IEEE Communications Standards Magazine, Volume 7, Issue 3, September 2023, pp. 16-23
DOI:10.1109/MCOMSTD.0005.2200052

Blockchain-Based Secure and Intelligent Data Dissemination Framework for UAVs in Battlefield Applications

Abstract

The modern warfare scenario has immense challenges that can risk personnel's lives, highlighting the need for data acquisition to win a military operation successfully. In this context, unmanned aerial vehicles (UAVs) play a significant role by covertly acquiring reconnaissance data from an enemy location to make the friendly troops aware. The acquired data is mission-critical and needs to be secured from the intruders, which can implicitly manipulate it for their benefit. Moreover, UAVs collect a large amount of data, including high-definition images and surveillance videos; handling such a massive amount of data is a bottleneck on traditional communication networks. To mitigate these issues, this article proposes a blockchain and machine learning (ML)-based secure and intelligent UAV communication underlying sixth-generation (6G) networks, that is, Block-USB. The proposed system refrain the disclosure of highly-sensitive military operations from intruders (either a rogue UAV or a malicious controller). The proposed system uses off-chain storage, that is, Interplanetary file system (IPFS), to improve the blockchain storage capacity. We also present a case study on securing UAV-based military operations by considering multiple scenarios considering controller/UAV malicious. The performance of the proposed system outperforms the traditional baseline 4G/5G and non IPFS-based systems in terms of classification accuracy, communication latency, and data scalability.

Introduction

In earlier years, the military communication transpired by the commanders to relay orders to their subordinates faced massive delays due to the isolated troops at various locations. Communication evolved with time, and the invention of the telegraph was one of the most significant communication methods used for military operation. Due to its inherent cost and reliability problems, it is not proliferated much in the war system. One of the pioneering improvements in the war system was the inclusion of unmanned aerial vehicles (UAVs) that allies radio, sound, light detection, and ranging to help in military operations. UAVs are remote-controlled air-crafts that can fly autonomously based on preprogrammed flight plans without any human involvement. From the few decades, UAVs gained much importance in diverse areas of the military, such as recognizing enemy forces, border surveillance, identification of weapon systems, moving vehicles, disaster management, communication relays, and reconnaissance [1]. It also helps remote networks to transmit and store military data quickly, where the physical interaction becomes unmanageable and expensive [2].

In general, there are three types of UAV communication: UAV-to-UAV (U2U), UAV-to-base, and UAV-to-satellite (U2S) communications [3]. In U2U, multiple UAVs can share information to increase military operation's scalability, reliability, and precision. A base station controls or directs UAVs through an air interface by reducing coverage gaps and network congestion in UAV-to-base station communication. It collects data from the environment and sends it to the base station, which is then forwarded to the ground control station (GCS) for analysis. On the other hand, U2S communication track UAVs when it goes beyond the LOS. Such communication is highly required for sending real-time coordinates of enemies via global positioning system (GPS) to military personnel. Even though U2S exhibits high maintenance cost, which is not feasible for commercial applications; hence it is used particularly for military operation [4]. The battlefield environment requires persistent surveillance and services, which minimizes soldier casualties and also capture enemy zone information. UAVs are managed and controlled remotely via smartphones and possess the capability to cover the surveillance of highly remote areas without the requirement for a massive workforce, time, and effort. This becomes the biggest reason for the adoption of UAVs in military applications.

The growing demand for UAVs invoke attackers to perform malicious activities, such as denial of service (DoS), GPS spoofing, UAV hijacking, information leakage, and traffic blockage attacks [5]. Here, machine learning (ML) plays a vital role in handling these security issues in a 5G-based UAV communication. Many approaches exist in the literature to address the aforementioned secu-

© 2023 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

rity issues. For example, the authors in [6] proposed an ML and 5G-based UAV system to detect cyberattacks and security vulnerabilities. Their model offers data integrity and security. Challita et al. [7] highlighted various security issues and challenges in UAV-based delivery systems. They have utilized LSTM-based deep reinforcement learning algorithms to deal with cyber-physical attacks, interference, mobility management, and authentication. Several researchers have used ML and encryption-based techniques to maintain secure, efficient, reliable, and low-latency communications between UAVs [8].

The encryption-based techniques are highly compute-intensive and require regular key generation and exchange, which is not ideally suitable for low-powered UAVs. To overcome this issue, blockchain is a perfect candidate, which is an immutable and time-stamped shared ledger managed by cluster of nodes [9]. It offers decentralized environment to UAVs for collecting and sharing data securely and reliably. In [10], Gupta et al. proposed a blockchain-based onion routing protocol for secure, trusted, and anonymous internet of military vehicles. They have used an interplanetary file system (IPFS) to make their system scalable and cost-effective. Then, Golam et al. [11] discussed a blockchain-based solution to prevent malicious activities and data loss for D2D communication in the military environment. However, they have not verified the efficiency of blockchain adoption in the military environment. Later, Ko et al. [2] proposed a security protocol to secure U2U communication. They have covered various security requirements but not emphasized on human or UAV intrusion detection in battlefield environment. The aforementioned analysis shows that much research is done on UAV communication. However, very few of them have focused on the security and scalability parameters for UAV-based battlefield applications. Nonetheless, they have not amalgamated key-enabler technologies (AI, blockchain, etc.) to enhance the security performance of UAV communication in military operations [2, 10, 11]. Motivated by this, we proposed an AI and blockchain-based secure data dissemination framework for a UAV-based battlefield environment Block-USB. Further, to make the proposed framework efficient and scalable, we integrate IPFS with blockchain technology. We also considered different scenarios, which indicate the possibility of various malicious activity on the UAV, and solutions to overcome those security issues.

