International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancement of Physical Layer Security in Flying Ad-hoc Networks by Intelligent Reflecting Metasurfaces

Arslan Asim[*1], Michael Cada[1, 2]

Submitted: 20/10/2022 **Revised**: 19/12/2022 **Accepted**: 05/01/2023

Abstract: Unmanned Aerial Vehicles (UAVs) serve a lot of key roles in human lives. It has been shown that UAVs can be clustered in different ways to form swarm networks. One such type of swarm network is a Flying Ad-Hoc Network (FANET). In a FANET, the ground station communicates with one focal UAV to control the entire network, which makes the focal UAV highly prone to a communication security attack. Such an attack has to be averted by introducing additional features of security into the network. A recent research emphasis has been on the use of Intelligent Reflecting Surfaces (IRS) for improving the physical layer security in communication networks. Hence, its relevance to UAV networks cannot be ignored because of the wide range of purposes that UAVs promise to serve in the coming days. These surfaces consist of nanoscale antennas that can tailor the wavefronts of incident electromagnetic waves and reflect them to the UAV. The communication in such metasurface-assisted swarm networks can be modelled by means of mathematical expressions. In this letter, a model for the enhancement of physical layer security of FANETs through phase control IRS has been proposed along with simulation results. The simulation results show the relationships between different network parameters and secrecy performance.

Keywords: *Metasurfaces, secrecy, communication.*

1. Introduction

Ever since the first human flight conducted by Wright brothers in 1903, the aircraft technology has progressed by leaps and bounds. Automation has also helped in bringing about tremendous developments in aircraft industry. Unmanned Aerial Vehicles (UAVs) happen to be among one of the most exciting developments in the recent days. UAVs have been in use even before the first human flight in 1903 [1]. UAVs date back to 1849 when unmanned balloons were used by Austria to bomb Venice. Since then, UAVs have been under discussion. Presently, UAVs serve in several areas encompassing military/ defence, agriculture, mining, surveying, surveillance and security, fire control and emergency services [2]–[5].

An emerging area of research pertaining to UAVs is the UAV swarm networks [6] – [7]. With this new area in discussion, a lot of effort has been dedicated to the design of communication architectures and algorithms for swarms of UAVs. A swarm consists of a formation of UAVs with a defined communication and control protocol as well as a specific objective.

There are a number of architectures for swarm communications [8]. One of the key ones is Flying Ad-hoc Network (FANET). The noteworthy feature of this protocol is that there is a gateway UAV that acts like the backbone of the entire network of UAVs. The ground infrastructure communicates with this particular gateway UAV. The gateway UAV, in turn, communicates with the rest of the UAVs in the network and ensures coordinated movement of the swarm. FANETS may be more complex and contain multiple layers of communication where there are more than one gateway UAVs communicating with their own individual groups of UAVs.

This can present as an alarming situation when eavesdroppers want to exploit the network for their own malicious objectives. This particular architecture gives them a very direct target to attack the network. The direct target is the gateway UAV. Once the gateway UAV is attacked, it becomes vulnerable. If the eavesdropper succeeds in breaching into the gateway UAV's configuration, the complete FANET is now at the disposal of the eavesdropper. Therefore, the enhancement of the physical layer security in FANETs is a pertinent concern and needs to be addressed.

This issue has been reported by a detailed review on FANETs [9] while discussing 'UAV direct communication'. The paper has elaborated on various FANET security issues. Another paper has presented a taxonomy of five UAV Ad Hoc Network (UAANET) routing protocols and explained their pros and cons [10]. A common issue reported for all the protocols has been lack of consideration for security. Noor et al. [11] have emphasized that the communication security issues in FANETs have to be addressed. They have mentioned eavesdropping as a possible security and privacy challenge in FANETs. Their discussion also involves the promising role of fifth/ sixth generation (5G/ 6G) technology towards the ubiquitous use of UAVs. A comprehensive survey has been done on the privacy issues related to UAV communications. The major issues have been classified into 4 categories: sensor level, hardware level, software level and communication level. A part of the discussion on communication level issues identifies points of cyber-attacks on the UAV networks. Backbone UAV has been identified as a

