Unmanned Aerial Vehicle Meets Vehicle-to-Everything in Secure Communications

Bodong Shang, Lingjia Liu, Junchao Ma, and Pingzhi Fan

The authors embrace UAV to V2X communications to enhance V2X security from the physical layer security's perspective. To be specific, they present security problems in V2X systems, highlight security threats in V2X networks, and illustrate some potential applications of UAVs in V2X security. Open problems for UAV-assisted V2X secure communications are also discussed.

Abstract

Enabling vehicles to communicate with other vehicles, infrastructure, pedestrians, and everything for use cases such as road safety, automatic driving, and infotainment is important for the future cellular networks. However, some vehicle-to-everything (V2X) services need secure transmissions and should be prevented from eavesdropping. Physical layer security, an information-theoretical framework, utilizes the randomness of underlying channels to ensure secrecy in the physical layer. Different from ground communications, unmanned aerial vehicles (UAVs) create line-of-sight connections to vehicles and mobile users making them an ideal platform to conduct physical layer security strategies. In this article, we embrace UAV to V2X communications to enhance the V2X security from the physical layer security's perspective. To be specific, we present security problems in V2X systems, highlight security threats in V2X networks, and illustrate some potential applications of UAVs in V2X security. Open problems for UAV-assisted V2X secure communications are also discussed.

Introduction

Recently, vehicle-to-everything (V2X) communication has emerged as a new paradigm for vehicles to be connected with everything in the proximity including other vehicles, infrastructure, pedestrians, Internet networks, and so on [1–3]. Meanwhile, secure information transmissions become critical in current data-oriented life, especially for certain services such as credit card information transfer, e-paying, health information, and particularly for V2X communications of control messages, maneuver command, and so on [4, 5]. Secure file transfers to customized vehicles also require secure V2X communications. Therefore, it is important to investigate strategies that facilitate more intelligent and secure future transportation systems.

Third Generation Partnership Project (3GPP) LTE-Advanced Pro spends much effort to address the potential security issues in V2X communications. To be specific, [6] lists a series of potential attacks and privacy issues in different V2X applications. Reference [7] stipulates security requirements based on different V2X services and their corresponding solutions. For autonomous driving, [8] discusses the update of a software module called the electronic control unit (ECU) that is responsible for controlling the electronics within a vehicle system and is of critical importance to an automatic vehicle. Moreover, security check is needed in the update process of an ECU to prevent updating from a wrong source and a wrong version.

Compared to the conventional security methods for file transfer today, which are based on bit-level cryptographic techniques and different protocols for the data processing stack, physical layer security techniques leverage the fluctuation of wireless channels of intended receivers and eavesdroppers. There are three major advantages of employing physical layer security techniques. First, it avoids the cryptographic key distribution in a highly complex and distributed wireless network, reducing the probability of filching important cryptographic information. Second, it does not rely on the computational complexity at the desired receivers. Third, the transmitters can cooperatively transmit information to receivers and can proactively interfere eavesdroppers by sending artificial noise (AN) jamming signals by pointing beams toward the eavesdroppers. On the other hand, physical layer security has several limitations. For example, it relies heavily on knowledge of underlying wireless channels.

Furthermore, the assumption that the channel between legitimate transceivers is better than that between legitimate transmitter and the eavesdropper reduces the applicability of physical layer security strategies in practical wireless networks.

In this article, we embrace unmanned aerial vehicles (UAVs) to V2X to enhance V2X security from the physical layer security's perspective. With UAVs, line-of-sight (LoS) connections can be created between UAVs and moving vehicles. Accordingly, UAV-assisted V2X communications can be used to improve the physical layer security of V2X communications [9–11] by greatly alleviating major limitations of underlying strategies. In addition, the flexible deployment of UAVs enables applications in tracking and pointing accurate AN jamming beams toward wiretappers [12]. Simple UAV-assisted secure V2X

Supports from U.S. National Science Foundation (ECCS-1802710, ECCS-1811497, and CNS-1811720) are acknowledged.

