6G Enabled Light Weight Authentication Protocol for UAVs

Subjects: Computer Science, Cybernetics

Contributor: Adnan Shahid Khan, Muhammad Ali Sattar, Kashif Nisar, Ag Asri Ag Ibrahim, Noralifah Binti Annuar, Johari bin Abdullah, Shuaib Karim Memon

In the 6G network, with blockchain and unmanned aerial vehicles (UAVs) authentication, the network decentralization and resource sharing would minimize resource under-utilization thereby facilitating PG targets. Furthermore, through an appropriate selection of blockchain type and consensus algorithms, the SG's needs of UAV authentication in 6G network applications can also be readily addressed.

Keywords: 6G ; unmanned aerial vehicles ; UAVs

1. Introduction

As 5G is heading closer to commercial status, prospects of unmanned aerial vehicles (UAVs) system integration with future 6G communication models are becoming a significant part of ongoing research in the field [1]. These papers identify a few key UAV systems in 6G flighty applications and administrations such as Human Bond Communication (HBC), Multi-sensory amplified Reality Applications (XR), Wearable Innovation-based Cutting edge Applications (WTech) and Large-scale associated independent frameworks (LS-CAS), and are more noteworthy for a few vertical spaces. All these applications show up in a combinational way beneath the space of the UAV system in 6G-based UAV communication. These applications have remarkably demanding information rates, inactivity and unwavering quality; thus, the nature of the information collected by a few UAV systems in 6G applications will be progressively delicate and fundamental. As 5G is entering the deployment phase, discussion on 6G networks is gradually gaining momentum [2]. The objective of 6G is to support faster connection. Hence, the performance of 6G will be degraded using an inefficient authentication scheme which also brings the possibility towards some security issues. The productive allocation of UAV frameworks in 6G-based UAV structures by the customers would thus require strict data security guarantees. **Figure 1** illustrates the UAV paradigm in 5G and beyond networks. This figure symbolizes future employment of UAVs in numerous applications in advanced network environments.

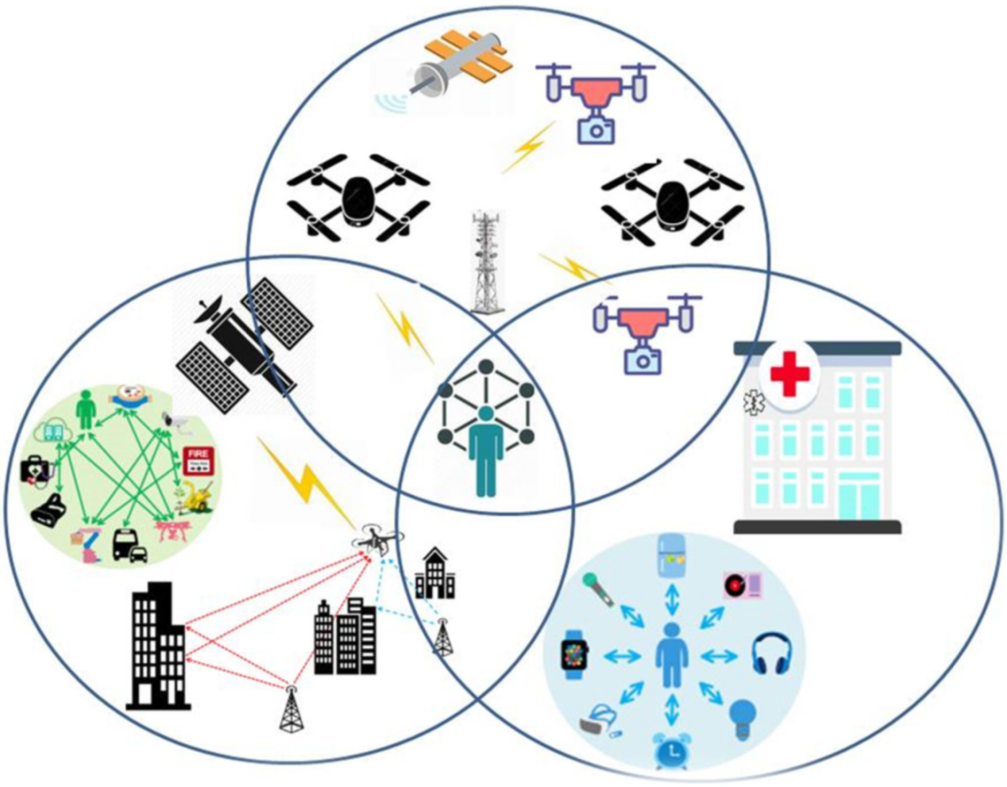

Figure 1. Illustration of future UAV applications in 5G and beyond network environments.

Blockchain could be a disseminated record innovation where cryptography and hash capacities are utilized to make a chain of information [3]. Blockchain, as it was initially utilized in crypto currencies is presently being utilized in other applications such as keen lattice, associated vehicles and Internet of Things [4][5][6]. The demanding prerequisites of these applications will require bolster of advances such as Reconfigurable Shrewdly Surfaces (RIS), TeraHertz (THz) communication, Artificial Intelligence (AI) and little cell systems. To enable a capable mix of these advances for the game plans of resources to achieve the execution essentials, collaboration and coordination in a straightforward and trustless environment is required [7]. Arranged decentralization will be needed to unravel the coordinate sending. Blockchain will give the required genuineness and verification within the decentralized UAV system in 6G-based UAV arrangements. Blockchain will also give the stern security essentials of the longer-term communication structure due to the built-in security highlights.

In order to tweak blockchain by the selection of suitable blockchain rudiments, its application essentials, decentralization, security and features such as adaptability are vital considerations. Blockchain offers relatively simple solutions to major issues of centralized systems. It is a pertinent fact that centralized systems have concerns including resilience, safety, scalability and privacy. Blocks chained together by a hash in between them is the simplest concept of blockchain. Genesis block is the originating block of blockchain. The key properties such as the number of tokens existing in the system reside in this first block. The last block in blockchain is named tip block. A potential new block must point to tip block. In a blockchain system, all the members that are part of network contribute to consensus and possess a copy of blockchain. In a blockchain system, each block contains a division of information: (i) transactions and account balances, (ii) block hash and (iii) the block ID. Each node in the blockchain requires the validity to be verified of any new transaction, that is added to the blockchain. This aspect of blockchain demonstrates the key properties such as transparency and distributed validations in the system.