1 Department of Electrical and Computer Engineering, Halifax – NS B3J 1B6, CANADA
ORCID ID: 0000-0001-7882-4948
2 IT4Innovations, VSB-Technical University of Ostrava, 17. listopadu 15, 708 00, Ostrava-Poruba, CZECH REPUBLIC
ORCID ID: 0000-0002-1150-4007
** Corresponding Author Email: arslanasim@dal.ca*

potential point of attack in a similar manner to this paper [12].
Researchers have also been trying to cater to the FANET security issues in the past. The authors of [13] have proposed an encryption scheme for UAV communications. In their scheme, all of the network devices can exchange encrypted messages which can be decrypted to extract the actual messages. In this way, the identities of the UAVs remain recognizable. The use of encryption techniques in UAV communications has also been reported in [14]. Zhang et al. have proposed another simulation framework for enhancing UAV network security. They have presented a scenario where the ground station communicates with an airborne UAV while a malicious entity on the ground tries to eavesdrop [15]. This scenario is similar to the one presented in this paper. The important difference is that in this paper, the eavesdropper is mobile and trying to attack the gateway UAV in the network.
In this paper, a FANET security issue has been identified and reported from literature. Then, a new solution to the mentioned problem has been proposed that includes the use of metamaterial-based surfaces to enhance the physical layer security of the network. Metamaterials are artificially engineered materials that display unique properties through which the electromagnetic waves can be altered to create interesting effects [16] – [18]. Metamaterials can be used to design and fabricate ultrathin surfaces that can engineer electromagnetic wavefronts on the sub-wavelength scale. Such surfaces, commonly known as metasurfaces, consist of nano-antennas that can change the properties of electromagnetic waves when they interact with them. For example, the phase and polarization of electromagnetic waves can be altered with the help of these nanostructures. This work primarily targets the use of nanostructures in changing the phase of incident electromagnetic waves.
It is very clear from the existing literature that the use of metasurfaces in the domain of communications is inevitable due to their special characteristics [19]–[23]. Coupled to this is the fact that physical layer security in communication architectures is a serious concern for network integrity, confidentiality and access. Therefore, a complete theoretical model and simulation-based analysis for phase change intelligent metasurfaces have been presented in the context of physical layer security of Flying Ad-hoc Networks. This makes it a unique and promising effort in securing UAV communication networks.

2. Problem Analysis

Nowadays, the concept of smart cities [24] is really being focused by many countries. One of the many prominent features of smart cities is the Intelligent Transport Systems (ITS). UAVs are a valuable part of the smart cities for the applications mentioned earlier.
UAVs can be clustered into different network architectures. In this paper, the primary focus is on the Flying Ad-hoc Networks (FANETs). Figure 1 shows the communication pathways and configuration of the proposed model for enhancing FANET security.
The design of the improved model has been depicted in figure 1. In the figure, the ground station can be seen to be communicating with the UAV, but the signal received by the UAV is not the same as that sent by the ground station. It is modified by the Intelligent Reflecting Surfaces (IRS) deployed on the building. The IRS contains a number of nano-antennas that cause a phase change in the incident signal. Since the IRS nanostructures' orientations can be reconfigured, the phase change in the incident signal can be reconfigured too. Through this controllable signal phase change, security aspect is enhanced in the ground to UAV communication.
It is imperative to compare this configuration with a traditional FANET without the presence of IRS. In the absence of the IRS building, the ground station directly communicates with the gateway UAV and the gateway UAV coordinates the entire network. The communication channel between the ground station and the gateway UAV clearly presents as a vulnerable link through which the security of the entire network can be compromised. This research aims to work on this aspect by improving the security of the ground station to gateway channel.
If the ground station signal is denoted by x, the signal received at the gateway UAV can be represented as

$$y = \left[\sum_{n=1}^{N}\left(h_s h_{u,n} e^{-j\emptyset,n}\right)\right] x + \varepsilon \quad (1)$$

In equation (1), h_s represents the channel coefficient for the path between the ground station and IRS building. h_u represents the channel coefficient for the path between the IRS building and the UAV. h_u can either mean h_g or h_e depending on whether the UAV under consideration, is the gateway or eavesdropper UAV respectively.

