Physical Layer Security Against Eavesdropping in The Internet of Drones (IoD) Based Communication Systems

Jehad M. Hamamreh

Abstract

Drones or unmanned aerial vehicles (UAVs) communication technology, which has recently been thoroughly studied and adopted by 3GPP standard (Release 15) due to its dynamic, flexible, and flying nature, is expected to be an integral part of future wireless communications and Internet of drones (IoD) applications. However, due to the unique transmission characteristics and nature of UAV systems including broadcasting, dominant line of site and poor scattering, providing confidentiality for legitimate receivers against unintended ones (eavesdroppers) appears to be a challenging goal to achieve in such scenarios. Besides, the special features of UAVs represented by having limited power (battery-operated) and precessing (light RAM and CPU capabilities), makes applying complex cryptography approaches very challenging and inefficient for such systems. This motives the utilization of alternative approaches enabled by physical layer security (PLS) concept for securing UAV-based systems. Techniques based on PLS are deemed to be promising due to their ability to provide inherent secrecy that is complexity-independent, where no matter what computational processing power the eavesdropper may have, there is no way to decrypt the PLS algorithms. This work is dedicated to highlight and overview the latest advances and state of art researches on the field of applying PLS to UAV systems in a unified and structured manner. Particularity, it discusses and explains the different, possible PLS scenarios and use cases of UAVs, which are categorized based on how the drone is utilized and employed in the communication system setup. The main classified categories include the deployment of the flying, mobile UAV as a 1) base station (BS), 2) user equipment (UE), 2) relay, or 4) jammer. Then, recommendations and future open research issues are stated and discussed.

Jehad M. Hamamreh is with the department of Electrical-Electronics Engineering, Antalya International (Bilim) University, Antalya, Turkey (email: jehad.hamamreh@gmail.com, jehad.hamamreh@antalya.edu.tr).

Part of this work has been considered for inclusion in a book chapter titled ” security in UAVs communications ” with CRC.

Index Terms

Drone communication, UAV, physical layer security, eavesdropping, spoofing, jamming, mobile relay, IoT, 5G systems, FANET, Jammer UAV.

I. Introduction

The rapid advancement in Internet of Things (IoT) technology enabled connectivity to a large number of smart devices where they can be accessed at any time, anywhere, and from everybody [1][2]. Meanwhile, Drone technology, known as Unmanned Aerial Vehicle (UAV), witnessed a vast attention in the recent years as well due to the tremendous advantages they can offer and their deployment flexibility. To this extend, both technologies form a promising paradigm that offers a wide range of applications in smart spaces known as Internet of Drones (IoD).

UAV (drone)-based communication is becoming one of the key promising applications of UAV systems, which can also be used for other inherited applications such as surveillance, tracking, transportation, environmental monitoring, industrial automation, agriculture, public safety, delivery, filmography, disaster relief (search and rescue), air exploration, target localization, fighting, etc. These enabled applications of UAVs and many others are attributed to their key features and characteristics, including aerial mobility with adaptive altitude, changeable location and direction, easy deployment, expandability, flexibility, and adaptive usage [1]–[4].

Particularly, UAV-based communication is becoming not only an achievable reality with many new benefits but also a key potential solution to a number of the communication and networking challenges that may result due to natural disaster scenarios. In fact, the 3GPP standardization community has identified and specified several possible deployment scenarios for UAVs-based communication in the domain of 5G systems as detailed in the standardization documents named TS 22.261, TR 22.862, and TR 36.777 [4], [5]. Specifically, UAV can be utilized as 1) an aerial base station providing connection links to multiple terrestrial or aerial users, 2) an aerial Internet of thing component, which is basically user equipment flying in the air, 3) an aerial relay that can be used to handover data traffic from one point to another. Plus, it can be used as a flying jammer to help enhance the security of certain scenarios.

Regardless of the deployment scenarios, there are several key, essential and vital requirements that have to be met in order to ensure the successful usage of UAV communication technology. Among the many design requirements of UAVs, especially for ultra-reliability and low-latency

communication (URLLC)-based 5G services, we mention low complexity, high reliability, high energy efficiency, low latency and robust security [6]. Among these design requirements, communication security comes as one of the most critical and important, key priority to fulfill in order to guarantee the successful deployment of UAV systems. To meet this design goal, novel security algorithms are needed.