2. UAV Communication

Unmanned aerial vehicles (UAVs) have enormous potential in the universal domains including civil, defense, media and public domains [8]. They have unprecedented and useful applications where human lives can otherwise be in danger. In addition to this, multi UAV systems are jointly mission capable and can accomplish the same but better economy, precision and efficiency compared with solo UAV systems. However, there are many concerns that are required to be resolved before the effective use of unmanned aerial vehicles for the provision of reliable, assured and context-focused networks. In view of the distinctive characteristics of the UAV networks and the need to address related issues, considerable work is yet to be carried out in this area. Current progress in the domain of mobile adhoc networks (MANETs) and vehicular adhoc networks (VANETS) is not sufficient to address the peculiar nature of UAV networks. UAV networks may vary from slow dynamic to dynamic as some have intermittent links and topology that is relatively fluid.

2.1. Characterizing the UAV Network

2.1.1. Multi UAV Network

The utilization of a single large UAV for a mission was common in the early days of UAV use. As a result, in these systems, the UAV-based communication network only had one aerial node and one or more terrestrial nodes. The UAVs in a multi UAV system are smaller and less expensive and they have the ability to work together. multi UAV systems may now be used to carry out most public and civic applications more efficiently [9]. The communication network, which ensures communication between UAVs and between UAVs and ground nodes, constitutes a key component in most multi UAV systems. These UAVs can be designed to cooperate together to provide services and function as relays to extend network coverage. The mobility of UAVs is determined by the application. For example, in order to provide communication in an earthquake-stricken area [10], UAVs would hover over the operation area and the linkages would be slow and dynamic. The fact that the UAVs may go out of service due to failure or battery drain demonstrates the dynamic nature of the network setup and connectivity. Agricultural and forest monitoring applications, on the other hand, demand UAVs to move across a vast region, with links breaking and reestablishing often. This is also true for UAVs that must hover over an area for extended periods of time. To take their place, new unmanned aerial vehicles must be launched.

Some of the UAVs may be pulled out of operation to save power until a more appropriate time comes. As a result, it would be a requirement that the linkages immediately reconfigure themselves in all such circumstances. Multi UAV systems, while beneficial in many ways, complicate the UAV communication network. Reliability and survivability through redundancy are two significant advantages of multi UAV systems. When a single UAV fails in a multi UAV system, the network must reorganize and retain communication through other nodes. In a single UAV system, this would be impossible. However, in order to gain the full benefits of numerous UAVs operating together in a multi UAV topology, the protocols in place must address concerns such as power limits, mobility and changing topology [11]. **Figure 2** illustrates the multi UAV system; each UAV struggles to address mobility and varying link' quality dividends in an ever changing topology during the flying role. As per interference requirements, the UAV link selection and topology should be dynamically optimized. The phenomenon is a governing element in terms of authentication protocol implementation in a multi UAV network. A single UAV system would have to maintain communication linkages with the control station(s), servers and base stations as well as provide access for functionality. The limited battery power and bandwidth are severely hampered as a result.

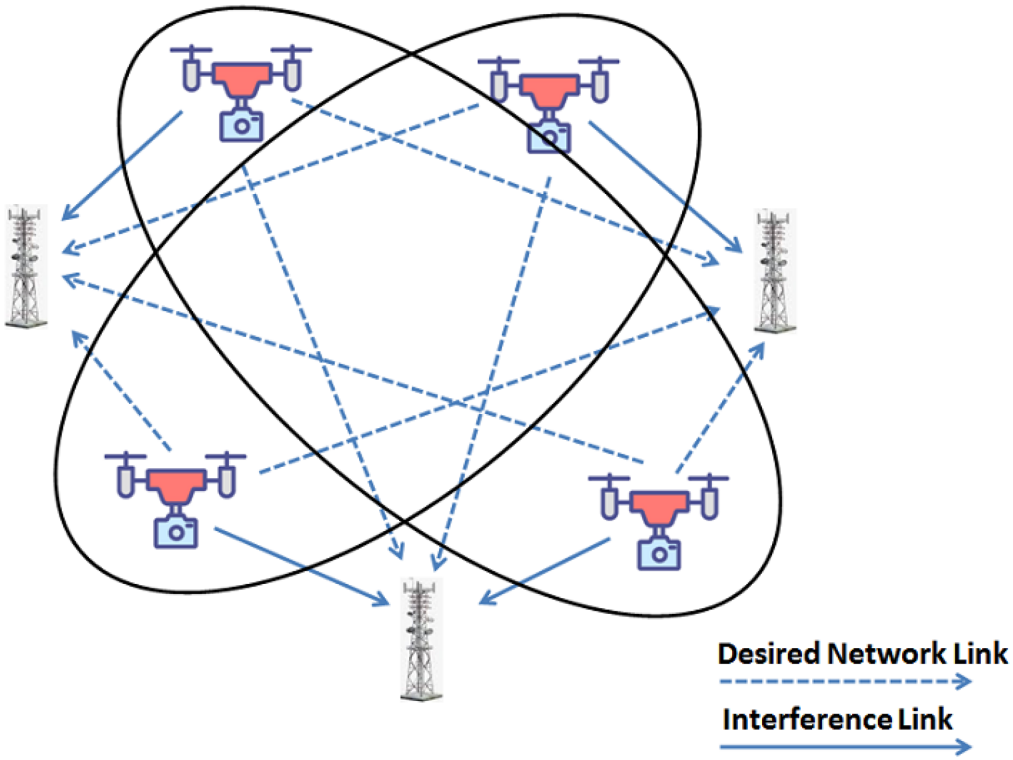

Figure 2. Multi UAV system and varying links' quality demands.

2.1.2. Infrastructure-Based or Adhoc UAV Networks

UAV networks are usually referred to as ad hoc networks in the existing literature. Most of the discussion in available research relates VANETs to UAV networks; moreover, MANETs are also related to UAV networks. However, the stated studies do not address the explicit properties of UAV networks entirely. Depending upon the utilization and nature of the

mission, the UAV network could be attributed to slow moving, feature-like hovering, high mobility missions and slow mobility profiles. One of the pertinent applications of UAV nodes is to function as a sky-based communication-based station, ensuring provision of reliable coverage over a good span of area [12]. UAV networks could perform functions such as infrastructure-based systems for applications dissimilar to VANET and MANET networks.

2.1.3. Server or Client?

Whether the node is in the role of server or client is another distinction. In vehicular networks, the nodes are usually servers and in adhoc networks, the nodes usually act as clients [13]. UAV nodes usually act as servers and perform relaying functions of sensor data and packet forwarding [14]. They are also utilized for provision of data forwarding to other UAV clients. **Figure 3** is a depiction of a widely used server–client implementation of UAV network is surveillance mode.