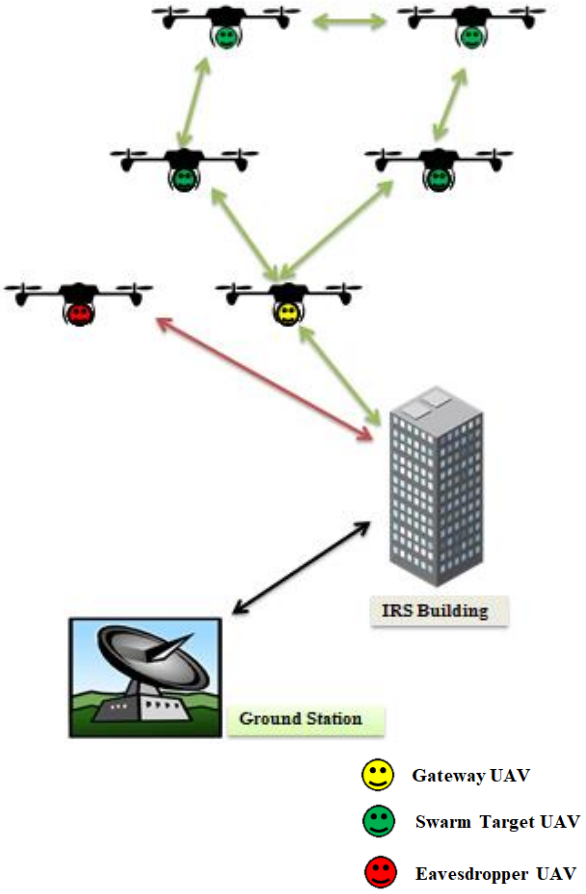


Fig. 1. Model of the Proposed Network.

Table I describes the symbols and notations used to formulate an expression for the average secrecy capacity of the proposed network. The formulation of the average secrecy capacity for the upgraded FANET (with IRS) has been given below.
The channel coefficients can be can be modeled by means of Rayleigh distribution, channel distances and phase components.

$$h_{s,n} = \sqrt{g_{s,n} d_s^{-\beta} e^{-j\theta,n}} \quad (2)$$

$$h_{u,n} = \sqrt{g_{u,n} d_u^{-\beta} e^{-j\psi,n}} \quad (3)$$

The channel coefficients lead to the expressions for the instantaneous Signal to Noise Ratio (SNR).

$$\gamma_e = \frac{\sum_{n=1}^{N} P|h_{s,n}|^2 |h_{g,n}|^2}{N_o} \quad (4)$$

$$\gamma_e = \frac{\sum_{n=1}^{N} P|h_{s,n}|^2 |h_{e,n}|^2}{N_o} \quad (5)$$

The secrecy capacity of the channels depends on the SNRs in the following way:

$$C_s = \log_2(1 + \gamma_g) - \log_2(1 + \gamma_e) \qquad \gamma_g > \gamma_e \quad (6)$$

Finally, expectation operator can be used to obtain average secrecy capacity:

$$\overline{C_s} = \mathbb{E}\left[C_s(\gamma_g, \gamma_e)\right] \quad (7)$$

Alternatively, analytical expressions for the average secrecy capacity are given as

$$\overline{C_s} = \int_0^\infty \int_0^\infty C_S\left(\gamma_g, \gamma_e\right) f(\gamma_g, \gamma_e)\, d\gamma_g\, d\gamma_e \quad (8)$$

Here, $f(\gamma_g, \gamma_e)$ represents the joint probability density function of the SNRs (25).

$$\overline{C_G} = \frac{1}{ln\,2} \int_0^\infty \frac{1}{z}\left(1 - M_G(z)\right) e^{-z} dz \quad (9)$$

$$M_G(z) = \mathbb{E}\left[e^{-\frac{P\, d_s^{-\beta} d_g^{-\beta}}{N_o} z \sum_{n=1}^{N} g_{s,n} g_{g,n}}\right] \quad (10)$$

$$\overline{C_E} = \frac{1}{\ln 2} \int_0^\infty \frac{1}{z}\left(1 - M_E(z)\right) e^{-z} dz \quad (11)$$

$$M_E(z) = \mathbb{E}\left[e^{-\frac{P\, d_s^{-\beta} d_e^{-\beta}}{N_o} z \sum_{n=1}^{N} g_{s,n} g_{e,n}}\right] \quad (12)$$

$$\overline{C_s} = \overline{C_G} - \overline{C_E} \quad (13)$$

The average secrecy capacity is the difference between the average capacities of the gateway and eavesdropper UAV channels [26] - [27].