Contributions

Following are the major contributions of the article:

- We highlight the adoption of UAV communication in military operations by addressing its security and privacy concerns.
- We propose a blockchain and AI-based secure UAV communication framework, that is, Block-USB a blockchain based secure data dissemination for UAVs in to deal with data security and integrity issues in a battlefield environment. We also integrate IPFS with the proposed system to improve the overall system scalability and efficiency.
- We evaluate the performance of Block-USB on classification accuracy, scalability, and communication latency.

Organization

The entire article is organized into six sections. The following section discusses the background concepts. Then we present our proposed framework. Following that, we describe various open issues and research challenges. We then present the case study, and finally we conclude the article.

Background and Important Concepts

This section describes the concepts of blockchain, AI, UAV, and integration of blockchain and AI with UAV communication.

Blockchain: A Distributed Ledger Technology

Blockchain is a technology in which the blocks are connected via a peer-to-peer (P2P) network, where the data is shared in blocks and each peer has the identical copy of the data [11]. Blockchain can also secure UAV communication by using immutability, transparency, traceability, and decentralization mechanisms as stated in Table 1. The decentralization feature is more robust and secure from the central authority system. It also provides entity and data authentication, fast synchronization, cooperation, and load sharing features in a battlefield environment. Additionally, it has a public and private key that avoids data hijacking and data integrity issues through a common channel [12]. Furthermore, a digital signature in blockchain identifies the origin of the data that can be traced on the battlefield and incorporates data and entity authentication between UAVs.

ML for Intruder Detection

ML is the key technology with complex decision-making capabilities to obtain a proper UAV placement, connectivity, trajectory identification, and security improvement in the battlefield environment. The adoption of ML techniques in UAV-based communication distinguish between an authorized and unauthorized person in GCS. Furthermore, It used to identify the malicious behavior of UAVs and classify the authenticated UAVs. The supervised and unsupervised solutions of ML are used for UAVs-based problems, such as identifying UAV's position, UAV's deployment, detection, and channel estimation. ML technique can also be used in intrusion and anomaly detection to create normal data behavior patterns.

UAV Communication

UAVs have become a crucial component in military applications, especially in battlefield environment, by embracing the characteristic of next-generation wireless networks, such as agility, LoS feature, low latency, and cost-efficient. UAVs are deployed for intelligence, reconnaissance, and surveillance in the battlefield environment [13]. They have ubiquitous coverage, act as a relay node to connect frontline troopers and headquarters and fast service recovery due to cellular infrastructure failure. In any military operation, UAVs require to have stringent security and low latency communication. Hence, researchers are utilizing crucial control and non-payload communication link for UAV communication which supports effi-

The encryption-based techniques are highly compute-intensive and require regular key generation and exchange, which is not ideally suitable for low-powered UAVs.

Blockchain characteristics	Description	Potential applications in the battlefield
Transparency	Every node of the network have the copy of digital ledger and they need to check the validity.	The information passed between UAVs and GCS of the battlefield is accessible to all the authorized troop members.
Shared ledger	The system does not have single person locking, it share the information between all the nodes.	Reconnaissance information acquire form enemy zone to alert the GCS users, which is not having single point failure.
Security	Blockchain provides better security because there is no chance of shutting down the system. It uses encryption that ensures another layer of security for the system.	Blockchain offers high security to the UAV data in battlefield so that malicious user can not modify the information stored in UAVs and we are able to identify the intrusion attacks on UAVs.
Trust management	Blockchain ensures the trust of information using unique tokens that contain the history of each previous owner. It uses digital signature and SHA256 to establish trust in the system.	In the battlefield environment, this blockchain feature insure the trust between UAVs and GCS user before passing the information.
Immutability	Once the information is stored in the blocks it can not tamper, it should be stored as a permanent and unalterable network.	This feature of blockchain can not allow to modify the critical information stored in UAVs for military operation.
Faster settlement	Information transfer relatively faster and saves lots of time in long run	Blockchain offers faster settlement between U2U, and UAV-to-GCS user of the battlefield. Using this feature troop member can get instant alert and act accordingly based on the enemies behavior.

Table 1. Characteristics of blockchain and their potential to resolve security issue in battlefield environment.

cient inter-UAV coordination eradicating interference, and faster response. However, they are remotely controlled for predetermined missions, which opens new challenges in terms of security and privacy. These remote connections are vulnerable to several security attacks, as shown in Fig. 1. Therefore, there is a requirement of adopting a 6G network that has concrete security technologies, such as intelligent AI/ML, cloudification, blockchain, and quantum computing.

Integration of Blockchain and AI with UAV Communication

Integrating blockchain and AI with UAVs provides a solution for secure and efficient data dissemination in the battlefield environment. UAVs are vulnerable to being lost, destroyed, cyber-attacks, or physically hijacked. There are several issues in intra-UAV communication, such as UAV security, air data security, data storage, and management, which need to be addressed. ML classification algorithms are used to identify the malicious attacks on UAVs and also to classify the authorized users controlling the UAVs. Here, the blockchain, a distributed ledger offers security to the data via cryptography primitives, such as public-private key infrastructure, hashing, and digital signature. The prime role of blockchain technology is to assure the truthfulness of the stored information and improve the security and transparency of the UAVs. ML and blockchain-based secure data dissemination approach has been proposed in this article for U2U communication in a battlefield environment.

