Opportunities for Physical Layer Security in UAV Communication Enhanced with Intelligent Reflective Surfaces

Wali Ullah Khan, Eva Lagunas, Zain Ali, Muhammad Awais Javed, Manzoor Ahmed, Symeon Chatzinotas,
Björn Ottersten, and Petar Popovski

Abstract

Unmanned aerial vehicles (UAVs) are an important component of next-generation wireless networks that can assist in high data rate communications and provide enhanced coverage.Their high mobility and aerial nature offer deployment flexibility and low-cost infrastructure support to existing cellular networks and provide many applications that rely on mobile wireless communications. However, security is a major challenge in UAV communications, and physical layer security (PLS) is an important technique to improve the reliability and security of data shared with the assistance of UAVs. Recently, the intelligent reflective surface (IRS) has emerged as a novel technology to extend and/or enhance wireless coverage by reconfiguring the propagation environment of communications. This article provides an overview of how the IRS can improve the PLS of UAV networks. We discuss different use cases of PLS for IRS-enhanced UAV communications and briefly review the recent advances in this area. Then, based on the recent advances, we also present a case study that utilizes alternate optimization to maximize the secrecy capacity for an IRS-enhanced UAV scenario in the presence of multiple Eves. Finally, we highlight several open issues and research challenges to realize PLS in IRS-enhanced UAV communications.

Introduction

The great demand for high data rates, massive connectivity, and protection from impending security attacks challenge next-generation wireless communication systems. In this regard, unmanned aerial vehicles (UAVs) can play a vital role in supporting reliable and secure communications without infrastructure coverage. UAVs provide several benefits in terms of cost-friendly rapid infrastructure deployment in low signal coverage zones, mobile relay nodes to enhance coverage range, communication access points in emergency areas, and enabling physical layer security (PLS) [1]. Compared to traditional terrestrial communications, UAVs provide strong channel conditions due to line-of-sight (LoS) transmission links. Therefore, there is high demand for deploying large numbers of UAVs to support next-generation wireless networks [2]. UAVs can be used for different applications in transportation systems, cellular communications, agriculture, and emergency management. In addition, the use of UAVs will be an integral part of next-generation wireless networks to support ultra-low-latency and extremely reliabley applications [3].

Despite the promising features, several challenges exist in deploying UAVs for next-generation wireless networks. Among different challenges, energy efficiency, security, and reliability are the major challenges in developing efficient UAV communications. Due to limited energy reserves onboard, intelligent energy usage and replenishment mechanisms are required for energy-aware UAV deployments and operations. Furthermore, with the increase in malicious attacks on static and mobile networks, it is critical to use robust cryptographic algorithms to mitigate them. However, more complex cryptographic algorithms entail significant overhead, thus increasing the packet size. It also significantly increases the required bandwidth and puts more transmission burden on the available spectrum. As a result, transmission reliability is compromised, and network capacity is reduced.

Cryptography-based information confidentiality seems inapplicable for next-generation technologies and networks for the following reasons: Cryptography algorithms are based on computationally hard problems, and today's adversaries have unlimited computing resources support and can be disastrous for crypto-systems [4]. In addition, conventional centralized key sharing and management processes for distributed networks like the Internet of Things (IoT), UAVs, and vehicular networks are challenging. Moreover, significant communication overhead is caused by complex upper-layer operations and can increase the cost and complexity of user equipments/devices. To overcome the challenges faced by traditional cryptographic security techniques, physical layer security (PLS) is a valuable technique

Wali Ullah Khan, Eva Lagunas, Symeon Chatzinotas, and Björn Ottersten are with the University of Luxembourg, Luxembourg; Zain Ali is with the University of California, Santa Cruz, USA; Muhammad Awais Javed is with COMSATS University Islamabad, Pakistan; Manzoor Ahmed is with Qingdao University, China; Petar Popovski is with Aalborg University, Denmark.

