed of the eavesdropper as well.

2) Resource Management and Handoff Issues: Due to mobility and the dynamically changing environment, it is essential to dynamically associate VUEs to different RSUs/eNBs, manage resources, and power allocation. This is a challenging task in order to maximize the long-term system utilities, performance, and reduce the handover rate [2], [13]. Moreover, the complexity of the problem escalates if eavesdroppers exist. In fact, many PLS approaches assume a single eavesdropper located at a certain location; however, eavesdropper may be another VUE with similar or different speed who can change the location to have better monitoring. PLS protocols must dynamically adapt and take countermeasures to improve security under these conditions.

3) Group Handoff and Moving Relay Concepts: One of the vital features of V2X networks is the need of communication between in-vehicle mobile units in high-speed trains and buses carrying a number of passengers and the rest of the network as shown in Fig. 3. Another challenging direction in this scenario is the elevated burden of the eNB to handle individual handoffs for all passengers' terminals. One interesting solution is the mobile relay concept, at which users inside the VUE are connected to one relay node or access point mounted on the VUE. In this case, group handoff and security management can be performed rather than handled individually.

B. Security-Reliability Tradeoff

In order to support autonomous self-driving vehicles, ultra-reliable low-latency communications must be guaranteed between the autonomous vehicle and both the infrastructure and other neighboring vehicles. If the signal received at the intended receiver is weak and overwhelmed by the background interference, the receiver would fail to decode the transmitted signal, which is referred to as an outage event. Increasing the transmit power enhances the received signal strength and improves reliability by reducing the probability of outage. However, this leads to an increase of the eavesdropper's received signal as well and thus degrades the secrecy rate. Accordingly, there exists a tradeoff between the security and reliability which needs to be carefully optimized [10]. Relay networks have been used in literature for improving reliability for edge users and users with bad channel conditions. In the following, we shed the light on two relaying scenarios for improving PLS in V2X.

1) Multi-hop V2V Secure Relaying: Each VUE can relay messages between RSUs and VUEs or between different VUEs in the absence of reliable direct links [9]. The process of selecting the appropriate VUE/VUEs to relay messages is crucial for achieving reliable and secure two or multi-hop communication as shown in Fig. 4. Since each candidate VUE relay node (R_1, R_2) has different channels with respect to both the receiver (R_x) and the eavesdropper (Evs), we need to select the one that improves the specified secrecy performance metric. Additionally, the joint relay selection and subcarrier allocation is an interesting research direction in V2X networks which needs more investigations.

2) Moving Relay for Promoting PLS of In-vehicle Users: Recent studies show that the signal can be attenuated as high as 25 dB at different frequencies due to the vehicle penetration loss (VPL) of buses or trains [14]. In [14], the VPL is solved by using the concept of moving relays (MRs), at which the VUE is equipped with an indoor antenna and an outdoor antenna, that are connected via cables as shown in Fig. 3. The outdoor antenna of the MR is used for the communication with the eNB and RSUs, while the indoor antenna is used for the commutation with the in-vehicle mobile units which improves the reliability.

On the other hand, from security perspective, the outside eavesdroppers cannot benefit from MR as the legitimate users since the eavesdroppers do suffer from VPL when the MR

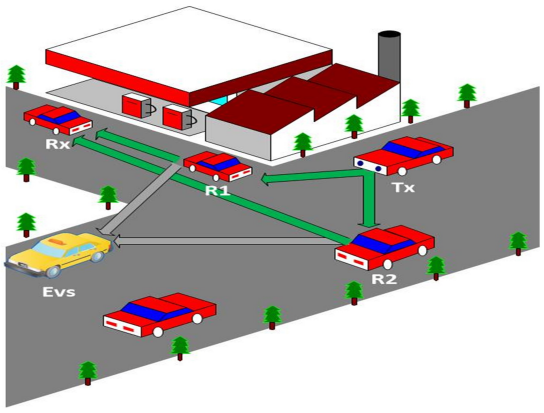

Fig. 4. Multi-hop Relaying for V2V Communication in the presence of Eavesdroppers.

indoor antenna relay messages from eNB. Consequently, using MR severely deteriorates signal-to-noise-ratios of the eavesdroppers, which substantially promotes PLS performance for in-vehicle users.

C. Challenges for a Group of PLS Threats

In this subsection, we discuss the challenges for four PLS threats and their implications in V2X networks as follows

1) Distributed Colluding Passive Eavesdroppers: Many PLS-based investigations assume a single eavesdropper [1], [10], [12]; however, it is possible that eavesdropping is performed by a group of non-colluding or colluding entities. In the former case, the PLS protocol should takes into consideration the worst case for the eavesdropper with the best achieved signal-to-interference-plus-noise-ratio, where the probability that one of these eavesdroppers is better than the legitimate receiver channel goes up with the independent observations. In the later case, the problem becomes harder since colluding collaborative adversaries can effectively lead to a zero secrecy rate if the system is not carefully designed.