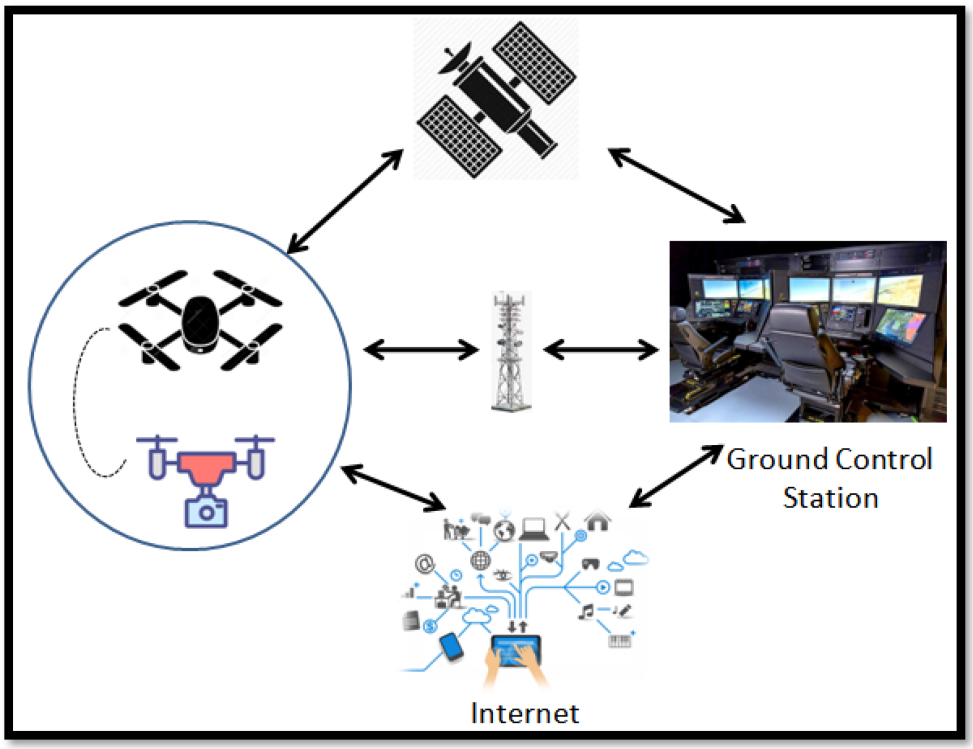

Figure 3. UAVs relaying packets for clients/sensor data to control centers.

2.1.4. Star or Mesh?

UAV network topology for communication applications is an area that has received little focus yet. A solo UAV driven by a single command and control station is the most fundamental system. Multi star, hierarchical mesh, star and mesh are network architectures that can be realized in a multi UAV system. In a star topology, all UAVs connect directly to ground nodes. Moreover, all types of communication are ensured through ground nodes between UAVs. In this scenario, there is the possibility of latency, intermittency in links and need for high capacity downlinks. Moreover, in view of the mobility aspect, steerable and direction-seeking antennas may be needed to keep a correct point of reference towards the ground node.

2.2. Security in UAV Communication

Internet of Things (IoT) acts as an interface between the physical world and computing systems; IoTs perform this role by transfer of information regarding the physical atmosphere after sensing and necessary analysis. Internet of Drones (IoD) is a classic mobile IoT system [15][16].

In the latest years, unmanned aerial vehicles and drones have become a popular application in several fields due to its inherent characteristics including reach, exploratory abilities, flexibility, speed, life safety in case of difficult missions and coverage, etc. Keeping in mind advancements in this domain, the public's demand has invariably increased. Moreover, there is increased demand against consumer grade drones across the globe as engagement of UAVs in different applications and roles is becoming widespread. The employment of UAVs in various fields has increased manifold, including in shooting movies, drone selfies, agriculture businesses, and security objectives; all are utilizing these aerial devices. Growth in UAV commerce is expected to accelerate upwards at a rate of at least 29.9% per annum in upcoming years. Moreover, the industry volume is expected to rise to approximately 4.9 billion dollars at the end of the coming three years [17].

Two critical properties of UAVs as a smart IoT apparatus are resource limitations and the varying environment. Moreover, UAV network connection conditions including AP servers are subject to constantly changing position and environments. Consequently, the identity of every element of the UAV network must be periodically authenticated in multiple cycles. Moreover, due to the mobility of these smart devices, which are embedded with smart features, they face noteworthy limitations such as power constraints and processing power. Furthermore, the endurance of these devices and other abilities will be adversely affected if an excessively recurrent and sophisticated authentication scheme is defined for them [18].

3. UAV 6G Networks

Figure 4 depicts future advanced applications that will work hand in glove with UAVs in 6G and beyond networks. Moreover, mandatory requirements in connection with the subject are also discussed. It is pertinent to mention that UAVs will be an integral part of such future applications in connection with several aspects of application needs. Most importantly, in many future scenarios, drones will act as Aerial base stations for the provision of wide area coverage of 6G networks.