Digital Object Identifier:
10.1109/MWC.001.2200125

1536-1284/22/$25.00 © 2022 IEEE

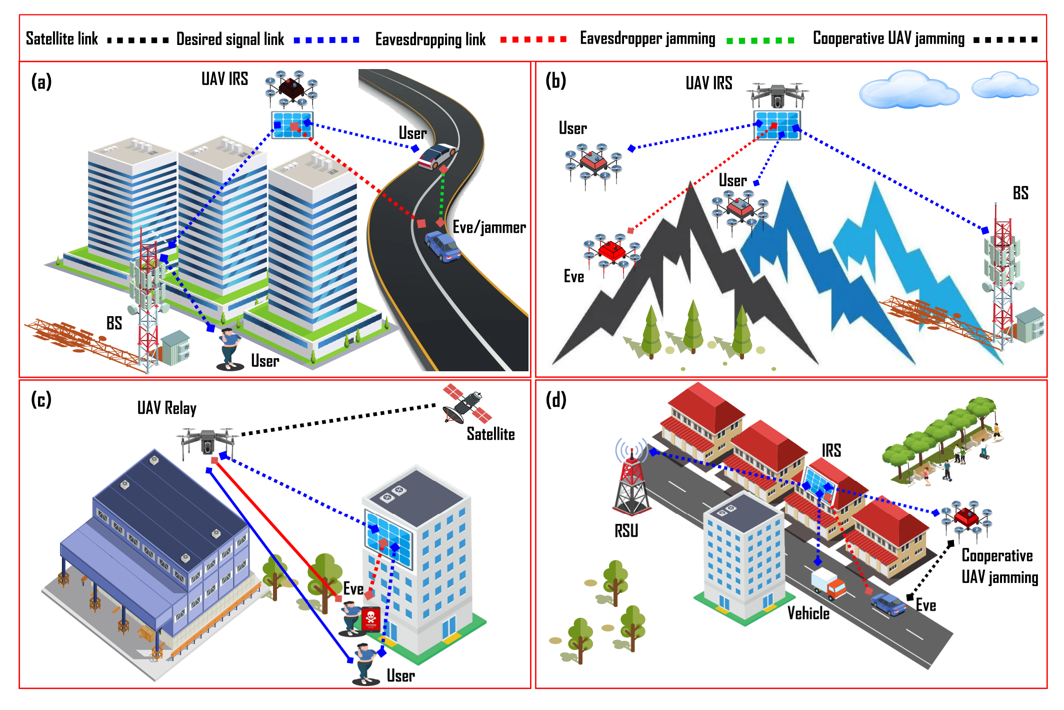

FIGURE 1. Different cases of IRS-enhanced UAV communication.

that can work in conjunction with cryptographic techniques to secure UAV communications while maintaining the reliability of transmissions [5]. PLS uses the randomness of the wireless medium to prevent transmissions from eavesdropping. However, as PLS-based UAV communications rely on the strength of signal transmissions between users and UAVs, their performance is degraded in low signal coverage areas and non-LoS (NLoS) scenarios [6].

The intelligent reflective surface (IRS) has recently emerged as a technology due to its high energy efficiency. IRS is very effective for secure coverage extension in non-line-of-sight communication scenarios. It can efficiently assist signal delivery if the transmitter and receiver do not have a direct link. IRS consists of a large number of passive reflecting elements that can intelligently reconfigure the signal direction toward the receiver. According to the IRS principle, the phase of the incident signal from the transmitter can be smartly shifted toward the receiver without consuming any energy. IRS has recently been integrated into UAV networks for energy-efficient and secure communications. IRS can improve the PLS of UAV communications by constructively adding the signal to a user and destructively to an Eve [7, 6, 8]. As a result, the secrecy performance of PLS in many UAV-to-UAV and UAV-to-user communication scenarios can be improved using IRS. However, a major challenge that hinders widespread adoption of PLS is the difficulty of accurately detecting Eves and their locations. UAVs can be equipped with cameras and sensors in such a way that they can map the environment and detect potential Eves.

This article provides an overview of IRS-enhanced PLS for UAV communications. We present four major use cases of IRS-enhanced PLS in UAV communications related to improving secrecy rate in NLoS scenarios, satellite communications, mobile IRS-enhanced UAVs, and cooperative jamming. We also discuss the recent work in the literature related to IRS-enhanced PLS for UAV communications. Moreover, we present a UAV communications-based case study highlighting the significance of IRS for PLS. Further, we propose an alternate optimization-based algorithm to maximize the secrecy rate of UAV communications in the presence of IRS. Finally, we highlight several open research challenges to realize IRS and PLS-based UAV communications.

IRS-Enhanced PLS for UAV Communication: Overview, Use Cases, and Recent Advances

This section provides an overview of IRS-enhanced PLS for UAV communications, and highlights several use cases and recent work in this area (Fig. 1).

Overview of IRS-Enhanced PLS for UAV Communications

PLS leverages wireless channel characteristics to improve the information received at the legitimate destination compared to Eve. There are different techniques to achieve efficient PLS, including coding, signal processing, transmission power control, and jamming techniques [5, 9]. PLS can provide efficient and secure key generation, authentication, and defense against Eves. A significant advantage of using PLS for security is its low cost of computation and packet sizes. PLS is thus particularly useful for energy-constrained devices such as UAVs and IoT nodes.

IRS is composed of meta-surfaces that can reflect an incoming signal toward the desired destination. A key feature of IRS is its reconfigurability, which allows controlling the phase shifts of its elements so that signal reception at the destination can be maximized. IRSs can be placed as standalone surfaces or installed at buildings and placed

IRS can be installed at strategic locations such as buildings, or a mobile UAV IRS can be used. IRS will improve the rate between the two UAVs or between the UAV and BS, thus improving the secrecy rate.