2) Emulating Attacks in V2X: There have been attempts to defend against EA by transmitter verification schemes which exploits the location information to verify whether a signal is coming from a legitimate user or not [5], [8]. However, the location information may not be available in some V2X scenarios, which necessitates to employ an authentication approaches such as using registered MAC addresses and physical-layer authentication [11]. The problem with this type of attacks is that the falsified messages injected by the attacker could lead to a risky and dangerous decisions especially for autonomous vehicles.

3) Adversary Jamming Attacks in V2X: Many investigations assume that the attacker is a passive one that merely eavesdrop and monitor communications. However, active attacks have severe implications on V2X networks if an adversary attempts to transmit a radio signal that interfere with the communications messages between legitimate parties in V2X especially during critical delay-sensitive maneuvers where the V2Us have to send/receive warning message for autonomous decisions or alerting drivers [5].

4) Cooperative Friendly Jamming for Improving PLS in V2X: In order to improve the chances of achieving positive secrecy rate, artificial noise could be injected within the null space of the intended receiver by the transmitter or other cooperating nodes in order to jam eavesdroppers' received signals by degrading their channels [5]. However, several studies show that a single antenna jammer can also interfere with the legitimate receiver, and thus the secrecy performance may be even worse. In this case, multiple VUEs or RSUs equipped with multi-antennas could cooperate to deteriorate the eavesdropper's channel. This leads to an increase in the difference between the capacity of the legitimate channel and that of the eavesdropper channel, which explicitly increases the achieved secrecy capacity.

D. Integration of PLS with Other Technologies in V2X

Significant enhancements are possible by incorporating hybrid schemes of 4G/5G technologies that co-exist together to fit in different applications. A hybrid scheme could harness the promised advantages of different technologies if it is carefully designed. In the following, we short list a couple of technologies to be integrated with PLS to improve V2X networks as follows

1) Secure Spectrum Sharing in V2X: Given the scarce resources, non-orthogonal multiple access (NOMA) technique can play a crucial role in supporting massive connectivity by serving multiple users on the same frequency-time resource simultaneously. NOMA is heavily investigated as a potential alternative to orthogonal multiple access (OMA) techniques for 5G cellular networks and V2X network with the expected massive number of connections. A significant effort is needed to efficiently provide hybrid PLS-NOMA schemes over V2X networks. Several challenges need to be resolved such as the dissimilar security clearance of different VUEs and cooperation among users to improve the secrecy performance [10].

2) Can Millimeter-Waves Promotes PLS in V2X: The need for Gigabits transmission capacity for autonomous and non-autonomous vehicles is one of the main factors that promote millimeter-wave technology as a promising candidate for V2X. However, there are other factors, such as delays, reliability, support for both unicast/broadcast transmission, and security. By assuming millimeter-waves eNBs and RSUs that are equipped with dozens of antennas, the V2X network can provide legitimate VUEs with large array gain or multiplexing gain and thus significantly enhance secrecy performance [15]. This gain can be achieved by incorporating different beamforming techniques (i.e., analog, digital, and hybrid) that produces millimeter-waves beams much narrower than the sub-6 GHz counterparts to degrade eavesdropping channels as shown in Fig. 5.

3) Physical-Layer Authentication and Key Generation: In practice, it is very challenging to efficiently establish random keys between legitimate users in large-scale and dynamic network as in V2X. Additionally, most current physical-layer authentications are limited to D2D authentication, since they depend on the characteristics of the direct links between the transmitter and receiver. Consequently, it is critical to develop

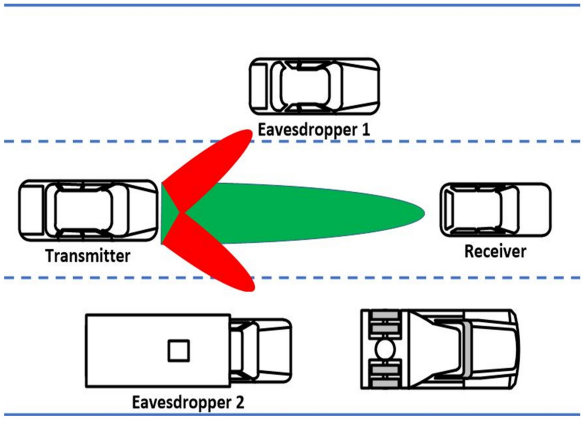

Fig. 5. V2V millimeter-wave beamforming under security threats.