The Proposed Framework

This section shows the working of the proposed framework, which is a blockchain and AI-based secure UAV communication for battlefield environment Block-USB. The proposed architecture is bisected into five relevant layers: data acquisition, analytics, communication, blockchain, and application, as shown in Fig. 2. A comprehensive description of each layer is as follows:

Data Acquisition Layer

In this layer, the controller deploys UAVs to acquire reconnaissance data from the battlefield environment (friendly/enemy zone). A controller can operate and manage UAVs either in controlled or autopilot mode, which benefits military personnel to track military-critical information such as tracking the enemy's location, artillery detection, monitoring missile threats, and tracking ground vehicle movements. The purpose of data accumulation is to develop a strategy to win the battle by analyzing the reconnaissance data. Multiple UAVs collect data from the battlefield in the form of high-quality images, videos, and land topography information via sensors. It is collectively sent to the analytics layer for further processing. In an enemy zone, the UAVs always fear getting caught by enemy radars, and therefore, small and compact UAVs are used. These small UAVs are energy-constrained and cannot be operable for a longer period [14]. Consequently, the collected reconnaissance data need to be transferred to the nearby UAVs via UAV-to-UAV communication.

Communication Layer

Military UAVs use 5G millimeter-wave communication, which operates in the spectrum range of 24GHz to 40GHz to communicate with each other and to exchange reconnaissance data with the GCS. However, this range is susceptible to climate conditions and affected by the multipath propagation, resulting in low data rate and high latency in the communication. To tackle these challenges, it requires installing more base stations in a cell, which makes this technology highly expensive. UAV communication in a combat operation needs high data rates, low latency, and secure communication for quick exchange of mission-critical data to the GCS, which is not possible

in the current 5G millimeter-wave communication. Therefore, there is a need for a 6G network that has converged all past features of a 5G network, such as ultra-low latency (<1ms), ubiquitous high-speed data connectivity (1Tb/s), scalable connectivity (10^7 devices/sq m), and ultra-high reliability (99.99999 percent). Employing 6G on the battlefield, the UAVs can fly at higher altitudes without any obstruction in the communication and conceal themselves from the enemies in an enemy zone. Furthermore, it brings less scattering and path loss of the signals, making it faster communication between UAVs and GCS. UAVs in this layer communicates with application layer to command-control purpose via a 6G interface.

Data Analytics Layer

UAVs collect reconnaissance data from acquisition layer to exchange it with application layer, but before this, it needs to be verified by the analytics layer for security and privacy purpose. The reconnaissance data is immensely critical to any military operation and needs to be secured from intruders. An intruder can modify the UAV's behavioral data, such as latitude, longitude, time, communication, read-write operation, and reconnaissance data to misguide the UAVs to win the battle. It is also essential to confirm the authenticity of controller, that is, whether the controller who gives the command and control to the UAVs is authenticated or not. From the viewpoint of ML, it is a binary classification problem, where we classify the normal UAVs with 1 and malicious UAVs with 0.

To accomplish the aforementioned objectives, ML has been incorporated due to its versatility in solving any binary classification problem and having a faster convergence rate. This layer has two stages wherein first stage, we classify the malicious and non-malicious UAVs by analyzing their behavioral data. For that, we used [15] dataset, which consist of UAVs behavior data, that is, speed, drift rate, magnetic field, control data, and so on, and network traffic data, that is, channel information, network speed, port numbers, source and destination address, and so on. In the second stage, the network data flowing between the acquisition and application layer is analyzed using the feature space of [15], where the classifier classifies the authenticate controller. Both the dataset is individually pre-processed by identifying any outliers, missing values, and normalization. While forming this classification problem, the dataset needs to be checked for an imbalanced issue, where the majority class dominates the minority class for the classification result.

To overcome this issue, appropriate resampling techniques, such as undersampling and oversampling can be applied to balance the dataset. Next, the dataset is split into the training and testing phase to validate the result. The training set is given as an input to the classifier, classifying the normal and malicious UAVs. Further, it also classifies the authenticate controller using network parameters such as protocol, port numbers, IP addresses, MAC address, and timestamps. It is difficult to decide which classifier need to be used for this problem, as each classifier has its pros and cons. To resolve this ambiguity, we consider modeling all classifiers into one classifier. To select the best classifier model, we rely on the Matthews correlation coefficient (MCC) value as a performance metric. Hence, the high MCC value classifier discard the malicious UAVs (0) from the further communication and let normal UAVs (1) send their reconnaissance data to the blockchain layer.

