

Authentication Framework by Using Lightweight Chaos-Driven Blockchain to Identify Malicious Nodes in WSNs

Maytham S. Jabor^{1*}, and Aqeel Salman Azez²

¹Instituto ITACA, Universitat Politècnica de València, Camino de Vera s/n, Valencia, España.
mayaz@doctor.upv.es, <https://orcid.org/0000-0002-4518-0290>

²Instituto ITACA, Universitat Politècnica de València, Camino de Vera s/n, Valencia, España.
aqaz@doctor.upv.es, <https://orcid.org/0000-0003-0543-4169>

Received: May 19, 2025; Revised: July 01, 2025; Accepted: August 21, 2025; Published: September 30, 2025

Abstract

Due to their decentralized and autonomous nature, Wireless Sensor Networks (WSNs) have been widely deployed, and this makes both efficient collective sensing and data processing possible. In particular, these networks must be secure in terms of their ability to withstand different attacks. WSNs are particularly sensitive to various forms of attack in hostile environments. This paper aims to provide a novel design based on blockchain technology for detecting and isolating malicious nodes in WSNs. In WSNs, malicious activities can have eco-centric consequences in addition to spreading false data and disrupting normal operations. Therefore, an urgent need arises for Intrusion Detection Systems (IDS) that require few resources, are effective, and are able to operate within the computational abilities of WSN nodes. The method we propose surpasses current IDS techniques by reducing the requirements for communication and computation. Above all, in comparison to traditional blockchain frameworks. The objective is to detect and eliminate compromised nodes, which can seriously affect network performance and cause sensor data to be misreported for longer periods. Chaos theory and a simplified algorithm are used to generate a validation hash. Node verification made easier by chaos theory generates a hash for verification. The simulation results confirm that our approach can accurately discover compromised nodes while optimizing resource utilization.

Keywords: WSNs, Blockchain, IDSs, Attack, Malicious Nodes.

1 Introduction

The WSNs consist of a large number of low-cost sensor nodes that make multi-hop networks in order to collect and analyze data in a certain area. Furthermore, in a network, the WSNs combine their results for a comprehensive analysis of data in an area, which is then sent to the base station (BS) (Jabor et al., 2023). The nature of WSN interconnectivity has mitigated the WSNs' limitations of limited power supply and computing abilities. Thus, WSN is used successfully in different applications such as environmental monitoring, military reconnaissance, health care, etc. (Khan et al., 2021). WSNs can only function perfectly if they cover a large area and have random deployment, self-organization, monitoring and accuracy, as well as fault tolerance (Kim et al., 2019).

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 16, number: 3 (September), pp. 134-154. DOI: 10.58346/JOWUA.2025.I3.009

*Corresponding author: Instituto ITACA. Universitat Politècnica de València. Camino de Vera s/n, Valencia, España.

In WSNs, sensor nodes transmit data to a central node, which is often called a sink node. Next, B.S. conduct computational process on the received data (Kim et al., 2019). However, because sensors are often operated in challenging environments, WSNs send data over unsecured wireless links, leaving themselves open not only to such risks as eavesdropping, interception, unauthorized data manipulation, but also the chance that data confidentiality could be infringed and more serious consequences might result (Mo et al., 2022). Mainly, WSNs have two types of attacks, namely: internal (insider) and external (outsider) attacks (Ojaghloo & Jannesary, 2015). These attacks may affect the network's reliability and effectiveness (Javaid, 2022). To address these problems, one by one, security measures need to be integrated into WSNs, including techniques such as encryption, authentication procedures, and intrusion detection systems (IDS) (Shanthi & Rajan, 2016). Owing to WSNs' limited resources, their traditional security methods are not suitable. IDSs are vital tools for monitoring network attacks and enforcing policy on cybersecurity (Aminanto et al., 2022). However, constructing an efficient IDS for WSNs in view of the diverse and intricate patterns of abnormal data and types of intrusion remains extremely difficult (Wu et al., 2022). By halting unauthorized access and protecting against known threats, IDSs deliver security. There are generally three types of IDS for WSNs, classified according to the data they have analyzed in order to meet the particular vulnerabilities and usage conditions of each network (Sudhakar et al., 2019). These systems are crucial to the proper functioning of WSNs in protecting the privacy and integrity of the data, and thus making it suitable for critical applications (Liu et al., 2022):

