Awareness of National Cyber Security Weaknesses Due to Cyber-Attacks Through the Use of UAV

[1*]Muhammad Quazy Bin Razali, [2]Adnan Shahid Khan, [3]Shalin Binti Shaheezam Khan and [4]Aruen Anak Manggau

[1]Jabatan Imigresen Malaysia, Negeri Sarawak, Aras 1, Bangunan Sultan Iskandar, Jalan Simpang Tiga, 93550 Kuching, Sarawak, Malaysia
[2, 3, 4]Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia

email: [1*]muhammad_quazy@imi.gov.my, [2]skadnan@unimas.my [3]21030393@siswa.unimas.my, [4]21030394@siswa.unimas.my

**Corresponding author*

Received: 04 September 2022 | Accepted: 14 March 2023 | Early access: 06 April 2023

Abstract - *Unmanned Aerial Vehicle (UAV) is a utility tool created to provide a simple task and provide an important impact in matters of national defence, especially on the military side to monitor terrorists in camp areas and also on the borders of the country, to preserve the well-being and prosperity of the people in our country is always guaranteed. However, UAVs have been misused by certain parties to fulfil their interests. This lack of integrity in the use of UAV equipment should be curbed so that it does not continue with proper disclosure and understanding. Every day, various issues arise due to the misuse of technology, which will affect society and the country. Therefore, the government is making every effort to deal with the problem because the limited awareness of the use of UAVs is very worrying, especially the monitoring from the authorities. The authorities should also play an important role in enacting regulations and laws against those who misuse these UAV devices.*

Keywords: Awareness, Unmanned Aerial Vehicle, Cyber Security, Threats, Responsibilities.

1 Introduction

Unmanned aerial vehicles (UAVs) are being used more and more every day. Now there are many models of UAVs because of demands for monitoring work for organizations such as agriculture, development, military, network services, traffic control, real estate, delivery of medical supplies and so on in facilitating business using UAV tools (Gromada & Stecz, 2021). Nevertheless, there are a few irresponsible parties who misuse UAV equipment for other uses such as espionage which can disturb the peace and privacy of other individuals, leading to sexual harassment more extreme at the moment, hacking such equipment is becoming more and more common. This matter should be given attention by the authorities by enacting new regulations and laws to deal with this non-permanent problem (Pan et al., 2022).

Various new models of UAVs are being created and marketed according to the demands of specific users or organizations in addition to current technology specifications. The market value of UAVs also depends on the quality of the features found on the vehicle, the more sophisticated the features found in the use of the UAV, the higher the market value, and it also depends on the size of the design and the ability of the UAV to bear the load carried. These UAVs are common in other countries where they are used as a service to deliver supplies to those living in high-rise apartment buildings (Asghar Khan et al., 2022).

Therefore, with the availability of UAV technology, those who use it should have adequate awareness to avoid misuse. Nowadays, it is more about the parties' understanding of the use of these UAVs for cyber security (Haider et al., 2022). The authorities must take various steps before the organization owns this UAV. They should know more about it, for example, place a license on the owner of this UAV. Although it looks like a machine, this UAV

does not have a driver but is controlled using various types of remote-control devices which can lead to misuse of the UAV (Wu et al., 2022). We can see in the diagram below an example of a basic UAV control.
In the current technology of IoT and Industry 4.0, UAV is a network that gathers data from IoT devices in other words, it has been implemented into one of today's technology networks, namely Green IoT and B5G (Beyond 5G) at the same time it makes the world smarter in crossing the telecommunications network, therefore this truth has been explained through the article "Ad Hoc Network" which describes how UAVs are used in today's network services (Tomaszewski et al., 2022; Alsamhi et al., 2021).