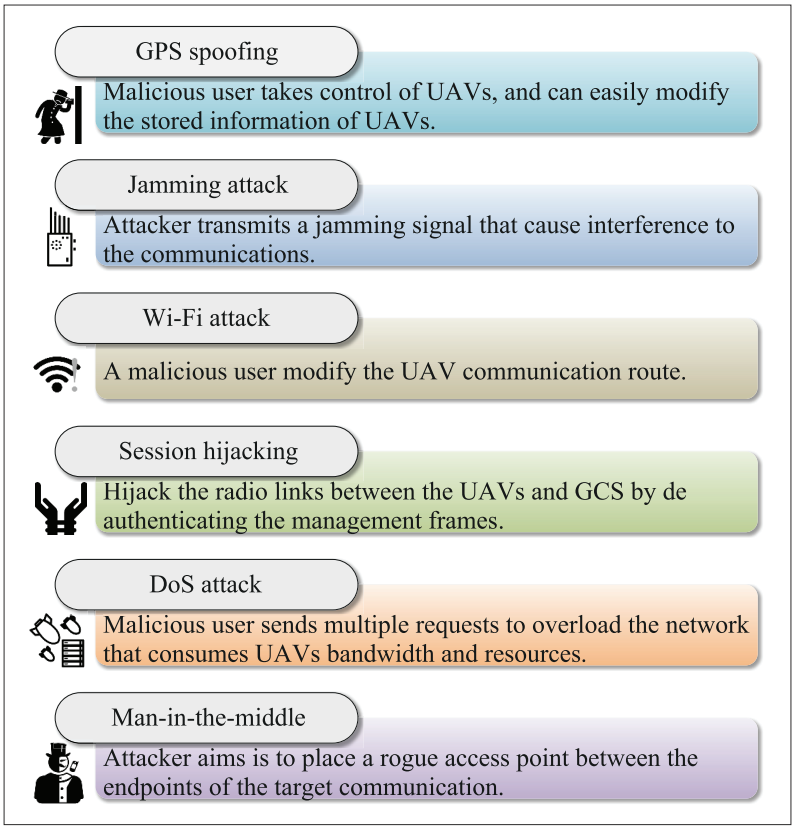

Figure 1. Vital threats to information security and malicious attacks on UAVs.

Blockchain Layer

A blockchain has a digital ledger that is decentralized, distributed, and unchangeable throughout a transaction. This layer represents a secure storage layer for the authentic UAV to store its reconnaissance data in the secure blockchain. We have considered a public blockchain, that is, Ethereum, to store the reconnaissance data from the UAVs in this layer. In any military operation, the reconnaissance data is mission-critical that requires to be secure from the attackers. Therefore, blockchain stores this data in a chain of immutable blocks and employs cryptography aided with public-private key pairs. Next, the data is passed through the smart contract, abolishing the need for third-party systems to conserve the trust between blockchain entities. They are simple programs written in solidity or python programming language on the blockchain, which executes when some predetermined conditions are met. Additionally, it is provisioned to design real-life decentralized solutions efficiently for various applications such as banking, insurance, gaming, real-estate and military operation. However, storing reconnaissance data in Ethereum block costs approximately 530 for 1MB of data, which is remarkably high. Therefore, the proposed architecture has adopted the interplanetary file system (IPFS), which has the same characteristic as

