Recapitulation of Survey on Taxonomy: Security Unmanned Aerial Vehicles Networks

[1]Veronica Sima Anak Kilat,[2*]Adnan Shahid Khan, [3]Eunice James and [4]Nayeem Ahmad Khan

[1,2,3]Faculty of Computer Science and Information Technology, 94300 Kota Samarahan, Sarawak, Malaysia
[4]Faculty of Computer Science and Information Technology, AlBaha University, AlBaha, Saudi Arabia

email: [1]22030072@siswa.unimas.my, [2*]skadnan@unimas.my, [3]21030614@siswa.unimas.my, [4]nayeem@bu.edu.sa

*Corresponding author

Received: 04 September 2022 | Accepted: 11 April 2023 | Early access: 26 April 2023

Abstract - *The operation of unmanned aerial vehicles (UAVs) presents various challenges for radio spectrum management. It is crucial to ensure safety, effective spectrum use, and compatibility with existing wireless networks. However, the dynamic nature of UAV networks requires adaptive spectrum decisions and resilient schemes that can provide reliable services. Current spectrum schemes may have limitations when used in UAV networks. Nevertheless, the integration of communication technology, computation power, and control modules in UAV networks can construct a comprehensive sequence of data detecting, intelligence transferring, deliberation, and final implementation, which facilitates cyber processes in physical devices. This integration turns the UAV network into a cyber-physical system (CPS). The internet of everything (IoE) is the concept of an all-encompassing network connecting everything. It is facing significant obstacles, such as limited broadband service and shortages in existing network technology. UAVs have recently gained attention due to their mobility, affordability, and versatility. They have the potential to circumvent the challenges faced by IoE. This paper aims to provide an overview of UAVs from a different perspective, highlighting the challenges they present and discussing future research directions to ensure a proper plan for the future. With the proliferation of UAVs, it is essential to address issues related to their safe operation, efficient use of spectrum, and compatibility with existing networks. Moreover, research should focus on developing resilient schemes that can deliver smooth and reliable services in UAV networks. In conclusion, the operation of UAVs poses several challenges for radio spectrum management, but they also offer opportunities for innovation and development. The integration of communication technology, computation power, and control modules in UAV networks turns them into cyber-physical systems with the potential to overcome the challenges faced by IoE. Further research is necessary to ensure safe and efficient operation, and to explore the possibilities that UAVs offer for the future.*

Keywords: Unmanned Aerial Vehicle (UAV), Security, IoE, Cyber Security.

1 Introduction

Unmanned aerial vehicles (UAVs), often known as drones, are becoming increasingly essential in a variety of fields, including both the military and the civilian spheres. These qualities, along with their relatively low cost and ease of deployment, contribute to the UAVs' growing prominence (Fotohi, 2020). When it comes to military applications, UAVs are anticipated to become an essential component of the future frontlines. Not only are they able to proactively capture a variety of information on a vast scale in terms of both time and location, but they may also benefit other unmanned and manned combat platforms in completing potentially hazardous operations. UAVs' flight can be remotely piloted by a human, similar to remotely piloted aircraft (RPA), or they can have varying ranges of autonomy, such as autopilot help, up to fully autonomous aircraft that don't allow for human intervention. Nowadays, the majority of UAVs have the ability to conduct both attack and surveillance missions. UAVs are also being utilised more frequently for non-commercial purposes, like putting out fires. UAVs are often used in missions that are very "boring, dirty, or dangerous" for a guided aircraft.

In addition to military applications, UAVs are being used in a wide range of civilian applications. They are being used for surveying and mapping, monitoring wildlife and environmental conditions, inspecting infrastructure such as bridges and power lines, conducting search and rescue operations, and delivering goods and services. In the agricultural sector, UAVs are being used to monitor crop health, track weather patterns, and optimize irrigation and fertilizer use. The construction industry is using UAVs for site surveying, tracking construction progress, and inspecting structures (Mohammad et al., 2023).

UAVs are also being used for entertainment purposes, such as in aerial photography and videography for film and television production. They are also used in sports broadcasting, providing unique and exciting camera angles and perspectives that were previously unavailable.

One of the most significant benefits of UAVs is their ability to access hard-to-reach areas, such as disaster zones or remote wilderness areas. UAVs can provide real-time information to emergency responders, allowing them to make more informed decisions and save lives. In the field of wildlife conservation, UAVs are being used to monitor endangered species and to identify and prevent illegal poaching.

As UAV technology continues to advance, there are increasing concerns about privacy and security. Regulations around the use of UAVs are being developed to address these concerns, with restrictions on where and when they can be flown and what they can be used for. Despite these concerns, the growing versatility and affordability of UAVs are driving their increased use in a wide range of applications.

This survey article will discuss conceptually related works, taxonomy from the perspectives of attacks, and techniques used to mitigate the attacks. Furthermore, the end of this article will elaborate more on research trends and challenges faced, and discuss the future direction of UAVs. A few figures and tables can be referenced based on related works from various authors. This paper includes the abstract, introduction, related summary, taxonomy, research trends, challenges, future directions, conclusion, acknowledgement, and references.