3. Simulation Results

It is of utmost importance to understand the dependence of the different parameters on the performance of the proposed model. For this purpose, the analysis of the mathematical model and its physical realization has been performed in MATLAB with the aim of thoroughly understanding the viability of the system as well as suggesting further improvements. The results of the simulations have been presented in the form of plots.

Figure 2 presents an interesting relationship between the number of metasurface unit cells and the secrecy capacity values. It also shows how the power levels of the ground base station affect the secrecy capacities. It is obvious from the figure that the increase in ground power results in an increase in the average secrecy capacity. The figure also highlights that the greater the number of unit cells on the metasurface, the better the secrecy capacity. It can clearly be seen that for the same level of ground station power, a larger number of meta-atoms of the IRS give rise to higher values of average secrecy capacity. The comparison has been shown between 0, 50, 100, 150, 200, 250 meta-atoms. The values of the constant parameters used for figure 2 are as follows: d_g = 10 meters, d_e = 20 meters and d_s = 40 meters.

Another significant insight into the parameters of this study is provided by figure 3. The figure explains the relation between different distance values and the secrecy performance of the model. The values on the x-axis in (a) indicate the distance between the base station and the IRS building. The simulations have been repeated for different values of distance between the IRS building and the gateway UAV, dg. It is easier to attack and take over the gateway UAV when it is far away from the IRS. On the figure, as the value of d_g increases, the secrecy capacity decreases. Meanwhile it can also be observed that an increase in the distance between the ground station and IRS affects the secrecy capacity. The secrecy capacity drops if the distance between the ground station and IRS is kept large. The values of the ground station power and d_e are kept constant at 500 Watts and 10 meters respectively for the simulations in (a). Similarly, (b) and (c) prove that a greater distance between the IRS building and eavesdropper UAV results in better secrecy performance. Figure (c) also provides evidence that for any given scenario, a greater ground station power would provide improved results. P = 500 W, d_s =10 m for (b) and d_s =10 m, d_g =8 m for (c).

These results provide a reasonable understanding of how the proposed model should be used in practical terms. It is imperative to acknowledge the role of MATLAB in running the rigorous simulations to generate detailed plots. In-built functions have been utilized to get probability distributions. Combinations of different parameters have been chosen to provide multi-dimensional perspectives on the problem since the UAVs are mobile, which makes the network dynamic.

This paper provides a way forward for the use of 2 dimensional surfaces in the smart cities of tomorrow. It also introduces the concept of metasurface secured UAV communication networks. This idea will start taking its practical form in the near future.