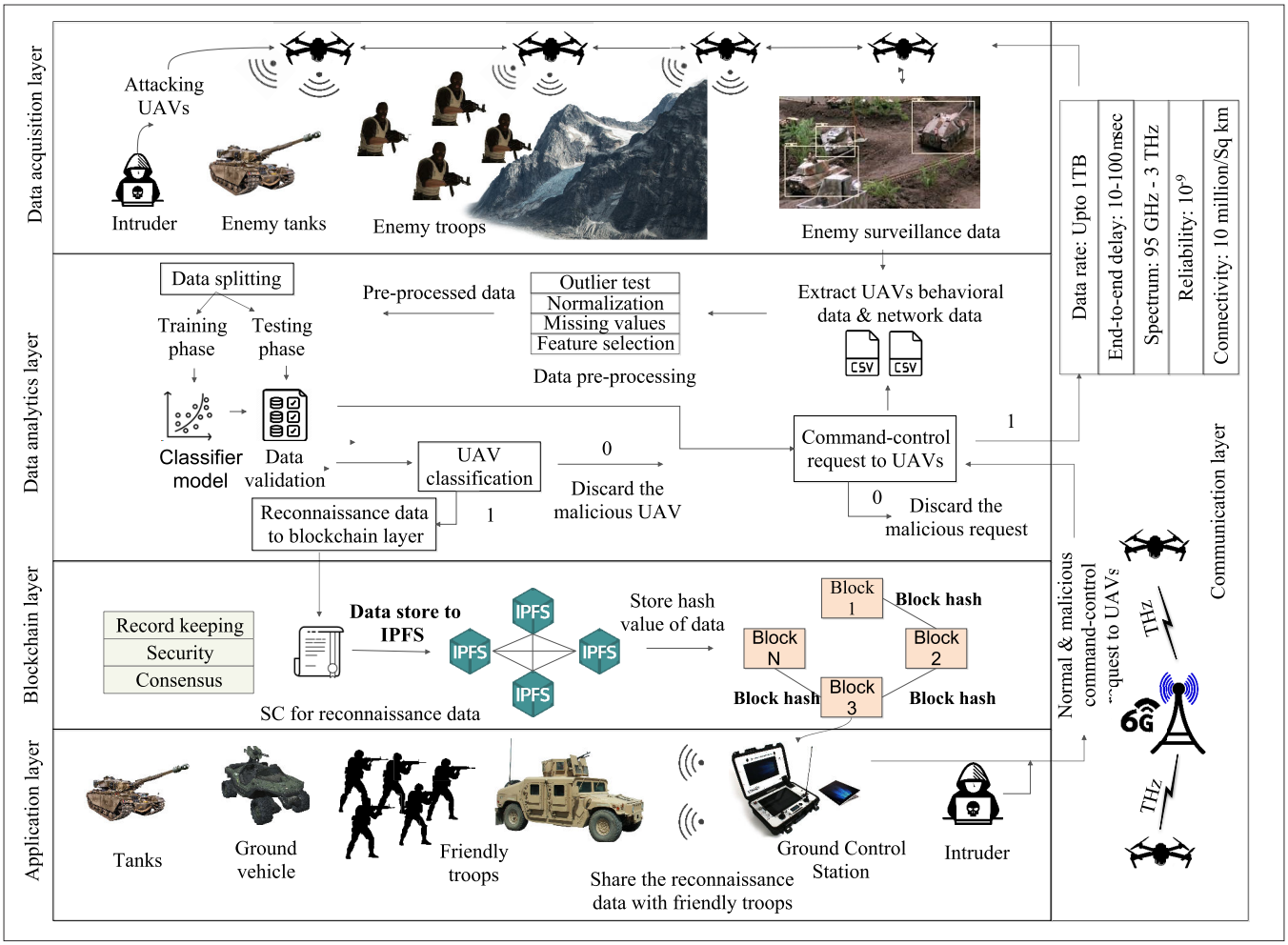

FIGURE 2. *Block-USB:* The proposed architecture for blockchain and AI-based secure UAV communication scheme for military operation.

Ethereum but is free of cost. It produces unique hash values (<<< 1MB) and stores them in the blockchain block. At regular intervals, the reconnaissance data from the Ethereum block is shared with the GCS, which is further shared with the friendly troops.

Application Layer

This layer commences the communication with UAVs for command and control purposes via the 6G interface. It mainly comprises military entities, such as friendly military troops, artillery, ground vehicles, and GCS, which control UAVs for data acquisition from the enemy zone. The collected data could be in the form of intelligence, reconnaissance, and surveillance of the enemies, which helps the friendly troops to get alerted and secure their premises. Additionally, this layer may consist of malicious intruders that can perform data tampering attacks to misguide the application layer. Therefore, prior to any communication between UAVs and the application layer, the communication is examined at the data analytics layer to classify a normal and malicious communication via the ML classifier.

Research Challenges

This section presents some of the significant concerns and research challenges while tackling the security aspects of UAV-assisted military operations. A description of each is as follows.

Security in Cluster UAVs: The security will be complex when there is a cluster of UAVs sharing reconnaissance data on the fly. A few rogue UAVs might be trying to acquire this data from normal UAVs in such a cluster. It is challenging to implement any detection system on UAVs as they are energy and memory constrained. Hence, there are plenty of attacks possible between UAVs on the fly.

Delay in Information Communication: When the communication is weak due to distorted channels and the distance between UAVs and friendly troops is larger, the reconnaissance data to arrive at friendly troops gets delayed. This makes lethal engagement easier for enemies as friendly troops are not aware of the current situation of enemies.

Vulnerability Assessment: Identification of known and unknown vulnerabilities in UAVs becomes important for military operations. Otherwise, the attacker can easily target the vulnerability to take control over the UAV.

Adversarial Attack on Dataset: In a UAV-based military operation, UAVs' behavior and network dataset are essential to analyze its effect in the battlefield. The validated data can assist friendly troops in winning the battle. However, an adversarial attack can flip this winning condition

by adding deceptive input into the machine learning models. Hence, there is a need to secure the dataset along with anomalies and UAV detection.

Physical Layer Attack: UAVs in battlefield are energy-constrained devices and are used to collect intelligence data. This makes it easy for an attacker to perform physical layer attacks, such as eavesdropping, hijacking, and jamming. This becomes an open challenge for researchers.

Secure UAV-assisted Military Operation : A Case Study

UAVs can assist friendly troops in any combat operation, where a personnel's life is at risk by providing intelligence data to win the battle. However, UAV-assisted battlefield have been leveraged by various security attacks. Consequently, there is a need for a secure architecture represented in Fig. 2, which can securely send the reconnaissance data to the friendly troops. This architecture is examined with two attack scenarios, which are as follows:

Scenario 1

In this scenario, multiple UAVs are waiting for a command from the application layer, which has GCS and friendly troops along with the intruders. We assume that the intruder disguised himself as an enemy spy, hacktivist, or state-sponsored attacker trying to win the battle from the enemy side. It can perform passive or active attacks on the UAVs for data manipulation. In passive attacks (such as sniffing, snooping, and man-in-the-middle attack), the attacker can silently listen to the conversation between a UAV and the controller. Further, it can inject manipulated commands, such as turning off any specific sensor and updating the latitude and longitude by hijacking the session. If the attack is active, an attacker can explicitly attack the UAVs, modifying or destroying the reconnaissance data collected by the UAVs in the acquisition layer. The ML classifier in Fig. 3 validates the authenticate controller to overcome this problem, allowing it to communicate with the UAVs for command and control purposes.