Generally speaking, UAVs should by default be able to satisfy the following conditions and requirements for achieving an acceptable level of security:

- Confidentiality: The confidentiality requirement for UAVs communication, or what is known in the literature as the eavesdropping problem, refers to the situation where a legitimate transmitter (Alice) tries to communicate secretly with another legitimate/intended user (Bob) under the presence of a third unauthorized/unintended user called eavesdropper (Eve), who tries to intercept and overhear the communication content between the legitimate parties (Alice and Bob). Thus, the primary objective of confidentiality-guaranteeing algorithms (eavesdropping-resilient methods) is to limit the data access to intended users only, while preventing the disclosure and leakage of information to unintended, malicious eavesdroppers.
- Authentication: reactions given by UAVs to events should be based on legitimate messages. Therefore proper light weight protocols of authentication should be employed by the senders and/or receiver either in public or private networks.
- Plausibility: the legitimacy of transmitted messages also includes the evaluation of their consistency with similar ones, as the legitimacy of the broadcaster can be assured while the contents of the message contain erroneous data. The way that the plausibility is confirmed will firmly depend on the type of data transferred.
- Availability: Even when we assume the existence of a robust communication channel, some attacks and malfunctions can weaken and bring down the network by finding flaws in the system. Therefore, it is paramount that availability of UAVs services should be also supported by alternative means. This can be achieved via a UAV to UAV or a UAV to Infrastructure solution with a backup protocol in place.
- Non-repudiation: UAVs causing illegal actions need to be reliably identified while the sender should not be able to pick and choose which message to broadcast or deny for a certain message.
- Time-Criticality: Considering the mobility factor in a typical UAV network, stringent con-

straints should be expected when dealing with time-sensitive data as it might not leave any room for mistakes and could have disastrous results if not met properly.

- Privacy: The privacy of UAVs and their messages against unauthorized observers has to be guaranteed. This is a chief concern as the development of UAVs is following a customer-based demand which cannot be realized unless the customer privacy is guaranteed.
- Trust: The primary element in any secure UAV system is trust and privacy. This is particularly true and critical in UAVs due to the high liability expected in their safety and security applications and consequently the members running them. With a significant number of independent nodes in the UAV network and the presence of the human factor, it is without a doubt highly probable that misbehaviour can occur. In a connected IoT-based spaces, users are increasingly concerned about their privacy and UAVs are by no means an exception. This is especially problematic as the lack of privacy and the potential tracking functionality inherent in UAVs can lead to severe privacy violence. Accordingly, UAVs and service providers, must be mutually controlled by a considerable presence of the governmental authorities.

Among the aforementioned security requirements for UAV communications, preserving data confidentiality, i.e., providing security against eavesdropping by allowing data access to only authorized/legitimate users, while forbidding unauthorized/unintended users (called eavesdroppers) from intercepting the information, comes at the highest priority. This is because of the fact that guaranteeing data confidentiality provides a first line of defense against not only eavesdropping, but also against many other attacks such as denial of service (DoS), data modification, man-in-the-middle(MITM), session hijacking, spoofing (impersonation), and sniffing.

In the context of drone communications, providing confidentiality for legitimate receivers against unintended ones (eavesdroppers) appears to be a challenging goal to achieve due to the unique transmission characteristics and nature of UAV systems including broadcasting, dominant line of site and poor scattering. Besides, it is believed that due to having strict requirements on the power, weight and processing capabilities of UAVs, complexity-based cryptographic algorithms [7]–[9] cannot be supported by the base station carried by the UAV, which is unlike a terrestrial base station that has enough processing capabilities to support sophisticated encryption schemes. As a result, light cryptography is considered as a potential approach to provide security while reducing complexity, which results in power saving that can be reused for operating UAVs

for longer required period of time. However, this approach comes at the expense of reducing the security level as it becomes easier for eavesdropper to perform hacking due to the fact the encryption algorithms are light and not complex. Consequently, this approach, although saves power and reduces complexity, can make the UAV susceptible to security threats and vulnerabilities.

This particular problem motives the use of Physical Layer Security (PLS) approaches for securing UAV-based systems against eavesdropping due to their complexity-independent secrecy. This is so because no matter what computational power and processing complexity the eavesdropper may have, there is no feasible way to decrypt the security algorithms [10]–[17].

This paper is dedicated to highlight and overview the latest advances and state of the art research attempts performed towards applying PLS to UAV/Drone communication systems. This is performed by classifying the existing research studies according to the deployment scenarios and use cases of UAVs (i.e., UAV-Relay, UAV-BS, UAV-UE, UAV-Jammer). Then, we propose recommendations and future research directions.

II. Physical Layer Security for UAV Systems

The classical solutions that are being used to deliver secure communication in UAV-based systems are based on cryptography approaches similar to other wireless technologies. However, conventional complexity-based encryption algorithms are deemed unsuitable for future technologies including UAVs communication systems due to the following practical reasons: Firstly, future networks are composed of heterogeneous and decentralized wireless access technologies, where key distribution, management and maintenance processes are deemed very difficult and challenging in such scenarios. Secondly, future networks need to support new wireless technologies like Internet of drones (IoD) to enable many diverse applications. The transceiver devices in these wireless technologies are naturally: 1) power-limited due to depending on battery sources, 2) processing-restricted due to having low computational capabilities in terms of RAM, CPU and memory, and 3) delay sensitive due to using for control-based applications. All these facts together make cryptography-based techniques infeasible and ineffective for such type of technology. Thirdly, future networks are expected to support diverse services, applications and scenarios with different levels of security requirements. However, the encryption-based algorithms lack the ability to deliver different levels of security.