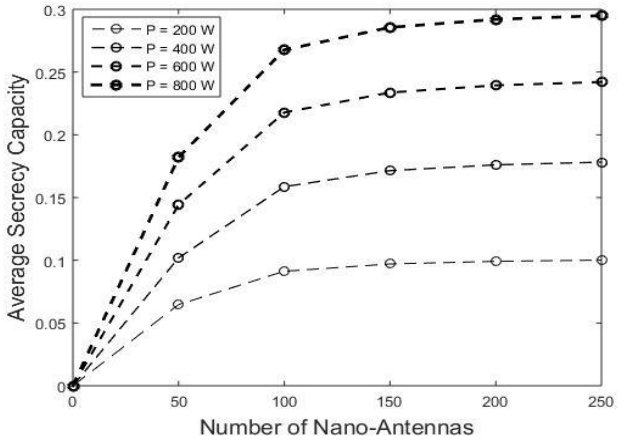
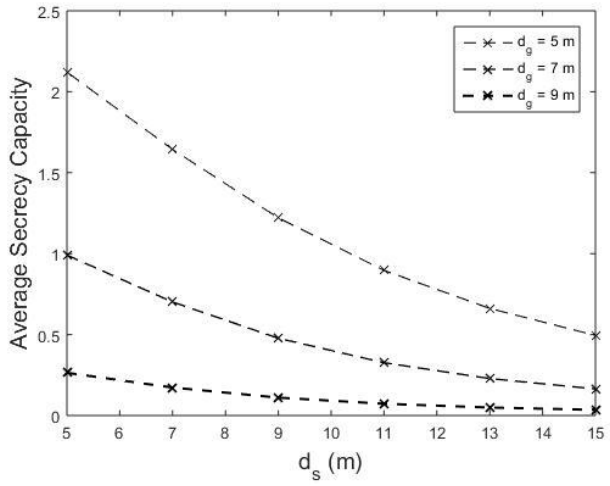
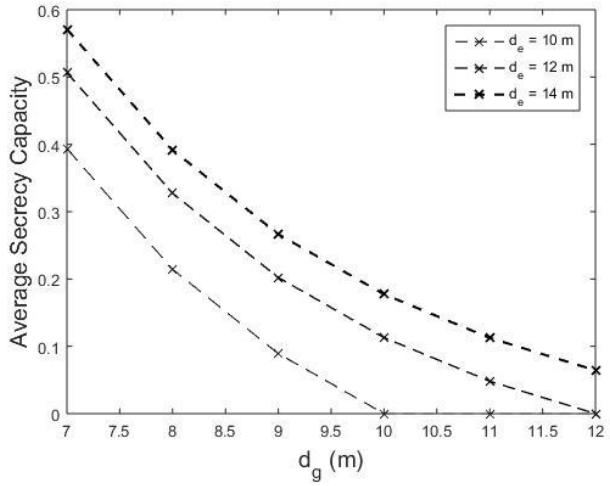


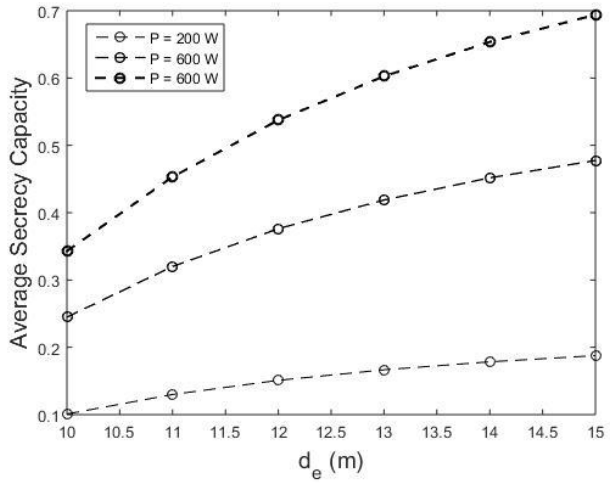
Fig. 2. Relationship between ground station/ number of meta-atoms and average secrecy capacity.



(a)



(b)



(c)

Fig. 3. Relationship between different distance values and average secrecy capacity.

4. Conclusion

This paper targets an important discussion in metasurface assisted communications and associated aspects. The rising interest in UAVs provides a clear indication of the significance of communication networks pertaining to them. It is paramount to make sure that critical areas, where UAVs are playing key roles, are kept safe from cyber-attacks. In the present day, there is a lot of emphasis on the use of sub-wavelength nanostructures to manipulate the properties of electromagnetic waves, carrying vehicular communication messages, to add an additional layer of security to the entire network. Several of these nanostructures can be fabricated onto planar surfaces called metasurfaces to provide a variety of control over the incident waves. In addition to that, the orientation of the nanostructures can also be reconfigured to change the ways in which wave matter interaction takes place. As discussed, the aim of this paper is to introduce the use of metasurfaces in UAV communication networks. Mathematical modelling and subsequent analysis of the Flying Adhoc Network (FANET) has been presented in the context of metasurfaces. The results present an encouraging view of the way ahead.

Table 1. List of symbols and notations.

