PAPER DETAILS

TITLE: Blockchain-Based Data Security in Military Autonomous Systems

AUTHORS: Pelin ANGIN

PAGES: 362-368

ORIGINAL PDF URL: https://dergipark.org.tr/tr/download/article-file/1390795

Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı, S. 362-368, Kasım 2020
© Telif hakkı EJOSAT'a aittir
Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue, pp. 362-368, November 2020
Copyright © 2020 EJOSAT
Research Article

Blockchain-Based Data Security in Military Autonomous Systems

Pelin Angin[1*]

[1] Middle East Technical University, Faculty of Engineering, Department of Computer Engineering, Ankara, Turkey (ORCID: 0000-0002-6419-2043)

(International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) 2020 – 22-24 October 2020)

(**DOI:** 10.31590/ejosat.824196)

ATIF/REFERENCE: Angin, P. (2020). Blockchain-based Data Security in Military Autonomous Systems. *European Journal of Science and Technology*, (Special Issue), 362-368.

Abstract

Advances in technology have enabled the increased use of autonomous systems such as unmanned aerial vehicles (UAVs) in military operations and other critical military communications. While the use of autonomous systems has greatly facilitated military operations, provided a global view of the operational environment and eased sensitive data collection, making possible reduced casualties, it has also created a greater cyber attack surface due to its high level of automation. The existence of adversaries targeting this attack surface can seriously damage military operations by tampering with critical message content used in autonomous systems decision making. In order to ensure the successful operation of autonomous military systems, mechanisms must be developed to strictly protect the integrity of the collected / exchanged data and messages, and an immutable record of each message must be provided. These mechanisms should also be used to control autonomous systems under critical failures or attacks occurring during or after military operations. Blockchain has recently emerged as a technology that provides a decentralized architecture to achieve an unchangeable history of interactions between parties that are part of a distributed network. While blockchain is currently used in various fields such as cryptocurrencies, supply chain management and e-voting systems, it also has the potential to provide secure communication in autonomous systems. In this study, a blockchain-based communication architecture is proposed that guarantees integrity assurance and permanent recording of messages exchanged between all parties, including UAVs and ground control stations, in a military autonomous system network. The proposed secure communication architecture has been theoretically evaluated in terms of its resistance to the types of cyber attacks frequently encountered in distributed systems, and it has been shown to provide protection against attacks that compromise data integrity as well as spoofed authentication attempts. The proposed blockchain-based architecture is promising to increase the resilience of military autonomous systems against cyberattacks that aim to hurt the success of military operations through data content manipulation.

Keywords: Blockchain, unmanned aerial vehicles, military autonomous systems, security.

Askeri Otonom Sistemlerde Blokzincir Tabanlı Veri Güvenliği

Öz

Yakın dönemde teknolojide yaşanan gelişmeler, askeri operasyonlarda ve diğer kritik askeri iletişimlerde insansız hava araçları (İHA'lar ve SİHA'lar) gibi otonom sistemlerin artan kullanımına olanak sağlamıştır. Otonom sistemlerin kullanımı askeri operasyonları büyük ölçüde kolaylaştırmış, hassas veri toplama ve operasyon ortamına küresel bir bakış sağlamış ve kayıpları azaltmış olsa da, içerdiği yüksek otomasyon seviyesi nedeniyle daha büyük bir siber saldırı yüzeyi yaratmıştır. Bu saldırı yüzeyinin düşmanlar tarafından kullanılması, otonom sistemlerin karar vermesinde kullanılan kritik mesaj içeriğinin manipüle edilmesi yoluyla askeri operasyonlara ciddi şekilde zarar verebilir. Otonom askeri sistemlerin başarılı bir şekilde çalışmasını sağlamak için, toplanan / değiş tokuş edilen veri ve mesajların bütünlüğünü sıkı bir şekilde koruyacak mekanizmaların geliştirilmesi ve her mesajın değişmez bir kaydının sağlanması gerekir. Bu mekanizmalar ayrıca askeri operasyon sırasında veya sonrasında meydana gelen kritik arızalar veya saldırılar altında otonom sistemleri denetlemek için de kullanılabilir olmalıdır. Blokzincir, dağıtık bir ağın parçası olan taraflar arasında değiştirilemez bir etkileşim geçmişi elde etmek için merkezi olmayan bir mimari sağlayan bir teknoloji olarak yakın zamanda ortaya çıkmıştır. Blokzincir şu anda kriptoparalar, tedarik zinciri yönetimi ve e-oylama sistemleri gibi çeşitli alanlarda kullanılırken, aynı zamanda otonom sistemlerde güvenli iletişim sağlama potansiyeline de sahiptir. Bu çalışmada, bir askeri otonom sistem ağındaki İHA'lar ve yer kontrol istasyonları dahil tüm taraflar arasında değiş tokuş edilen mesajların bütünlük güvencesini ve kalıcı bir kaydını garanti eden blokzincir