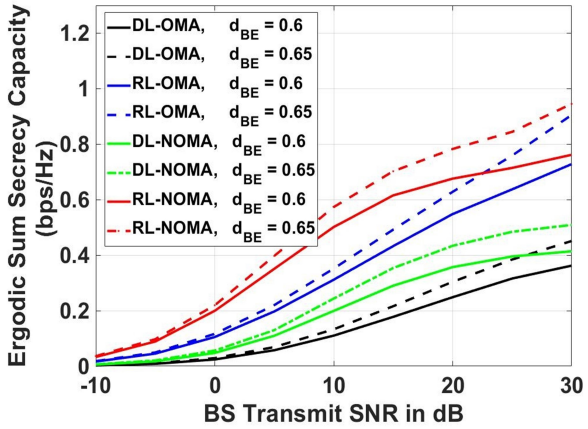

Fig. 6. Comparison of ergodic sum secrecy capacities (ESC) of NOMA and OMA schemes using both direct link and mobile relay under VPL.

a key generation process that is not restricted to the channel of directly communicating devices.

4) Integration with Higher-Layer Protocols: In order to harness benefits from PLS and higher-layers security protocols, it is an interesting challenge to consider the process of integrating security features from both higher and physical-layers [11].

IV. Case Study: Coexistence of Hybrid Challenges and Technologies

In this section, we emphasis that different challenges could exist simultaneously within a V2X scenario. For example, Fig. 3 shows multi-users that are riding a bus which is equipped to work as a moving relay to solve the VPL problem. If we would like the MR to serve those users simultaneously, the MR could exploit NOMA for serving multiple users on the same resources. However, two questions arise about the confidentiality of the users' messages in the presence of eavesdropper as follows: (1) It is an interesting research direction to investigate the PLS of multi-user against external eavesdropper in a NOMA-based moving relay V2X system. (2) What about the possibility of internal eavesdropper in V2X similar to the work investigated for a non-V2X NOMA system in [10].

In this section, we provide preliminary results to compare the ergodic sum secrecy capacity (ESC) of a two-users scenario inside a bus in the presence of an external eavesdropper. We compare four possible schemes to show the effect of exploiting the moving relay concept and the NOMA spectrum sharing on the PLS. The four schemes are given as follows

1) **DL-OMA:** In this scheme, the two users receive messages from the base station (BS) through direct links (DL) and suffers from VPL without using the moving relay's external and internal antennas. This transmission scheme is based on orthogonal multiple access (OMA), where the transmission time is divided equally between the two users into two time-slots.
2) **DL-NOMA:** In this scheme, the two users receive messages from the BS through DLs and suffers from VPL too. However, the transmission scheme is based on non-orthogonal multiple access (NOMA), where the BS transmits a linearly combined symbol to both users using power-domain NOMA [10] in one time-slot.
3) **R-OMA:** In this scheme, the two users receive OMA transmissions from the BS through decode-and-forward (DF) moving relay in four time-slots. The relay receives the message of each user using its external antenna in the one time-slot, decodes and forwards the detected message to the corresponding user using its internal antenna in another time-slot to avoid VPL effect on the inside users. Notice that the outside eavesdropper can not benefit from the relay as it suffers from VPL when MR relays messages using its internal antenna.
4) **R-NOMA:** In this scheme, the two users receive NOMA transmissions from the BS through the DF moving relay in two time-slots. The relay receives the combined message of the two users using its external antenna in the first time-slot, decodes and re-combine the detected messages, then forwards it to the two users using its internal antenna in the second time-slot.

Monte Carlo simulation have been conducted to evaluate the performance of the four investigated schemes in terms of the ergodic sum secrecy capacity (ESC) in bit/second/Hz, which is the sum of the ergodic secrecy capacities of the two users. The simulation parameters are given as follows: path-loss constant is 0.1, path-loss exponent is 3, cell radius is 500 meters, normalized bandwidth of 1 Hz, distance from the BS to the bus is 250 meters, distance from the relay internal antenna to the two users is 2 meters, and the distance from the BS to the eavesdropper (d_{BE}) is 300 and 325 meters. Fig. 6 shows the ESCs of the four schemes for two d_{BE} normalized distances with respect to the cell radius (i.e., d_{BE} = 0.6 and 0.65).

Fig. 6 shows the variations of the ESCs as a function of the BS transmit SNR in dB. The results show that the moving relay is beneficial for improving the PLS of both OMA and NOMA transmissions. We see that R-OMA outperforms DL-OMA, while R-NOMA outperforms DL-NOMA as a consequence of avoiding VPL for the users and introducing VPL to the

eavesdropper when MR relays the messages.

The results also reveal that combining non-orthogonal spectrum sharing improves the ESC, where R-NOMA outperforms all schemes. Additionally, the ESC is improved when the eavesdropper is faraway ($d_{BE} = 0.65$).