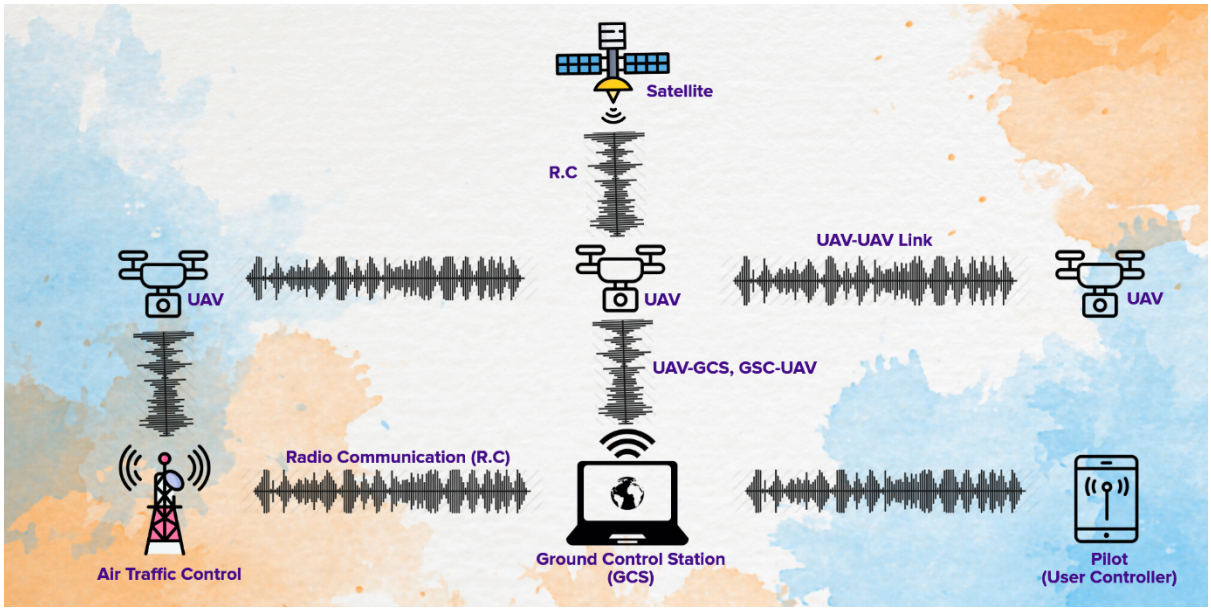

Figure 1: Basic and generic architecture of UAV

The rest of the paper is organized as follows: The abstract is in the first part and Section 1 provides a brief introduction to Unmanned Aerial Vehicle's general overview. Section 2 discusses the literature review which includes a summarization of 10 articles. Section 3 discusses the taxonomy of technology from perspectives of attacks and techniques used to mitigate attacks. Section 4 elaborates on research trends, and challenges faced by this technology and predicts future research directions. Finally, conclusions are made in Section 5 followed by acknowledgement and references.

2 Literature Review

Alrefaei et al. (2022) examine the effects of UAV wireless network's jamming and spoofing assault as well as the earlier traditional security detection and defensive mechanisms. It also discusses the advantages of deep learning technology and demonstrates how it may be used to safeguard UAV networks. The UAV demonstrates its adaptability to usage and application for various tasks. The performance of the UAV system degrades due to threats that might affect natural UAV communication connections. The adversary discovered that it is simple to carry out their easy task by listening to the transmission data. This article discusses several assault defence strategies and threat detection methods.

This study suggests BISSIAM, a unique framework that can recognise UAVs' existence, varieties, and operational modes (Li et al., 2021) this sentence is incomplete. A sampling procedure is provided to maximise the training sample size without sacrificing model correctness or training effectiveness. Also, to detect unseen UAVs without retraining the entire model, developing a similarity-based fingerprint-matching approach this sentence is incomplete. The results of the experiments demonstrate that the method beats existing baselines and can detect UAVs with 92.85% accuracy in unsupervised learning settings.

Li et al. (2020) discuss physical layer security problems in unmanned aerial vehicles (UAVs) communication networks. An iterative technique is suggested to achieve this goal by simultaneously optimising the trajectory and transmit power of the two UAVs. Simulation results show that, compared to the standards, the suggested system may significantly increase secrecy rates. Simulations showed that the suggested optimization technique presents

more desirable flying trajectories compared to the benchmarks and may greatly increase the system secrecy rate performance.
In the article by Abhishek et al. (2022), UAV-aided networks introduced the Malicious Aerial Vehicle Detection (MaDe) lightweight data integrity preservation technique. Every sensor in MaDe periodically sends out a feedback packet. MaDe will spot any UAV tampering with the packets which carry authentication on each packet sent or received by the sensor and base station. None of these computationally intensive cryptographic methods is used to do this. MaDe delivers much lower overhead and latency than existing techniques, according to communication overhead and latency measurements. The outcomes demonstrate MaDe's exceptional effectiveness in detecting data tampering attempts and identifying rogue UAVs.