[*] Corresponding author: Middle East Technical University, Faculty of Engineering, Department of Computer Engineering, Ankara, Turkey (ORCID: 0000-0002-6419-2043), pangin@ceng.metu.edu.tr

tabanlı bir iletişim mimarisi önerilmiştir. Önerilen güvenli iletişim mimarisi dağıtık sistemlerde sıklıkla rastlanılan siber saldırı türlerine dayanıklılığı açısından incelenmiş, veri bütünlüğünü bozma ve kimlik denetimini yanıltma saldırılarına karşı koruma sağladığı gösterilmiştir. Blokzincir tabanlı bu mimari, askeri ortamlarda son derece güvenilir iletişimi sağlama ve bu sistemleri veri içeriği manipülasyonu yoluyla yanıltmayı amaçlayan siber saldırılara karşı direnç artırmayı vaat etmektedir.

Anahtar Kelimeler: Blokzincir, insansız hava araçları, askeri otonom sistemler, güvenlik.

1. Introduction

The use of autonomous systems such as unmanned aerial vehicles (UAVs) in military settings has become exceedingly commonplace in the past decade due to the advantages they provide, including reduced casualties, an enhanced and comprehensive mapping of the field of operation and fast decision-making capabilities they provide. Common scenarios include swarms of unmanned combat aerial vehicles sent out for missions to dangerous territories, where human life should not be risked, UAVs for reconnaissance missions and military aid delivery among many others. In such settings, the nodes in the autonomous system network almost always need to communicate with the other nodes to take collective actions based on the data they gather using their various sensors. Such decisions can include coordinating routes to be taken to prevent collisions or actions to be taken by drones based on environment conditions, analysis of captured video etc. It is important to rely on data validated by multiple autonomous systems in such critical missions, as making mistakes due to malfunctioning or misguided decisions of some of the nodes in the network could have grave consequences.

While military autonomous systems provide the abovementioned advantages, they suffer from an enlarged cyberattack surface that could be exploited by adversaries to alter the decisions made by these systems, which could seriously damage mission-critical operations. The integrity and accuracy of the data collected by military autonomous systems is of utmost importance due to their effects on the success of the decisions taken by networks of these systems. It is also important to record an immutable history of these decisions and the actions taken by the nodes in autonomous system networks in order to effectively trace back faults that occur in these systems and attribute them to particular nodes, which helps solve the issues swiftly to provide high fault tolerance and protect these systems against attacks by adversaries.

The blockchain technology became an increasingly popular solution in the past few years (Bahtiyar et al., 2020) for providing decentralized trust and security in many digital systems after its success with Bitcoin (Nakamoto, 2008). As blockchain removes the requirement for a trusted third party in a transaction system, it has been applied in domains such as access management (Di Pietro et al., 2018), digital content distribution (Kishigami et al., 2015), supply chain management (Hofmann & Johnson, 2016), smart contracts in the Internet of Things (IoT) domain (Christidis & Devetsikiotis, 2016), distribution and verification of sensitive business documents (Aitzhan & Svetinovic, 2016), enhancing privacy in healthcare (Yue et al., 2016; Aydar & Çetin, 2020), firmware update of embedded devices (Lee & Jong-Hyouk, 2016) and many more.

Although blockchain has been used in many fields ranging from supply chain management to cryptocurrencies and electronic voting, its use in the military communications domain has been quite limited so far. Sudhan & Nene (2017) proposed using blockchain for providing integrity and provenance of data shared in military operations. Tosh et al. (2018) proposed a blockchain-based platform for Internet-of-Battlefield Things (IoBT) to handle trust, security, and privacy challenges that arise in battlefield data exchanges. Wrona & Jarosz (2019) proposed an architecture for secure metadata binding in military IoT using blockchain technologies compliant with STANAG 4774 and 4778. Jensen et al. (2019) proposed the application of blockchain technologies to provide security against threats for the UAV swarm environment, however details regarding group communication in the autonomous system network were not provided.