V. Conclusion

This article has provided a comprehensive overview of the applicability of physical-layer security in the area of vehicle-to-everything. The discussion has identified challenges and hurdles that need to be addressed to establish viable PLS protocols for V2X. The scope of future research when PLS meets V2X is broad, therefore, we presented a few interesting and challenging research topics we believe are worth further investigations. We share the belief, among others, that PLS will have a tremendous impact as a security approach for V2X and energy-constrained Internet-of-Things systems.

Acknowledgment

This research was partially supported by the China NSFC Grant (61872248, U1736207), in part by Benha University, Egypt research fund (Project 2/1/14), in part by Guangdong NSF 2017A030312008, Fok Ying-Tong Education Foundation for Young Teachers in the Higher Education Institutions of China(Grant No.161064), GDUPS (2015). This work is partially supported by Tianjin Key Laboratory of Advanced Networking (TANK), School of Computer Science and Technology, Tianjin University, Tianjin China, 300350. Kaishun Wu is the corresponding author.

References

[1] L. Liang, H. Peng, G. Y. Li, and X. Shen, "Vehicular communications: A physical layer perspective," *IEEE Trans. on Vehic. Tech.*, vol. 66, no. 12, pp. 10 647–10 659, Dec 2017.

[2] L. P. Qian, Y. Wu, H. Zhou, and X. Shen, "Dynamic cell association for non-orthogonal multiple-access V2S networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2342–2356, Oct 2017.

[3] X. Ge, Z. Li, and S. Li, "5G software defined vehicular networks," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 87–93, July 2017.

[4] J. Shi, Z. Yang, H. Xu, M. Chen, and B. Champagne, "Dynamic resource allocation for LTE-based vehicle-to-infrastructure networks," *IEEE Trans. Veh. Technol.*, pp. 1–1, 2019.

[5] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.* , vol. 20, no. 2, pp. 760–776, Feb 2019.

[6] V. Marojevic, "C-V2X security requirements and procedures: Survey and research directions," *arXiv preprint arXiv:1807.09338*, 2018.

[7] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 45, no. 8, pp. 1355–1387, Oct 1975.

[8] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, June 2015.

[9] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: state of the art and beyond," *IEEE Commun. Mag.* , vol. 53, no. 12, pp. 32–39, Dec 2015.

[10] B. M. ElHalawany and K. Wu, "Physical-layer security of NOMA systems under untrusted users," in *Proc. IEEE GLOBECOM*, Dec 2018, pp. 1–6.

[11] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, June 2016.

[12] N. Ahn, D. Lee, and S. Oh, "Vehicle communication using secrecy capacity," in *Proc. FTC*, K. Arai, R. Bhatia, and S. Kapoor, Eds. Cham: Springer International Publishing, 2019, pp. 158–172.

[13] X. Ge, H. Cheng, G. Mao, Y. Yang, and S. Tu, "Vehicular communications for 5G cooperative small-cell networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7882–7894, Oct 2016.

[14] X. Wang, "Moving relays in downlink multiuser networks - a physical-layer security perspective," in *Proc. IEEE VTC Spring*, June 2018, pp. 1–5.

[15] F. J. Martin-Vega, M. C. Aguayo-Torres, G. Gomez, J. T. Entrambasaguas, and T. Q. Duong, "Key technologies, modeling approaches, and challenges for millimeter-wave vehicular communications," *IEEE Commun. Mag.* , vol. 56, no. 10, pp. 28–35, Oct 2018.

Basem M. Elhalawany received the Master's degree in 2011 from Benha University, Egypt, and Ph.D in 2014 from Egypt-Japan University of Science & Technology, Egypt. Since March 2017, he is postdoctoral fellow with Shenzhen university, China. He also holds the position of an assistant professor at Benha University. He served as a visiting researcher with Kyushu University at Japan (2013-2014). His research interests include performance analysis in wireless networks, NOMA, D2D Communication, and Physical-Layer Security.

Ahmad A.Aziz El-Banna received the Master's degree in 2011 from Benha University, Egypt, and Ph.D in 2014 from Egypt-Japan University of Science & Technology, Egypt. Since March 2018, he is postdoctoral fellow at Shenzhen university, China. He also holds the position of an assistant professor at Benha University. He served as a visiting researcher with Osaka University at Japan (2013-2014). His research interests include cooperative networking, MIMO, space-time coding, IoT, and underwater communication.

Kaishun Wu received his Ph.D. degree in computer science and engineering from HKUST in 2011. After that, he worked as a research assistant professor at HKUST. In 2013, he joined SZU as a distinguished professor. He has co-authored 2 books and published over 90 high quality research papers in international leading journals and primer conferences. He is the inventor of 6 US and over 80 Chinese pending patent. He received 2012 Hong Kong Young Scientist Award, 2014 Hong Kong ICT Awards: Best Innovation and 2014 IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award. He is an IET Fellow.