Scenario 2

This scenario has multiple UAVs along with malicious UAVs from the enemy side. Each malicious UAV behaves like a normal UAV and tries to perform an impersonation attack. In this attack, when a malicious UAV communicate with the controller, which thinks it is normal and provides them with the command and control request along with the current situation of the battlefield. This way, the malicious UAV wins the trust of the controller, and alongside, it passively collects the reconnaissance data from the friendly side and sends it to the enemy side controller. From the perspective of ML, such malicious UAVs are anomalies and are required to uncover them using anomaly detection. One way to find them is by verifying their behavioral data; this is because all normal UAVs behave according to the command and control request. However, the anomaly UAV resist this request; for example, they fly at different latitudes and longitudes compared to normal UAVs as they have to collect reconnaissance data from the friendly side. Moreover, they can

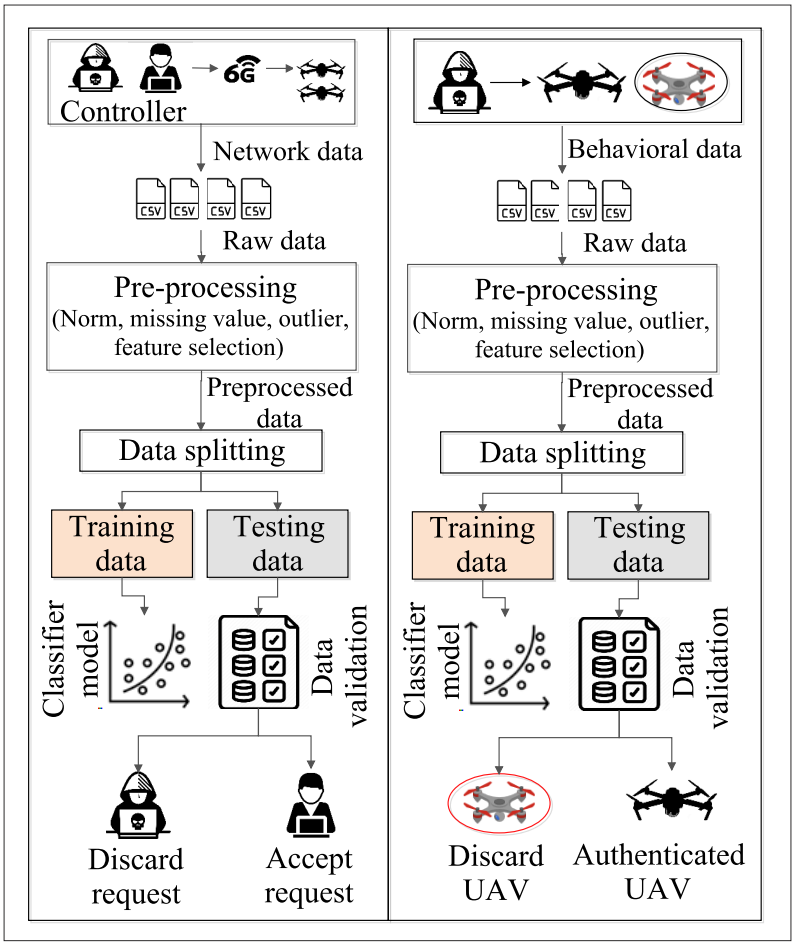

Figure 3. Secure UAV communication scenario using ML to tackle intrusion attacks in military operations.

be compromised by observing their communication data as they have previously contacted and shared reconnaissance data with the enemies. Outlier detection assisted with ML can discover such rogue UAVs as their behavior is distinct from the normal UAVs.

Performance Evaluation

This subsection illustrates the performance of the proposed blockchain-based UAV communication in military operations. Figure 4 shows the performance evaluation of the proposed architecture based on the different scenarios and with conventional approaches in terms of classifier accuracy, scalability, and latency. Figure 5 shows the comparison of data processing complexity, that is, the time taken to process each data packet by [10] and the proposed framework. From the graph, it is clear that the proposed framework has lower complexity (at 8th data packet, processing time = 55.2 ms) than [10] because of the incorporation of AI algorithms, which bifurcates malicious and non-malicious UAVs. The proposed framework has to only process the data of non-malicious UAVs; contrary, the [10] has to process both malicious and non-malicious data because they have not utilized the benefits of AI in their work; therefore, they have high complexity in their work (at 8th data packet, processing time = 64.7 ms). Figure 4a shows the comparison of classification accuracies of various ML algorithms,