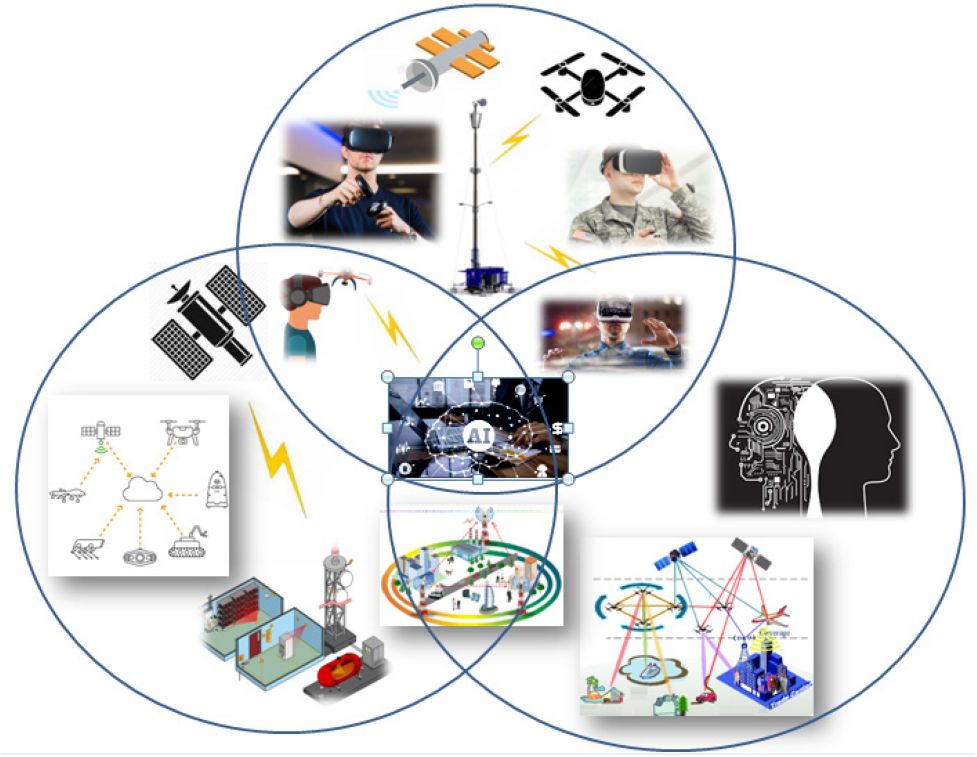

Figure 4. Future applications supported by UAV system in 6G environment.

3.1. 6G Applications

Future advanced applications will work hand in glove with UAVs in 6G environments. Imagining the role of drones in futuristic applications in 6G environments has unprecedented dimensions. UAVs will have countless employment roles in future applications. Brain computer interface, wearable clothing and technology are futuristic ideas that demand robust security for sharing the data. Current wireless networks including 5G are not capable to utilize numerous future prospects that are beyond the traditional medical ways. Extended reality multi-sensory applications are designed in a way for the provision of user experience that is entirely enchanting by amalgamating the reception from human sensory, environment and, human body moves, and several data originators.

3.2. 6G Application Requirements

With the goal of making blockchain utility more understandable, 6G applications are separated into two major groups. Ultra-reliability, low latency, increased data speeds and huge connection are among the typical criteria. I view of the pertinent factor in almost entire wireless communication generations, these needs are made part of the first category. These are referred as Qualification Group-I (QG-I). QG-I standards necessitate considerable improvement for potential 6G applications. The prime features for any reliable and secure network include non-reputability, confidentiality, defined level of secrecy, data integrity and auditability. These features are catered in second group named Qualification Group-II (QG-II).

3.2.1. High-Precision Positioning and Seamless Coverage

Unmanned aerial vehicles performing operations while airborne at various level of air space necessitate accurate positioning, precise navigation and excellent network coverage and the same aspects are vital for the network's growing infrastructure, expansion and convergence as shown in **Figure 5**. While the UAVs are flying independently, a secure connection and vast network coverage ensures uninterrupted connectivity. Covering a wide range of coverage at varied elevations while maintaining seamless connectivity is a critical problem for 4G/5G cellular networks. Positioning based on high precision is expected to be provided by 6G while employing radar technology. Moreover, utilization of modern concepts such as 3D placement permits the accurate locating of unmanned aerial vehicles and moving devices in the sky [19]. Upcoming, 6G communication networks may enhance the quantity of connected unmanned aerial vehicles in densely populated scenarios by 107 devices/km^2 which is 10 times greater than its predecessor, wireless communication model density. Beyond the vision line of sight, improved quality, robust, reliable and secure networks with vast speedy coverage, the 6G network is expected to provide connectivity that is efficient, cost effective and speedy, promising the future needs of the world [20]. The high-speed OWC system's high-capacity backhaul network enables a significant volume of UAV traffic data.

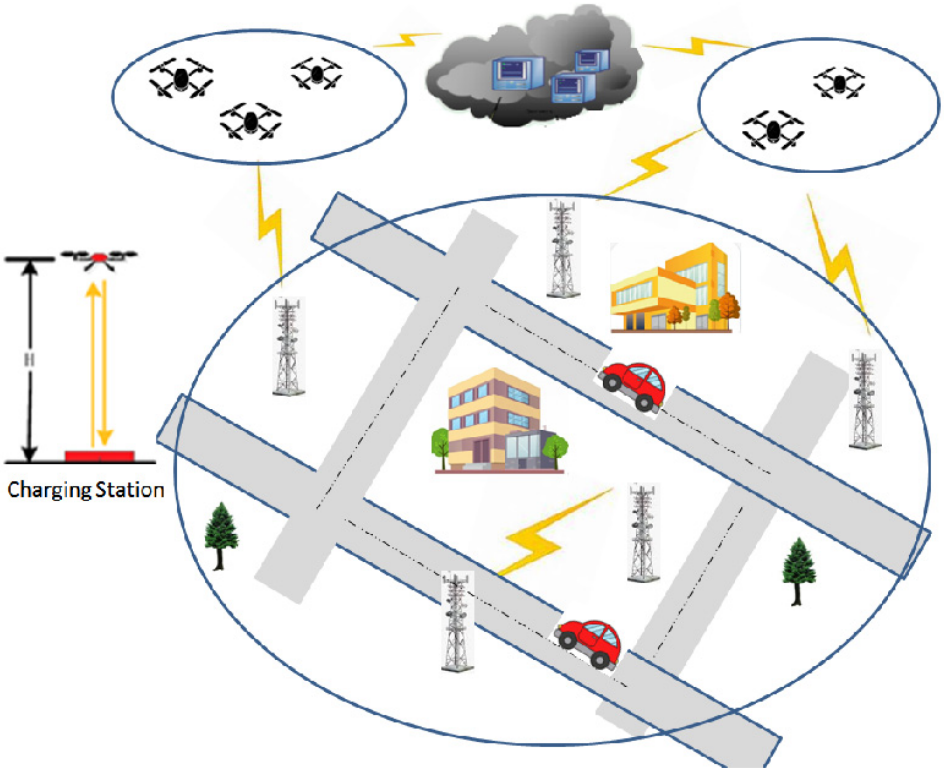

Figure 5. Multiple layers of the airspace with high-precision positioning.

3.2.2. Remote and Real-Time Control (RRC)

Unmanned aerial vehicles are operated through remote and real-time links and a continuous feedback from designated UAVs is received by establishing links through this media. Equipment status, location and other sensory data are received at ground stations from UAVs. In order to ensure seamless command and control of UAVs over wireless communication media, latency and data rate are pertinent considerations and specific required criteria must be fulfilled. In potential 6G networks, a bigger number of unmanned aerial vehicles can be operated and even these machines can accomplish different mission profiles in autonomous mode without direct operator control [21].