In this work, we propose a blockchain-based approach for ensuring the integrity of messages exchanged between the nodes in a military autonomous system network by creating a permissioned blockchain. The design of the blockchain considers the aspects of device authentication, privacy-preserving communication and verification of messages before they are used for making decisions by the nodes in the network and are committed to the blockchain. We study common attacks in military autonomous system communications and evaluate the security of the proposed solution against the identified threats. As opposed to previous work, the approach we propose in this paper is a more generalized secure communications architecture for military autonomous systems, applicable to different scenarios and types of nodes in the network.

2. Material and Method

2.1. Blockchain Overview

A blockchain is a distributed ledger that a group of networked independent parties maintain. It provides an immutable record of data in a peer-to-peer (P2P) network, where nodes validate all transactions against the ledger, using the cryptographic hash of each data block in the chain, which provides a link to the previous block (Angin et al., 2018). For each new transaction, the transaction message is broadcast to the whole network and a distributed consensus algorithm is run by special participants of the network, the validators, to include the message in the ledger (Laurence, 2017). Eventually a consistent copy of the ledger is attained by the whole network, enabling transaction transparency. One of most important features of blockchain for providing security at scale is that it does not rely on trust in network nodes, and no central trusted authority is involved. The security of blockchain relies purely on cryptography and distributed consensus in the network (Angin et al., 2018).

Among important properties of blockchain, which make it an important tool for security and trust in complex and unknown operation environments are the following:

- The distributed ledger in blockchain is a list of records that continuously grows and provides a history of all interactions/transactions that were ever committed to the ledger in its lifetime. This provides the chance to track the history of transactions, and because the ledger is maintained by a large number of nodes, protection against data loss is provided. In the event of failure of one node, which is common in environments like military settings, the data in the ledger can be easily recovered from the other participant nodes. Through this property, the ledger can serve like the black box in an airplane, recording everything that happened during the operation of the network, which will be available for investigation later as well.
- A high-level structure of *chaining* of blocks using cryptographic hashes in blockchain is shown in Figure 1. Here each block contains a block identifier, a timestamp declaring when the block was formed, a cryptographic hash value calculated based on the contents of the block, the cryptographic hash value of the block whose index immediately precedes this block and the data items in the block. The chaining of transaction blocks using cryptographic hashes of previous blocks makes it computationally very hard to change anything in the history the ledger. This property protects the ledger from malicious tampering, which is significant in safety-critical environments such as military operations by autonomous systems.
- The security of the network does not strongly rely on trustworthiness of individual nodes. Transactions are committed to the ledger based on consensus, going through the validation by multiple nodes in the network. Depending upon the consensus algorithm used, as discussed in the subsection below, the network is able to tolerate failures or adversarial actions of some of the nodes and still function correctly. This provides a high degree of integrity assurance for all data recorded in the ledger.