2 Related Works

2.1 Survey on Networks of Unmanned Aerial Vehicles: Considerations from a Cyber-Physical Perspective

According to Wang (2019) discussion on dual cyber-physical systems (CPS), unmanned aerial vehicle (UAV) networks are gaining significant interest due to the benefits they offer in expanding human behavior without direct human involvement. Wang (2019) suggests that embedding UAVs into the CPS platform or creating UAV networks from the perspective of CPS could enhance their efficiency in performing various complex tasks. The study aims to conduct a comprehensive analysis of the CPS in relation to UAV networks.

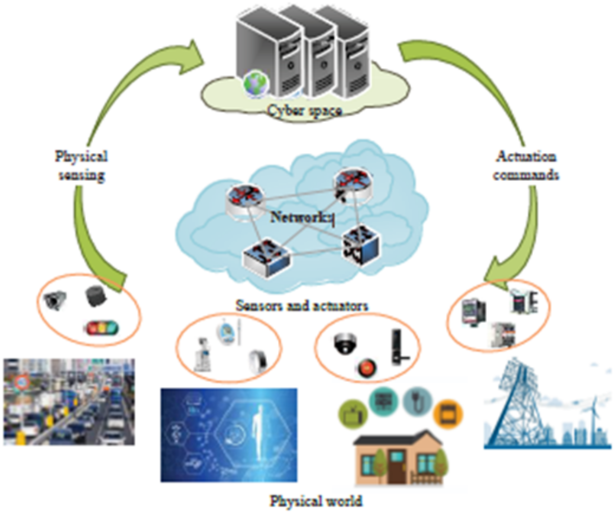

Figure 1: A conventional CPS framework

The author (Wang, 2019) acknowledges that both CPS and UAV networks are interdisciplinary, challenging, but exciting fields. The requirements, difficulties, and technology involved are numerous and continually evolving. This brief overview aims to provide a concise primer for newcomers and a cutting-edge CPS perspective to help researchers address the interdisciplinary issues. The author is confident that encouraging collaboration between CPS and UAV networks will strengthen both fields and improve our quality of life.

The National Aeronautics and Space Administration (NASA) was the first organization to recommend cyber-physical systems (CPS) for use in space research with unmanned aircraft. Since then, CPS has been applied to combat situations to reduce losses, where soldiers can remain in a staging area and operate weapons remotely, without physically being present on the battlefield. CPS has now been widely implemented in many society-critical areas as part of the "Industry 4.0" movement. This includes areas such as transportation, energy, healthcare, and manufacturing.

2.2 Opportunities and challenges presented by unmanned aerial vehicles in the context of the Internet of Everything

Research by Liu et al. (2020) aims to enhance the capabilities of the Internet of Everything (IoE) by utilizing unmanned aerial vehicles (UAVs) to improve its comprehensive understanding, flexible intelligence, and more varied applications. The implementation of IoE faces several obstacles related to coverage, battery, processing, and security concerns to meet the three IoE expectations of scalability, intelligence, and diversity. UAVs, with their high mobility and adaptable deployment, have the potential to assist IoE in overcoming these difficulties. In this context, Liu et al. (2020) have conducted a thorough analysis of the possibilities and fixes for UAVs in IoE, with two key components of the review being the UAS design and the analysis of UAV communication networks. The authors have investigated a variety of UAV applications in IoE, including ubiquitous connections, on-demand aerial intelligence, self-maintenance, power supply, sensor recycling, and more. Additionally, the authors have discussed current problems and Ue-IoE directions. Overall, the authors have thoroughly analyzed the advantages and disadvantages of deploying UAVs in IoE. For future investigations on Ue-IoE, this survey can serve as a study direction.

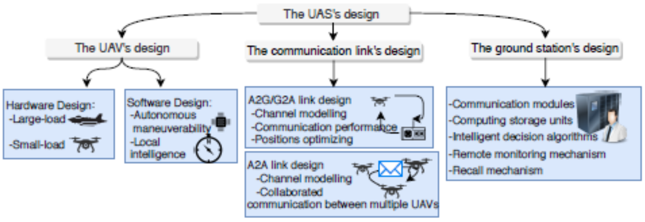

Figure 2: A system's unmanned aircraft design methodology (UAS)

2.3 Autonomous Spectrum Management for UAV Disaster Relief

In their research, Shamsoshoara et al. (2020) addressed the issue of spectrum scarcity in UAV networks during crucial missions, such as search and rescue operations, monitoring disasters, and wildfires. These missions require high-speed data transfers, including real-time streaming of speech, pictures, and video, and the spectrum allocated to the UAV network may not be sufficient to provide the required Quality of Service (QoS). Therefore, the researchers proposed a model for sharing the spectrum, in which one UAV serves as a relay, which transmits data to a grounded network in exchange for the necessary spectrum. Other UAVs can then use this spectrum to communicate the sensed data. The proposed approach was compared to other random distributions and assignments. The researchers also suggested offline learning to create a predetermined Q-table for larger grid-size planes, taking into account the exact location of the grid's aircraft for unsafe and dangerous areas, which saves time. Afterward, the UAVs can automatically move to the best place based on the Q-table in a completely greedy manner. The proposed approach can provide the necessary spare spectrum to the UAV network during crucial missions, improving the network's performance and maintaining QoS. The researchers' proposed approach can be useful in various applications, including monitoring disasters, search and rescue operations, and wildfires.