3.2.3. Multimedia Transmission

Based on mission profiles and to ensure the prompt provision of data to ground stations, unmanned aerial vehicles transport live data such as video, other sensors data for timely analysis and subsequent decision making. In future, modern multimedia services will be one of major demands through UAV platforms. These include multimedia applications related to virtual reality, 4K and beyond films, holograms, etc. These advance multimedia services require high data rates and bandwidth to provide true experience to users in connection with applications such as virtual reality and 3D holograms. The envisaged 6G network is capable of providing high bandwidth and throughput in UTM [22]. In order to ensure, seamless communication of UAVs with the ground control station and reliable traffic between the two ends, mandatory high bandwidth requirements are required to be promised, which will be offered by 6G in future. A data rate of 10 Gbps is anticipated in upcoming 6G technology [23]. The multimedia application of UAV is depicted in **Figure 6**.

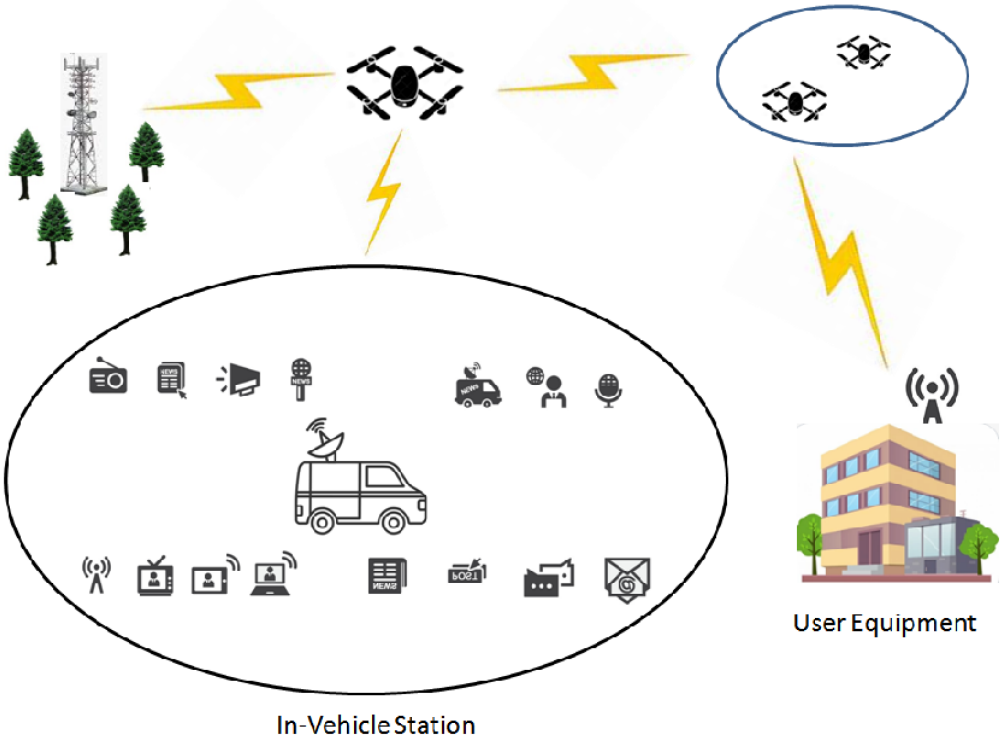

Figure 6. Multimedia application of UAVs.

3.2.4. Aircraft Identification and Regulation

An automated dependent surveillance broadcast (ADS-B) system is utilized for the identification of commercial aircrafts. Because of the increased number of UAVs in future applications, the usage of ADS-B may inundate the designated frequency band [24]. In view of this fact, a new scheme for the identification of commercial flights is deemed necessary. Radio waves are used to convey the remote ID. Registration, identification, tracking and regulation of aircraft all require reliable cellular network connectivity. In the same way, remote ID data can be utilized in the integration with future 6G networks. By effective monitoring of UAVs status data, positioning and related information, early warning along with subsequent remedial measures can be executed on the basis of monitoring parameters. Probable threats can also be contained after due analysis of the received data [25].

4. Authentication in UAV Networks

Unmanned aerial systems (UASs) consist of one or more than one UAVs. The stated unmanned aerial vehicles are operated and controlled through a reliable communication channel by GCS [26]. Utilization of UAVs is found in commercial, civilian and military uses. From surveillance to reconnaissance, security purposes, traffic monitoring, items delivery, etc., all are applications of UAVs employing modern communication networks in the future. Swarm employment is providing promising advantages in multiple civilian applications [27]. Graceful degradation is achieved in case of any technical fault as alternate UAV can take over the mission role and task in such scenarios. Moreover, robustness as well as availability of communication with GCS is ensured beyond the line of sight through establishment of the Adhoc network [28]. The probability of mission failure is minimized as in the swarm system, multiple UAVs are employed which act as system redundancy.

One of the pertinent advantages of these systems is reduced maintenance cost. Communication is of key importance in a flock of UAVs. The major reasons for communication needing to be robust and reliable in operation of such UAV networks is the high mobility of UAVs, irregular distance between each UAV nodule which results in inconsistent link quality, limited capacity of UAVs in terms of onboard available power and the ever-changing topology of the UAV network due to the mobile nature. Moreover, due to limited battery storage, unmanned aerial systems communication becomes challenging [29]. Secure networks are an essential requirement of worldwide users in connection with different applications and have been an unvarying challenge for researchers in ever-evolutionary modern communication models. Similarly, it has been a growing concern in unmanned aerial vehicle systems. It is a significant consideration in wireless networks that they are intrinsically insecure [30].

Wireless networks can be victim of sniffing, eavesdropping and other related wireless network attacks that include MitM, impersonation attacks, DoS [31] and Sybli. These attacks are vulnerable as they compromise privacy; moreover, they can result in major denial of the overall system by exhausting system bandwidth, memory, power, etc. [32]. The jamming of

wireless communication between unmanned aerial vehicle system elements can be devastating. Functional as well as operational control of the unmanned vehicle can be lost through such attacks, causing overall system hacking by the enemy [33]. The classic example of eavesdropping is through man in the middle attacks as malicious element records and the transport of information is through passive means to attacker.

UASs work with a minimum or no human interaction and the authentication process in such system is node to node. Approaching GCS by any node in UAS, it is vital that all nodes are authenticated. However, the limited computing and power resources of UAVs make off-the-shelf security solutions impractical [34]. To construct a secure communication channel, authentication and encryption are essential security features [35]. Cryptography is frequently employed in authentication systems. Typical authentication systems utilize cryptography during the basic steps of verification and certification [36][37].