In the article by Yang et al. (2022) the security concerns and solutions for the Internet of Things are thoroughly reviewed, along with the security needs specific to the Internet of Things and the most recent developments in IoD security research. A variety of significant security technologies are examined in this analysis, with a focus on authentication methods and blockchain-based systems. The researchers outline the difficulties that existing approaches confront and suggest future IoD security research options based on a thorough review. This study reviews security vulnerabilities in the IoD discusses solutions already in place, and analyses the difficulties that IoD security faces. Although there are other defences and fixes, this research focuses on two key strategies: authentication and blockchain-based methods.

Maikol et al. (2021) suggest a brand-new authentication method for mobile users of cloud computing. The suggested remedy uses a key agreement mechanism with two layers of protection. The impersonation attack and MITM can be reduced, according to a thorough review of the current authentication technique and the suggested scheme. As it offers mutual authentication between sender and recipient, it helps to lower the danger of impersonation attacks. The likelihood of MITM will be reduced since the domain parameter used to generate the digital signature is chosen at random. The suggested remedy will entice more studies into cryptography-based two-layer security by researchers. The investigation demonstrates that these techniques would significantly improve and reinforce the medical system's data protection security.

3 Taxonomy

In this taxonomy, some things will be expressed in the awareness of the use of UAVs that are a weakness to the country's cyber security that refers to attacks and also techniques to repel from attacks:

3.1 Cyber Attack

A statement, in an article by Khoei et al. (2022) is a fraudulent attack through the GPS signal that can direct the UAV to lose control of the owner who will be disturbed by hackers who may once intend to steal the UAV from its original owner. According to Yang et al. (2022), the effort of hackers who want to hack specific organizations such as the military through IoD is very worrying when they can penetrate cyberspace through UAVs that are being done by the army. Similarly, Alrefaei et al. (2022) state that the hacker's act of jamming and spoofing is through the communication network of the UAV control device, and the hacker will penetrate the database in an organization. According to Pan et al. (2022), the hacker will turn off the cellular network which is the cellular service installed on the UAV itself as soon as the hacker can penetrate the network into the user's device that currently has a line with the UAV's cellular network. In addition, Abhishek et al. (2022) state that hackers will access data through UAVs in cyber data space, and it is very dangerous if hackers successfully enter this cyber data space.

3.2 Techniques Used to Mitigate Attacks

There are several methods and techniques to reduce attacks from hackers, namely, through the Classification Group Tree method and also the Regression technique that can detect the actions of hackers who want to hack through the UAV communication network (Khoei et al., 2022). On the other hand, Yang et al. (2022) suggest improving IoD techniques on UAVs by applying authentication techniques and block-powered schemes to avoid hacker attacks. According to Asghar Khan et al. (2022), a method of increasing the application of the authentication scheme is hyperelliptic curve cryptography (HECC), a technique aimed at digital signatures in preserving the privacy of the UAV user itself. Another technique is applying Blockchain Technology to UAVs (Tan et al., 2022) by storing UAV verification information at a low cost to industries and organizations that use these UAVs. Qiu et al. (2020) suggest applying blockchain on UAVs by increasing the chain spectrum on cellular networks installed on UAVs. The spectrum-sharing technique on UAVs stated in the article by Li et al. (2020) is designed to combat the eavesdropping of system secrecy and to further optimise the trajectory in further increasing

the rate of secrecy with benchmarks. The method in the article by Na et al. (2022) further optimizes the trajectory in UAV communication that provides Internet of Things (IoT) resources to the community whose mobility has been installed on the UAV and with the results of the researcher's study of this article, it further increases the confidentiality of the IoT user's information itself.