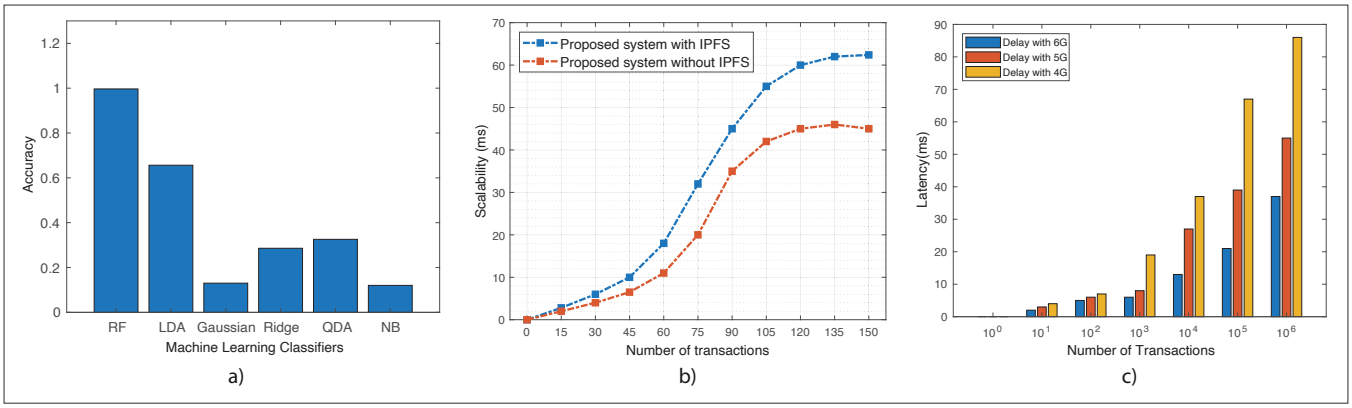

FIGURE 4. Performance comparison of the proposed system with different performance metrics: a) classification accuracy; b) scalability comparison; c) latency comparison.

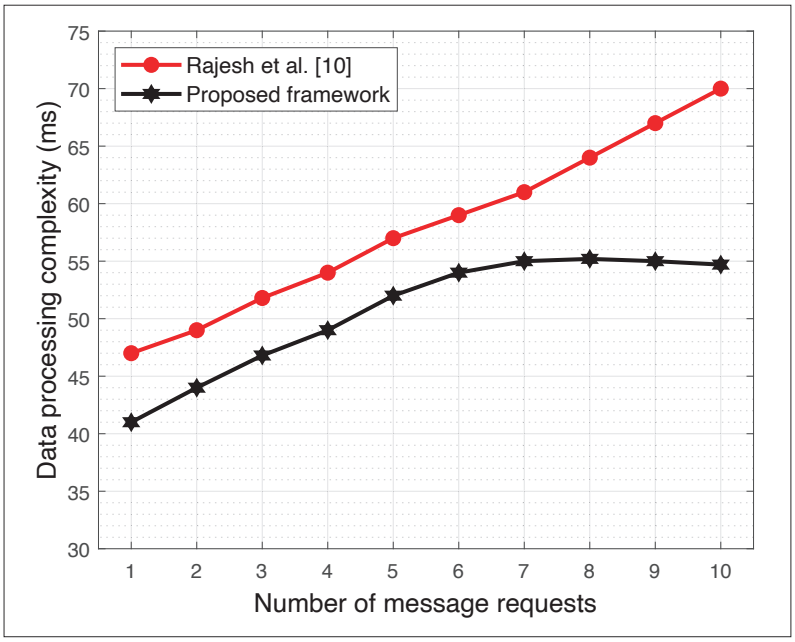

FIGURE 5. Data processing complexity comparison between [10] and the proposed framework.

such as random forest, linear discriminant analysis, naive Bayes, and ridge classifiers. Due to the efficient decision-making capabilities, the RF algorithm outperforms, compared to the other classifiers. Figure 4b shows the scalability comparison of the proposed framework with the conventional schemes. The proposed scheme performs better with increasing transactions between controllers and UAVs over the blockchain network. This is because of the integration of IPFS and 6G networks. Figure 4c reveals the comparison of latency and number of transactions for the proposed framework. The comparison describes that as the number of transactions increases, the latency of the 6G enabled proposed system gets reduced than 5G and 4G systems.

Conclusion

In this article, we introduced an architecture for blockchain and AI-based secure UAV communication based on a 6G network for military operations, that is, Block-USB. First, we discussed various challenges associated with military operations, such as risking human life, information delay, ineffective communication, and lack of a guidance system. To overcome these issues, UAV-based military operations were deployed on a 6G network that allows UAVs to communicate and share reconnaissance data with the GCS quickly. Then, this data is analyzed for security and privacy purposes using ML classifiers, restricting intruders trying to infiltrate military communication. Further, an IPFS storage protocol is integrated with the proposed system to store and access reconnaissance data securely. Finally, for the proposed architecture, various research challenges in terms of security are discussed. In the future, we will investigate zero-day attacks on the proposed system along with other performance metrics of a 6G network, such as throughput and packet loss ratio against the number of users.

References

[1] M. Mozaffari *et al.*, "A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems," *IEEE Commun. Surveys Tutorials*, vol. 21, no. 3, 2019, pp. 2334–60.

[2] Y. Ko *et al.*, "Drone Secure Communication Protocol for Future Sensitive Applications in Military Zone," *Sensors*, vol. 21, no. 6, 2021.

[3] A. Kumari *et al.*, "A Taxonomy of Blockchain-Enabled Softwarization for Secure UAV Network," *Computer Commun.*, vol. 161, 2020, pp. 304–23.

[4] J.-P. Yaacoub *et al.*, "Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations," *Internet of Things*, vol. 11, 2020, p. 100218.

[5] G. Choudhary *et al.*, "Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey," *Proc. 2018 14th Int'l. Wireless Commun. Mobile Computing Conf.*, 2018, pp. 560–65.

[6] R. Shrestha *et al.*, "Machine-Learning-Enabled Intrusion Detection System for Cellular Connected UAV Networks," *Electronics*, vol. 10, no. 13, 2021.

[7] U. Challita *et al.*, "Machine Learning for Wireless Connectivity and Security of Cellular-Connected UAVs," *IEEE Wireless Commun.*, vol. 26, no. 1, 2019, pp. 28–35.