To cope up with the aforementioned issues, PLS concept has emerged as a promising solution that is capable of addressing some of the hurdles associated with cryptography. PLS exploits the dynamic nature of wireless channel along with its features including randomness, location-dependency, fading, dispersion, spreading, interference and noise, etc., to prohibit the eavesdropper from decoding the received data, while guaranteeing that the legitimate user can decode it successfully.

These aforementioned facts and reasons motivate the use of physical layer security as a promising solution to address to security concern in UAVs systems. In this section, we discuss and overview the latest advances in this area.

A. UAV as a Mobile Relay (UAV-Relay)

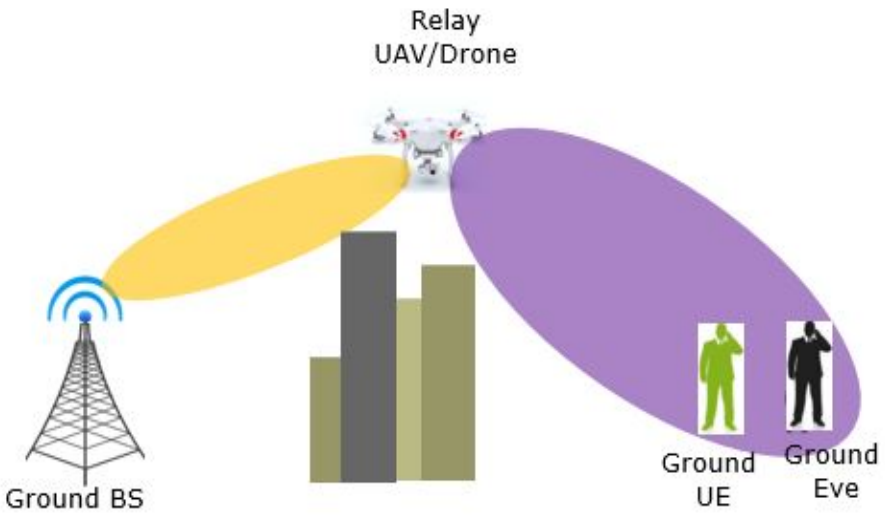

Fig. 1. A communication scenario composed of a ground transmitter base station (BS), relay UAV, ground legitimate receiver user equipment (UE), and ground eavesdropper (Eve).

The first work in the literature that studies using drones to improve the physical layer security of wireless communication systems is conducted by Wang *et al.* in [18]. In this work, the authors maximize the secrecy rate of a system composed of four nodes: a transmitter source (Alice), a UAV (mobile relay), a ground receiver destination (Bob), and an eavesdropper (Eve) located near Bob as shown in Fig. 1. The authors show that the resulting secrecy problem

formulation of such scenario is non-convex and hard to solve. Therefore, an iterative algorithm is developed by exploiting the difference of concave program to solve the optimization problem. The obtained results show that the use of mobile relaying enabled by UAV can significantly give better performance in terms of secrecy than the use of static relaying [18].

Similar to the previous study [18], the authors in [19] investigate the transmission secrecy of a system composed of a four-node setup (source, destination, mobile relay, and eavesdropper). Specifically, the secrecy rate of the system is maximized by performing joint optimization for both; trajectory of the relaying UAV and the transmitted power of source and relay. It is shown that the resulting secrecy rate maximization problem is difficult to solve due to the direct influence between the power allocation and the trajectory optimization. Therefore, an alternating optimization strategy is proposed, by which the trajectory design and power allocation are handled in an alternating way. Sequential convex programming is also utilized to overcome the nonconvexity of the problem of trajectory optimization, and thus enabling the derivation of an iterative, convergent algorithm. The obtained results verify the effectiveness of the proposed joint power and trajectory optimization in enhancing the secrecy performance.

In [20], an effective security scheme is introduced to guarantee the security of UAV-relayed wireless networks against eavesdropping with caching via jointly optimizing the UAV trajectory and time scheduling.

The authors of [21] study the secrecy outage performance resulting from using opportunistic relaying for a low-altitude UAV swarm[1] in the presence of multiple UAV eavesdroppers. Particularly, multiple UAV transmitter, which are served by a ground base station, and multiple UAV relays are optimally selected to help enhance the secrecy of transmitted confidential messages to a far ground user under the presence of multiple flying eavesdroppers.