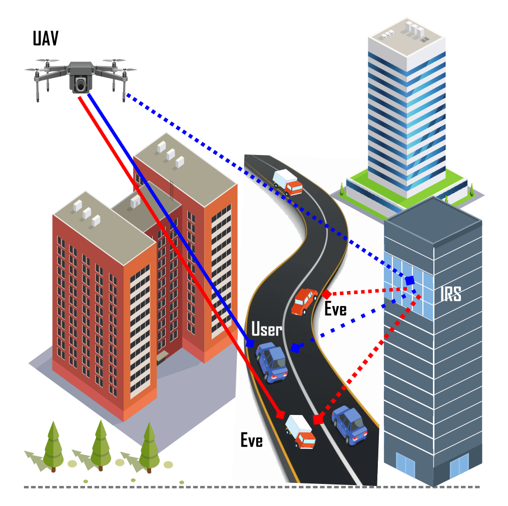

FIGURE 2. System model.

in areas where signal coverage is low. IRS can be beneficial in NLoS communication scenarios, improving the reliability of communications [6, 8].

IRS can play a vital role in improving information confidentiality of UAV communications by providing an enhanced secrecy rate. In fact, UAVs can also be furnished with IRS and assist in secure communication in low coverage areas on the fly. With the help of reconfigurable reflecting elements, IRS can significantly improve the PLS of UAV communications. Specifically, IRS adds the incident wireless signal constructively to the user receiver but destructively to the Eve. Moreover, it can also act as a green jammer to attack Eve by producing jamming signals without consuming external energy. Besides security problems, IRS-assisted UAVs can provide reliable and energy-efficient communications, thus improving the battery life of UAVs.

Use Cases of IRS-Enhanced PLS for UAV Communications

IRS can provide multiple benefits to improve PLS working in UAV networks. We discuss a few of these use cases in this subsection as highlighted in Fig. 2.

Mobile IRS-Enhanced UAVs: The mobility of a UAV can be used in collaboration with the intelligent signal reflection feature of IRS to enhance ground-to-ground and air-to-air communications, as presented in Fig. 2a. IRS can be placed on a UAV to improve the communications and security of vehicular networks (for vehicle-to-vehicle communication). The base station (BS) can identify the areas on the road where the secrecy rate is low based on the channel quality values received from different vehicles and Eves. The mobile IRS can be directed to areas where PLS is compromised and act as a relay to improve the desired signal and the secrecy rate.

Improved Secrecy Rate in Non-LoS Scenarios: UAV communication faces challenges of difficult terrain and signal blockages. As shown in Fig. 2b, two UAVs connected in a mountainous area can face signal disconnections, making PLS less effective. An eavesdropper UAV can take advantage of this scenario as the secrecy rate will be reduced. Similarly, in air-to-ground communication between a UAV and a BS, such LoS blockages can reduce the security levels. IRS can be very effective in the above scenarios as it can improve the LoS communications in case of signal blockages. IRS can be installed at strategic locations such as buildings, or a mobile UAV IRS can be used. IRS will improve the rate between the two UAVs or between the UAV and BS, thus improving the secrecy rate.

Satellite Communications: Satellite communications use IRS as a relay for transmitting signals to the ground BS as described in Fig. 2c. Generally, the downlink communication from UAV to BS suffers attenuation and fading. Therefore, IRS can be installed between the path of UAV and BS (i.e., on buildings), thus facilitating better communication of the BS with the satellite. Similarly, UAVs equipped with IRS can be configured such that satellite signals can reach the desired destination with high reliability.

Cooperative Jamming: Eavesdropper jamming signals are a significant threat to PLS in UAVs. A sample scenario is shown in Fig. 2d, where an Eve sends jamming signals to the user. By using IRS, the signal-to-noise ratio of the desired signal can be further strengthened. In addition, intelligent beamforming at IRS can decrease the signal strength of the actual message received by the Eve. Moreover, cooperative jamming in which the BS generates artificial noise and IRS directs it to the Eve can mitigate the impact of jamming attacks by the Eve.