4.1. Light Weight Authentication Protocols

The use of WiFi has significantly increased over the years both at individual and commercial levels. Due to no complexity involved in installation and operational use of WiFi technology, the popularity of this wireless communication system is ever-increasing [38]. Moreover, it is a cost-effective solution in comparison to typical cable network. wireless sensor nodes are exploding in popularity, with applications as diverse as in any possible fields for the future [39]. These sensors are expected to be a ground-breaking addition in the consumer and business world. For example, the information collected by these sensors in a market place, in a particular section of a store, can turned into meaningful data for targeted advertisement, thus engaging visitors through tapped data by these small sensors for attracting customers and providing better services in consumer field [40].

In a wireless sensor network (WSN), each sensor collects a query from numerous wireless nodes and transports it to a database for subsequent analysis for converting data into meaningful information. The vital requirement in a secure network is authentication of network nodes. Similarly, in WSN, valid authentication of each element is vital. Light weight authentication is considered to be one of the time efficient schemes, mandatory in a heterogeneous network to reduce the period required for authentication process [41]. Reducing handoff latency is thought to be a difficult task. Once a mobile user requires to maintain utilizing the wireless service uninterrupted and remain connected while during a journey across the diverse communication network, this issue arises. For example, the access networks are switched by a user during traveling, staying connected on internet and accessing real-time mobile applications [42]. Interruptions, link quality and reliability issues, security concerns, loss of data packets is experienced whenever there is delay in vertical handoff. Security, reliability, negligible interruption, appropriate handoff scheme are demanded in such applications [43]. In this arena, a number of strategies for reducing authentication delays have been presented. These solutions, on the other hand, do not entirely solve all of the concerns in the problem area; for example, they have security, monetary cost, signaling cost and packet latency flaws.

4.2. 6G Enabled Light Weight Authentication Protocols

In the study [44], a light weight authentication protocol is described that promises the privacy and security of a wireless network that is 6G enabled and supports a maritime IoT-based transportation mechanism. In order to critically verify the security features, methods such as real or random oracle scheme are employed. IoT integrated with blockchain schemes is one of the promising designs in connection with future applications ensuring inherent requirements including security-focused authentication-based needs on data integrity, non-reputability and audibility. Major light weight authentication domains in UAV systems are shown in **Figure 7**.

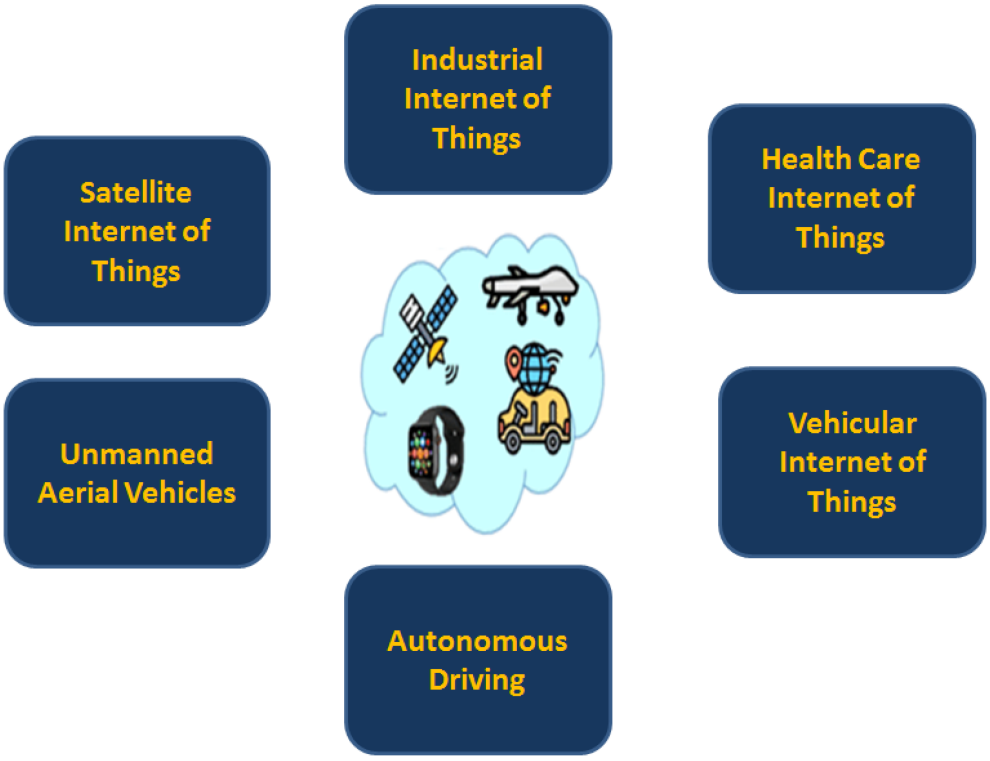

Figure 7. UAV systems light weight authentication domains.

Routinely, Internet of Things networked together employs a relatively weak model of security in use of the communication link. The communication is encrypted through the utilization of session keys. Moreover, in networked IoTs, the limitation of resource utilization is experienced which gives way to inefficient algorithms such as dynamic key generation. Secure interoperability and operation of IoT protocols is a significant issue in embedded devices with several resource limitations. It offers a new scheme of dynamic key generation that is capable of functioning and producing a hefty number of keys that are unique. The suitability of such key generation algorithms is principally proven for Internet of Things modules and dependent conditions in which such devices cannot depend upon re-utilization of already in use keys for encryption and on unvarying key conciliation [45]. Light weight authentication in UAV systems is shown in **Figure 8**.