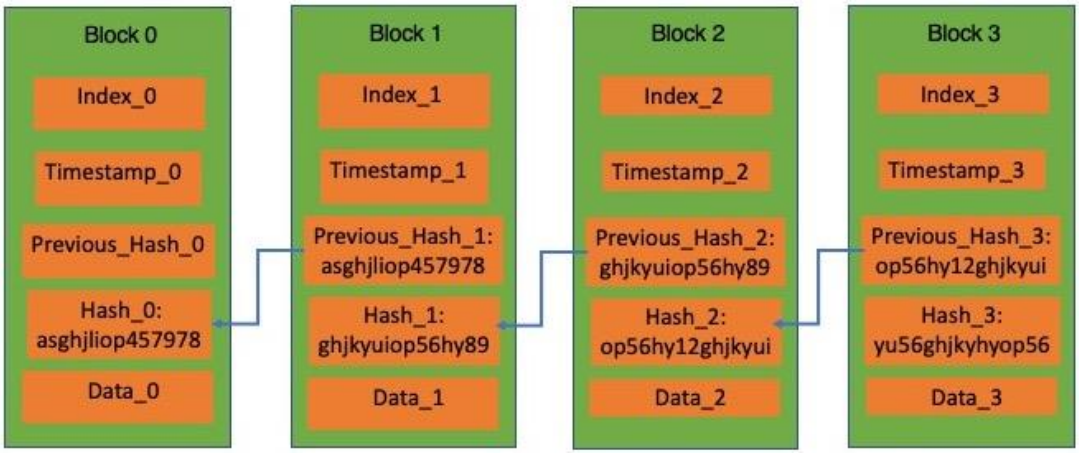

Figure 1. Blockchain structure

2.1.1. Distributed Consensus in Blockchain

Central to the security provided by blockchain are distributed consensus algorithms, especially in highly complex and unknown environments, where it is difficult to trust all nodes participating in a network. As decisions regarding the transactions to include in the distributed ledger are made collectively by the participant nodes, how the decision is taken, especially in safety-critical systems with possibly malfunctioning or adversarial nodes, is vital for the correctness of the operation of the system.

The blockchain literature includes many consensus algorithms that have been designed for different purposes, taking into consideration various parameters like membership methods, network size, real time requirements, fairness etc. The computation-heavy proof of work (PoW) was the preferred consensus method in the early days of blockchain, due to networks consisting of completely unknown, public participants, who could not be trusted. With the evolution of blockchain structures allowing for permissioned and private networks with finer-grain access control, more lightweight consensus mechanisms were designed. In the context of a military setting, where collective actions need to be taken and some of the nodes might be unreliable due to operational failures or being captured by adversaries, utilization of a fault-tolerant consensus mechanism is of utmost importance. One such algorithm that was originally designed to solve the famous Byzantine Generals Problem in the distributed systems literature is Practical Byzantine Fault Tolerance (PBFT) (Castro & Liskov, 1999). PBFT provides the ability to reach correct distributed consensus in an environment where there are 3F+1 nodes and at most F nodes among those are unreliable.

Istanbul Byzantine Fault Tolerance (Moniz, 2017) on the other hand, is an adaptation of PBFT for blockchain. Figure 2 below demonstrates how IBFT works using a state diagram.

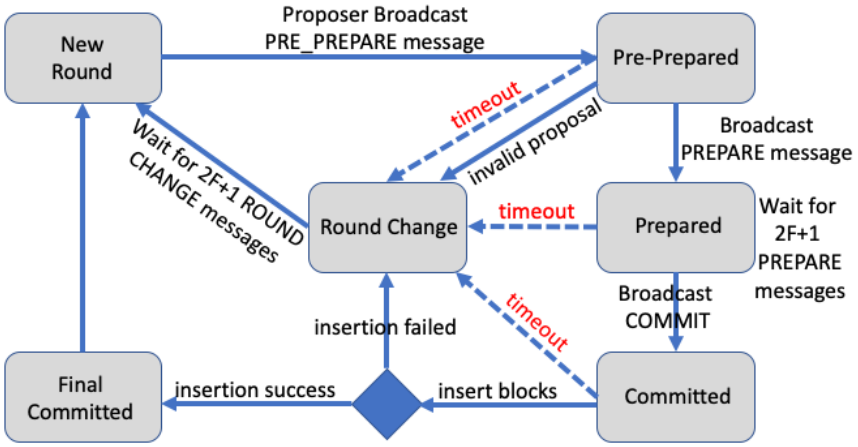

Figure 2. State diagram of Istanbul Byzantine Fault Tolerance (re-created from (Moniz, 2017))

The algorithm basically executes the following processes through its runtime:

- **Validator selection:** A validator called "the proposer" is chosen in a round-robin fashion from among all possible validator nodes in the network.
- **New block proposal:** The selected validator proposes a new block to the other nodes with a PRE-PREPARE message.
- **Validator checks:** Each validator receiving the message and validating the block broadcasts a PREPARE message, which has the purpose of making sure all validators are processing the same block and are on the same round. In this state, each validator waits until they receive 2F+1 PREPARE messages, at which point they are ready to commit the block.
- **Commit phase:** In the COMMIT phase, each validator informs others that it is ready to integrate the block into its copy of the ledger. After receiving 2F+1 COMMIT messages, each validator commits the transaction into the ledger.