Digital Object Identifier: 10.1109/MCOM.001.1900170

Bodong Shang and Lingjia Liu are with Virginia Tech; Junchao Ma and Pingzhi Fan are with Southwest Jiaotong University; Junchao Ma is currently a visiting student at Virginia Tech.

0163-6804/19/$25.00 © 2019 IEEE

communications is shown in Fig. 1, where UAVs act as jammers and/or aerial mobile relays to interfere eavesdroppers' received signals and/or enhance the desired signal strength resorting to the underlying LoS links.

However, despite various benefits and applications of UAVs, there are still many challenges for adopting UAVs in wireless networks. For example, due to the limited size and payload capacity of a UAV, the battery lifetime is constrained by the onboard energy. Since the main power consumption of a UAV's battery is to fly rather than to communicate, the limited battery lifetime prevents long operation time of UAVs. Therefore, energy-efficient designs are critical for UAV systems.

In this article, we first illustrate security threats in vehicle-to-vehicle (V2V) communications considering passive, active, and collusive eavesdroppers and their corresponding attack patterns. Then we present potential applications of UAVs in V2X security enhancement. Open problems for UAV-assisted V2X secure communications are also discussed.

Security Threats in V2V Communications

In this section, we discuss security threats in V2V communications under scenarios of passive, active, and collusive eavesdroppers, shown in Fig. 2.

Passive Eavesdroppers

In many cases, eavesdroppers hide their existence and attempt to decode the information sent from transmitters to receivers. It is envisioned that multiple-input multiple-output (MIMO) techniques will be enabled to enhance the communication performance of the underlying V2V link. Since roads are generally straight, moving vehicles are approximately located in a line. In V2V communications, potential passive eavesdroppers may be on the road driving in the same direction as the receiving vehicle, shown at the top of Fig. 2. In this case, the information leakage can be extremely severe since the main lobe of the beamformed information covers potential passive eavesdroppers in a certain time period. On the other hand, information leakage may be little for the case where the passive eavesdroppers are statically located along the road. This is because these passive eavesdroppers may not receive the pointing beam coherently sent by transmitting vehicles. In addition, passive static eavesdroppers may not even know when and which of the moving vehicle will transmit in a short passing time period. Meanwhile, the received signal strength at passive static eavesdroppers will fluctuate rapidly due to the mobility of the transmitter.

Active Eavesdroppers

In the time-division duplex (TDD) mode of vehicular MIMO communications, a legitimate receiver sends pilot signals to a corresponding transmitter. After estimating the channel, the transmitter sends precoded symbols to the receiver. However, some eavesdroppers can pretend to be legitimate receivers by sending the same pilot signals to the transmitter. In this way, the beamform will be pointed to the eavesdropper instead of the intended receiver,

Figure 1. UAV-assisted V2X secure communications.

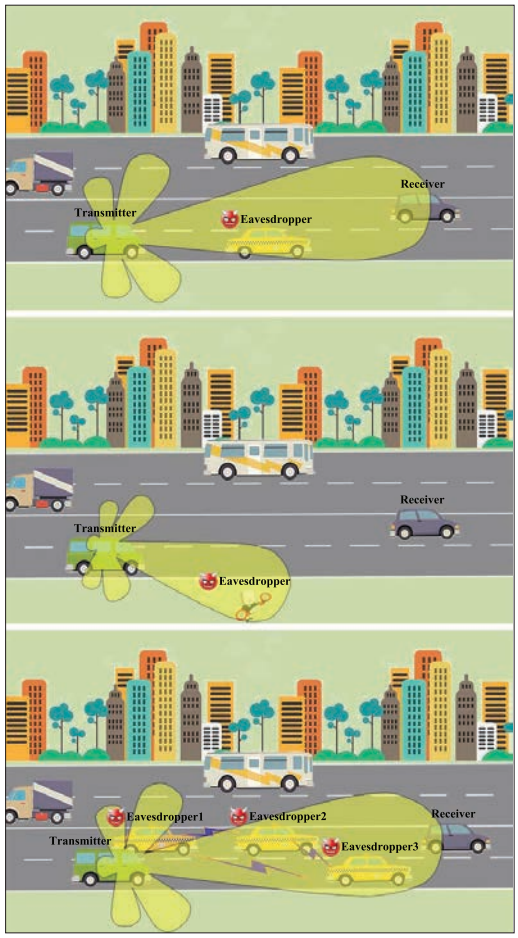

Figure 2. Security threats in V2V communications.