[8] A. Sharma et al., "Communication and Networking Technologies for UAVs: A Survey," *J. Network and Computer Applications*, vol. 168, 2020, p. 102739.

[9] P. Zhang *et al.*, "BC-EdgeFL: Defensive Transmission Model Based on Blockchain Assisted Reinforced Federated Learning in IIoT Environment," *IEEE Trans. Industrial Informatics*, vol. PP, no. 09, 2021, pp. 1–1.

[10] R. Gupta, S. Tanwar, and N. Kumar, "B-IoMV: Blockchain-Based Onion Routing Protocol for D2D Communication in an IoMV Environment Beyond 5G," *Vehicular Commun.*, 2021, p. 100401.

[11] M. Golam, J.-M. Lee, and D.-S. Kim, "A UAV-Assisted Blockchain Based Secure Device-to-Device Communication in Internet of Military Things," *Proc. 2020 Int'l. Conf. Information and Commun. Technology Convergence*, 2020, pp. 1896–98.

[12] R. Kakkar *et al.*, "Coalition Game and Blockchain-Based

Optimal Data Pricing Scheme for Ride Sharing Beyond 5G," *IEEE Systems J.*, 2021, pp. 1–10.
[13] R. Iqbal, T. Maniak, and C. Karyotis, "Intelligent Remote Monitoring of Parking Spaces Using Licensed and Unlicensed Wireless Technologies," *IEEE Network*, vol. 33, no. 4, 2019, pp. 23–29.
[14] A. Mukherjee *et al.*, "Resource-Optimized Multiarmed Bandit-Based Offload Path Selection in Edge UAV Swarms," *IEEE Internet of Things J.*, vol. 6, no. 3, 2019, pp. 4889–96.
[15] Z.-X. Xu, "UAV Traffic Dataset for Learning based UAV detection," 2022.

Biographies

Nilesh Kumar Jadav is a full-time Ph.D. Research Scholar in the Computer Science and Engineering Department, at Nirma University, Ahmedabad, India, supervised by Sudeep Tanwar. His research interest includes artificial intelligence in IoT applications and network security.

Tejal Rathod is a full-time Ph.D. Research Scholar at the Department of CSE, Institute of Technology, Nirma University, Ahmedabad, India, under the supervision of Sudeep Tanwar. Her area of interest includes big data analytics and modeling artificial intelligence for wireless network applications.

Rajesh Gupta is working as an Assistant Professor in the Department of CSE, Nirma University. His research interests include blockchain technology and device-to-device communication.

Sudeep Tanwar is working as a Professor at Nirma University, India. He received his Ph.D. in Computer Science and Engineering from Mewar University, India. His research interests includes WSN, blockchain technology, fog computing, and smart grid. He has authored 442+ research articles and 31 books. He is an Associate Editor of IJCS, COMCOM, CSA, and Security and Privacy Journal.

Neeraj Kumar is working as a Professor at Thapar Institute of Engineering and Technology, Deemed to be University, India. He received his Ph.D. from SMVD University, India in CSE and was a postdoctoral research fellow at Coventry University, United Kingdom. He is an Associate Editor/Technical Editor of IEEE Communication Magazine, IEEE Networks Magazine, IJCS-Wiley, JNCA-Elsevier, ComCom-Elsevier, Security and Privacy, Wiley.

Rahat Iqbal is a senior academic, director, inventor, and consultant with 20 years experience in industrial and academic roles. He currently is working at the University of Dubai. Dr Iqbal has supervised to completion 20 Ph.D. students, and examined 17 doctorate theses. He has published more than 150 papers in international journals, conferences and books.

Shadi Atalla is an Associate Professor in Computing and Information Systems of the IT academic department at the College of Engineering and IT, University of Dubai. He is a data science evangelist and certified big data trainer. Dr Attalla has published several papers in international scientific journals and international conferences, and is the chair of computer society of IEEE UAE during 2018-2022.

Mohammad Hijji is currently the Vice Dean for Development and Quality, Faculty of Computers and Information Technology (FCIT) at University of Tabuk, Saudi Arabia. Prior to this, he was the chairman of Computer Science Department at FCIT, University of Tabuk, Saudi Arabia, from 2020 to 2022. His research interests include AI, cyber security, Internet of Things (IoT), smart city, energy optimization, and disaster and emergency management.

Saba Al-Rubaye is Head of Advanced Connectivity & System Integration research group in the School of Aerospace, Transport and Manufacturing at Cranfield University. Dr Rubaye is participating in developing industry standards by being an active research group member of IEEE P1932.1 standard of License/unlicensed Interoperability and IEEE P1920.2, Standard for Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems

Cranfield University

CERES https://dspace.lib.cranfield.ac.uk

School of Aerospace, Transport and Manufacturing (SATM) Staff publications (SATM)

2023-09-30

Blockchain-based secure and intelligent data dissemination framework for UAVs in battlefield applications

Jadav, Nilesh Kumar

IEEE

Jadav NK, Rathod T, Gupta R, et al., (2023) Blockchain-based secure and intelligent data dissemination framework for UAVs in battlefield applications. IEEE Communications Standards Magazine, Volume 7, Issue 3, September 2023, pp. 16-23

https://doi.org/10.1109/MCOMSTD.0005.2200052

Downloaded from Cranfield Library Services E-Repository