2.4 Framework for a Mutual Authentication Protocol that is Both Safe and Effective for Use with Unmanned Aerial Vehicles

Bansal and Sikdar’s (2021) study focuses on the security and privacy concerns of UAV-based applications, such as man-in-the-middle, replay, and physical attacks. The authors suggest using a lightweight mutual authentication method, which utilizes Physically Unclonable Functions (PUF) devices, to counter these threats and provide network and communication security. The significance of this solution lies in the protection it provides against threats like man-in-the-middle, replay, and physical attacks, as the communications between base stations and UAVs are already encrypted. The attackers' primary motive for targeting UAVs is to hijack them for personal interests. The UAV applications discussed in the study include medical surveillance, traffic monitoring, military operations, and package delivery. To assess the feasibility of this solution for future proposals and research, one could consider adopting and applying the technology in any of the aforementioned fields, such as medical surveillance, military operations, or package delivery.

Figure 3: one example of a commonly used Drone or UAV

2.5 Efficient Certificateless Signcryption for UAV Cluster Network

In their article, Da et al. (2021) focus on the security risks associated with wireless channels used for UAV-to-UAV and UAV-to-CS interactions in open environments, such as eavesdropping, SQL intrusions, and denial-of-service attacks. The authors suggest that limited computational and storage capabilities of single UAVs make it difficult for them to transmit large amounts of data over long distances. To overcome these limitations and to address security and privacy concerns in UAV cluster network applications, the authors propose the use of a Certificateless Aggregate Signcryption (CL-ASC) system that ensures data privacy and the reliability of data sources. This approach is particularly important for UAV applications in both military and civilian settings, including freight transportation, security patrols, regional surveillance, disaster rescue, and catastrophe monitoring. The authors suggest that future research should focus on developing and implementing CL-ASC systems as the best solution for securing UAV cluster network applications.

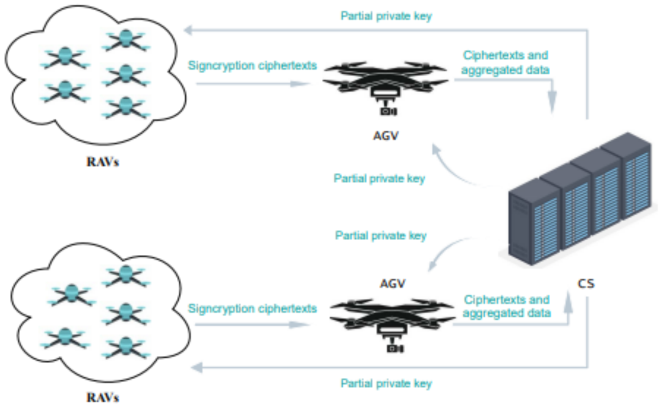

Figure 4: UAV cluster network data-collection model

2.6 Threats, opportunities, and research ahead for secure UAV swarm mesh networks

A study conducted by Lopez et al. (2021) aimed to address the security and reliability issues of Wireless Mesh Networks (WMNs) for UAV swarm networking. The authors highlighted the vulnerabilities of WMNs and suggested a security-focused UAV mesh communication architecture to provide a solution to the challenges encountered in using mesh technology in the context of UAV swarms. The significance of implementing this solution is to overcome the weaknesses in the communication stack and to address the major obstacles to using mesh technology in UAV swarms. The primary goal of attackers targeting UAV swarms is to disrupt or manage communication within the network as mesh UAV communications have vulnerabilities that can be easily exploited at every level of the network. The UAV swarm's application discussed in the article aims to provide an ad hoc networking architecture for various tasks, from simple ones like geographic mapping, to complex missions like military operations or natural disaster response. Future recommendations include the implementation of the proposed architecture to address the vulnerabilities in UAV swarm communication.

Table 1: A breakdown of the hazards and openings facing mesh swarm connection for unmanned aerial vehicles

Layer	Threat/Vulnerability	Exploits	Defence/Opportunity
Physical	Passive Eavesdropping RF Jamming	Broadcast Nature of Wireless Channels Wireless contention	Strong Encryption Avoid Interference Zones
Link	Spoofing Frame Modification	Intentional Collision MAC Spoofing	Intrusion Detection Systems (IDS) Encryption
Network	Routing Forwarding Data Forwarding	Selfish Attacks Collusion Attacks	Intrusion Detection System (IDS) Firewall
Transport	Packet Corruption Protocol Weakness	Denial of Service (DoS) Session Hijacking	Intrusion Detection Systems (IDS) Transport Layer Security (TLS)
Application	ROS2 Bugs Open Protocols	Malware Injection/Modification	Authentication Encryption

2.7 A hypothetical method for self-adaptive UAV routing to reduce the risk of forest fires

In a study by Kilic and Ozkan (2019), a paradigm is presented for reducing the risk of forest fires using self-adaptive, autonomous UAVs. The authors use the memoryless exponential distribution to calculate the probability of forest fires. Due to the stochastic and dynamic nature of the problem and the mathematical complexity of the scheduling technique, a simulation analysis was performed.