2.2. Proposed Approach

Our proposed approach provides secure, integrity-preserving communication between the nodes in an autonomous military network by integrating the messages sent by each node into the distributed ledger maintained by the nodes collectively. Note that as opposed to a public blockchain, where nodes are allowed to become part of the network without meeting any special conditions, the blockchain network proposed in this work is a permissioned network, where nodes need special approval before they can be included in the network and each may have different roles. Due to the closely controlled membership in the permissioned network, a computationally expensive consensus mechanism such as proof-of-work (PoW) as in Bitcoin (Nakamoto, 2008) is not needed. The particular consensus mechanism we propose to use in this work is Istanbul Byzantine Fault Tolerance (IBFT) as described above, which ensures that as long as less than one-third of the nodes in the network are faulty or malicious, correct consensus will be reached. For achieving the privacy of message communication, a group key is established using any secure group key management protocol such as in the work of Fernandes & Duarte (2011), which handles processes like group membership changes and key revocations.

Let

G: Group key established between the nodes in the military autonomous system network

$a(X)$: Public key of UAV_X

$p(X)$: Private key of UAV_X

$E_G(M)$: Symmetric encryption of data item M using secret key G

$D_G(C)$: Symmetric decryption of ciphertext C using secret key G

$f(p, t)$: Digital signature on transaction t, signed using private key p

$v(t, s, a)$: Validation of signature s on transaction t using signer's public key a

ID_X: Idenfiying information for UAV_X

The communication of a single data item M in the system (e.g. a thermal reading, LIDAR data, hyperspectral image data etc.) works as follows:

1. The sender node UAV_X prepares the ciphertext and appends identifying information in the established transaction format:

   $C = E_G(M)$

$t = C \parallel ID_X$ (where $\parallel$ is the concatenation symbol)

2. *UAV_X* signs the transaction:

$Sig = f(p(X), t)$

$Msg = (t, Sig)$

Msg is disseminated in the network by each receiving node using a gossip protocol as seen in Figure 3.

Upon receipt of *Msg*, the following operations are performed by each node in the network:

1. Check = v(t, Sig, a(X))
2. if Check = invalid signature, discard Msg and perform no action
   else go onto Step 3
3. Extract C from t
4. $M' = D_G(C)$
5. If Step 4 fails, stop
   else go onto Step 6
6. Check the content of M' and prepare verification vote to broadcast to the network
7. Run consensus

An overview of the signature verification process for the received data items is demonstrated in Figure 4. During the consensus phase, upon receiving the same vote from at least two-thirds of the network, each node integrates the data item into their copy of the ledger and takes an action based on its content if the item requires them to take any action. To illustrate, let us assume that the data broadcast in the network is the estimated location of a specific target and the action to be taken based on consensus in the network is to fly to that location if the current position of a UAV is within a certain threshold of the target. The location estimate will be broadcast by one of the nodes in a transaction message and verified by others in the blockchain network. If it is not approved by a sufficient number of nodes in the network based on the consensus algorithm, the target location will not become part of the distributed ledger and no action will taken by the nodes in the network based on this piece of information. This verification process protects the network from being misguided by adversaries trying to attract other nodes with decoys or malfunctioning nodes creating incorrect data. The formation of transaction blocks and block chaining with the cryptographic hash of each block is handled by the specific blockchain platform of choice.