Recent Advances in IRS-Enhanced PLS for UAV Communication

Little work has been reported related to IRS-enhanced PLS for UAV communications (Table 1). The work in [10] proposes physical security and an IRS-enhanced UAV framework. The scenario considers UAV transmission to the desired destination node in the presence of an Eve that can intercept the message. The work aims to jointly optimize the UAV's transmit power and trajectory and control IRS's phase shift to maximize the secrecy rate using an alternate convex approximation algorithm. The algorithm selects an initial transmit power and UAV trajectory values to obtain an optimal solution and calculates the IRS phase shift value. Then the secrecy rate for the above parameters is also evaluated. The transmit power and trajectory are evaluated alternately until the algorithm converges and provides the maximum secrecy rate. Results show that the secrecy rate of the IRS-enhanced UAV network is maximized. In [11], the authors consider a millimeter-wave (mmWave) network in which a single UAV BS transmits the message to the desired destination node in the presence of a single Eve. The article aims to design the position and beamforming of both UAV BS and IRS to maximize the secrecy rate. The article assumes an ideal beamforming model in which the signal is received only by the desired receiver, and the Eve cannot intercept the message. The proposed algorithm is split into two phases. In the first phase, the UAV and IRS positions are designed to maximize the secrecy rate. An alternate optimization technique is used in the second phase to optimize the UAV BS beamforming vector and IRS passive beamforming. Finally, a semidefinite relaxation technique is

PLS aspect	IRS aspect	UAV aspect	Scenario	Technique	Results
Maximize secrecy rate [10]	Phase shift control	Trajectory control Power control	UAV to single receiver Single Eve	Alternate optimization	Improved secrecy rate
Maximize secrecy rate [11]	Beamforming design Position design	Beamforming design Position design	UAV BS to receiver Single Eve	Ideal beamforming model; alternate optimization; semidefinite relaxation	Improved secrecy rate
Maximize secrecy rate [12]	Phase shift control	Power control Position design	UAV to ground user Single Eve	Fractional programming; alternate optimization	Improved secrecy rate
Maximize secure EE [13]	Phase shift control User association	Power control Trajectory design	BS to users; IRS-enhanced UAV; single Eve	Linear programming; SCA; alternate optimization	Improved secure EE
Maximize secrecy rate [14]	Beamforming design	Trajectory design	UAV to ground user Single Eve	SCA S-procedure; semidefinite relaxation; alternate optimization	Improved secrecy rate
Maximize secrecy rate [15]	Phase shift control	Position design	BS to users Single Eve	Iterative algorithm	Improved secrecy rate

TABLE 1. Recent advances in IRS-enhanced PLS for UAV communications.

used to reduce the complexity of the optimization. As a result, the proposed protocol achieves a higher secrecy rate than the other techniques in the literature.

The work in [12] proposes an algorithm to maximize the secrecy rate for UAV-to-ground-user transmissions in the presence of a single Eve. The optimized parameters to achieve the above goal include the UAV's transmit power and location, and the IRS's phase shift. At first, the transmit power is selected for a fixed UAV location and IRS phase shift. Then the UAV location problem is solved using the convex algorithm's difference, and the IRS phase shift is optimized using fractional programming. Finally, an alternate optimization is applied to find the optimal values of three parameters. The secrecy rate of the proposed technique has been shown to outperform other baseline algorithms.

In [13], the authors aim to maximize the network's secure energy efficiency (EE) consisting of a BS, an IRS-equipped UAV, multiple users, and a single Eve. EE is the value of the minimum secrecy rate per total power used by the network. The user association problem is relaxed using continuous variables and solved via linear programming. Further, the user association problem's integer output is obtained using the rounding technique. The power control is optimized using the Successive Convex Approximation (SCA) method. The trajectory design and phase shift control problems are solved using alternate optimization. Simulation results verify the improvement in the secure EE of the network.

The work in [14] considers a UAV and ground user communication scenario assisted by an IRS in the presence of a single Eve. A time-division multiple access technique is used for uplink and downlink communication. In addition, the work considers imperfect channel state information. The proposed algorithm jointly optimizes the UAV trajectory, beamforming of IRS, and users' transmit power. To solve these problems, three techniques, namely SCA, S-procedure, and semidefinite relaxation, are used along with alternate optimization. Performance evaluation of the proposed algorithm highlights the significance of IRS in improving PLS and secrecy rate.

In [15], the authors propose an iterative algorithm to maximize the secrecy rate for BS-to-user communications in the presence of a single Eve. The proposed algorithm controls the phase shift of IRS and the UAV's position to improve the transmissions' secrecy rate. The role of the UAV is to act as a passive relay and facilitate the PLS.

Most of the works in the literature consider a single Eve for PLS and IRS-enhanced UAV communications. Moreover, they also assume that the location/position of the user and Eve is static. In the next section, we present a more practical case study highlighting the advantages of using IRS when multiple Eves are considered in the vehicular network, that is, mobile users and Eves.

Optimizing PLS of IRS-Enhanced UAV Communications: A Case of Multiple Eavesdroppers

As shown in Fig. 2, we consider a communication system where a UAV communicates with a legitimate vehicle on the road in the presence of *K* non-colluding Eve vehicles. The UAV and vehicles are equipped with a single antenna. To improve the channel capacity, the considered system model also consists of an IRS with *M* passive elements mounted on top of the building. Thus, the vehicle receives a signal from a UAV through a direct link and an IRS-assisted link. Further, it is assumed that the transmitted signal is received by both the legitimate vehicle and the Eve vehicles through direct and indirect links. We aim to maximize the system's secrecy capacity subject to the constraints of UAV battery capacity and the phase designing matrix of the IRS passive component, where the secrecy capacity is defined as the difference in the rates of the legitimate vehicle and the Eve vehicle with maximum signal-to-interference-plus-noise ratio.