Symbol	Description
x	Station signal
ε	Additive White Gaussian Noise (AWGN)
$\emptyset_{,n}$	Phase induced by the nth nano-antenna
h_s	Source to IRS channel coefficient
$h_{u,n}$	IRS to UAV channel coefficient
N	Number of nano-antennas on the metasurface
$\theta_{,n}$	Source to IRS channel phase component
$g_{s,n}$	Rayleigh fading for source to IRS channel
d_s	Source to IRS distance
d_u	IRS to UAV distance
d_g	Distance between IRS to Gateway UAV
d_e	Distance between IRS and Eavesdropper UAV
β	Path loss exponent
$g_{u,n}$	Double Rayleigh distribution (IRS to UAV channel)
$\psi_{,n}$	Phase Component (IRS to UAV channel)
P	Station Transmit Power
N_o	Power spectral density of AWGN
γ_g	Instantaneous SNR at Gateway UAV
γ_e	Instantaneous SNR at Eavesdropper UAV
C_s	Secrecy Capacity
$\mathbb{E}$	Expectation Operator
$\overline{C_G}$	Average Capacity of Gateway UAV
$\overline{C_E}$	Average Capacity of Eavesdroppe$_r$ UAV
$\overline{C_s}$	Average Secrecy Capacity
M_G	MGF of SNR at Gateway UAV
M_E	MGF of SNR at Eavesdropper UAV

[a]MGF stands for Moment Generating Function

Acknowledgements

This work was supported by NSERC (Natural Science and Engineering Council) of Canada, and by the IT4Innovations National Supercomputing Center - Path to exascale project (EF16_013/0001791), of Czech Republic.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] L. Reade, "Bombs over Venice," History Today, vol. 8, no. 6, Jun. 1958.

[2] M. Erdelj, E. Natalizio, K. R. Chowdhury and I. F.

Akyildiz, "Help from the sky: Leveraging UAVs for disaster management", IEEE Pervasive Comput., vol. 16, no. 1, pp. 24-32, Jan. 2017.

[3] R. Beard, T. McLain, D. Nelson, D. Kingston and D. Johanson, "Decentralized cooperative aerial surveillance using fixed-wing miniature UAVs", Proceedings of the IEEE, vol. 94, pp. 1306-1324, 2006.

[4] C. Yuan, Y. Zhang, and Z. Liu, "A survey on technologies for automatic forest fire monitoring, detection, and fighting using unmanned aerial vehicles and remote sensing techniques", Canadian Journal of Forest Research, vol.45, no.7, pp.783-792, 2015. J. Y.

[5] C. Chen, ''UAV-guided navigation for ground robot tele-operation in a military reconnaissance environment,'' Ergonomics, vol. 53, no. 8, pp. 940–950, Jul. 2010.

[6] A. Tahir, J. Böling, M.-H. Haghbayan, H. T. Toivonen and J. Plosila, "Swarms of unmanned aerial vehicles—A survey", J. Ind. Inf. Integr., vol. 16, Dec. 2019, [online] Available: http://www.sciencedirect.com/science/article/pii/S2452414X18300086.

[7] M. R. Brust and B. M. Strimbu, "A networked swarm model for uav deployment in the assessment of forest environments," in Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2015 IEEE Tenth International Conference on, pp. 1–6, IEEE, 2015.

[8] X. Chen, J. Tang, and S. Lao, "Review of Unmanned Aerial Vehicle Swarm Communication Architectures and Routing Protocols," Applied Sciences, vol. 10, no. 10, pp. 3661, May 2020.

[9] A. Chriki, H. Touati, H. Snoussi, and F. Kamoun, "FANET: Communication, mobility models and security issues," Comput. Netw., vol. 163, Nov. 2019, Art. no. 106877.

[10] J. A. Maxa, M. S. B. Mahmoud, and N. Larrieu, "Survey on UAANET Routing protocols and network security challenges," Ad Hoc Sensor Wireless Netw., 2017.

[11] F. Noor, M. A. Khan, A. Al-Zahrani, I. Ullah, and K. A. Al-Dhlan, "A review on communications perspective of flying ad-hoc networks: Key enabling wireless technologies, applications, challenges and open research topics," Drones, vol. 4, no. 4, p. 65, 2020.