B. UAV as a Mobile Transmitter Base Station (UAV-BS)

Unlink the aforementioned work that uses UAV as a mobile relay to enhance secrecy, Zhang *et al.* [22] consider the PLS of a system composed of a UAV node (Alice) that acts as a mobile transmitter base station (UAV-BS) and sends secret information to a legitimate receiver (Bob)

[1]UAV Swarm is a communication engineering term, which is similar to the flying ad hoc network (FANET) term used in networking literature.

Fig. 2. A communication scenario composed of an aerial, flying transmitter base station (UAV-BS), ground legitimate receiver user equipment (UE), and ground eavesdropper (Eve).

located on the ground in the presence of an eavesdropper who is also situated on the ground as depicted in Fig. 2. The authors maximize the secrecy rate of the aforementioned system setup by using joint optimization of the transmit power and trajectory of the mobile UAV over a finite horizon. The formulated non-convex optimization problem of the aforementioned system setup is solved by an iterative algorithm that is based on successive convex optimization and block coordinate descent methods. The presented results in [22] demonstrate the capability of the algorithm to significantly enhance the secrecy rate of the UAV system, as compared to other schemes that neither consider transmit power control nor trajectory optimization.

In [23], the authors target enhancing the PLS performance of a system that consists of a mobile UAV-BS (Alice) communicating with a ground receiver node (Bob) under the presence of K number of potential eavesdroppers (Eves), who are located on the ground as well, and their locations information is imperfect at the UAV-BS. To achieve that, the authors formulate an optimization problem to maximize the average worst case secrecy rate of the system through designing the robust trajectory and transmit power of the UAV over a given flight duration.

The resulting optimization problem is shown to be hard to solve optimally due its nonconvexity from one hand and the imperfect location information of the eavesdroppers from another hand. Therefore, an iterative suboptimal algorithm is proposed to tackle this problem effectively by using the S-procedure algorithm, block coordinate descent method, and successive convex optimization method. Numerical results show a noticeable, significant improvement in the average worst case secrecy rate by using the proposed design in comparison with other designs that do not consider joint optimization.

The downlink (UAV-to-ground) and uplink (ground-to-UAV) communications with a ground node, subject to an eavesdropper located on the ground is considered in [24]. In this study, the high mobility of the UAV alongside its trajectory design is exploited to create a good-quality channel for the legitimate link, and a degraded (low-quality) channel for the eavesdropping link. New problems are formulated to maximize the average secrecy rates of the donwlink and uplink transmissions via jointly optimizing the transmit power of the legitimate transmitter and the trajectory of the UAV. Iterative algorithms are proposed to effectively solve the formulated problems as they are found to be non-convex. This is attained by using the successive convex optimization and block coordinate descent methods. The acquired results exhibit performance enhancement in the secrecy rates by the proposed algorithms, in comparison to other reference designs that neither use trajectory optimization nor power control.

The integration between UAV and mm-Wave systems has recently been studied in the literature. Particularly, the PLS aspect of this integration has been investigated and analyzed in a recent work performed by Zhu*et al.* in [25]. In this work, the authors consider a downlink mmWave network composed of multiple UAVs that serve and work as aerial, flying base stations to provide wireless converge and connectivity to multiple legitimate receivers on the ground, which are surrounded by multiple eavesdroppers.

C. UAV as Mobile Jammer (UAV-Jammer)

Besides using UAV as a mobile base station as explained in [22] or as a mobile relay as shown in [18], Zhang *et al.* in [26] propose the use of UAV as a jammer to improve communication secrecy. Particularly, they consider a scenario in which a source base station on the ground (Alice) communicates with a legitimate receiver (Bob), who is also located on the ground, whereas an eavesdropper (Eve) tries to intercept the ongoing legitimate transmission link [26] as shown in

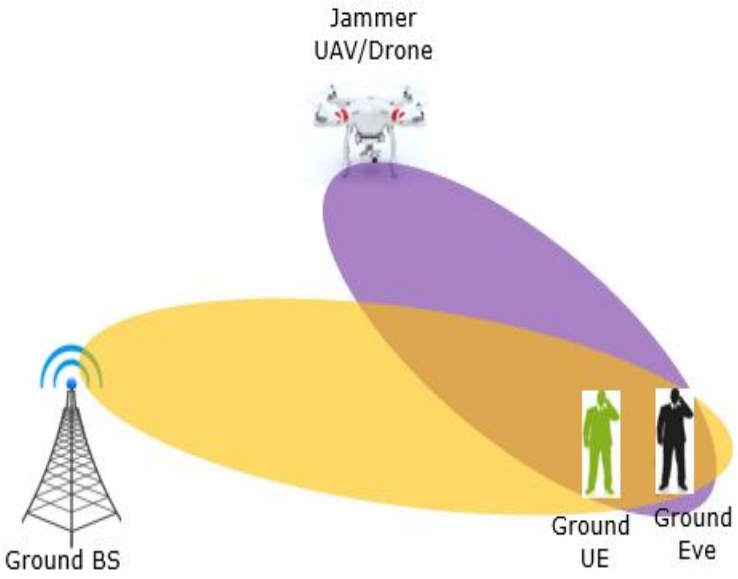

Fig. 3. A communication scenario composed of a ground transmitter base station (BS), UAV-jammer, ground legitimate receiver user equipment (UE), and ground eavesdropper (Eve).