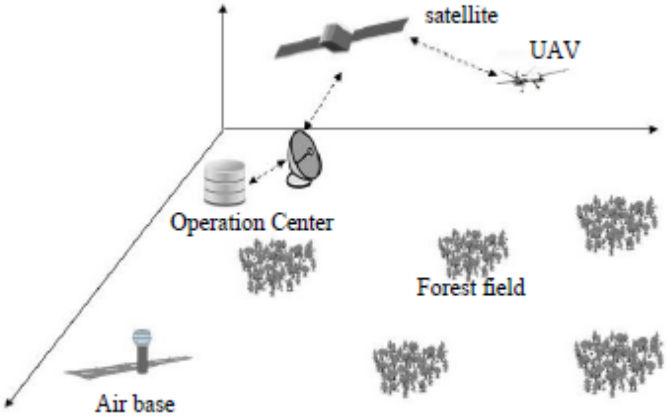

Figure 5: The proposed model's concept map (taken from Kilic & Ozkan, 2019, pp 1-12)

The main contribution of the proposed model is the assessment of the impact of inaccessible time and fire likelihood in candidate fields during UAV routing for forest fire detection. The suggested dispatching rule would make a significant contribution due to its memoryless nature if time delays for fire events in a field follow an exponential distribution.

The proposed conceptual model could also be seen as an earlier investigation for a data integration model. By using the proposed dispatching rule, a model that combines a repository of historical data, wireless sensors in fields, and satellite communications to collect and draw conclusions from data about the likelihood of fires in fields could lead to UAVs that can navigate on their own.

2.8 A study on the advancements, standardisation, and applications of UAVs in various sectors.

A study conducted by Mohsan et al. (2022) focuses on the drone industry, which has generated significant interest as a case study for the convergence of production, service, and delivery in various emerging sectors. UAVs offer several advantages, such as longer flight durations, higher cargo capacities, quick mobility, and access to remote and disaster-prone areas. The authors of this study examined recent UAV research developments in both the commercial and academic sectors. They provided a comprehensive analysis of UAV types, classifications, swarms, and charging methods, as well as the standardisation of UAVs. The authors demonstrated a growing interest in utilising UAV technology among government agencies, commercial organisations, and researchers. The study briefly discussed UAV characteristics such as flying time, acceleration, distance, altitudes, and capacity. Furthermore, the research offers a comprehensive analysis of UAV applications, challenges, and security issues. Specifically, the study explored the role of UAVs in IoT networks and 5G innovations. The authors concluded their analysis by identifying the research gap in UAV technology and outlining potential future research directions. The research offers a valuable insight into the current state of UAV technology and highlights its potential applications in various sectors. The study provides a foundation for further research to expand the capabilities of UAVs and increase their adoption in commercial and government applications.

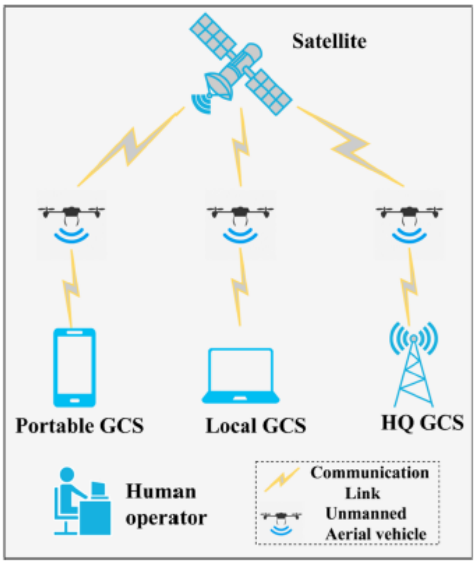

Figure 6: Architecture of UAV system

2.9 Computation offloading using heterogeneous and collective intelligence in aerial edge networks

A recent study by Su et al. (2022) focused on unloading tasks with the help of unmanned aerial vehicles (UAVs) on aerial edge networks (AEN). The authors propose a strategy that optimizes the offloading job options and the positioning of UAVs while considering the constraints of latency and overall UAV energy consumption. The objective of this study is to minimize the overall energy usage of all user equipments (UEs). This is a highly nonlinear problem that involves the coupling of several optimization variables. To overcome this challenge, the authors used reformulation linearization technology to convert the original optimization problem into a linear convex optimization problem. Then, they suggested using the alternating direction method of multipliers (ADMM) technique to arrive at the approximate optimal solution. The suggested ADMM method successfully reduces the total amount of energy consumed by UEs while maintaining their uninterrupted functioning, as per the numerical data. The authors also developed an ADMM-based incremental alternating strategy and inserted auxiliary variables into the equation to transform the problem into a linear form once again. Numerical data revealed that the suggested offloading technique has the potential to substantially reduce the total energy usage in comparison to the benchmarks. In the future, the research will investigate the dynamic distribution of processing capacity in collaborative computing networks that include many UAVs.