4 Research Trends

The awareness of UAV users is to provide an understanding of using UAVs today, as stated in the article by Durfey and Sajal (2022), this UAV is a machine that can change the world today towards danger in putting an individual at risk involving the country. This article has researched the issue of cyber threats with the efforts of researchers so that the users of this UAV are safe from any cyber threats. Abhishek et al. (2022) stressed that the lack of integrity of data and information in the country should be curbed so that it does not leak to irresponsible parties, even though with the current technology, the country's cyber security should be tightened against any threat. While Lu et al. (2022) emphasized that the repeated algorithm is safe if it is applied to the use of UAVs, and this shows that this should be applied in the awareness course of the use of UAVs nowadays to be better understood.

Sun et al. (2022), noted that network collaboration is more secure in the use of this UAV because it has the characteristics of secure and energy-efficient communication multi-objective optimization problem (SECMOP) which can guarantee the safety of the community and the country. According to Ferrao et al. (2020), to increase the productivity and economy of the country, there are increasing market demands for UAVs because they greatly facilitate business for industries and organizations that practice the use of UAVs in addition to improving the characteristics of safety features for UAV users from time to time the original sentence is too long and confusing. Therefore, the awareness of the use of UAVs should be evaluated for the weaknesses and also the ability of these UAVs to be used in the future because the safety of the community and the country should be emphasized so that it is guaranteed and safe to be used in various sectors in the country today Chaari et al. (2020).

5 Challenges

In the challenge of giving awareness to UAV users, this should be studied and researched first before providing exposure to those who use this UAV tool so that its use is clear. Therefore, based on the article by Ying et al. (2019) safety involving air traffic may occur because it depends on the Automatic Dependent Surveillance-Broadcast (ADS-B) system used by the aviation department during monitoring by the International Civil Aviation Organization (ICAO) which points to measure a movement in space. Likewise, as stated in the article by Romesburg et al. (2021) the use of UAVs exploring the space path area in addition to the existence of Software-Defined Radio (SDR) because it applies a game system such as a UAV and also a penetration test for the radio system for the aviation department today, this is important to know in the challenge of widespread use of UAVs the meaning in this sentence is not clear. In addition to that, according to Tiu and Zolkipli (2021), a significant challenge is ransomware attacks which are no stranger nowadays because they are an alternative for hackers to carry out cyber-attacks.

Breaking down the cyber threat in the article by Durfey and Sajal (2022) it is a challenge to cyber security today. Moreover, it is widely used in various industries and also organizations to facilitate their work, the national defence department in cooperation with the authorities has taken the initiative in terms of misuse of this UAV tool. At the same time according to Wang et al. (2020) the most critical challenge is interference with CPS, especially with the data and information available in the country, the invasion can happen at any time without notification in detecting the country's cyber threat. We must look at this from all aspects so that the national communication network is always safe from any national cyber security intruding.