Fig. 3. On the other hand, a UAV-based jammer is considered to be deployed in the system setup to improve the secrecy performance by emitting intelligent artificial noise.

The authors of [27] introduce an effective secrecy scheme that uses a UAV as a mobile jammer to enhance the secrecy rate of a ground wiretap channel. In particular, a UAV is employed to protect transmission against eavesdropping by transmitting intelligent jamming signals that can affect an eavesdropper more than the legitimate receiver as the UAV-enabled jammer can move away from the legitimate receiver so that it can get closer to the eavesdropper (if its location is known). The approach here is to jointly optimize the jamming power and UAV's trajectory in order to maximize the average secrecy rate. A closed-form lower bound on the achievable secrecy rate is derived to make the problem analyzable and more tractable. By using this bound, the transmit power and UAV trajectory are optimized alternately by employing an iterative algorithm that uses the successive convex optimization and block coordinate descent techniques. Numerical results demonstrate significant improvement in the secrecy rate of the considered wiretap system by the adopted joint design as compared to other non-optimized schemes in the literature.

The utilization of UAV nodes for the benefit of cognitive radio communication seems to be an

effective solution for certain challenges. Most importantly, the physical layer security aspect of this utilization has been introduced in [28]. In this work, physical layer security is considered for cognitive radio networks using UAV-enabled jamming noise. Specifically, a secondary transmitter sends confidential messages to a secondary receiver in the presence of an external eavesdropper (Eve), and the UAV acts as a friendly jammer that degrades the decoding capability of Eve. To maximize the secrecy rate of such a scenario while guaranteeing a certain signal-to-interference threshold at the primary receiver, resource allocation has to jointly optimize the transmit power and trajectory of UAV. The resulting design problem is found to be non-convex; therefore, in an attempt to solve the problem, it is proposed to convert the problem into a tractable form, and then use an effective, feasible, and low complexity algorithm based on successive convex approximation. The obtained results verify the superiority of the proposed solution, compared to other available ones.

D. UAV as a Flying User Equipment (UAV-UE)

The general goal in this category is to study the physical layer security of a system consisting of a ground base station transmitter (Alice) that acts as a control center/base station, and a UAV (Bob) that represents a flying user equipment (UAV-UE) under the presence of a flying eavesdropper (UAV-Eve) as shown in Fig. 4. In [29], directional modulation (DM) is utilized by Alice to improve the secrecy rate performance of a system similar to the aforementioned one.

To further enhance the secrecy level, an alternating iterative structure between power allocation and beamforming is proposed to be employed by the system. Simulation results demonstrate that the proposed scheme can achieve substantial secrecy rate gains. Particularly, in the case of small-scale antenna array, the gain of the secrecy rate performance achieved by the proposed scheme is very significant.

The uplink (ground-to-UAV) and downlink (UAV-to-ground) communications with a ground node, subject to an eavesdropper located on the ground is considered in [24]. In this study, the high mobility of the UAV alongside its trajectory design is exploited to create a good-quality channel for the legitimate link, and a degraded (low-quality) channel for the eavesdropping link. New problems are formulated to maximize the average secrecy rates of the donwlink and uplink transmissions via jointly optimizing the transmit power of the legitimate transmitter and the trajectory of the UAV. Iterative algorithms are proposed to effectively solve the formulated