1. Host-Based IDS: Focuses on the internal data of the system and not on the network data. However, extensive computational power affects the WSN device, which already has limited resources.
2. The Network-Based Intrusion Detection System operates on live network data. There is also significant resource consumption when updating to deal with new security threats.
3. A combination of both of these methods gets data from the host and network sources for better monitoring.

Deploying IDS in WSNs is full of significant challenges. Traditional IDS methods require more data and resources for a WSN than can be provided, meaning the mere use of existing IDS methods will not work (Liu et al., 2022). There are several key barriers to implementing WSN-based IDS, including a lack of essential functions such as encryption and real-time routing, nodes being physically accessible to manipulating and unauthorized manipulation, the danger of falsifying information by compromised nodes that appear normal, susceptibility to intercept and disruption attacks, and the rarity that decisions must be taken jointly without a central authority (Kuldeep & Zhang, 2020; Butun et al., 2014). Blockchain technology has the potential to increase security in Internet of Things (IoT) and WSN applications. With the use of blockchain technology, IDSs in these areas can handle data security requirements satisfactorily; they provide secure and safe storage for data (Mansour, 2022). Blockchains offer a decentralized way of reaching agreements, using encryption and incentives to build trust without a central authority; they maintain a record that is extremely visible and not easily altered, together with many distributed networks through cryptographic means (Javaid, 2022; Shin et al., 2024). Through its implementation, blockchain technology ensures the integrity of data, prevents unauthorized changes, and allows validation of transactions (Moreau & Sinclair, 2024). Data stored in a blockchain consists of blocks that are interlinked and utilize cryptographic hashes to preserve the integrity of the data (CAICT, 2018). Blockchain, with its unique characteristics of trust, can significantly revolutionize applications in diverse industries. By resolving the mentioned constraints, blockchain-based IDSs have the potential to improve security for IoT and WSNs significantly. Additional investigation is necessary to fully exploit the advantages of blockchain technology in these domains (CAICT, 2018). Cryptographic algorithms are utilized in blockchains for both signing and verifying procedures, as well as establishing

connections between different blocks to authenticate transactions. In order to verify the accuracy of entries, a hash function is employed to condense hashed data into blocks, thereby guaranteeing the integrity of the data (Wu, 2015). As illustrated in Figure 1, each block in the blockchain structure incorporates the hash value of the preceding block in its header (Moubarak et al., 2018).

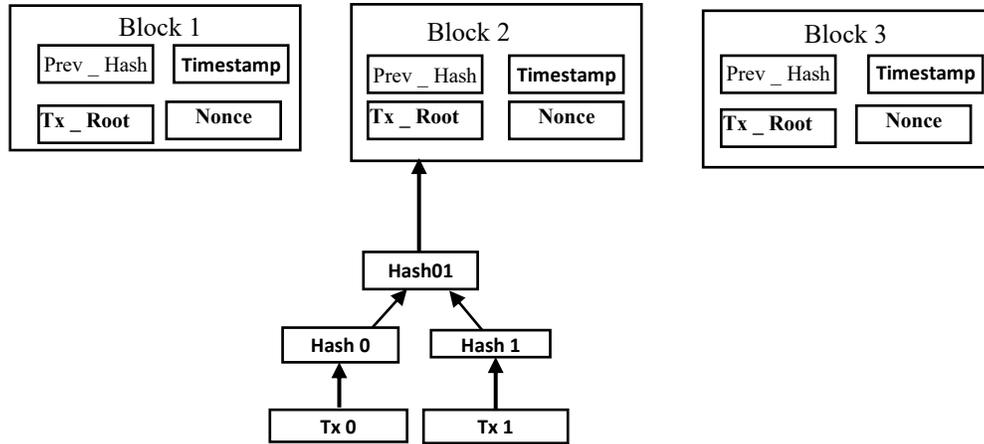


Figure 1: Blockchain Structure (Jabor et al., 2023)