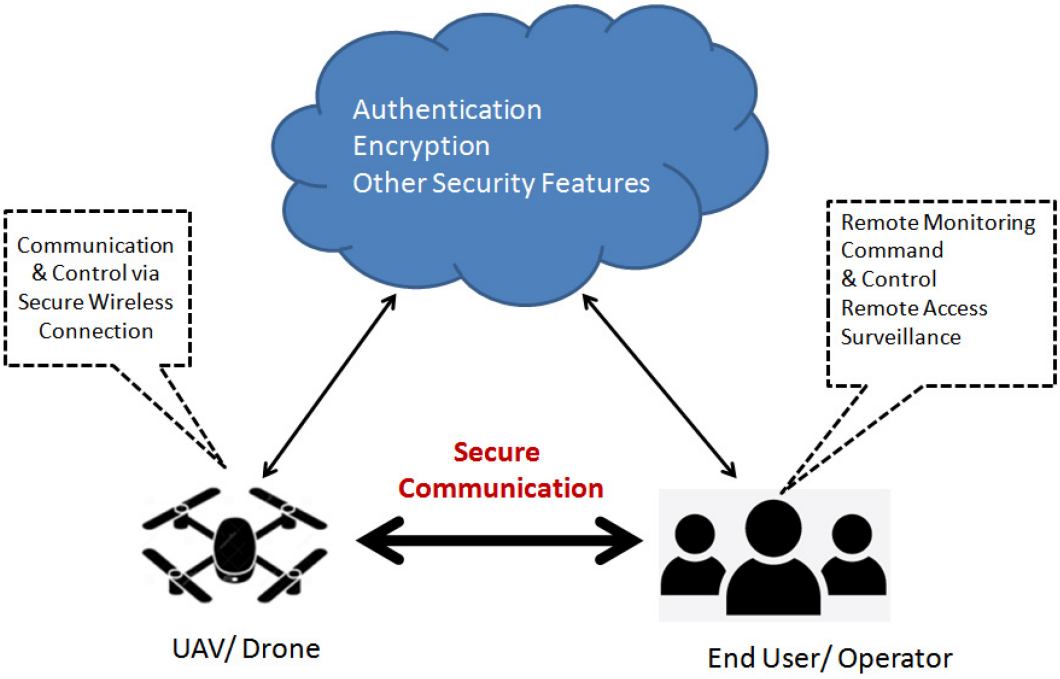

Figure 8. Light weight authentication in UAV systems.

References

1. Popovski, P.; Chiariotti, F.; Huang, K.; Kalør, A.; Kountouris, M.; Pappas, N.; Soret, B. A perspective on time toward wireless 6G. Proc. IEEE 2022, 110, 1116–1146.

2. Khan, A.; Javed, Y.; Abdullah, J.; Nazim, J.; Khan, N. Security issues in 5G device to device communication. Int. J. Comput. Sci. Netw. Secur. 2017, 17, 366.
3. Premkumar, R.; Priya, S.S. Blockchain and Internet of Things: Applications and practices. In Proceedings of the 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Pichanur, India, 25–27 March 2021; pp. 1376–1380.
4. Gupta, R.; Nair, A.; Tanwar, S.; Kumar, N. Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges. IET Commun. 2021, 15, 1352–1367.
5. Moşteanu, N.; Faccia, A. Digital Systems and New Challenges of Financial Management–FinTech, XBRL, Blockchain and Cryptocurrencies. Qual.-Access Success J. 2020, 21, 159–166.
6. Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure trust-based blockchain architecture to prevent attacks in VANET. Sensors 2019, 19, 4954.
7. Safdar, H.; Fisal, N.; Ullah, R.; Maqbool, W.; Asraf, F.; Khalid, Z.; Khan, A. Resource allocation for uplink M2M communication: A game theory approach. In Proceedings of the 2013 IEEE Symposium on Wireless Technology & Applications (ISWTA), Kuching, Malaysia, 22–25 September 2013; pp. 48–52.
8. Kazmi, S.H.A.; Masood, A.; Nisar, K. Design and Analysis of Multi Efficiency Motors Based High Endurance Multi Rotor with Central Thrust. In Proceedings of the 2021 IEEE 15th International Conference on Application of Information and Communication Technologies (AICT), Baku, Azerbaijan, 13–15 October 2021; pp. 1–4.
9. Raja, G.; Anbalagan, S.; Ganapathisubramaniyan, A.; Selvakumar, M.S.; Bashir, A.K.; Mumtaz, S. Efficient and secured swarm pattern multi-UAV communication. IEEE Trans. Veh. Technol. 2021, 70, 7050–7058.
10. Li, T.; Hu, H. Development of the Use of Unmanned Aerial Vehicles (UAVs) in Emergency Rescue in China. Risk Manag. Healthc. Policy 2021, 14, 4293.
11. Zhu, K.; Han, B.; Zhang, T. Multi-UAV Distributed Collaborative Coverage for Target Search Using Heuristic Strategy. Guid. Navig. Control 2021, 1, 2150002.
12. Khan, I.U.; Shah, S.B.H.; Wang, L.; Aziz, M.A.; Stephan, T.; Kumar, N. Routing protocols & unmanned aerial vehicles autonomous localization in flying networks. Int. J. Commun. Syst. 2021, e4885.
13. Nagpal, S.; Aggarwal, A.; Gaba, S. Privacy and Security Issues in Vehicular Ad Hoc Networks with Preventive Mechanisms. In Proceedings of the International Conference on Intelligent Cyber-Physical Systems; Springer: Singapore, 2022; pp. 317–329.
14. El Haber, E.; Alameddine, H.A.; Assi, C.; Sharafeddine, S. UAV-aided ultra-reliable low-latency computation offloading in future IoT networks. IEEE Trans. Commun. 2021, 69, 6838–6851.
15. Yahuza, M.; Idris, M.Y.I.; Ahmedy, I.B.; Wahab, A.W.A.; Nandy, T.; Noor, N.M.; Bala, A. Internet of drones security and privacy issues: Taxonomy and open challenges. IEEE Access 2021, 9, 57243–57270.
16. Jan, S.U.; Abbasi, I.A.; Algarni, F.; Khan, A.S. Corrections to “A Verifiably Secure ECC Based Authentication Scheme for Securing IoD Using FANET”. IEEE Access 2022, 10, 105496.
17. Lei, Y.; Zeng, L.; Li, Y.-X.; Wang, M.-X.; Qin, H. A lightweight authentication protocol for UAV networks based on security and computational resource optimization. IEEE Access 2021, 9, 53769–53785.
18. Oteafy, S.M. Resource augmentation in Heterogeneous Internet of Things via UAVs. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021.
19. Gandra, C.; Hansson, J. Application of Value Proposition Design to a High-Tech Business Market Product; Lund University: Lund, Sweden, 2021.
20. Baltaci, A.; Dinc, E.; Ozger, M.; Alabbasi, A.; Cavdar, C.; Schupke, D. A Survey of Wireless Networks for Future Aerial Communications (FACOM). IEEE Commun. Surv. Tutor. 2021, 23, 2833–2884.
21. Zhang, T.; Wang, Z.; Liu, Y.; Xu, W.; Nallanathan, A. Joint Resource, Deployment, and Caching Optimization for AR Applications in Dynamic UAV NOMA Networks. IEEE Trans. Wirel. Commun. 2021, 21, 3409–3422.
22. Kaiser, M.S.; Zenia, N.; Tabassum, F.; Mamun, S.A.; Rahman, M.A.; Islam, M.; Mahmud, M. 6G access network for intelligent internet of healthcare things: Opportunity, challenges, and research directions. In Proceedings of the International Conference on Trends in Computational and Cognitive Engineering; Springer: Singapore, 2021; pp. 317–328.
23. Hamza, B.J.; Saad, W.K.; Shayea, I.; Ahmad, N.; Mohamed, N.; Nandi, D.; Gholampour, G. Performance enhancement of SCM/WDM-RoF-XGPON system for bidirectional transmission with square root module. IEEE Access 2021, 9, 49487–49503.