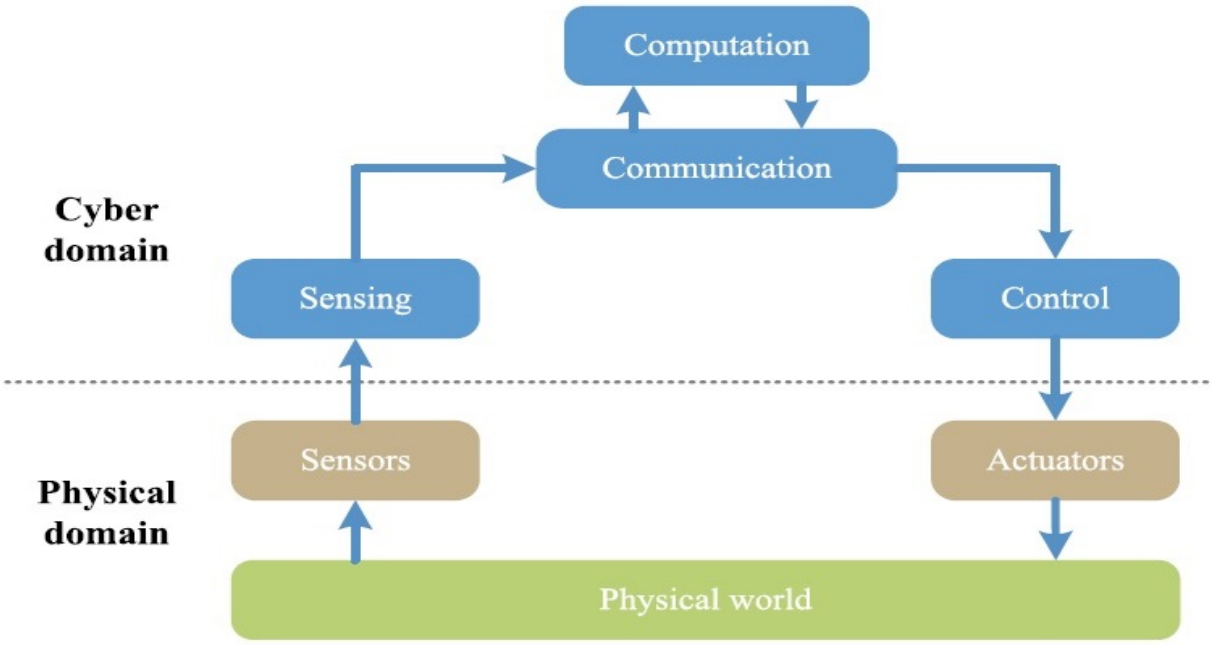

Figure 2: Cyber-physical system (CPS) diagram

Wang et al. (2020) discussed the integration of embedded systems on UAVs that allow them to be integrated with cyber processes into the physical UAV itself. Therefore, UAV is a Cyber-Physical System (CPS) which has three components which are cell level, system level, and system level in addition it is combined with CPS components as shown in figure 2 which is clear in dealing with any threat cyber-physical.

6 Future Direction

In the future direction, we can observe the widespread use of UAVs due to the many market requests, especially because they have the latest technological features to facilitate all work or affairs from various industries and organizations. According to Li et al. (2021), the production of UAV machinery needs to provide features that have been studied by researchers such as Bispectrum Siamese (BISSIAM) because these features will better guarantee security in applying network coding on UAV devices so that it is not misused in the future. Heo et al. (2022) considered the existence of UAVs as a contributor to the IoT today by establishing a block verification network with network coding widely which can guarantee any threat to UAV user misconduct. While Ma et al. (2022) stressed that this UAV has been promoted as a tool for providing data replacement services, content caching and also the implementation of computing tasks through Edge Computing Devices (ECD). With the existence of ECD, it focuses on algorithms for computing resources optimally in performing tasks, therefore, various workload tasks can be effectively overcome if applied with the characteristics stated by the researcher.

According to Al-Khafaji and Elwiya (2022), to further improve today's industrial technology such as Artificial Intelligence (AI) and Machine Learning (ML) is an important thing that must be further improved so that the country can progress with a sustainable economic position for the country and also the community. Abhishek et al. (2022) suggested that the spirit of increasing the integrity of UAV users should be fostered so that it is in line with the rules and laws in the use of UAVs to give more trust to the authorities. Some features must be present in the creation of UAVs in the future by applying Secure Internet-of-Drones (IoD) because applying Secure IoD is a low cost for the creation of UAVs in the future as stated by Pu et al. (2022). The most important thing for the future direction is to provide exposure and understanding to UAV users so that they are more alert to any cyber threat as stated by Abo Mosali et al. (2022). This is important in providing training or courses to those who apply its use in facilitating their tasks to industry and also organizations. In addition, Xing et al. (2022) emphasized that the features of UAVs can help in post-disaster situations, especially when there is a possibility of unexpected things happening such as no one has a cellular network due to the disaster and it is an alternative that will make it easier for the organization to carry out tasks such as monitoring. Lastly, deep learning methods, Blockchain and multifactor authentication methods can also be used and implemented to mitigate several communication attacks (Ahmad et al., 2020; Khan et al., 2021; Khan et al., 2022; Asim et al., 2022).

7 Conclusions

In conclusion, it is crucial for users in various industries nowadays to be exposed to and to be aware of using UAV tools. If necessary, users must have a license and have completed an official authority course before using UAVs. It is crucial to guarantee cyber security and strengthens the nation's defence against cyber threats by today's irresponsible actors. Therefore, the NGO side or the legislative body of the ministry of cyber security in Malaysia always emphasizes the responsibility of the superiors in an organization who need to play a critical role in cyber security and not just rely entirely on the information and technology (IT) department. At the same time, a strategic approach must be taken in addition to ensuring that their employees are aware of cyber security through workshops or courses implemented by the organization.