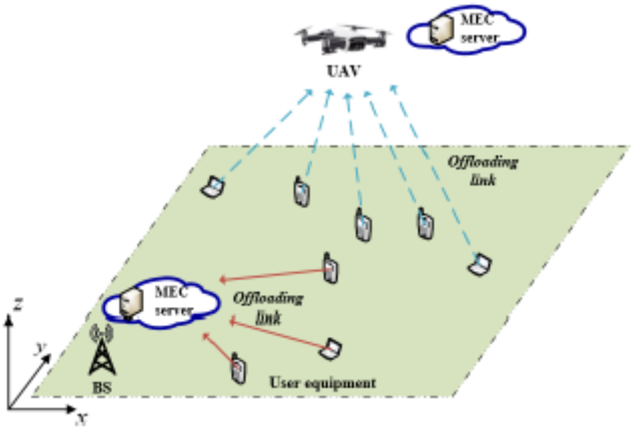

Figure 7: Model of MEC network aided by UAVs

2.10 Autonomous vehicle-based upcoming security and surveillance systems

Ayub (2018) conducted a study on the development and design of Unmanned Ground Vehicles (UGV) and Unmanned Aerial Vehicles (UAV) for safeguarding highly sensitive areas against incursion or any suspicious activity. The study described the development of a self-governing navigation algorithm and repetitive path following for UGV, which was effectively tested for both indoor and outdoor sites. The study also proposed a new approach for geolocation and autonomous flight of UAVs, which uses the Haver-Sine formula for complex geometry calculations and a reliable sensor network to adapt to UAV flight behavior. Ayub (2018) stated that an intelligent security and surveillance system was provided in the study, where the developed UGV can follow an user-selected path independently and broadcast live video feed from the site. Additionally, a fully autonomous flight control algorithm based on the straight earth approximation and Haversian Formula was proposed to utilize the surveillance and monitoring potential of UAVs. For autonomous flight, RC control, which has a limited operating range, is bypassed. To translate the 6-channel RC controlled signals for THROTTLE, YAW, ROLL, and PITCH, the study established the following information: 54.3% frequency, 5.55% to 10.88% duty cycle, and 784 mV to 1.08 vrms range. The MyRio then generates these signals and sends them to the remote control, whose operations are managed at the ground station. To ensure end-to-end authentication, the study proposed other solutions that can also be deployed (Khan et al., 2015, 2017, 2021, Maikol et al., 2020).

Designing a security and monitoring system for high-risk areas requires an innovative approach that integrates the functionalities of UGVs and UAVs, especially as centralised command and control systems become more prevalent (Dildar et al., 2017; Ahmad et al., 2020; Alqarni et al., 2022; Alshehri et al., 2023; Khan et al., 2023;). The study by Ayub (2018) offers a novel approach that can improve the capabilities of UGVs and UAVs for security and surveillance purposes. Further research can explore the potential of integrating these vehicles with other technologies to enhance security measures in high-risk areas.

3 Taxonomy

3.1 Attacks

1. Replay Attacks: In this attack, an attacker intercepts data packets between the sender and receiver, stores them, and later uses them to communicate with the receiver. This attack can occur between the server and the UAV or between the UAV and the BSH.
2. Unauthorized Data Tampering: This attack involves the unauthorized modification of data, which compromises the reliability of the information stored. Both insiders and outsiders can be the attacker in this scenario, and the attack can result in the data being changed if the USB or server is compromised.
3. Unlawful Access: This attack involves the installation of malware on a system to gain unauthorized access to critical data. The attacker may steal data covertly or cause damage to the system.

4. Man-in-the-Middle Attacks: In this type of attack, an external attacker intercepts communication between the server and UAV or between the UAV and the BSH. The attacker can gather sensitive data and modify it, compromising the system's security.

In summary, the proposed autonomous unmanned vehicle health monitoring system based on Blockchain by Raj (2021) faces various security threats such as replay attacks, unauthorized data tampering, unlawful access, and man-in-the-middle attacks. These attacks can compromise the integrity and confidentiality of the data stored in the system, and insiders and outsiders can be potential attackers. Hence, it is crucial to have effective security measures in place to mitigate these threats (Khan et al., 2019; Khan et al., 2021).