We formulate the secrecy capacity maximization problem subject to the UAV battery capacity and the IRS passive component. The considered problem is non-convex, where obtaining the global optimal solution is challenging. However, alternate optimization techniques can be employed to solve such problems efficiently. Alternate optimization provides an efficient way of decoupling the problem into the optimization variables. Then the problem is solved for one variable at a time, while alternating between the different variables multiple times. This provides an effective method to find efficient joint solutions for all the variables while

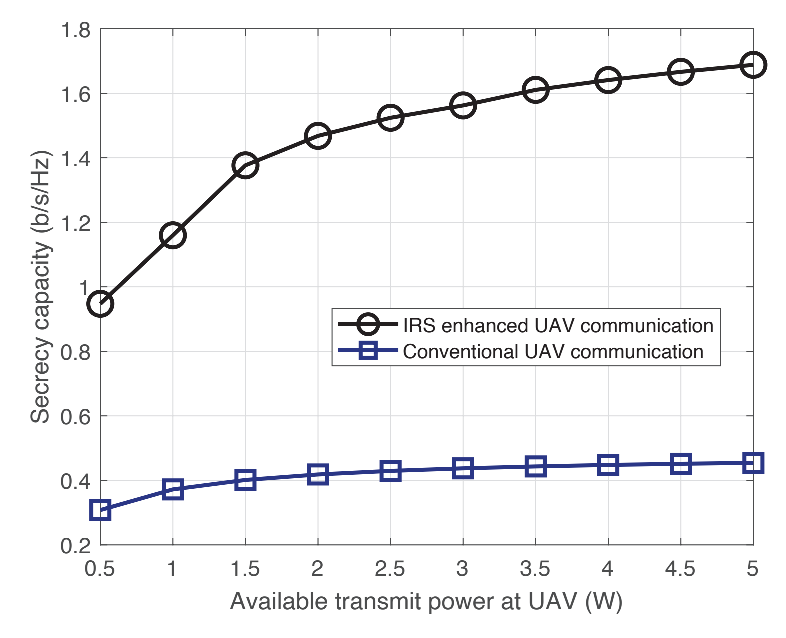

FIGURE 3. The figure shows the impact of increasing available transmission power at the UAV on the secrecy capacity of the system. This figure shows the advantage of using IRS in communication systems clear.

considering a single variable at a time. Therefore, an alternate optimization-based gradient descent optimizer is adopted to find the suboptimal but efficient solution to the formulated secrecy capacity maximization problem.

For the results, we adopt a Monte Carlo simulation where 10,000 independent experiments were conducted, and the figures show the average performance of the scheme. Further, we consider independently and identically distributed Rayleigh fading channels drawn from complex normal distribution with unity variance and 0 mean. Unless stated otherwise the simulation parameters are set as follows. The transmit power of UAV is 3 W, the number of IRS passive elements is 10, the number of non-colluding Eve vehicles is 8, path loss exponent is 3, height of UAV is 80 m, and noise variance is 0.01. Moreover, we define a passive reflection matrix of IRS as θ =diag{$\varphi_1 e^{j\theta_1}$, $\varphi_2 e^{j\theta_2}$, ... , $\varphi_M e^{j\theta_M}$}, where

$$j = \sqrt{-1},$$

$\varphi_M \in [0, 1]$ denotes the amplitude, and $\theta_m \in [0, 2\pi]$ is the phase shift of element *m*. Finally, we compared two scenarios: IRS-enhanced UAV communication and conventional UAV communication without IRS. This comparison aims to highlight the advantage of using the IRS to enhance the system's secrecy capacity.

To ensure positive secrecy capacity at all times, many works in the literature considered that the channel's gain from the transmitter to Eve is always less than the channel gain from the transmitter to the user. Although this assumption is reasonable in many cases, it is not always possible to have a better channel to the user than the channels between the transmitter and Eve. Therefore, we consider a more practical scenario where the channels are independent in the true sense, and Eve can have a better channel than the user.

In the system without IRS, it was observed that the channel conditions at the Eve vehicle are better than the optimization results in 0 W transmit power. However, as in this case, it is impossible to have a greater rate value at the legitimate vehicle than the Eve vehicle. Hence, to avoid a negative value of secrecy capacity, the system decides not to transmit, resulting in 0 secrecy capacity. However, when the system is equipped with an IRS, even if the channel from UAV to Eve vehicle is better than the channel between UAV and legitimate vehicle, the IRS elements can be adjusted to achieve positive secrecy capacity. Thus, a significant gain in the secrecy capacity is obtained with IRS, as shown in Figs. 3 and 4.