Therefore, the disclosure that provides ethics and integrity courses to UAV users is very important for the well-being of various parties especially when it can reduce the risk of cyber threats. In addition, the administration or human resources in an organization should always emphasize the Professional Development of Cyber Security in Malaysia, with the help of external agencies in cyber security which has now developed into a new platform to cultivate information security practitioners and knowledge sharing with leading industry experts and academics as well as fostering local and international cooperation to intensify the prevention of cyber security threats such as these UAVs from being misused by certain parties. At the same time fostering information security competence and specific training in Malaysia and is also the presenter of a line of competence courses from various programs and professional certifications aimed at meeting the needs of a fast and secure cyber landscape from unwanted threats. Therefore, the study of this article is expected to give awareness to UAV users to increase understanding as well as integrity and ethics in using UAV tools to deal with any threats from irresponsible parties in particular.

References

Abhishek, N. V., Aman, M. N., Lim, T. J., & Sikdar, B. (2022a). PIC: Preserving Data Integrity in UAV-Assisted Communication. IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). https://doi.org/10.1109/infocomwkshps54753.2022.9798213

Abhishek, N. V., Aman, M. N., Lim, T. J., & Sikdar, B. (2022b). MaDe: Malicious Aerial Vehicle Detection using Generalized Likelihood Ratio Test. ICC 2022 - IEEE International Conference on Communications. https://doi.org/10.1109/icc45855.2022.9838465

Abo Mosali, N., Shamsudin, S. S., Alfandi, O., Omar, R., & Al-Fadhali, N. (2022). Twin Delayed Deep Deterministic Policy Gradient-Based Target Tracking for Unmanned Aerial Vehicle With Achievement Rewarding and Multistage Training. IEEE Access, 10, 23545–23559. https://doi.org/10.1109/access.2022.3154388

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1). https://doi.org/10.1002/ett.4150

Al-Khafaji, M., & Elwiya, L. (2022). ML/AI Empowered 5G and beyond Networks. 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). https://doi.org/10.1109/hora55278.2022.9799813

Alrefaei, F., Alzahrani, A., Song, H., & Alrefaei, S. (2022). A Survey on the Jamming and Spoofing attacks on the Unmanned Aerial Vehicle Networks. 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS). https://doi.org/10.1109/iemtronics55184.2022.9795809

Alsamhi, S., Afghah, F., Sahal, R., Hawbani, A., Al-qaness, M. A., Lee, B., & Guizani, M. (2021). Green internet of things using UAVs in B5G networks: A review of applications and strategies. Ad Hoc Networks, 117, 102505. https://doi.org/10.1016/j.adhoc.2021.102505

Asghar Khan, M., Ullah, I., Alkhalifah, A., Ur Rehman, S., Ali Shah, J., Uddin, I., Alsharif, M. H., & Algarni, F. (2022). A Provable and Privacy-Preserving Authentication Scheme for UAV-Enabled Intelligent Transportation Systems. IEEE Transactions on Industrial Informatics, 18(5), 3416–3425. https://doi.org/10.1109/tii.2021.3101651

Asim, J., Khan, A. S., Saqib, R. M., Abdullah, J., Ahmad, Z., Honey, S., Afzal, S., Alqahtani, M. S., & Abbas, M. (2022). Blockchain-based Multifactor Authentication for Future 6G Cellular Networks: A Systematic Review. Applied Sciences, 12(7), 3551. https://doi.org/10.3390/app12073551

Chaari, L., Chahbani, S., & Rezgui, J. (2020). Vulnerabilities Assessment for Unmanned Aerial Vehicles Communication Systems. 2020 International Symposium on Networks, Computers and Communications (ISNCC). https://doi.org/10.1109/isncc49221.2020.9297293