24. Mitkas, D.Z.; Lovell, D.J.; Venkatesh, S.; Young, S. Activity Identification using ADS-B data at General Aviation Airports. In Proceedings of the AIAA AVIATION 2021 FORUM, Virtual Event, 2–6 August 2021.
25. Ahmad, Z.; Shahid Khan, A.; Wai Shiang, C.; Abdullah, J.; Ahmad, F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Trans. Emerg. Telecommun. Technol. 2021, 32, e4150.
26. Munusamy, R.; Kumre, J.; Chaturvedi, S.; Bandhu, D. Design and Development of Portable UAV Ground Control and Communication Station Integrated with Antenna Tracking Mechanism. In Intelligent Infrastructure in Transportation and Management; Springer: Singapore, 2022; pp. 193–212.
27. Adnan, W.H.; Khamis, M.F. Drone use in military and civilian application: Risk to national security. J. Media Inf. Warf. 2022, 15, 60–70.
28. Mohammed, I.; Collings, I.B.; Hanly, S.V. Line of sight probability prediction for UAV communication. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
29. Tang, S.; Zhou, W.; Chen, L.; Lai, L.; Xia, J.; Fan, L. Battery-constrained federated edge learning in UAV-enabled IoT for B5G/6G networks. Phys. Commun. 2021, 47, 101381.
30. Sehrawat, H.; Siwach, V. Security vulnerabilities in Wireless Sensor Networks. J. Inf. Assur. Secur. 2010, 5, 31–44.
31. Javed, Y.; Khan, A.S.; Qahar, A.; Abdullah, J. Preventing DoS attacks in IoT using AES. J. Telecommun. Electron. Comput. Eng. (JTEC) 2017, 9, 55–60.
32. Nazir, M.; Sabah, A.; Sarwar, S.; Yaseen, A.; Jurcut, A. Power and resource allocation in wireless communication network. Wirel. Pers. Commun. 2021, 119, 3529–3552.
33. Ly, B.; Ly, R. Cybersecurity in unmanned aerial vehicles (UAVs). J. Cyber Secur. Technol. 2021, 5, 120–137.
34. Chierici, A.; Malizia, A.; Di Giovanni, D.; Ciolini, R.; d'Errico, F. A High-Performance Gamma Spectrometer for Unmanned Systems Based on Off-the-Shelf Components. Sensors 2022, 22, 1078.
35. Maikol, S.O.; Khan, A.S.; Javed, Y.; Bunsu, A.L.A.; Petrus, C.; George, H.; Jau, S. A novel authentication and key agreement scheme for countering MITM and impersonation attack in medical facilities. Int. J. Integr. Eng. 2021, 13, 127–135.
36. Balan, K.; Abdulrazak, L.; Khan, A.; Julaihi, A.; Tarmizi, S.; Pillay, K.; Sallehudin, H. RSSI and public key infrastructure based secure communication in autonomous vehicular networks. Int. J. Adv. Comput. Sci. Appl. 2018, 9, 298–304.
37. Mahmood Saqib, R.; Shahid Khan, A.; Javed, Y.; Ahmad, S.; Nisar, K.; Abbasi, I.A.; Haque, M.R.; Ahmadi Julaihi, A. Analysis and intellectual structure of the multi-factor authentication in information security. Intell. Autom. Soft Comput. 2022, 32, 1633–1647.
38. Memon, S.K.; Nisar, K.; Hijazi, M.H.A.; Chowdhry, B.; Sodhro, A.H.; Pirbhulal, S.; Rodrigues, J.J. A survey on 802.11 MAC industrial standards, architecture, security & supporting emergency traffic: Future directions. J. Ind. Inf. Integr. 2021, 24, 100225.
39. Uribe-Leitz, T.; Matsas, B.; Dalton, M.K.; Lutgendorf, M.A.; Moberg, E.; Schoenfeld, A.J.; Goralnick, E.; Weissman, J.S.; Hamlin, L.; Cooper, Z. Geospatial analysis of access to emergency cesarean delivery for military and civilian populations in the US. JAMA Netw. Open 2022, 5, e2142835.
40. Talpur, M.R.H.; Talpur, M.S.H.; Talpur, F.; Haseeb, A.; Kehar, A.; Fatima, S. A Model for Secure Inter-Institutional Communication Based on Artificial Intelligence (AI) and Blockchain. Int. J. Comput. Intell. Control 2021, 13, 145–154.
41. Javed, Y.; Khan, A.S.; Qahar, A.; Abdullah, J. EEoP: A lightweight security scheme over PKI in D2D cellular networks. J. Telecommun. Electron. Comput. Eng. (JTEC) 2017, 9, 99–105.
42. Deebak, B.D.; Fadi, A.-T. Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing. Future Gener. Comput. Syst. 2021, 116, 406–425.
43. Lafta, S.A.; Abdulkareem, M.M.; Ibrahim, R.K.; Kareem, M.M.; Ali, A.H. Quality of service performances of video and voice transmission in universal mobile telecommunications system network based on OPNET. Bull. Electr. Eng. Inform. 2021, 10, 3202–3210.
44. Chaudhry, S.A.; Irshad, A.; Khan, M.A.; Khan, S.A.; Nosheen, S.; AlZubi, A.A.; Zikria, Y.B. A Lightweight Authentication Scheme for 6G-IoT Enabled Maritime Transport System. IEEE Trans. Intell. Transp. Syst. 2021.
45. Pothumarti, R.; Jain, K.; Krishnan, P. A lightweight authentication scheme for 5G mobile communications: A dynamic key approach. J. Ambient Intell. Humaniz. Comput. 2021, 1–19.