For the results in Fig. 3, we considered 10 reflecting elements at the IRS and three Eve vehicles. Figure 3 shows that when the UAV's available power increases, the system's secrecy capacity also increases. However, the increase in secrecy is logarithmic as at the lower values of available power, a more significant gain in secrecy is observed when power is increased. Further, with the increase in power, the gap in the secrecy provided by IRS and non-IRS systems also increases. Similarly, for the results in Fig. 4, we considered the available power to be 3 W, and the number of Eve vehicles is also 3. The figure shows that increasing the number of reflecting elements in the IRS improves the secrecy performance of the system, and the gap in the performance of IRS and non-IRS systems also increases. However, just as in the previous case, when the number of reflecting elements increases, the gain in secrecy is logarithmic.

Open Issues and Future Research Directions

IRS-enhanced UAV communication is an emerging area of research, and dealing with the security challenges that come with it is key to achieving its full potential. We list several open issues and challenges for future development and work.

PLS against Malicious IRS-Enhanced UAV Attacks

High mobility and flexibility are essential in the case of IRS-enhanced UAV communication to improve the PLS, intercept sensitive information, and even jam the legitimate links of UAVs to decrease their quality. In particular, in the case when a malicious UAV is equipped with IRS and can intercept the information of other UAVs, safeguarding the communication of UAV systems could provide more challenges than dealing with a traditional terrestrial Eve. However, no research works have been performed on this crucial topic from the perspective of communication theory. Therefore, it is preferred to explore advanced methods in terms of PLS to protect against malicious IRS-enhanced UAV attacks.

PLS against Pilot Contamination Attacks

Effective beamforming requires that accurate CSI for secure IRS-enhanced UAV communication can be obtained by utilizing the pilot signals. However, in some cases, intentional deterministic pilot samples are sent by an active Eve, similar to those transmitted by legitimate transmitters to deceive the UAV and facilitate eavesdropping. As a result, the UAV formulates an ineffective transmission technique that can benefit the signal reception of malicious Eves. For example, although information leakage is possible for confidential data delivery, the UAV may misunderstand the network environment and fly too close to the Eve. Thus, finding some efficient guidelines to minimize the impacts of pilot contamination attacks is complex but essential for IRS-enhanced UAV safety.

Cooperative Jamming for IRS-Enhanced UAV Communications

The IRS-enhanced UAV can act as a friendly jammer to protect the user data by sending artificial noise toward a malicious attacker. In this way, the PLS of a system can improve; however, it requires additional energy consumption of energy-constrained UAVs. It is important to note that energy efficiency is crucial for UAVs because of their limited onboard energy reservoirs, which becomes a bottleneck and affects the performance of UAVs. Thus, energy efficiency solutions that reduce the total energy consumption without affecting the system performance need to be further investigated. Moreover, IRS mounted over the UAVs can be used to tune the phase shift of the signals smartly. As a result, the original and reflected signal adds constructively to the legitimate user to enhance signal-to-noise ratios. Further, IRS can also be used as a friendly jammer to reduce the effect of Eves. For instance, IRS can use different phase shifts to produce destructive signals to reduce signal strength in any specific direction and decrease eavesdropping chances. In this regard, more research on secure communication techniques is needed when combining IRS and UAVs.

Artificial Intelligence/Machine Learning Approaches for IRS-Enhanced UAV Communication

Optimizing large-scale IRS-enhanced UAV communications is challenging, especially when UAVs are deployed in a partially unknown environment. In particular, optimizing UAV trajectory, IRS reflecting elements, and resource optimization of the entire network is challenging to design due to nonlinear models. Thus, designing approaches with low complexity and efficient system performance is challenging. Artificial intelligence/learning approaches are powerful tools for designing and optimizing such networks. These approaches are rapidly developing, and provide promising and robust tools for designing and optimizing challenging scenarios. Moreover, the hybrid models, data-driven methods, and hybrid offline and online methods to improve secrecy performance can be used to analyze the complex system. However, several challenges still need to be investigated — for example, large computational processing power, high energy consumption, and latency.

Key Size Reduction of Cryptographic Algorithms

PLS can be useful to reduce the size of transmitted data by reducing the reliance on complex cryptographic algorithms. Furthermore, PLS can work in conjunction with cryptographic algorithms to improve the level of security at low transmission cost. For example, the Elliptic Curve Digital Signature Algorithm (ECDSA) with a reduced key size may be used for UAV communications if PLS also provides defense against Eves. The advantage of using low-key-size algorithms is twofold. One is the reduced message size and improved use of the available spectrum. The other advantage is reduced latency as transmission delay and signature verification delay are reduced. In the future, there is a need to investigate the optimal key sizes that may be sufficient for different UAV application scenarios.