3.2 Techniques used to mitigate attacks

1. Replay Attack Protection Technique:
   Replay attacks can be detected through physical watermarking, which adds random noise to control inputs and looks for system reactions (Zhao & Smidts, 2020):
   a. A chi-squared test can be used with sensor measurements to determine a null hypothesis or alternative hypothesis (Zhao & Smidts, 2020).
   b. Random noise can be optimized to maximize replay attack detection while minimizing control performance loss (Khan et al., 2020).
   c. A zero-sum, finite-horizon stochastic game can be used to find the best strategy for alternating between ideal and undesirable controllers (Iqbal et al., 2011).
2. Unauthorized Data Tampering Protection Technique:
   a. A Wireless Channels Radio Checking Subsystem (WCRCS) can be incorporated into the design of the IoD monitoring system to provide cyber control and protection against RF vulnerabilities (Torianyk, 2021).
   b. WCRCS control capabilities can be augmented with transmitting and receiving protection, IoD restructuring, and other activities to form an RFV protection system (RFVPS) (Torianyk, 2021).
   c. RFVPS can be integrated into an overall cybersecurity assurance system (CSAS) to reduce the risk of vulnerabilities on RFVs and cyber failures caused by attacks (Torianyk, 2021).
3. Illegal UAV Access Protection Technique:
   a. Anti-UAV techniques can be employed to prevent attacks from UAVs, including intercepting communication channels and disrupting flight patterns (Chamola, 2021).
   b. Case studies of intentional UAV attacks can help understand the harm caused and how it can be prevented (Chamola, 2021).
   c. Techniques for monitoring and attacking UAVs, such as disrupting communication networks and removing autopilot software, can be employed (Chamola, 2021).
4. Man in the Middle UAV Attack Protection Technique:
   a. DroneSig uses a Duffing map to create a digital signature for encoding and decoding binary data without using popular cryptographic techniques like DES or AES (Li & Pu, 2020).
   b. DroneSig includes byte substitution, matrix transformation, and random shuffle operations (Li & Pu, 2020).

4 Challenges associated with drones

Drones present several significant challenges, one of which is their potential to violate privacy by capturing images and videos without consent. This issue is especially concerning in residential neighborhoods and public places. Additionally, drones can be used for illegal activities like drug trafficking and smuggling, which pose significant security concerns. Another challenge is the vulnerability of drones to hacking, as wireless communication systems can be intercepted and manipulated by hackers. Hacked drones can then be controlled by someone else, posing threats to public safety. Physical attacks like shooting down drones, using nets, or jamming their communication systems can also compromise drone security. However, there are various ways to defend against drone attacks. Anti-drone technology, including jamming devices and detection systems, can help authorities identify and respond to potential threats. Physical defenses like netting systems or trained birds of prey can capture drones, while defensive mechanisms like countermeasures and emergency landing systems can deflect and mitigate attacks. Governments can also impose regulations on the use of drones, such as requiring registration and licensing for their operation. Overall, effective defense against potential drone attacks requires a combination of technological and legislative measures.

5 Research trends, challenges and future direction

Research trends in Malaysia are influenced by security challenges arising from the use of drones or unmanned aerial vehicles (UAVs) that pose a threat to public safety and national security. The lack of regulation and monitoring of drone sales in the market has contributed to this problem (Abdullah et al., 2021). Although regulations have been introduced under the Malaysian Civil Aviation Regulations 2016 (MCAR 2016), they only apply to airport areas, making it difficult to ensure compliance for every drone owned by individuals. The sale of affordable drones in Malaysia has made it challenging for authorities to control and enforce regulations (Ismail et al., 2020).

Apart from security challenges, the Internet of Everything (IoE) faces several obstacles, including coverage, battery, computing, and security constraints (Lian et al., 2020). To overcome these challenges, efficient preventative measures need to be implemented. This includes constructing adaptable and recoverable networks to extend IoE coverage, creating environmentally friendly energy-supply systems to extend the lifecycle of IoE nodes, and coordinating the use of edge computing with local and cloud computing to make the most of available computing resources. Lastly, trustworthy security solutions need to be developed to safeguard data stored in pervasive IoE networks against intrusion attempts (Al-Fuqaha et al., 2015).

The use of drones with multiple layers presents several challenges that need to be addressed. According to Sekander et al. (2018), drones with multitiered capabilities have the potential to take control of cellular signals, especially during a catastrophe. However, the integration of drone networks into terrestrial networks can also bring potential benefits, such as unloading traffic and reducing the number of handovers for mobile users. To fully harness these benefits, the deployment of drone-aided cellular networks and air traffic control systems must first be addressed to avoid congestion in the future. Additionally, the confidentiality and safety of connected sensor devices in the Internet of Drones (IoD) must be given higher importance in the design of drone applications. The susceptibility of these devices to theft, malfunction, and misplacement poses significant risks that require mitigation strategies, such as controlling the electromagnetic field of carrier signals and employing risk reduction principles in court. Coordination and task scheduling also pose a challenge in the integration of cloud and edge computing for computationally expensive Internet of Things applications. Abdelmaboud (2021) suggests that external intelligent network applications require adequate centralised AI analysis and individual big data analysis to facilitate collaboration. Sequencing of computing jobs and evaluating the necessity of remote cloud migration require modifications to computer architecture and networking for optimal performance on a global scale.