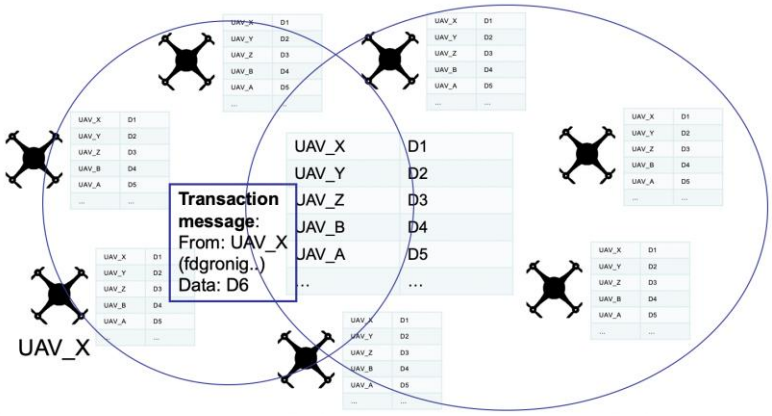

Figure 3. Transaction broadcast in military autonomous system blockchain

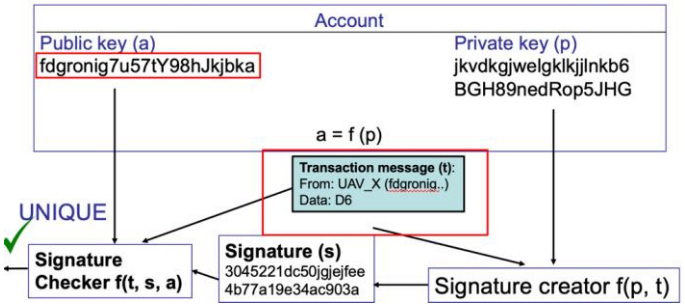

Figure 4. Military autonomous system node signature verification

3. Results and Discussion

In this section, we provide a security evaluation of the proposed approach against common possible attacks on and failures in military autonomous systems. Table 1 summarizes the security properties provided by the blockchain-based military autonomous system communications approach and the mechanisms within the solution, which provide each security property.

3.1. Attacks against Data Integrity

Messages in military autonomous networks could face many attacks on their integrity to disrupt operations, and message integrity could also be breached due to bit errors in communication.

Let an adversary replace the content of message *Msg=(t,Sig)* broadcast by UAV_X with *Msg2=(t2,Sig)*, where t≠ t2. When node UAV_Y receives Msg2, v(t2, Sig, a(X)) will fail, as Sig = f(p(X), t). Hence, messages in the network are protected from tampering due to the use of digital signatures on the messages, which would not pass verification by the peer nodes in case of alteration.

Let us further consider the case where the adversary sends *Msg3 = (t3, Sig3),* where t3 = C' || ID_X. When UAV_Y receives Msg3, it will first run v(t3, Sig3, a(X)). This will fail, as the adversary cannot create Sig3 verifiable using a(X), due to not being in possession of p(X). Hence, tampering with either the signature or the message itself will result in the message being discarded by all honest nodes in the network.

Attacks against data integrity can also target historical data on the ledger. Let adversary *E* try to modify data in block B_X of the ledger. This will require updating the hash value of B_X in at least two-thirds of all copies of the ledger in the network. Furthermore, the hash value of B_{X+1} also depends on the hash value of B_X, the hash value of B_{X+2} depends on the hash value of B_{X+1} and so on, until the last block in the ledger. Trying to change any data in B_X will therefore require recalculation of all cryptographic hash values in all blocks starting with B_X. In essence, once the messages become part of the ledger, writing an alternative history would require taking control of more than one-third of the network and performing all cryptographic hash calculations again. Note that it also requires knowledge of the group key due to the encryption of the data during all communication.

3.2. Man-in-the-middle (MITM) Attacks

MITM attacks have the purpose of establishing communication with nodes *A* and *B* at the two ends of a channel, trying to trick them into thinking they are communicating with each other, while in actual fact they are each communicating with an adversary *E*. MITM attacks are common threats against communication scenarios involving sensitive data exchanges, where adversaries try to figure out the contents of private messages exchanged between parties by actively establishing communication channels with them. Such attacks have significant potential to hurt missions by communicating misleading messages to both ends of the communication channel, as well as discovering the actual secret content shared.

Let UAV_E intercept the communication channel between UAV_A and UAV_B and send message Msg=(t, Sig') to UAV_B, where t = C || ID_A. When UAV_B receives this message, it will run v(t, Sig', a(A)), and signature verification will fail, as *E* cannot sign *t* using *A*'s private key, which it is not in possession of. Therefore, the MITM attack will fail.

3.3. Attacks against Message Privacy

Privacy is an important concern especially in military settings, due to the sensitivity of the data exchanged in the network. While adversaries could try to intercept and make sense of messages in the proposed military autonomous systems network, the privacy of the messages is protected from eavesdropping due to their encryption with the group key, which is only available to the permissioned members of the blockchain network. To ensure high privacy, the group key management algorithm needs to be secure and keys should be updated frequently.

3.4. Faulty Sensors

In some cases, sensors of particular nodes may produce incorrect readings due to malfunctioning even if they are not under the control of adversaries. The proposed approach mitigates such situations as well through verification of the message content by all peers in the network. The nodes in the network would be capable of detecting abnormalities in the message communicated and reject using the data/taking action in such cases.

3.5. Non-repudiation

Non-repudiation is an important property in systems where the agent responsible for certain actions needs to be established with certainty. The system provides non-repudiation of the messages shared by each node through digital signatures on each message, as no other node than the node itself can possibly know the private key of that node.