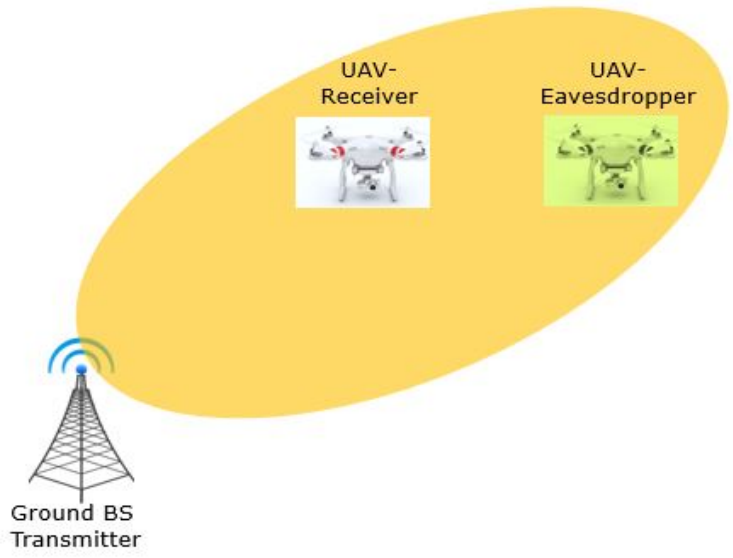

Fig. 4. A communication scenario composed of a ground transmitter base station (BS)r, UAV receiver user equipment (UE), and UAV eavesdropper (Eve).

problems as they are found to be non-convex. This is attained by using the successive convex optimization and block coordinate descent methods. The acquired results exhibit performance enhancement in the secrecy rates by the proposed algorithms, in comparison to other reference designs that neither use trajectory optimization nor power control.

E. Hybrid Usage: One UAV as a Cooperative Jammer and Another as a Transmitter

To improve the secrecy performance of a UAV-based communication system supporting ground users, it is possible to utilize one UAV as a mobile cooperative jammer and another UAV as a source base station transmitter as shown in Fig. 5.

In this direction, the authors of [30] present a UAV-aided mobile jamming strategy to further improve the achievable average secrecy rate for UAV-ground communications. Specifically, an extra cooperative UAV is used as a mobile jammer to broadcast jamming signals that can help keep the source UAV transmitter closer to the ground receiver, thus producing a good-quality legitimate link that results in enhancing the secrecy performance of the system. The design objective is achieved by maximizing the achievable secrecy rate through jointly optimizing the transmit power and trajectories of both jammer UAV and source UAV. An iterative

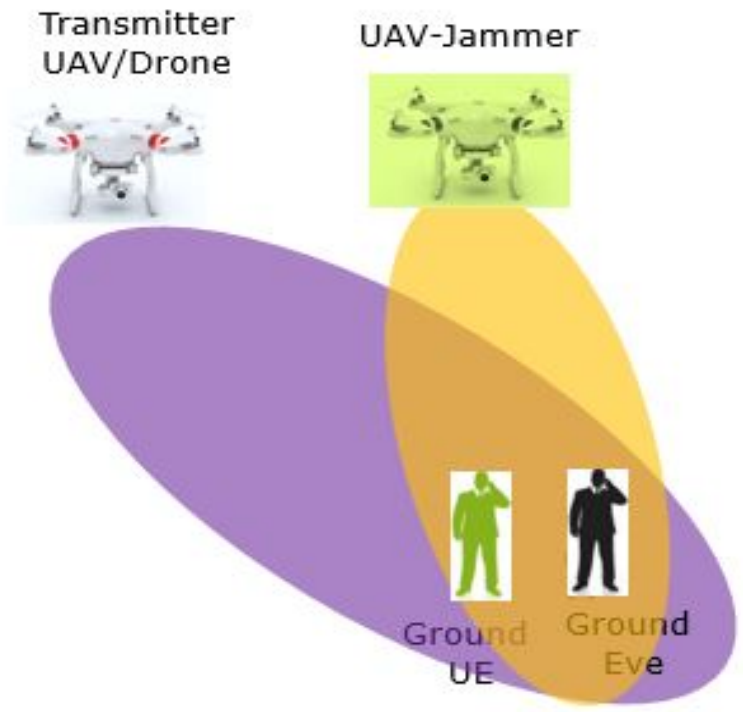

Fig. 5. A communication scenario composed of a UAV transmitter base station (BS), UAV-jammer, ground receiver user equipment (UE), and ground UAV eavesdropper (Eve).

algorithm based on a block coordinate descent method is used to solve the considered non-convex optimization problem.

In [31], the authors study a scenario in which a mobile UAV tries to broadcast secret messages to multiple ground users. To enhance the secrecy performance of the system, a cooperative UAV that acts as a jammer is considered. In this setup, the lowest secrecy rate of the ground users is maximized by jointly optimizing the transmit power and the trajectory of the UAVs as well as the scheduling of the user. Block successive minimization techniques are adopted to efficiently solve this nonconvex problems.

In another work in [32], the authors introduce an effective cooperative jamming approach to secure the UAV communication by utilizing jamming from other nearby UAVs to provide confidentiality and defend against external eavesdropping. Particularity, the authors consider a scenario composed of a two-UAVs where one UAV acts as a source transmitter trying to send confidential information to a ground node (GN), and anther UAV acts as a jammer which

transmits artificial noise to confuse the ground eavesdropper.