Given these challenges, it is crucial to conduct a study on consumer behaviour and trends in drone use in Malaysia. This study can provide essential information to relevant agencies to find solutions to the raised issues. Specifically, the deployment of drone-aided cellular networks and air traffic control systems must be addressed to prevent congestion in the future. The confidentiality and safety of connected sensor devices in the IoD must also be given higher importance in the design of drone applications, and mitigation strategies such as controlling the electromagnetic field of carrier signals must be employed. Lastly, coordination and task scheduling pose a challenge in the integration of cloud and edge computing for computationally expensive Internet of Things (IoT) applications, requiring modifications to computer architecture and networking for optimal performance on a global scale.

In conclusion, the challenges presented by the integration of drones into terrestrial networks and the IoT require significant attention to harness their potential benefits. While addressing these challenges, it is important to consider the safety and confidentiality of connected sensor devices, as well as the coordination and scheduling of tasks. By conducting a study on consumer behaviour and trends in drone use, relevant agencies can develop effective solutions to these issues, leading to the safe and efficient deployment of drone networks in the future.

The next research plan involves the creation of a UAV swarm digital twin system. Professor Michael Grieves from the University of Michigan is credited with the concept of digital twins, which refers to virtual models that mimic the behaviour of real-world objects (Zhou, 2020). The digital twin system is designed to perceive data from the real-world UAV cluster and utilize it to make accurate predictions, estimates and observations about dynamic changes (Kar et al., 2022). With the development of this system, it is possible to understand complex commands, execute tasks autonomously and identify the best course of action in a given situation. Additionally, deep learning methods, blockchain and multifactor authentication techniques can be employed to counteract communication attacks (Kar et al., 2020; Zeeshan et al., 2021; Khan et al., 2021; Khan et al., 2022; Asim et al., 2022). It is anticipated that the proposed UAV swarm digital twin system will provide significant benefits in terms of improving task execution, operational efficiency and overall performance.

6 Conclusion

In conclusion, this survey article has provided an overview of unmanned aerial vehicles (UAV), also known as drones, and their potential to increase productivity in various industries. With the integration of embedded systems, communications technology, and control modules, the UAV network has the ability to establish a complete sequence of data perceiving, information transferring, deliberation, and final implementation, creating a cyber-physical system (CPS). Additionally, the concept of the internet of everything (IoE) has been discussed as an extension of the internet of things (IoT). This article has also presented a taxonomy of attacks and techniques to mitigate them, along with research trends, challenges, and future directions for the use of drones. Overall, this article has summarized related works and provided a comprehensive understanding of the current state of drones and their potential for the future.

References

Abdelmaboud, A. (2021). The Internet of Drones: Requirements, Taxonomy, Recent Advances, and Challenges of Research Trends. Sensors, 21(17), 5718.

Ahmad, Z., Khan, A. S., Cheah, W. S., Abdullah, J., & Ahmad, F. (2020). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, vol. 32 no.1, pp. e4150.

Alqarni, A. A., Alsharif, N., Khan, N. A., Georgieva, L., Pardade, E., & Alzahrani, M. Y. (2022). MNN-XSS: Modular neural network based approach for XSS attack detection. Computers, Materials and Continua, 70(2), 4075-4085.

Alshehri, A., Khan, N., Alowayr, A., & Alghamdi, M. Y. (2023). Cyberattack Detection Framework Using Machine Learning and User Behavior Analytics. Computer Systems Science and Engineering, 44(2), 1679-1689.

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. Appl. Sci., 12, 3551.https:// doi.org/10.3390/app12073551.

Ayub, M. F., Ghawash, F., Shabbir, M. A., Kamran, M., & Butt, F. A. (2018). "Next Generation Security And Surveillance System Using Autonomous Vehicles,". Ubiquitous Positioning, Indoor Navigation and Location-Based Services (UPINLBS), pp. 1-5, doi: 10.110.

Bansal, G., & Sikdar, B. (2021). A Secure and Efficient Mutual Authentication Protocol Framework for Unmanned Aerial Vehicles. In 2021 IEEE Globecom Workshops (GC Wkshps). pp. 1-6.

Chamola, V. K. (2021). A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. Ad hoc networks, 111, 102324.

Da, L., Wang, Y., Ding, Y., Xiong, W., Wang, H., & Liang, H. (2021). "An Efficient Certificateless Signcryption Scheme for Secure Communication in UAV Cluster Network IEEE Intl Conf on Parallel & Distributed Processing with Applications, p 884-891.

Dildar, M. S., Khan, N., Abdullah, J., & Khan, A. S. (2017) "Effective way to defend the hypervisor attacks in cloud computing." In 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), pp. 154-159. IEEE, 2017.

Fotohi, R. (2020). Securing of Unmanned Aerial Systems (UAS) against security threats using human immune system. Reliability Engineering & System Safety, 193, 106675.

Iqbal, A. M., Iqbal, S., Khan, A. S., & Senin, A. A. (2013). "A Novel Cost Efficient Evaluation Model for Assessing Research-Based Technology Transfer between University and Industry." Jurnal Teknologi 64(2).