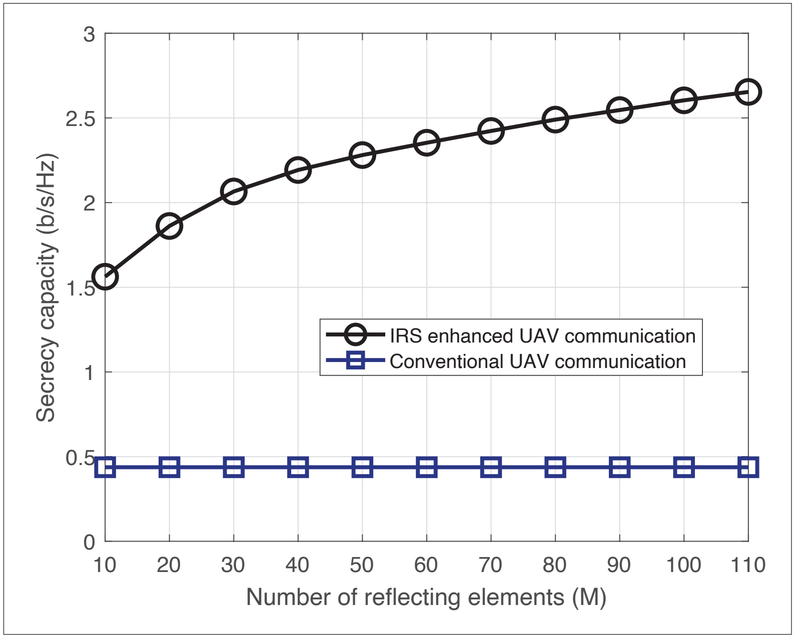

FIGURE 4. This figure shows that increasing the number of reflecting elements of the IRS improves the secrecy capacity of the system.

Resource Optimization for IRS-Enhanced UAV Communications

Optimal resource allocation is essential in wireless communications to enhance performance. Compared to conventional UAV communication, IRS-enhanced UAV communication adds a new dimension to improve PLS by optimizing IRS phase shift of passive elements and beamforming. Since IRS and resource allocation (trajectory design, sub-carrier, power allocation, etc.) are frequently connected, the design optimization issue becomes intractable, and the existing designs are sub-optimal. However, the performance variances between optimal and the current sub-optimal solutions are not apparent. Therefore, optimal techniques are needed to enhance the PLS of IRS-enhanced UAV communication in different applications while balancing computational complexity and system performance.

Availability of CSI in IRS-Enhanced UAV Communications

The recent studies on PLS of IRS-enhanced UAV communication assume the availability of perfect CSI at the transmitter and/or the IRS. However, estimating the channel for the IRS-enhanced UAV system is challenging because of the large number of passive elements. More specifically, these elements are passive in nature without signal processing capabilities. Thus, they do not have active transmitting and receiving abilities. Based on the above observation, the transmitter can achieve imperfect CSI in practice. Another critical point is to note that the CSI of the legitimate user is only available when it is active or registered with the network. However, the CSI of the passive Eve is not available.

Conclusion

This article provides an introduction to IRS-enhanced PLS for UAV communications. The work discusses the major use cases of IRS to improve the PLS working in UAV communications. We discuss recent works in this area, mainly related to UAV and ground user communications in the presence of a single Eve. We also present a case study that maximizes the secrecy rate of UAV communications in the presence of multiple Eves. The proposed work uses alternate optimization to control the phase shift of IRS and the UAVs' trajectory to enhance UAV communications. Simulation results show that IRS significantly improves the secrecy rate of UAV communications. We also discuss future research challenges related to IRS and PLS in UAV communication scenarios.

Acknowledgment

This work was supported by the Luxembourg National Research Fund (FNR) under the CORE projects RISOTTI, grant C20/IS/14773976, and 5G-Sky, grant C19/IS/13713801.

References

[1] A. Fotouhi *et al.*, "Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges," *IEEE Commun. Surveys & Tutorials*, vol. 21, no. 4, 2019, pp. 3417–42.

[2] M. Li *et al.*, "Secrecy Energy Efficiency Maximization in Uav-Enabled Wireless Sensor Networks Without Eavesdropper's CSI," *IEEE IoT J.*, vol. 9, no. 5, 2022, pp. 3346–58.

[3] J. Liang *et al.*, "An Intelligent and Trust UAV-Assisted Code Dissemination 5G System for Industrial Internet-of-Things," *IEEE Trans. Industrial Informatics*, vol. 18, no. 4, 2022, pp. 2877–89.

[4] M. Ahmed *et al.*, "Socially Aware Secrecy-Ensured Resource Allocation in D2D Underlay Communication: An Overlapping Coalitional Game Scheme," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, 2018, pp. 4118–33.