The two UAVs can flexibly adopt and modify their trajectories (locations over time) to enable secure communication that is leveraging and exploiting not only the fully-controllable mobility of the UAVs but also the ability to use them as cooperative jammers. It is assumed that the location of the ground nodes is perfectly known by the two UAVs whereas the eavesdropper's location is partially known ahead of time.

The design goal in this study is to maximize the average secrecy rate from the UAV transmitter to the ground node within a certain period of time. This is attained by optimizing the UAVs trajectories, jointly with their communicating/jamming power allocations. Again, similar to other optimization secrecy problems in UAV-based scenarios, the formulated problem is found to be non-convex, and thus a numerical solution is proposed by utilizing alternating optimization and successive convex approximation techniques.

III. Open research issues

According to the analysis on literature, we present the following open research gaps that future efforts may consider:

- Extension of the physical layer security studies to multi-link and multi-node scenarios under the effect of different channel conditions and network topologies.
- Development of resilient physical layer security schemes to protect the transmission not only from passive attacks such as eavesdropping but also from active ones such as spoofing and jamming.
- The integration of drone/UAV technology with other emerging radio access communication technologies such as mm-wave and visible light communications is worth investigation and analysis to understand the capability of UAVs in enhancing the security of such high-frequency technologies.
- Development of Doppler-resilient secure designs for UAV communications. This is of paramount importance because of the continuous mobility of UAVs/Drones in the network. Therefore, it would be very useful and beneficial to come up with new security schemes that exploit the inherent immunity of some transmission techniques such as orthogonal time frequency space (OTFS) to Doppler spread.

- Facilitation of random and controlled deployment methodologies as to enhance network security and user privacy.
- Development of integrated security optimization schemes that consider the trade-offs between data reliability and confidentiality.
- Secure design of the drone-based hardware and software used in critical applications.
- Assessment of medium blockage effects on drone security.
- Simultaneous integration of different security paradigms, in order to achieve more reliable performance.
- Assessment of surrounding conditions that affect drone security against external attacks.
- Design of data intensive and time sensitive secured drones, especially for emergency cases where drone efficiency is crucial.
- Optimization of dynamic drone trajectory in secured spaces for more trusted solutions.

IV. Conclusion

Due to the rapid technological advances and unprecedented growth in the number and type of flying vehicles, many applications utilizing UAVs have emerged. Regardless of these UAV-enabled applications, which have different set of requirements and performance targets to meet in terms of reliability, latency, coverage, spectral and energy efficiency, etc., communication and networking security comes as the most critical and important objective to meet in order to guarantee the safe operation and utilization of UAVs-based systems.

However, due to the unique transmission characteristics and nature of UAV systems including broadcasting, dominant line of site and poor scattering, security appears as a challenging goal to meet in such scenario. Besides, the special features of UAVs represented by having limitation on power (run by battery) and precessing (light RAM and CPU capabilities), makes applying complex cryptography approaches very challenging and ineffective for such systems.

This has motived the use of physical layer security-based approaches for securing UAV-based systems due to their complexity-independent secrecy, as no matter what complexity the eavesdropper may have, there is no way to decrypt the security algorithms. This study has highlighted and overviewed, in a structured and unified manner, the latest advances and state of art researches on the field of applying physical layer security to UAV systems under different use cases and scenarios such as utilizing the UAV as a base station, relay, user equipment, and/or jammer. In addition, different future research directions have been identified and discussed.

REFERENCES

[1] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surv. Tut.*, vol. 18, no. 2, pp. 1123–1152, Secondquarter 2016.

[2] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint," *IEEE Commun. Surv. Tut.*, vol. 18, no. 4, pp. 2624–2661, Fourthquarter 2016.

[3] R. Shakeri, M. A. Al-Garadi, A. Badawy, A. Mohamed, T. Khattab, A. K. Al-Ali, K. A. Harras, and M. Guizani, "Design challenges of multi-UAV systems in cyber-physical applications: A comprehensive survey, and future directions," *CoRR*, vol. abs/1810.09729, 2018. [Online]. Available: http://arxiv.org/abs/1810.09729

[4] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. García-Rodríguez, and J. Yuan, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *CoRR*, vol. abs/1809.01752, 2018. [Online]. Available: http://arxiv.org/abs/1809.01752

[5] Z. Yuan, J. Jin, L. Sun, K. Chin, and G. Muntean, "Ultra-reliable IoT communications with UAVs: A swarm use case," *IEEE Communications Magazine*, vol. 56, no. 12, pp. 90–96, December 2018.

[6] J. M. Hamamreh, Z. E. Ankarali, and H. Arslan, "CP-Less OFDM with alignment signals for enhancing spectral efficiency, reducing latency, and improving PHY security of 5G services," *IEEE Access*, vol. 6, pp. 63 649–63 663, 2018.

