Chapter 13
Blockchain-Based IoD Networks in Military Operation and Security Surveillance

Sandeep Maan
https://orcid.org/0000-0002-7610-7504
Government College for Girls Sec 14. Gurugram, India

Gian Devi
https://orcid.org/0000-0002-7539-6404
Government College for Girls Sec 14. Gurugram, India

Lakshya Mann
The North Cap University, Gurugram, India

ABSTRACT

Modern wars is changing at an incredible pace and the major game changers are Drones. They offer remarkable precision and efficiency. These days, drone find application in many areas. Concept of IoT when extended to the drone networks, is termed IoD (Internet of Drones). These drone or IoD networks may have to work in an enemy territory and work over unreliable wireless networks. Blockchains can provide a natural solution to the security threats in a drone based implementation. Drone networks generate huge data. 5G networks offer QoS based fast services. So, we propose that communication channel between D2D, D2G, D2B are all 5G. This would ensure low latency and required QoS level to sustain real time services over these IoD networks. During this chapter different important aspects of above concepts i.e. drone networks, blockchain and 5G networks are covered. Finally, an integrated architectures are studied to sustain and secure the real time communications over IoD networks.

INTRODUCTION

Modern wars are changing at an incredible pace. War is not decided by the size of army one has rather the advanced technology has transformed the way battles are being fought and won. Major game changer are Drones. They offer remarkable precision and efficiency. Countries including India have recognized

DOI: 10.4018/979-8-3373-4277-1.ch013

these shifts. Modern armies are incorporating drones into its operations. During recent India Pakistan conflict drones were used lavishly to launch attacks as well as for surveillance. Such strategic move reflects resolute to leveraging technology to enhance national security and maintain tactical superiority. Different areas where Drones are being used include surveillances & reconnaissance, tactical support in combat, logistics & supply chain, humanitarian aid and electronic warfare.

Apart from military operations, drones are primarily used for aerial monitoring including crowd control, country border surveillance, infrastructure inspection including civil operation.

Adoption of Drones in such strategic areas including military operations and surveillance bring challenges. Data is transmitted over insecure wireless medium. Drones are part of a Mobile Adhoc Network formed on the go in emergencies. The network topology keeps on changing. Success of MANETs depends upon the cooperation between participating nodes.

Drones (also known as Unmanned Aerial Vehicles) are generally not designed with security in mind, and there are fundamental security and privacy issues that need study. They are primarily designed for controlling airspace and providing support to various navigation activities. Several other applications of drones ranges to military, newsgathering, security, agricultural, logistics deployments, surveillance, medicine, traffic-monitoring applications etc. Gartner predicts that the UAV industry will increase at a rate more than 35% per year from 2018 to 2028 (Lv et al., 2021). The number of UAVs in use will rise to around 9 million around the world. Due to increase of commercial drones applications, recent forecasts indicate that there will be a 100 USD billion market opportunity over the coming years based on the drones.

Drones or UAVs are equipped with multiple type sensors. These sensors can expand the scope of task execution and have potential wide range utilities used in disaster rescue, industrial inspection, logistics, and transportation scenarios. Thereby comes the concept of Internet of Drones. Advent of 5G network has further promoted the technical breakthrough of drones. Especially in the application scenarios like emergency rescue and security monitoring. The kind of ultra-wideband and low-delay network environment provided by 5G networks not only meets the high demand of UAVs for data link in these scenes, but also provides the network environment of UAV swarm cooperation (Xiao et al., 2021).

Drones can work together or alone, and they can send information between other devices. Xiao et al. (2021) describes one of the biggest problems is how to make sure the system is safe and private when the drone works together as a network or IoD, especially for crowd monitoring, which is a very sensitive task. This is because drone networks are open to attacks like passive eavesdropping, data tampering, and identity theft. If hazardous eavesdroppers get their hands on these surveillance data about public safety, the results will be bad.

Any malicious node can launch numerous attacks, data threats and disrupt the working of the network. These includes replay attack, impersonation, man-in-middle, privileged insider attack, Ephemeral Secret Leakage (ESL), Denial of Service attacks. The above list is illustrative only and not exclusive. Drones flying over an insecure zone may even be captured and attacks like Power analysis attacks that exploit the power consumption of a device can be utilized to extract sensitive information, including credentials like passwords or encryption keys stored in the drones. This enhances scope of attacks enormously that can be launched further with the help of compromised drones. Most dangerous of these attacks include impersonation and ESL.

Recentrly, the Blockchain technology has been envisioned owing to its robustness in providing trust and anonymity (Aloqaily et al., 2021). Chang et al. (2021) mentions that blockchain has established

Investigating Public Acceptance on Public Oriented Human Space Commercialization
Alex Monchak, Ki-Young Jeongand James Helm (2013). *International Journal of Space Technology Management and Innovation (pp. 1-19).*
www.irma-international.org/article/investigating-public-acceptance-on-public-oriented-human-space-commercialization/85342