as shown most clearly in the middle of Fig. 2. This active pilot contamination attack can occur when eavesdroppers are statically located along the road in V2V communications. Under this attack, the eavesdropper can receive consecutive beams during a short passing time period with higher signal strength compared to that of the legitimate receiver. If the active pilot contamination attack is detected, the transmitting vehicle can simply switch to silent mode until the legitimate transceivers drive further away from the active static eavesdropper. However, this "simple" approach reduces the efficiency of the underlying V2V communication. When

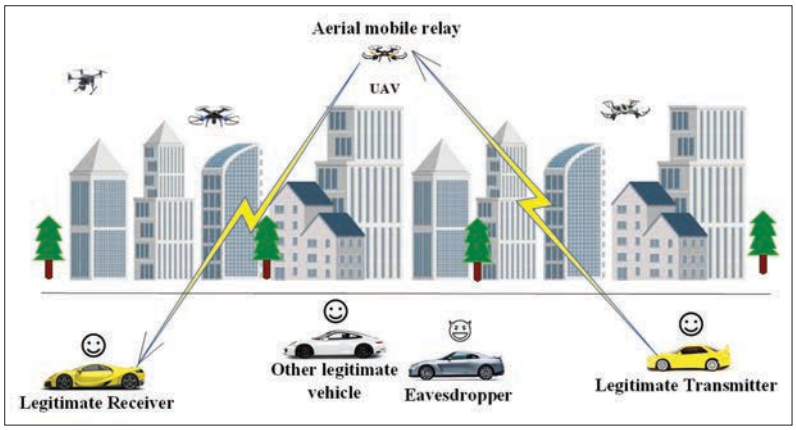

Figure 3. UAV performs as an aerial mobile relay in V2V communications.

the active eavesdropper is able to move along the road, it can track the legitimate transmitter and continuously conduct pilot contamination attacks. Therefore, advanced strategies, such as UAV-assisted V2V secure communications (on account of the agility of UAVs), need to be developed and explored to overcome such security threats.

Collusive Eavesdroppers

If there are multiple eavesdroppers and they can collude to cooperatively exchange and decode the wiretapped information, the secrecy outage would increase, and the secrecy rate may be significantly reduced, as shown in the bottom of Fig. 2. In this case, collusive eavesdroppers experience different channel variations from the transmitting vehicle, and they can utilize techniques like energy accumulation or mutual information accumulation to increase the interception rate. Furthermore, collusive eavesdroppers can redesign their precoding and beamforming matrices considering the effects of their changed relative positions resulting from the relative movement. Therefore, collusive eavesdroppers can filch the information cooperatively and achieve improved eavesdropping performance. Meanwhile, in V2V communications, due to the moving nature of vehicles, collusive eavesdroppers may gather together, forming a cluster around the desired receiver to cooperatively filch the information. In any case, the security performance of the legitimate vehicles will decrease dramatically. It is critical to design efficient secure algorithms and leverage advanced techniques to combat collusive eavesdroppers in V2V communications.

Potential Applications of UAVs in V2X Security

In this section, we present several potential applications of UAVs in V2X security.

Aerial Mobile Relays for V2X Communications

There are usually many blockages such as buildings and trees between roads. When V2X communications happen on different roads, the underlying links are non-line-of-sight (NLoS), resulting in low received signal powers. On the other hand, when V2X communication occurs on the same road with a long transceiver distance, other vehicles moving on the same road may act as blockages. This impedes the LoS link of the legitimate transmitter-receiver vehicle pair, and a positive secrecy rate may not be guaranteed. To protect the V2X secure communications suffering from dissatisfying channel conditions of the desired signals, we can utilize UAVs as trusted relays to increase the secrecy performance by providing reliable LoS transmissions of ground-to-air (G2A) and air-to-ground (A2G) links. In addition, when there are other legitimate vehicles in the proximity of an eavesdropper, sending AN jamming signals from the UAV may interfere with other legitimate vehicles. Therefore, in this case, the UAV is expected to perform as an aerial mobile relay to forward the legitimate transceiver's information by using spatial beams, as shown in Fig. 3. When a UAV is equipped with multiple antennas to perform MIMO communications as a trusted relay, according to the 3GPP realistic antenna patterns [13], the information leakage by the side-lobes at the UAV should be considered in the system operation. The optimal altitude and the beamforming matrix of the UAV need to be carefully designed. It is important to note that the scalability of the approach can be improved when an aerial mobile relay can serve multiple vehicle users using techniques such as multi-user MIMO [14].