As mentioned earlier, WSNs encounter remarkable security vulnerabilities and resource limitations that hinder the effectiveness of intrusion detection systems (Liu et al., 2022; Nematillaev et al., 2025). Nevertheless, the decentralized structure, cryptographic security, and unchangeable records of blockchain technology can assist in reducing these problems (Ramasamy et al., 2021). Blockchain technology strengthens the operational resilience of systems by distributing functions across nodes, facilitating transparent and encrypted data sharing, using cryptographic checks to verify data integrity, and leveraging network consensus protocols (Marchang et al., 2019). These blockchain capabilities lead to robust systems that effectively safeguard against cyberattacks, malware, and unauthorized data manipulation - threats that are pervasive in WSNs (Almaiah, 2021). For public blockchains that use distributed consensus to preserve the ledger, the probability of an attacker successfully altering existing records or inserting illegitimate blocks is negligible. This configuration enables distributed access to a WSN through a blockchain, inherently safeguarding against attacks that undermine the accuracy and integrity of data. Furthermore, the characteristics of blockchain effectively mitigate denial-of-service attacks carried out by malicious nodes (Ramasamy et al., 2021). Blockchain-based solutions for WSNs guarantee the verification of all transactions using blockchain addresses, thereby preventing the occurrence of false transaction verifications (Ramasamy et al., 2021; Liu et al., 2017). In order to mitigate the computational burden of blockchain-associated operations such as hashing and encryption, we propose a dedicated circuit architecture incorporating efficient Compressive Sensing (C.S.) encryption and chaotic hashing techniques tailored to suit the restricted resources of wireless sensor networks (Jabor et al., 2023; Ofoghi, 2015). By integrating encryption and recovery procedures and ensuring the confidentiality of the measurement matrix, the requirement for distinct decryption operations is minimized, and computational requirements are reduced (Zhang et al., 2018; Zhang et al., 2018). The measuring and masking matrices in this cryptosystem are derived from a chaotic system employed as the secret key (Ponuma & Amutha, 2019).

Chaotic maps necessitate the specification of initial conditions and control parameters to undergo iteration, resulting in the generation of exceedingly random keys, thereby guaranteeing a vast and diverse key space. This application of chaos theory is influenced by prior research in reference (Nesa et al., 2019), providing a substantial reduction in processing demands compared to the widely employed RSA

encryption system used in (Yang et al., 2014). The security analysis demonstrates resilience against statistical attacks, reliance on secret keys, and a significant ability to withstand brute force attacks (Ponuma & Amutha, 2019). Guarantees confidentiality by employing a unique sensing matrix for each measurement, similar to the One Time Pad, where the sensing matrix is utilized only once, and the text is enclosed in the tag. This approach utilizes a chaotic algorithm to generate irreversible hash functions.

It shows its efficacy and adaptability in fulfilling hash function requirements while exhibiting a remarkable avalanche effect and sensitivity to initial messages. Chaos theory is the study of dynamic systems that display chaotic behavior, meaning they are susceptible to their initial conditions. These systems can be mathematically described using chaotic maps, which exhibit characteristics such as diffusion, confusion, ergodicity, uniform data distribution, and aperiodicity. These properties align with the requirements of cryptography (Teh et al., 2019).

The objective of this paper is to create a highly effective system for encrypting data and detecting intrusions by utilizing blockchain technology. We have incorporated a specialized circuit, known as a dedicated Circuit, that utilizes chaos technology to streamline the encryption process in the field of C.S. Additionally, we have employed chaos-based authentication to generate less intricate hash codes. The primary contribution entails a comprehensive approach to enhance the security of WSNs, taking into account the constraints imposed by limited resources. An energy-efficient hardware architecture employs Field-Programmable Gate Arrays (FPGAs) to enhance circuitry and minimize power usage. A responsive intrusion detection system detects and isolates nodes that have been compromised while also identifying the methods used by attackers to breach the system. This method allows for the dynamic quarantine of threats and improves the encryption on edge devices, thereby increasing the level of confidentiality for data.