Durfey, N., & Sajal, S. (2022). A Comprehensive Survey: Cybersecurity Challenges and Futures of Autonomous Drones. 2022 Intermountain Engineering, Technology and Computing (IETC). https://doi.org/10.1109/ietc54973.2022.9796881

Gromada, K. A., & Stecz, W. M. (2021). Designing a Reliable UAV Architecture Operating in a Real Environment. Applied Sciences, 12(1), 294. https://doi.org/10.3390/app12010294

Haider, M., Ahmed, I., & Rawat, D. B. (2022). Cyber Threats and Cybersecurity Reassessed in UAV-assisted Cyber Physical Systems. 2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN). https://doi.org/10.1109/icufn55119.2022.9829584

Heo, G., Chae, K., & Doh, I. (2022). Hierarchical Blockchain-Based Group and Group Key Management Scheme Exploiting Unmanned Aerial Vehicles for Urban Computing. IEEE Access, 10, 27990–28003. https://doi.org/10.1109/access.2022.3157753

Khan, A. S., Ahmad, Z., Abdullah, J., & Ahmad, F. (2021). A Spectrogram Image-Based Network Anomaly Detection System Using Deep Convolutional Neural Network. IEEE Access, 9, 87079–87093. https://doi.org/10.1109/access.2021.3088149

Khan, A. S., Balan, K., Javed, Y., Tarmizi, S., & Abdullah, J. (2019). Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. Sensors, 19(22), 4954. https://doi.org/10.3390/s19224954

Khan, A. S., Javed, Y., Abdullah, J., & Zen, K. (2021). Trust-based lightweight security protocol for device to device multihop cellular communication (TLwS). Journal of Ambient Intelligence and Humanized Computing. https://doi.org/10.1007/s12652-021-02968-6

Khan, A. S., Javed, Y., Saqib, R. M., Ahmad, Z., Abdullah, J., Zen, K., Abbasi, I. A., & Khan, N. A. (2022). Lightweight Multifactor Authentication Scheme for NextGen Cellular Networks. IEEE Access, 10, 31273–31288. https://doi.org/10.1109/access.2022.3159686

Khoei, T. T., Gasimova, A., Ahajjam, M. A., Shamaileh, K. A., Devabhaktuni, V., & Kaabouch, N. (2022). A Comparative Analysis of Supervised and Unsupervised Models for Detecting GPS Spoofing Attack on UAVs. 2022 IEEE International Conference on Electro Information Technology (EIT). https://doi.org/10.1109/eit53891.2022.9813826

Li, T., Hong, Z., Cai, Q., Yu, L., Wen, Z., & Yang, R. (2021). BISSIAM: Bispectrum Siamese Network Based Contrastive Learning for UAV Anomaly Detection. IEEE Transactions on Knowledge and Data Engineering, 1–1. https://doi.org/10.1109/tkde.2021.3118727

Lu, X., Xiao, L., Niu, G., Ji, X., & Wang, Q. (2022). Safe Exploration in Wireless Security: A Safe Reinforcement Learning Algorithm With Hierarchical Structure. IEEE Transactions on Information Forensics and Security, 17, 732–743. https://doi.org/10.1109/tifs.2022.3149396

Ma, X., Su, Z., Xu, Q., & Ying, B. (2022). Edge Computing and UAV Swarm Cooperative Task Offloading in Vehicular Networks. 2022 International Wireless Communications and Mobile Computing (IWCMC). https://doi.org/10.1109/iwcmc55113.2022.9824275

Na, Z., Ji, C., Lin, B., & Zhang, N. (2022). Joint Optimization of Trajectory and Resource Allocation in Secure UAV Relaying Communications for Internet of Things. IEEE Internet of Things Journal, 9(17), 16284–16296. https://doi.org/10.1109/jiot.2022.3151105

Pan, X., Jin, Y., Wang, Z., & Li, F. (2022). A Pairing-Free Heterogeneous Signcryption Scheme for Unmanned Aerial Vehicles. IEEE Internet of Things Journal, 9(19), 19426–19437. https://doi.org/10.1109/jiot.2022.3167102

Pu, C., Wall, A., Ahmed, I., & Choo, K. K. R. (2022). SecureIoD: A Secure Data Collection and Storage Mechanism for Internet of Drones. 2022 23rd IEEE International Conference on Mobile Data Management (MDM). https://doi.org/10.1109/mdm55031.2022.00033