[12] Y. Mekdad et al., "A Survey on Security and Privacy Issues of UAVs," 2021, [Online]. Available: http://arxiv.org/abs/2109.14442.

[13] S. He, Q. Wu, J. Liu, W. Hu, B. Qin, and Y.-N. Li, ''Secure communications in unmanned aerial vehicle network,'' in Proc. Int. Conf, Inf. Security Pract. Exper. Springer, vol. 2017, pp. 601–620.

[14] J. Won, S.-H. Seo, and E. Bertino, "A secure communication protocol for drones and smart objects," in Proc. 10th ACM Symp. Inf. Comput. Commun. Security (ASIA CCS), 2015, pp. 249–260.

[15] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via joint trajectory and power control," IEEE Trans. Wireless Commun., vol. 18, no. 2, pp. 1376–1389, Feb. 2019.

[16] J. Hu, S. Bandyopadhyay, Y. H. Liu, and L. Y. Shao, "A Review on Metasurface: From Principle to Smart Metadevices," Front. Phys., vol. 8, no. January, pp. 1–20, 2021, doi: 10.3389/fphy.2020.586087.

[17] J. Hu, S. Bandyopadhyay, Y. H. Liu, and L. Y. Shao, "A Review on Metasurface: From Principle to Smart Metadevices," Front. Phys., vol. 8, no. January, pp. 1–20, 2021, doi: 10.3389/fphy.2020.586087.

[18] A. Li, S. Singh, and D. Sievenpiper, "Metasurfaces and their applications," Nanophotonics, vol. 7, no. 6, pp. 989–1011, 2018, doi: 10.1515/nanoph-2017-0120.

[19] N. A. Otman and M. Cada, "Phase-Matched Mid-Infrared Difference Frequency Generation Using a Nanostructured Gallium Arsenide Metamaterial with Nanoholes," IEEE Photonics J., vol. 12, no. 3, 2020, doi: 10.1109/JPHOT.2020.2992192.

[20] H. Zhao, Y. Shuang, M. Wei, T. J. Cui, P. del Hougne, and L. Li, "Metasurface-assisted massive backscatter wireless communication with commodity Wi-Fi signals," Nat. Commun., vol. 11, no. 1, pp. 1–10, 2020, doi: 10.1038/s41467-020-17808-y.

[21] A. Raza, S. H. R. Bukhari, F. Aadil, and Z. Iqbal, "An UAV-assisted VANET architecture for intelligent transportation system in smart cities," Int. J. Distrib. Sens. Networks, vol. 17, no. 7, 2021, doi: 10.1177/15501477211031750.

[22] S. Taravati and G. V. Eleftheriades, "Intelligent-Metasurface-Assisted Full-Duplex Wireless Communications," pp. 1–7, 2021, [Online]. Available: http://arxiv.org/abs/2105.09436.

[23] A. Asim, "Ultraviolet Vortex Generation through All-Dielectric Nano-Antennas for Free Space Optical Communication," vol. 96, no. February, pp. 121–128, 2021.

[24] H. Chourabi, T. Nam, S. Walker, J. R. Gil-Garcia, S. Mellouli, K. Nahon, T. A. Pardo, and H. J. Scholl, "Understanding smart cities: An integrative framework," in System Science (HICSS), 2012 45th Hawaii International Conference on. IEEE, 2012, pp. 2289–2297.

[25] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li, and R. Kharel, "Physical Layer Security in Vehicular Networks with Reconfigurable Intelligent Surfaces," IEEE Veh. Technol. Conf., vol. 2020-May, pp. 3–8, 2020, doi: 10.1109/VTC2020-Spring48590.2020.9128438.

[26] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, "On Physical Layer Security of Double Rayleigh Fading Channels for Vehicular Communications," IEEE Wireless Commun. Lett., vol. 7, no. 6, pp. 1038–1041, Dec. 2018..

[27] J. Salo, H. M. El-Sallabi, and P. Vainikainen, "The distribution of the product of independent Rayleigh random variables," IEEE Trans. Antennas Propag., vol. 54, no. 2, pp. 639–643, Feb. 2006.