The paper is organized in the following manner: Section II provides an overview of pertinent literature and previous studies. A blockchain trust model intended to detect malicious nodes in WSNs is presented in Section III. Model execution analyses and simulation evaluations are covered in Sections IV and V. Section VI concludes the paper.

2 Related Work

This section will analyze the most relevant studies that employ blockchain technology for WSNs. This paper summarizes the significant advancements scholars have made in this specific field of research.

The authors propose a system in (Mishra & Tyagi, 2019) that utilizes blockchain technology to withstand both internal and external attacks effectively. The key components of the proposed system of work in (Mishra & Tyagi, 2019) are as follows: Tokens are generated for a specified duration once the user's authenticity has been confirmed by means of their contact number, such as the provision of a One-Time Password (OTP). The system is being fortified using blockchain technology, which will employ encryption to safeguard the data stored in the token, the user's information, and the user's activities at every stage until their session is concluded. In this scenario, the analysis of blockchain activity logs can potentially enable the identification of internal attackers who are present within a network. The blockchain offers an immutable log of every user authentication event and password modification.

In their study, the authors introduce a blockchain trust model (BTM) to detect and handle the existence of malicious nodes in wireless sensor networks (She et al., 2019). Sensor nodes are classified as either functional or non-functional based on their packet loss rate. Each node conducts a distributed algorithm to monitor its surrounding nodes for occurrences of packet loss with precision. If a node detects that its neighbor exceeds a predefined threshold for lost packets, that neighbor is categorized as

both non-functional and malevolent. Afterwards, these non-functioning nodes are quickly removed from the network. The three elements indicated below are gathered for the operational nodes that remain below the packet drop threshold:

1. **Transmission Delay Factors:** WSN aims to find out the packet timing of these factors, which is to detect malicious nodes and use packet timing tests to measure the actual time from the receiver of a complete set of packets through relaying them to their endpoints (the time delay due to proportional elapsed durations).
2. **Forwarding Rate Influences:** That the contiguously forward packets of a relay are genuine reduces the likelihood for malicious nodes to manipulate them. Individual nodes document quantities of packets exchanged with neighbors. Comparative evaluation of these totals enables the identification of discarding versus forwarding behaviors at adjacent nodes. Post-transmission, the source verifies successive forwarding via confirmation of packet count increments at next-hop nodes. Dropped rates below a threshold limit indicate inadequate packet forwarding.
3. **Response time (Rt) factors** analyze node maliciousness through timing metrics. By calculating the interval between the initial request and eventual accurate data receipt within bounded periods, the overall durations required for valid responses are quantified. The derived proportional elapsed times assess behavior. Simulations demonstrate that the model capably detects and manages malevolent nodes in wireless sensor networks. Incorporating four node types introduces topological intricacies. Also, Proof of Work (PoW) consensus will result in these low-power nodes being hit by huge costs, entirely unsuitable for the targets of their energy and bandwidth wireless sensor network. Furthermore, security is achieved by the blockchain and PoW, but there still needs to be additional analysis on how best we can deploy with these limited resources of sensor devices.

The intrusion detection method proposed in (Almaiah, 2021) leverages the inherent unchangeable records and consensus mechanisms associated with blockchain technology. The CH node can validate the hashes of sensor messages against the blockchain to classify nodes as malicious or benign according to historical categorizations. Comparing newly received signatures with existing blockchain entries enables signature verification. Reported simulations exhibit 94.9% malicious message identification and categorization accuracy using this blockchain-based approach. However, key rotations increase overheads like time and energy burdens. Cryptographic hashing also challenges resource-restricted devices. While enhancing security and authentication, the proposed solutions must enhance the efficiency of exchanges and hashing required for blockchain transactions.