Security Region Provided by UAV Jammer

When the potential eavesdroppers are unknown to legitimate vehicles and assisting UAVs, a UAV can act as a friendly jammer in the sky by providing an effective security region on the ground in which the signal-to-interference-plus-noise ratio (SINR) at a location point is below a certain value statistically. In this case, the transmit power and the trajectory of the UAV jammer should be carefully designed, since it may increase the outage probability of other V2X communications when the UAV jammer moves along or hovers on the road. A UAV jammer may be refrained from extending its protection region due to the limited energy availability. Therefore, the position of the UAV jammer plays an important role in maximizing legitimate users' coverage probability and/or minimizing potential eavesdroppers' intercept probability. In addition, due to the mobility of underlying UAV jammers, UAV jammers can be scheduled to move to different places according to the diverse traffic densities on roads and the various required secure services by vehicles.

Flying Distributed MIMO

Although UAVs can carry multiple antennas to bring the beamforming gain of jamming signals, the number of antennas at a UAV would be limited due to elevating the heavy burden of antennas and processing units. On the other hand, UAVs can cooperatively exploit the spatial domain of A2G fading channels to generate narrow jamming beams toward multiple eavesdroppers in a V2X system. The use of simultaneously transmitted narrow beams with LoS channel links definitely improves the secrecy performance of V2X communications by increasing the interference at eavesdroppers. Such distributed MIMO (cooperative MIMO) communications enables

UAVs to form self-organizing UAV swarm networks. However, forming a UAV swarm to perform distributed MIMO communication cooperatively is indeed difficult to achieve nowadays because it requires increased overhead and more energy consumption.

Detecting and Tracking Vehicle Eavesdroppers

Due to the high altitude of UAVs, a UAV can detect and locate potential vehicle eavesdroppers on the road by using its optical camera and synthetic aperture radar with intelligent image and video processing technology and pattern recognition. Furthermore, due to its agility and mobility, a UAV can track the moving vehicle eavesdropper in the 3D airspace and provide continuous and precise AN jamming signals to the adversary. Other than performing proactive detection, a UAV can also receive reports regarding the information of a known/detected eavesdropper. These reports may be obtained from a legitimate transceiver vehicle pair that already detects the underlying eavesdropper. Due to the strong channel gain of the underlying LoS A2G links, a UAV can provide strong jamming signals to eavesdroppers to significantly reduce the interception rate. When the number of eavesdroppers increases, UAVs may need to cooperate with vehicular jammers to improve the scalability.

In the following, we compare the V2V communication secrecy rate under three cases: A) there is a UAV jammer; B) there is a ground jammer; and C) there is no jammer. The network scenario of case A is shown in Fig. 4. In case B, we consider that the legitimate receiving vehicle serves as the receiver as well as a ground jammer. Therefore, it broadcasts AN jamming signals to its nearby regions to prevent information interception from eavesdroppers.

The V2V secrecy rate is shown in Fig. 5 over simulation time. We assume that the velocities of transmitter, receiver, passive eavesdropper, and UAV are constant: V_T = 25 m/s, V_R = 20 m/s, V_E = 25 m/s, and V_U = 30 m/s, respectively. The bandwidth is 10 MHz, and the noise power is −90 dBm. The ground-to-ground communication links experience Rayleigh fading, and the path loss exponent is 4. The channel model for A2G links follows that specified in [15]. The flight height of the UAV is 50 m, and the number of antennas at the UAV is 4. Transmit powers of the legitimate transmitter, the ground jammer, and the UAV jammer are 0.5 W, 0.2 W, and 0.1 W, respectively. The initial distance between the legitimate vehicle transmitter and receiver is 500 m, and the initial distance between transmitter and eavesdropper is 100 m. The initial horizontal distance between UAV and eavesdropper is 300 m. We observe that, compared to cases B and C, the secrecy rate of V2V communication with the help of a UAV jammer in case A can be improved due to the small attenuation of jamming signals in the A2G links. At the eavesdropper, the received strong AN jamming power generated from the UAV jammer impairs the eavesdropper's decoding process of its intercepted information.