Table 1. Security Properties Provided by the Blockchain-based Military Autonomous System Communications

Security Property	**Mechanism**
Authentication	Public key cryptography- digital signatures
Integrity	Digital signatures and cryptographic hash
Availability	Broadcasting messages to the P2P network
Confidentiality	Encryption with group key
Fault tolerance	Message content verification by nodes

4. Conclusions

In this paper, we proposed a secure military autonomous systems communications architecture based on blockchain. The proposed permissioned blockchain-based approach focuses on the aspects of data integrity, privacy-preserving message communication and immutability of the data communicated in an autonomous military network. The security evaluation of the proposed system architecture demonstrates the effectiveness of the approach for mitigating common attacks on autonomous military systems and shows that it is promising for large-scale adoption in mission-critical military autonomous systems. In future work, we will perform an implementation of the proposed system and perform experiments to evaluate its performance in terms of consensus speed, security capabilities and scalability.

References

Aitzhan, N. Z. & Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, *15 (5),* 840-852.

Angin, P., Mert, M. B., Mete, O., Ramazanli, A., Sarica, K. & Gungoren, B. (2018). A blockchain-based decentralized security architecture for IoT. *International Conference on Internet of Things (ICIOT)*, June 25-30, Seattle, WA, USA, 3-18.

Aydar, M. & Çetin, S. C. (2020). Blokzincir Teknolojisinin Sağlık Bilgi Sistemlerinde Kullanımı. *Avrupa Bilim ve Teknoloji Dergisi*, *(19)*, 533-538.

Bahtiyar, Ş., Paksoy, O., Güldöşüren, E. & Pekel, M. E. (2020). Öğrenciler Arasında Blokzincir Farkındalığı Üzerine Bir Araştırma. *Avrupa Bilim ve Teknoloji Dergisi, (18)*, 424-434.

Castro, M. & Liskov, B. (1999). Practical Byzantine Fault Tolerance. *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, 22-25 February, New Orleans, LA, USA, 173-186.

Christidis, K. & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things, *IEEE Access*, *4,* 2292–2303.

Di Pietro, R., Salleras, X., Signorini, M. & Waisbard, E. (2018). A Blockchain-based Trust System for the Internet of Things. *23nd ACM on Symposium on Access Control Models and Technologies*, 13-15 June, Indianapolis, IN, USA, 77-83.

Fernandes, N. C. & Duarte, O. C. M. B. (2011). A lightweight group-key management protocol for secure ad-hoc-network routing. *Computer Networks, 55 (3),* 759-778.

Hofmann, E. & Johnson, M. (2016). Supply chain finance–some conceptual thoughts reloaded. *International Journal of Physical Distribution & Logistics Management*, *46 (4),* 1–8.

Jensen, I. J., Selvaraj, D. F. & Ranganathan, P. (2019). Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs). *IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, 10-12 June, Washington, DC, USA, 1-7.

Kishigami, J., Fujimura, S., Watanabe, H., Nakadaira, A. & Akutsu, A. (2015). The blockchain-based digital content distribution system. *5th IEEE International Conference on Big Data and Cloud Computing*, 26-28 August, Dalian, China, 187–190.

Laurence, T. (2017). *Blockchain for Dummies*. Hoboken, NJ, USA: For Dummies.

Lee, B. & Jong-Hyouk, L. (2016). Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. *The Journal of Supercomputing*, *73 (3),* 1152–1167.

Moniz, H. (2017). Istanbul Byzantine Fault Tolerance. Available: https://github.com/ethereum/EIPs/issues/650 [Accessed: 10 October 2020].

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: 10 October 2020].

Sudhan, A. & Nene, M. J. (2017). Employability of blockchain technology in defence applications. *International Conference on Intelligent Sustainable Systems (ICISS)*, 7-8 December, Palladam, India, 630-637.

Tosh, D. K., Shetty, S., Foytik, P., Njilla, L. & Kamhoua, C.A. (2018). Blockchain-empowered secure Internet-of-Battlefield Things (IoBT) architecture. *IEEE Military Communications Conference (MILCOM)*, 29-31 October, Los Angeles, CA, USA, 593-598.

Wrona, K. & Jarosz, M. (2019). Use of blockchains for secure binding of metadata in military applications of IoT. *IEEE World Forum on Internet of Things (WF-IoT)*, 15-18 April, Limerick, Ireland, 213-218.

Yue, X., Wang, H., Jin, D., Li, M. & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems, 40 (10),* 218.