The suggested (Cho & Cho, 2020) proactive defense model distributes identified internal attacker lists across sensor networks via blockchain-based trust mechanisms, even among collaborative attackers already within the system. Sensor nodes detect internal threats and immediately notify others once confirmation occurs. Individual nodes monitor local neighbourhood cooperation, scoring transactions. Ratings below thresholds indicate untrustworthy internal adversaries. Such decentralized trust computations mitigate reliance on particular determination sources. Embedding list distribution atop blockchain protocols also hardens security. According to the analysis, internal attackers potentially hamper exchange security. In contrast, the proposed model reliably shares attacker identifications among all sensors through distributed middleware constructs in the wireless sensor network, leveraging inherent blockchain security attributes. Quantified comparisons exhibit 59-67% reductions in packet-dropping harms relative to conventional trust techniques.

In (Li et al., 2019), a blockchain-based architecture called CBSigIDS is proposed, which combines blockchains with distributed signature-based intrusion detection systems (IDSs) in an Internet of Things context. Multiple IDS nodes can collaborate to progressively develop and validate a signature database in the context of CIDNs using this technique. Using blockchains, CBSigIDS can offer a reliable method for exchanging signatures across various nodes, eliminating the requirement for a trusted third party to facilitate the exchange of signatures. Using CBSigIDS, each network traffic monitoring node (or blockchain node) in the consortium blockchain continuously monitors network traffic to identify threats or anomalies. When a node detects a new threat pattern, it can generate a signature (rule) that characterizes that threat. It signs the new rule using its private key to indicate it is the source, then broadcasts the signed rule to all other nodes in the consortium blockchain. The new rule can be checked by a receiving node in its local database before it accepts the rule. In this manner, nodes can, over time, collectively set up a robust signature database by consistently contributing new rules and validating each other's. If we are to establish the source of transmitted rules, we must confirm the authenticity of these with a private key from the originating node.

These regulations will only be adopted by other nodes after first cross-checking against local records to establish validity. Under this framework, the blockchain grows only if most nodes have ratified that the new block obeys trusted protocols. The findings suggest that implementing a CBS Interactive Signature Identification Database System (CBSigIDS) improves the resilience and performance of signature-based threat detection under adverse network conditions.

The researchers in (Mbarek et al., 2022) propose an adaptive blockchain-enabled methodology called Adaptive Blockchain-based Anti-Jamming Solution (ABAS) to protect against jamming attacks targeting wireless sensor networks. They suggest a decentralized approach to detecting multi-channel jamming by identifying congested channels. Each channel will have an IDS agent to create a decentralized trust network via consensus. The agents can monitor channels for signs of interference like increased noise, packet loss, or connectivity issues. They can update the status of channels on the distributed ledger. However, all database communications occur on the blockchain. ABAS has two key features. To promptly detect jammers and notify the ledger, IDS agents leverage Hyperledger Fabric (Mbarek et al., 2022). The private blockchain, built on Hyperledger Fabric, includes all entities like cluster heads and sensor nodes. This private blockchain improves communication efficiency and consensus among nodes. Moreover, the solution not only mitigates jamming but proactively counters the specific node causing it. This is done by transmitting radio signals to occupy the jammer, eradicating its ability to predict future communication channels. Additionally, blocked nodes can change channels by checking the ledger's list of available channels.

The authors in (Narayana & Midhunchakkaravarthy, 2020) proposed a model outlining the architecture of blockchain data, specifically to identify and isolate malicious nodes at defined intervals. The proposed method can efficiently identify malicious nodes within Mobile Ad Hoc Networks (MANETs) - wireless networks with no fixed infrastructure where nodes function as routers and communicate directly (Quy et al., 2022). After forming the MANET and completing routing, a Network Block Monitoring Node (NBMN) is designated to oversee blocks from node transactions. Node communications are encrypted and linked in a blockchain. When nodes route packets per the routing table, the model chooses an NBMN. Nodes sending data notify the NBMN node, which verifies the transaction against the table. The NBMN only creates a block if both are valid nodes, repeating this through successful data transmission. The proposed model accurately detects nodes deliberately dropping packets. Compared to a traditional malicious node detection model, the proposed model better identifies malicious nodes.