Figure 6 compares the V2V communication secrecy rate with respect to various UAV flight velocities. The results are averaged on the simulation time T = 400 s. We can observe that there is an optimal UAV velocity to maximize the V2V communication secrecy rate. This is because when the UAV velocity is small, it is difficult for the UAV to catch up with the moving eavesdropper and provide jamming signals. On the other hand, when the UAV velocity becomes large, the UAV may pass the moving eavesdropper quickly. Accordingly, the time

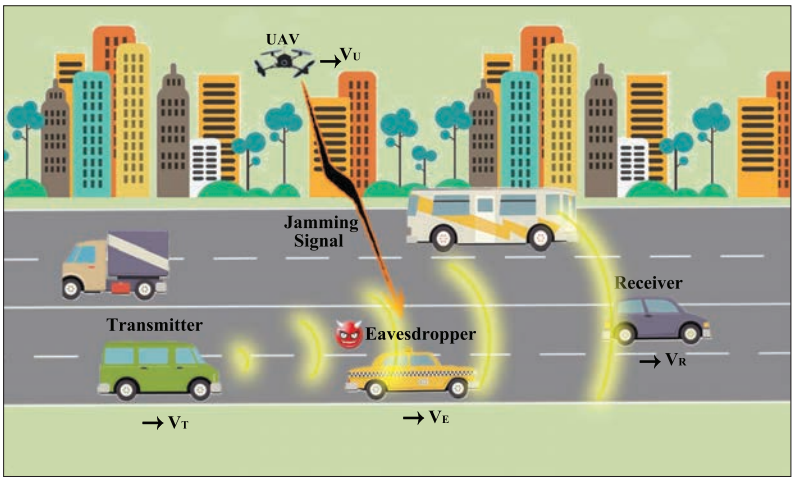

Figure 4. A UAV sends jamming signals to guarantee V2V secure communications.

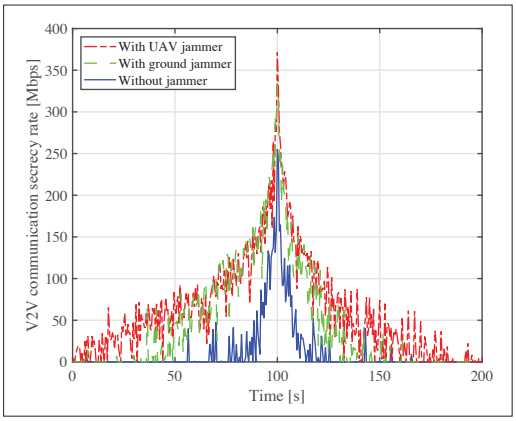

Figure 5. Secrecy rate of V2V communications over simulation time.

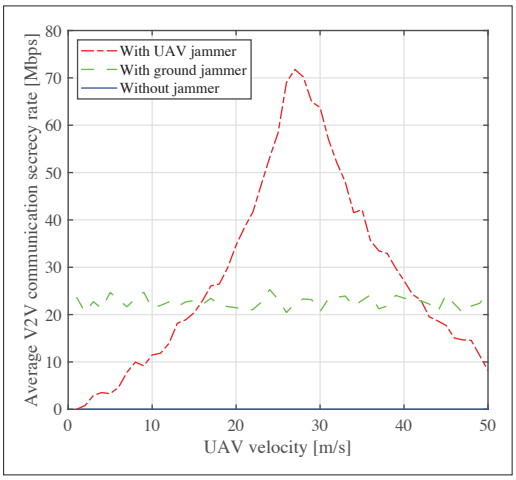

Figure 6. Average secrecy rate of V2V communications with respect to the UAV velocity for an eavesdropper traveling at constant speed of 25 m/s.