Iqbal, A. M., Khan, A. S., Abdullah, J., Kulathuramaiyer, N., & Senin, A. A. (2021). Blended system thinking approach to strengthen the education and training in university-industry research collaboration. Technology Analysis & Strategic Management DOI: 10.1080/09537325.2021.1905790

Kar, H. A., & Rather, G. M. (2020). Multilayer Software Defined Networking Architecture for the Internet of Things. International Journal of Computing and Digital Systems, 9(4), 735-746.

Kar, H. A., & Rather, G. M. (2020, March). An analytical and simulation study of round trip transmission time of an edge based Internet of Things network. In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 538-543). IEEE.

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

Khan, A.S., Balan, K., Javed, Y. Abdullah., J. & Tarmizi, S. (2019). Secure trust-based blockchain architecture to prevent attacks in VANET. Sensors (Switzerland), 19(22), 1.

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

Khan, A. S., Javed, Y., Saqib, R., Ahmad, Z., Abdullah, J., Zen, K. & Khan, N. (2022). Lightweight Multifactor Authentication Scheme for NextGen Cellular Networks. IEEE Access. 10, 31273–31288.

Khan, A.S., Yahya, M. I., Zen, K., Abdullah, J., Rashid, R. A., Javed, J., Khan, N. A., & Mostafa, A. M "Blockchain-Based Lightweight Multifactor Authentication for Cell-Free in Ultra-Dense 6G-Based (6-CMAS) Cellular Network," in IEEE Access, doi: 10.1109/ACCESS.2023.3249969.

Kilic, S. & Ozkan, O. (2019, July). A self-adaptive UAV routing for forest fire risk mitigation: a conceptual model. In Proceedings of the 2019 Summer Simulation Conference, pp. 1-12.

Li, Y., & Pu, C. (2020, December). Lightweight digital signature solution to defend micro aerial vehicles against man-in-the-middle attack. In 2020 IEEE 23rd international conference on computational science and engineering (CSE), (pp. 92-97.

Liu, Y., Dai, H. N., Wang, Q., Shukla, M. K., & Imran, M. (2020). Unmanned aerial vehicle for internet of everything: Opportunities and challenges. Computer communications, 155, 66-83.

Lopez, M. A., Baddeley, M., Lunardi, W.T., Pandey, A., & Giacalone, J-P. (2021). "Towards Secure Wireless Mesh Networks for UAV Swarm Connectivity: Current Threats, Research, and Opportunities. 17th International Conference in Distributed Computing in Sensor Systems (DCOSS), pp 319-326.

Maikol, S. O., Khan, A. S., Javed, Y., Bunsu, A. L., Petrus, C., George, H., & Jau, S. (2020). A novel authentication and key agreement scheme for countering MITM and impersonation attack in medical facilities. International Journal of Integrated Engineering, vol. 13, no. 2.

Mohammad. Y., Alzahrani, N., Khan, L., Georgieva, A. M., Bamahdi, O. A., & Abdulkader, A. H. (2023). Protecting Attacks on Unmanned Aerial Vehicles using Homomorphic Encryption, Indonesian Journal of Electrical Engineering and Informatics, Vol. 11, No. 1.

Mohsan, S. A. H., Khan, M. A., Noor, F., Ullah, I., & Alsharif, M. H. (2022). Towards the Unmanned Aerial Vehicles (UAVs). A Comprehensive Review. Drones, 6(6), 147.

Raj, J. S. (2021). Security enhanced blockchain based unmanned aerial vehicle health monitoring system. Journal of ISMAC, 3(02), 121-131.

Sekander, S., Tabassum, H., & Hossain, E. (2018). Multi-tier drone architecture for 5G/B5G cellular networks: Challenges, trends, and prospects. IEEE Communications Magazine, 56(3), 96-103.

Shamsoshoara, A., Afghah, F., Razi, A., Mousavi, S., Ashdown, J., & Turk, K. (2020). An autonomous spectrum management scheme for unmanned aerial vehicle networks in disaster relief operations. IEEE Access, 8, 58064-58079.

Su, J., Yu, S., Li, B., & Ye, Y. (2022). "Distributed and Collective Intelligence for Computation Offloading in Aerial Edge Networks. IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2022.3160594.

Torianyk, V. K. (2021, March). IMECA Based Assessment of Internet of Drones Systems Cyber Security Considering Radio Frequency Vulnerabilities. In IntelITSIS, pp. 460-470.

Wang, H. Z. (2019). Survey on unmanned aerial vehicle networks: A cyber physical system perspective. IEEE Communications Surveys & Tutorials, 22(2), 1027-1070.

Zhao, Y., & Smidts, C. (2020). A control-theoretic approach to detecting and distinguishing replay attacks from other anomalies in nuclear power plants. Progress in Nuclear Energy, 123, 103315.

Zhou, Y. R. (2020). UAV swarm intelligence: Recent advances and future trends. IEEE Access, 8, 183856-183878.