The researchers in (Arifeen et al., 2021) developed a Sybil attack detection mechanism for underwater wireless sensor networks (UWSNs) using blockchain. Here, sensor nodes request to join the network by sending their unique ID to the C.H. Due to the dynamic environment, sensor nodes consistently update their status and positions. The CH utilizes a trust model to evaluate nodes' reliability. Nodes meeting the trust criteria get a transaction appended to the blockchain by the C.H. In situations where an illegitimate node duplicates the identity of an authorized node to infiltrate the network, the C.H. leverages the blockchain to identify the Sybil attack.

Previous researches have investigated integrating blockchain technology into WSNs to enhance security, but there remain open issues and possibilities for enhancement. A key challenge is that executing blockchain's computationally demanding cryptographic and consensus protocols directly on WSN nodes with limited processing capacity can rapidly deplete their constrained energy and computing resources. While methods exist to detect invalid sensor nodes trying to enter the network, such as checking for duplicated node identifiers, the authentication process can be expensive and burdensome.

Furthermore, in existing solutions, the encryption algorithms protecting information tend to be left rather vague. Future research ought to investigate methods for better integrating blockchain and WSNs, which also conserves energy: perhaps it could offload resource-intensive operations on cryptography or consensus procedure to more powerful edge nodes or nodes with less computing capacity while limiting the noise level. Through a detailed study of the system level, it is possible to construct a secure trust architecture that is decentralized based on blockchain principles. In this way, some of the remaining security flaws in WSN may be remedied without overburdening the capacity provided for sensors.

Current intrusion detection methods for WSNs rely heavily on simple heuristics like packet drop rate thresholds and routing table lookups to identify threats. Advanced algorithms integrating machine learning are necessary to improve detection accuracy and minimize false positives. Additionally, most blockchain-based security frameworks cover only specific aspects of WSN defense rather than an end-to-end solution spanning cryptographic key distribution, malware signature sharing, and beyond. Developing a comprehensive blockchain framework could significantly bolster security and capabilities. There has also been insufficient analysis around agreement protocols and consensus models best suited for resource-constrained WSN nodes, like comparing proof-of-work and proof-of-stake. While external attacks have received focus, blockchain technology could also help identify compromised insider nodes.

Moreover, assessments of overhead, scalability, and cost-benefit trade-offs for blockchain integration in large-scale WSNs are currently lacking. Evaluating performance impacts will be vital for tailoring blockchain security to fit stringent WSN communication and energy restrictions. The critical issue of encrypting sensitive intrusion detection data on the blockchain is also frequently overlooked, exposing networks to potential data leakage risks. Incorporating robust encryption is imperative to mitigate such vulnerabilities. Overall, opportunities remain for enhancing blockchain-enabled security for WSNs through comprehensive frameworks, optimized consensus protocols, detection of insider threats, and thorough evaluation of performance overheads and data privacy techniques.

3 Detecting Malicious Nodes in WSN with Blockchain

In this section, the framework of the proposed model is reviewed. Our model mainly builds on WSNs based on the Low Energy Adaptive Clustering Hierarchy (LEACH) routing protocol, as illustrated in Figure 2. Although we use LEACH in the proposed model, other routing protocols might be used, such as TEEN or APTEEN (Asqui et al., 2020) for employing lightweight encryption and clustering. For our proposed model, the LEACH protocol has the main required criteria to achieve clustering topology and

maintain low complexity by employing a hierarchical structure and executing cryptographic tasks at the individual node level. Our proposal involves implementing data encryption through a circuit, which offers a cost-effective solution. Furthermore, this approach enables us to utilize lightweight authentication, based on chaos theory, for verifying transactions in decentralized networks. This authentication is facilitated by a manager who manages secure data traffic in wireless sensor networks, ensuring proper organization and content structure. Additionally, we consider the scenario of pinpointing the attacking node as well as the case of effectively detecting the attack itself.