The pricing strategy for security services and the economic interactions between the requester of security communications and the service provider are of significance to be investigated. In addition, if the UAVs are possessed by private users, auction and/or bargaining based security services offering in such V2X communications systems are also important research topics.

duration of the guaranteed V2V secure communication is reduced, which decreases the average V2V communication secrecy rate in a certain time period.

Challenges and Opportunities

In this section, we briefly illustrate some important research challenges and potential opportunities for UAV-assisted V2X secure communications.

Trajectory Design for UAVs

Previous works on UAV trajectory design for cellular security systems assume that the locations of ground legitimate users and eavesdroppers are fixed while optimizing the UAV's horizontal trajectory. For V2X security systems, the mobility characteristics of legitimate vehicles and eavesdroppers, and the opportunistic NLoS transmission links due to the changed elevation angles should be considered. In addition, the altitude of a UAV and its horizontal trajectory should be jointly designed for V2X secure communications when UAV jammers provide security regions. Higher altitude of the UAV jammer leads to less interference at legitimate vehicles. However, this will also increase the intercept probability of eavesdroppers.

Resource Allocation for UAV-V2X Systems

Which types of spectrum resources (licensed, unlicensed, spectrum sharing) can be used for UAVs in V2X communications systems still remains open. Efficient spectrum and power allocation strategies for different levels of V2X security required by various legitimate vehicles are important to investigate. The coexistence between UAV trusted relays and terrestrial communications also needs to be carefully studied. In the meantime, the interference power at other legitimate vehicles and users generated by UAVs' jamming signals should be limited under a certain threshold value, which leads to a joint design of resource allocation and UAVs' trajectory.

Precoding and Jamming Vectors Design

For a UAV equipped with MIMO or a flying distributed antenna system, the transmit and jamming beamforming can be jointly designed to enhance the physical layer security. Note that it is possible to measure the channel gain between UAV and eavesdropper to evaluate the secrecy performance, since the LoS link is mainly determined by the link distance if the locations of the potential eavesdroppers are known a priori. Practical issues for the design of precoding and jamming vectors at a UAV are the frequent channel feedback and the reference signal sent by moving vehicles. In addition, designing secure approaches to defend the pilot contamination attack is also important when the adversaries are active eavesdroppers on and beside the roads.

UAV Deployment and V2X Secrecy Rate

For the network planning and secrecy performance analysis of such UAV-assisted V2X communication systems, we can use the tools from stochastic geometry to obtain the ergodic secrecy rate and to optimize the density and altitude of UAVs from a system-level perspective. The roads can be modeled as a Poisson line process, and the vehicles can be modeled as 1D Poisson point process, thereby forming a Cox process. Network design insights can be concluded by deriving the coverage probability of legitimate vehicles, the intercept probability of eavesdroppers, and the ergodic secrecy rate. Such statistical analysis may also shed light on capturing the randomness of the locations of eavesdroppers as well as the unknown adversaries given by the density of eavesdroppers on and beside roads.

Network Energy Efficiency

Driven by both economical and environmental interests, service providers will pay more attention to energy-efficient communication strategies for "green communications." In addition, due to the fact that UAVs are always energy constrained, it is crucial for service providers to efficiently utilize the battery energy carried by UAVs. Therefore, security energy efficiency, defined as the ratio of the security rate and the total energy consumption in UAV-V2X networks, is a reasonable metric to reflect "green secure communications." With this in mind, energy-efficient algorithms are expected to be designed.

Economics in V2X Security

In V2X security systems, additional spectrum and power consumption for secure communications should be considered by the service provider. Accordingly, V2X security communications should be categorized into different security levels and can be treated as customized services for V2X communications with different prices. As such, the pricing strategy for security services and the economic interactions between the requester of security communications and the service provider are of significance for investigation. In addition, if the UAVs are possessed by private users, auction and/or bargaining-based security services offered in such V2X communications systems are also important research topics.

Conclusion

This article discusses the blueprint of applying UAVs to V2X secure communications. The security threats in V2X communications are presented. We further elaborate the roles and the potential applications of UAVs in V2X security. Challenges and research opportunities are also presented.