[5] X. Sun *et al.*, "Physical Layer Security in UAV Systems: Challenges and Opportunities," *IEEE Wireless Commun.*, vol. 26, no. 5, Oct. 2019, pp. 40–47.

[6] M. A. Javed *et al.*, "Reliable Communications for Cybertwin Driven 6G IoVs Using Intelligent Reflecting Surfaces," *IEEE Trans. Industrial Informatics*, 2022, pp. 1–1.

[7] H.-M. Wang, J. Bai, and L. Dong, "Intelligent Reflecting Surfaces Assisted Secure Transmission Without Eavesdropper's CSI," *IEEE Signal Processing Letters*, vol. 27, 2020, pp. 1300–04.

[8] H. Ren, K. Wang, and C. Pan, "Intelligent Reflecting Surface-Aided URLLC in a Factory Automation Scenario," *IEEE Trans. Commun.*, vol. 70, no. 1, 2022, pp. 707–23.

[9] Z. Wei *et al.*, "Energy- and Cost-Efficient Physical Layer Security in the Era of IoT: The Role of Interference," *IEEE Commun. Mag.*, vol. 58, no. 4, Apr. 2020, pp. 81–87.

[10] S. Fang, G. Chen, and Y. Li, "Joint Optimization for Secure Intelligent Reflecting Surface Assisted UAV Networks," *IEEE Wireless Commun. Letters*, vol. 10, no. 2, 2021, pp. 276–80.

[11] G. Sun *et al.*, "Intelligent Reflecting Surface and UAV Assisted Secrecy Communication in Millimeter-Wave Networks," *IEEE Trans. Vehic. Tech.*, vol. 70, no. 11, 2021, pp. 11,949–61.

[12] Z. Chu, W. Hao, and J. Shi, "Intelligent Reflecting Surface Aided Secure UaV Communications," 2020; https://arxiv.org/abs/2011.04339.

[13] H. Long *et al.*, "Joint Trajectory and Passive Beamforming Design for Secure UAV Networks with RIS," *Proc. 2020 IEEE GLOBECOM Wksps.*, 2020.

[14] S. Li *et al.*, "Robust Secure UAV Communications with the Aid of Reconfigurable Intelligent Surfaces," *IEEE Trans. Wireless Commun.*, vol. 20, no. 10, 2021, pp. 6402–17.

[15] J. Fang *et al.*, "Secure Intelligent Reflecting Surface Assisted UAV Communication Networks," *Proc. 2021 IEEE ICC Wksps.*, 2021.

Biographies

Wali Ullah Khan [M] (waliullah.khan@uni.lu) received a Ph.D. degree in information and communication engineering from Shandong University, Qingdao, China, in 2020. He is currently working with the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg.

Eva Lagunas [SM] (eva.lagunas@uni.lu) received a Ph.D. degree in telecommunications engineering from the Polytechnic University of Catalonia (UPC), Barcelona, Spain, in 2014. She currently holds a research scientist position in the SIGCOM Research Group, SnT, University of Luxembourg.

Zain Ali (zainalihanan1@gmail.com) received his Ph.D. degree in electrical engineering from COMSATS University, Islamabad, Pakistan, in 2021. He was awarded HEC's indigenous scholarship for M.S. and Ph.D. studies. Currently, he is working as a postdoctoral researcher in the Department of Electrical and Computer Engineering, University of California, Santa Cruz.

Muhammad Awais Javed [SM] (awais.javed@comsats.edu.pk) is currently an associate professor at COMSATS University Islamabad, Pakistan. His research interests include intelligent transport systems, vehicular networks, protocol design for emerging wireless technologies, and the Internet of Things.

Manzoor Ahmed (manzoor.achakzai@gmail.com) received a Ph.D. from Beijing University of Posts and Telecommunications and completed a postdoctoral fellowship from China in 2015 and 2018, respectively. He was an associate professor at Qingdao University and is currently a professor with the School of Computer and Information Science and also with the Institute for AI Industrial Technology Research, Hubei Engineering University, Xiaogan, China

Symeon Chatzinotas [F] (symeon.chatzinotas@uni.lu) received Ph.D. degrees in electronic engineering from the University of Surrey, Guildford, United Kingdom, in 2009. He is currently a full professor or Chief Scientist I and the co-head of the SIGCOM Research Group, SnT, University of Luxembourg.

Björn Ottersten [F] (bjorn.ottersten@uni.lu) received his Ph.D. degree in electrical engineering from Stanford University, California, in 1990. He is currently the director for SnT, University of Luxembourg.

Petar Popovski [F] (petarp@es.aau.dk) is a professor at Aalborg University and a visiting Excellence Chair at the University of Bremen. He received his Ph.D. degree from Aalborg University, Denmark, in 2004. His research interests are wireless communications/networks and communication theory.