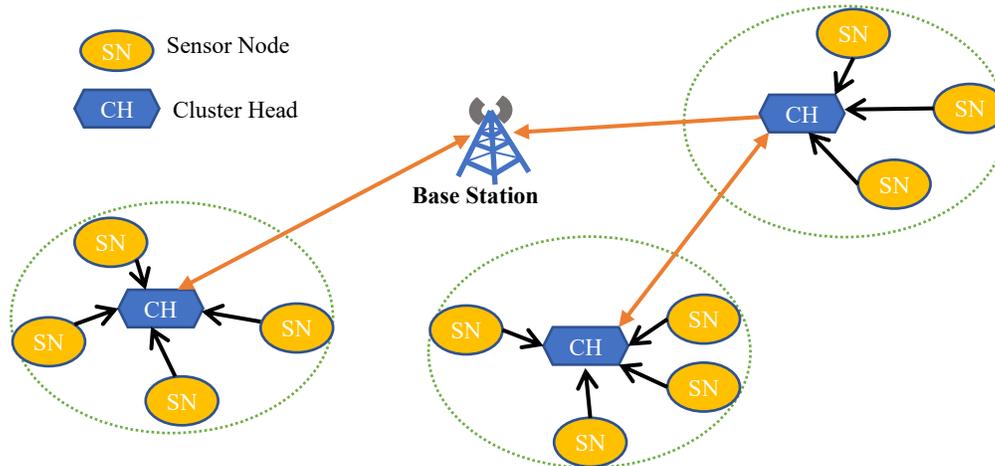


Figure 2: Blockchain Network Architecture (Jabor et al., 2023)

3.1 WSN Architecture and Blockchain Integration

The incorporation of blockchain technology into wireless sensor networks substantially improves their security and resilience. As WSNs become increasingly prevalent in critical infrastructure monitoring, healthcare, defense, and other domains requiring stringent security (Heinzelman et al., 2002), blockchain's distributed ledgers, cryptography, and authentication substantively bolster WSN protections. However, accompanying computational and communication overheads pose meaningful challenges given the constrained processing and battery capacities characterizing WSN devices (Rhea et al., 2019). These challenges are propelling collaborative hardware and software co-design efforts (Gad et al., 2020). Dedicated compression, encryption, and hashing circuits reduce processor workloads (Hsieh et al., 2018), though practical sensor-level Application-Specific Integrated Circuit (ASIC) integration remains restricted. Lightweight chaotic algorithms demonstrate superior efficiency over software blockchain hashing (Hsieh et al., 2018), and cryptographic support circuits have succeeded in strengthening security while improving energy efficiency and lifespan (Farooq et al., 2010). Still, more compatible protocols suited to WSN resource limitations are needed. For instance, Proof of Authority offers a lighter consensus than Proof of Work. Ongoing research also evaluates Merkle trees to decrease communication bandwidth requirements for blockchain dissemination (Dai et al., 2019).

In hierarchical WSN topologies employing clustered routing protocols like LEACH (Heinzelman et al., 2002), blockchain functionality localizes at cluster heads and nodes, protecting individual sensor nodes. Cluster heads handle the predominant encryption and hashing duties prior to distributing blocks network-wide. Hardware compression leveraging chaotic sequences boosts this performance while enhancing security via randomization properties (Rhea et al., 2019). Though challenges persist in tailoring blockchain for optimal WSN capability, purpose-built hardware relieves strains on existing

sensor platforms to enable blockchain's security advantages. The resulting fairer energy consumption distribution fortifies network longevity by preventing premature node failures (Farooq et al., 2010).

