Enhancement of Security Constraints in UAV-assisted IoT Deployment Using Blockchain Technology in Military Operations

Mohtasin Golam, Jae-Min Lee and Dong-Seong Kim,
Networked System Laboratory, School of Electronics Engineering,
Kumoh Institute of Technology, Gumi, South Korea.
(golam248, ljmpaul, dskim)@kumoh.ac.kr

***Abstract*—Internet of things (IoT) is currently adopted in every possible areas such as industrial, healthcare, traffic-monitoring, and military applications. The deployment of IoT in military area has a huge concern of security. Unmanned aerial vehicle (UAV) is being used in military applications since it is first invented and with the rapid growth of IoT devices the use of UAV has become more essential. Blockchain is a peer-to-peer network which in recent has been occupied by every field for the security purpose. In this paper, we analyzes the security challenges towards the deployment of UAV and IoT devices to create wireless communication in military networks. To provide the security and reliability we adopted the blockchain technology. The significant impact of using blockchain technology on the deployment of UAV and IoT devices is discussed thoroughly. Finally, future research direction and open issues are discussed in conclusion.**

***Index Terms*—Blockchain, internet of things (IoT), military networks, unmanned aerial vehicle (UAV).**

I. Introduction

Since the discovery of unmanned aerial vehicle (UAV) many countries are adopting it specially in military environments because of the convenience of easy deployment, low cost and high mobility. Many military operations like search and rescue (SaR), surveillance, reconnaissance and battlefield network is now leading by UAV. UAV can be deployed as tether less base station to increase the network capacity and enhance the coverage area for existing network [1]. However, security and reliability is the prime concern for deploying UAVs in the military operations. Because military operations (e.g., surveillance, search and rescue, reconnaissance) can be interrupted by the adversary.

Internet of things (IoT) has brought a revolution in the industrial network which follows by the military network. The intelligence and effectiveness of IoT devices applied to the military to create infrastructure is referred to as the internet of military things [2]. The introduction of IoT in the military network brings challenges with it. The deployment and efficient implementation of IoT architecture in a military network need an extensive study because of its delicate characteristics [3]. Security assurance is the key problem of IoT from the very beginning. There will be no effect of deploying IoT architecture without mitigating the security constraints for the military network.

Blockchain is a peer-to-peer (P2P) network which creates a chain of many connected blocks. In blockchain network, each block hold an unique hash which content the identity of the block that generated based on the transaction information [4]. Blockchain is being adopted in diverse applications because of its decentralization, immutability, and decentralized features. Blockchain has adopted asymmetric encryption to provide security for the networks [5].

II. Security Challenges of IoT in Military Network

A. Data Integrity

Data generated from IoT devices is very important and confidential in military operations, and can contain the secrets of the future missions. Conventional storage such as cloud storage can suffer from its implicit vulnerabilities because of its centralized server system. The centralized server can cause a single point of failure, suffer response delay and system scalability problem.

B. Data Sharing

A large amount of data is produced from IoT devices which are used for communication, location sharing, mission instruction and so on. The prime object of IoT infrastructure in the military network is to share data between devices which contents valuable information of secret operations. However, these information are normally not free for everyone uses, and a convenient and reliable data sharing system is needed.

C. Privacy

In military network IoT infrastructure collects data from different smart devices, sensors, and actuators and make important decision based on the collected data. Privacy can be violated in different ways (e.g., data acquisition, data exchange, raw data processing) in the complex military IoT infrastructure. The misuse of data produced from IoT devices can eventually harm user privacy.

D. Authentication & Access Control

Unauthorized access to the resources and steal sensitive information in the IoT system is another common issue, which can lead to destruction in the military network. Conventional

centralized authentication system and access control management for user is based on access policies in which IoT system can create a bottleneck when the number of devices grows exceedingly. Besides the dynamic characteristics of IoT deployment in military network may lead towards complex trust management issue and can cost the system scalability.

III. Proposed Blockchain based IoT Framework

In this section, the proposed blockchain based solution for IoT deployment in military network in going to be discussed. The system architecture of blockchain based IoT network with the assistance of UAV is shown in Fig. 1. The proposed architecture consists of two components (1) IoT devices and (2) UAV, and both component is combined with blockchain technology. UAV is used to provide extended connectivity wirh base station (BS) and low power transmission and works as a validator in the blockchain network. UAV hovers all over the area and collects data from IoT devices to provide information to BS. Each IoT devices is considered as a user and each user collects data from their own surrounding area. The collected data of every user is shared among the neighbor users and the nearest hovering UAV via a P2P network. Then the collected data from the authorized devices is verified by the other devices in order to store in blockchain network.