References

[1] J. E. Siegel, D. C. Erb, and S. E. Sarma, "A Survey of the Connected Vehicle Landscape Architectures, Enabling Technologies, Applications, and Development Areas," *IEEE Trans. Intell. Transp. Sys.*, vol. 19, no. 8, 2018, pp. 2391–2406.
[2] H. Seo *et al.*, "LTE Evolution for Vehicle-to-Everything Services," *IEEE Commun. Mag.*, vol. 54, no. 6, June 2016, pp. 22–28.
[3] F. Abbas, P. Fan, and Z. Khan, "A Novel Low-Latency V2V Resource Allocation Scheme Based on Cellular V2X Communications," *IEEE Trans. Intell. Transp. Sys.*, 2018, pp. 1–13.
[4] K. J. Ahmed and M. J. Lee, "Secure LTE-Based V2X Service," *IEEE Internet of Things J.*, vol. 5, no. 5, 2018, pp. 3724–32.
[5] B. Brecht *et al.*, "A Security Credential Management System for V2X Communications," *IEEE Trans. Intell. Transp. Sys.*, vol. 19, no. 12, 2018, pp. 3850–71.
[6] 3GPP TR33.885, "Study on Security Aspects for LTE Support of Vehicle-to-Everything (V2X) Services (Release 14)," 2017.
[7] 3GPP TS33.185, "Security Aspect for LTE Support of Vehicle-to-Everything (V2X) Services (Release 15)," 2018.
[8] 3GPP TR22.886, "Study on Enhancement of 3GPP Support for 5G V2X Services (Release 16)," 2018.

[9] H. Menouar *et al.*, "UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges," *IEEE Commun. Mag.*, vol. 55, no. 3, Mar. 2017, pp. 22–28.
[10] Z. Yuan *et al.*, "Ultra-Reliable IoT Communications with UAVs: A Swarm Use Case," *IEEE Commun. Mag.*, vol. 56, no. 12, Dec. 2018, pp. 90–96.
[11] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless Communications with Unmanned Aerial Vehicles: Opportunities and Challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, May 2016, pp. 36–42.
[12] G. Zhang *et al.*, "Securing UAV Communications Via Joint Trajectory and Power Control," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, 2019, pp. 1376–89.
[13] G. Geraci *et al.*, "Understanding UAV Cellular Communications: From Existing Networks to Massive MIMO," *IEEE Access*, vol. 6, 2018, pp. 67,853–65.
[14] L. Liu *et al.*, "Downlink MIMO in LTE-Advanced: SU-MIMO vs. MU-MIMO," *IEEE Commun. Mag.*, vol. 50, no. 2, Feb. 2012, pp. 140–47.
[15] R. Amorim *et al.*, "Radio Channel Modeling for UAV Communication over Cellular Networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 4, Aug 2017, pp. 514–17.

Biographies

Bodong Shang received his M.S. degree from the School of Telecommunications Engineering at Xidian University, Xi'an, China, in 2018. He is currently pursuing a Ph.D. degree in the Bradley Department of Electrical and Computer Engineering at Virginia Tech, Blacksburg. His research interests include UAV, V2X security, and MIMO.

Lingjia Liu (ljliu@ieee.org) received his Ph.D. degree in electrical and computer engineering from Texas A&M University. He is an associate professor in the Bradley Department of Electrical and Computer Engineering at Virginia Tech. His research interests include machine learning for wireless communications, 5G and beyond, and the Internet of Things.

Junchao Ma received his M.S. degree in wireless communication from Southwest Jiaotong University, Chengdu, China, in 2014, where he is currently pursuing a Ph.D. degree. His research interests include V2X communication, point cloud, video coding, mobile edge caching, and age of information.

Pingzhi Fan received his M.Sc. degree in computer science from Southwest Jiaotong University in 1987 and his Ph.D. degree in electronic engineering from Hull University, United Kingdom, in 1994. He is currently a professor and director of the Institute of Mobile Communications, Southwest Jiaotong University. His research interests include vehicular communications and wireless networks.