[7] S. A. Alabady, F. Al-Turjman, and S. Din, "A novel security model for cooperative virtual networks in the IoT era," *International Journal of Parallel Programming*, Jul 2018.

[8] F. Al-Turjman and S. Alturjman, "Confidential smart-sensing framework in the IoT era," *The Journal of Supercomputing*, Aug 2018.

[9] ——, "Context-sensitive access in industrial internet of things (IIoT) healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2736–2744, June 2018.

[10] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2018.

[11] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret key generation using channel quantization with SVD for reciprocal MIMO channels," in *2016 Int. Symp. Wirel. Commun. Syst.* IEEE, sep 2016, pp. 597–602.

[12] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Secure pre-coding and post-coding for OFDM systems along with hardware implementation," in *13th Int. Wireless Commun. and Mobile Comput. Conf., IWCMC 2017, Valencia, Spain, Jun., 26-30, 2017*, 2017, pp. 1338–1343.

[13] H. M. Furqan, J. M. Hamamreh, , and H. Arslan, "Enhancing physical layer security of OFDM systems using channel shortening," in *IEEE Annual Int. Symp. on Personal, Indoor, and Mobile Radio Commun., PIMRC 2017, Montreal, Canada, Oct., 8-13*, 2017, pp. 100–105.

[14] E. Guvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Phy. Commun.*, vol. 25, pp. 14 – 25, Aug. 2017.

[15] J. M. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," *IEEE Access*, vol. 5, pp. 25 863–25 875, 2017.

[16] J. M. Hamamreh and H. Arslan, "Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1191–1194, May 2017.

[17] ——, "Joint PHY/MAC layer security design using ARQ with MRC and null-space independent PAPR-aware artificial noise in SISO systems," *IEEE Transactions on Wireless Communications*, vol. 17, no. 9, pp. 6190–6204, Sept 2018.

[18] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 310–313, June 2017.

[19] Q. Wang, Z. Chen, H. Li, and S. Li, "Joint power and trajectory design for physical-layer secrecy in the UAV-aided mobile relaying system," *IEEE Access*, vol. 6, pp. 62 849–62 855, 2018.

[20] F. Cheng, G. Gui, N. Zhao, Y. Chen, J. Tang, and H. Sari, "UAV relaying assisted secure transmission with caching," *IEEE Transactions on Communications*, pp. 1–1, 2019.

[21] H. Liu, S. Yoo, and K. S. Kwak, "Opportunistic relaying for low-altitude UAV swarm secure communications with multiple eavesdroppers," *Journal of Communications and Networks*, vol. 20, no. 5, pp. 496–508, Oct 2018.

[22] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via trajectory optimization," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Dec 2017, pp. 1–6.

[23] M. Cui, G. Zhang, Q. Wu, and D. W. K. Ng, "Robust trajectory and transmit power design for secure UAV communications," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 9042–9046, Sep. 2018.

[24] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via joint trajectory and power control," *IEEE Transactions on Wireless Communications*, pp. 1–1, 2019.

[25] Y. Zhu, G. Zheng, and M. Fitch, "Secrecy rate analysis of UAV-enabled mmwave networks using matrn hardcore point processes," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1397–1409, July 2018.

[26] Y. Zhou, P. L. Yeoh, H. Chen, Y. Li, W. Hardjawana, and B. Vucetic, "Secrecy outage probability and jamming coverage of UAV-enabled friendly jammer," in *2017 11th International Conference on Signal Processing and Communication Systems (ICSPCS)*, Dec 2017, pp. 1–6.

[27] A. Li, Q. Wu, and R. Zhang, "UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel," *IEEE Wireless Communications Letters*, pp. 1–1, 2018.

[28] P. Nguyen, H. Nguyen, V.-D. Nguyen, and O.-S. Shin, "UAV-enabled jamming noise for achieving secure communications in cognitive radio networks," 11 2018.

[29] F. Shu, Z. Lu, J. Lin, L. Sun, X. Zhou, T. Liu, S. Zhang, W. Cai, J. Lu, and J. Wang, "Alternating iterative secure structure between beamforming and power allocation for UAV-aided directional modulation networks," *Physical Communication*, vol. 33, pp. 46 – 53, 2019.

[30] A. Li and W. Zhang, "Mobile jammer-aided secure UAV communications via trajectory design and power control," *China Communications*, vol. 15, no. 8, pp. 141–151, Aug 2018.

[31] H. Lee, S. Eom, J. Park, and I. Lee, "UAV-aided secure communications with cooperative jamming," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 10, pp. 9385–9392, Oct 2018.

[32] C. Zhong, J. Yao, and J. Xu, "Secure UAV communication with cooperative jamming and trajectory control," *IEEE Communications Letters*, pp. 1–1, 2019.