Qiu, J., Grace, D., Ding, G., Yao, J., & Wu, Q. (2020). Blockchain-Based Secure Spectrum Trading for Unmanned-Aerial-Vehicle-Assisted Cellular Networks: An Operator's Perspective. IEEE Internet of Things Journal, 7(1), 451–466. https://doi.org/10.1109/jiot.2019.2944213

Romesburg, H., Wang, J., Jiang, Y., Wang, H., & Song, H. (2021). Software Defined Radio based Security Analysis For Unmanned Aircraft Systems. 2021 IEEE International Performance, Computing, and Communications Conference (IPCCC). https://doi.org/10.1109/ipccc51483.2021.9679408

Maikol, S. O., Khan, A. S., Javed, Y., Bunsu, A. L., Petrus, C., George, H. & Jau, S. (2021). A Novel Authentication and Key Agreement Scheme for Countering MITM and Impersonation Attack in Medical Facilities. The International Journal of Integrated Engineering, 13(2), 127–135. https://doi.org/10.30880/ijie.2021.13.02.015

Sun, G., Li, J., Wang, A., Wu, Q., Sun, Z., & Liu, Y. (2022). Secure and Energy-Efficient UAV Relay Communications Exploiting Collaborative Beamforming. IEEE Transactions on Communications, 70(8), 5401–5416. https://doi.org/10.1109/tcomm.2022.3184160

Tan, Y., Wang, J., Liu, J., & Kato, N. (2022). Blockchain-Assisted Distributed and Lightweight Authentication Service for Industrial Unmanned Aerial Vehicles. IEEE Internet of Things Journal, 9(18), 16928–16940. https://doi.org/10.1109/jiot.2022.3142251

Tiu, Y. L., & Zolkipli, M. F. (2021). Study on Prevention and Solution of Ransomware Attack. Journal of IT in Asia, 9(1), 133–139. https://doi.org/10.33736/jita.3402.2021

Tomaszewski, L., Kołakowski, R., Dybiec, P., & Kukliński, S. (2022). Mobile Networks' Support for Large-Scale UAV Services. Energies, 15(14), 4974. https://doi.org/10.3390/en15144974

Wang, H., Zhao, H., Zhang, J., Ma, D., Li, J., & Wei, J. (2020). Survey on Unmanned Aerial Vehicle Networks: A Cyber Physical System Perspective. IEEE Communications Surveys &Amp; Tutorials, 22(2), 1027–1070. https://doi.org/10.1109/comst.2019.2962207

Wu, J., Guo, J., & Lv, Z. (2022). Deep Learning Driven Security in Digital Twins of Drone Network. ICC 2022 - IEEE International Conference on Communications. https://doi.org/10.1109/icc45855.2022.9838734

Xing, R., Su, Z., Luan, T. H., Xu, Q., Wang, Y., & Li, R. (2022). UAVs-Aided Delay-Tolerant Blockchain Secure Offline Transactions in Post-Disaster Vehicular Networks. IEEE Transactions on Vehicular Technology, 71(11), 12030–12043. https://doi.org/10.1109/tvt.2022.3184965

Yang, W., Wang, S., Yin, X., Wang, X., & Hu, J. (2022). A Review on Security Issues and Solutions of the Internet of Drones. IEEE Open Journal of the Computer Society, 3, 96–110. https://doi.org/10.1109/ojcs.2022.3183003

Yin, Z., Jia, M., Cheng, N., Wang, W., Lyu, F., Guo, Q., & Shen, X. (2022). UAV-Assisted Physical Layer Security in Multi-Beam Satellite-Enabled Vehicle Communications. IEEE Transactions on Intelligent Transportation Systems, 23(3), 2739–2751. https://doi.org/10.1109/tits.2021.3090017

Ying, X., Mazer, J., Bernieri, G., Conti, M., Bushnell, L., & Poovendran, R. (2019). Detecting ADS-B Spoofing Attacks Using Deep Neural Networks. 2019 IEEE Conference on Communications and Network Security (CNS). https://doi.org/10.1109/cns.2019.8802732