Before sending the collected data to the UAV, each user creates its own secret key s_k and then generates a public key key Pr_k from s_k. To create the s_k it uses the mac address of the device Δ_{mac}, a random text tx, and timestamp T. After generating the Pr_k user send request to the nearest UAV for registration. Upon receiving request UAV sends its public key Pu_k to encrypt the basic information. After the validation (if it is successful) the user get access to the blockchain network and can share data among the other connected devices.

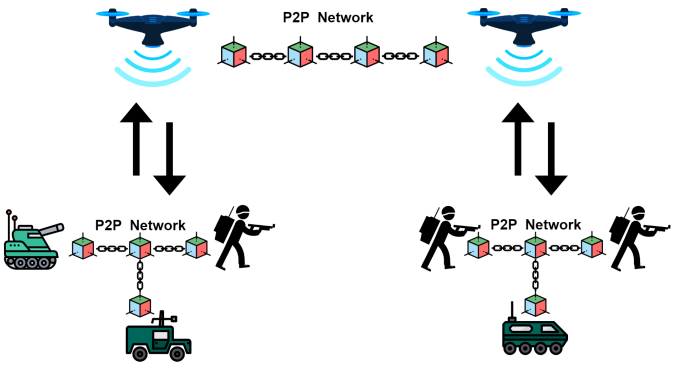

Fig. 1. System architecture of blockchain based IoT networks

IV. Result Discussion

To overcome these issues mentioned above the proposed system has a significant impact. Blockchain plays an important role in IoT system for data management, access control and security. Blockchain provides a decentralized server system which can be a potential solution.

- Data Integrity: To ensure the data integrity the proposed blockchain based IoT infrastructure can provide solution to protect data pollution and deletion and provide a decentralized server system which is a potential solution for data integrity issues.
- Data Sharing: The proposed blockchain based system can provide a solution for the data sharing system in which the user shares data between them via P2P network that ensure the secure data sharing for both IoT devices and UAVs.
- Privacy: To protect the privacy in the blockchain based IoT system, blockchain uses pseudonyms, such as public keys, to achieve anonymity. Different consensus algorithm and cryptographic techniques uses to achieve anonymity to secure privacy of the user. Moreover, encryption method in blockchain technology can alleviate the privacy of the user to ensure secure communication.
- Authentication: In proposed system each user needs to create its own private key to register in the network which can provide authentication and access control for IoT devices. Furthermore, blockchain can provide a decentralized authentication and access control system which removes the dependency of centralized service.

V. Conclusion

In this paper, a blockchain based IoT deployment system with the assistance of UAV is proposed in military network to enhance the security constraints. In proposed system, IoT is connected with the UAV for secure data transmission via a blockchain network. The aim is to reduce the unauthorized access, secure data sharing, control privacy and prevent data stealing. Moreoever, open issues like computational complexity, timing constraints, resource constraints and many more is much more concerning prior to apply blockchain technology which can be a subject of future research.

VI. Acknowledgement

This work was supported by National Research Foundation of Korea(NRF) grant funded by Korea government(MSIT)(2019R1F1A1064055).

References

[1] M. Mozaffari, A. Taleb Zadeh Kasgari, W. Saad, M. Bennis and M. Debbah, "Beyond 5G With UAVs: Foundations of a 3D Wireless Cellular Network," in IEEE Transactions on Wireless Communications, vol. 18, no. 1, pp. 357-372, Jan. 2019, doi: 10.1109/TWC.2018.2879940.

[2] A. Kott, A. Swami and B. J. West, "The Internet of Battle Things," in Computer, vol. 49, no. 12, pp. 70-75, Dec. 2016, doi: 10.1109/MC.2016.355.

[3] N. Suri et al., "Analyzing the applicability of Internet of Things to the battlefield environment," 2016 International Conference on Military Communications and Information Systems (ICMCIS), Brussels, 2016, pp. 1-8, doi: 10.1109/ICMCIS.2016.7496574.

[4] Y. Yu, Y. Li, J. Tian and J. Liu, "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," in IEEE Wireless Communications, vol. 25, no. 6, pp. 12-18, December 2018, doi: 10.1109/MWC.2017.1800116.

[5] A. A. Monrat, O. Schelén and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," in IEEE Access, vol. 7, pp. 117134-117151, 2019, doi: 10.1109/ACCESS.2019.2936094.