3.2 Blockchain WSNs for Detecting Malicious Nodes

We establish the following framework assumptions before model testing and potential malware attack identification:

1. Our previous work (Jabor et al., 2023) enabled blockchain-integrated WSNs, where smart devices control networks and leverage blockchain to detect threats
2. In our WSNs, CHs gather data from constituent sensor nodes within transmission range for relay to the BS. The proposed blockchain links CHs with each other and the BS. The CHs delay block generation until they receive full sensor data. Compressive Sensing CS techniques first compress and then encrypt readings to minimize sizes before transmission.
3. The CHs bid for new block creation responsibilities. The BS compiles a time-ordered table of CH bids following First Come, First Served (FCFS) principles that represent clusters during generation equitably. Consensus protocols adhere to predefined authentication rules. Once the BS finalizes a bids table, it instructs listed CHs to monitor the winning CH producing the block for distribution and validation checks depicted in Figure 1.
4. The system's primary role is to ensure accurate data transactions and update blockchain statuses. Unlike traditional devices, our sensor nodes employ chaos theory-based encryption for data transmission, as detailed in section 4.6. This advanced approach significantly bolsters network security and data integrity, protecting against unauthorized access and intrusions. By integrating this specialized encryption, the sensor nodes maintain confidentiality and robustness in the network, offering a secure and efficient solution for monitoring and communication within the blockchain framework.
5. Chaos theory-based encryption is proposed to improve wireless sensor network data transmission security. Leveraging chaotic systems' sensitivity to initial conditions and parameters, this method provides cryptography via a dedicated circuit generating a random sequence functioning as an encryption key.
6. Sensor nodes utilize this chaotic sequence for obfuscating data before transmitting it to cluster heads. By keeping the sequence parameters confidential, cluster heads can directly recover the original data without separate decryption, minimizing computational overhead. The chaos-based scheme has lower complexity and is compatible with constrained sensor resources compared to conventional ciphers. Chaos encryption also enhances brute force attack resilience through unpredictability and vast key possibilities. Therefore, the specialized chaotic circuit enables efficient and secure node-to-cluster head communication.

Attackers compromising Block N may attempt data modifications. However, even minor changes significantly alter hashes. Therefore, mismatching will occur between Block N's updated hash and the prior hash stored in Block N-1. Adversaries must also access hashing parameters, which chaos hash functions make improbable to predict precisely, even upon theft.

Nodes rejected by a majority get designated as attackers. Subsequently, the network isolates these nodes via their addresses/IDs.

3.2.1 Modification Attack

Modification attacks involving unauthorized data access and manipulation by intruders remain prevalent and jeopardize both the network and application layers of WSNs (Kavitha & Sridharan, 2010; Hossain et al., 2015). This type of attack is a very popular attack agent in blockchain, so we use it to verify whether the proposed circuit is able to detect the compromised nodes and the circuit's ability to produce hashes as well.

Furthermore, by infiltrating and altering shared data, attackers disrupt interconnected nodes and undermine information integrity and reliability. Adversaries may manipulate various data properties, including origin, destination, and contents, or selectively delete packets to induce corruption. Assessments were executed to modify attacks to evaluate two key defensive capabilities: cryptographic hash effectiveness in detecting unauthorized data changes and identifying/isolating attacking nodes by location. Evaluating manipulation detection resilience builds confidence in maintaining data integrity. In WSNs, modification attacks refer to malicious nodes deliberately bypassing security measures to infiltrate sensor nodes or communication channels before intercepting and altering transmitted packet contents (Kavitha & Sridharan, 2010). Attackers may inject fabricated readings or manipulate authentic sensor data. Recipients then unknowingly process contaminated data, causing downstream decision errors. Potential impacts encompass false alerts, inaccurate surveillance, and flawed analytics. For instance, manipulating pollution readings could mislead systems into missing actual incidents.

To check if a cryptographic function intercepts unauthorized changes, we modified an attack from end-to-end asynchronous mode accordingly. Once it is known who the attackers are, what they are up to, and where they are happening, these features make it possible for WSNs to provide robust manipulation detection and attacker isolation. This is necessary to establish correctness as well as reliability permanently in WSN. Even if under attack, a WSN must keep providing the service it was designed for.

3.2.2 Hash Function and Consensus Algorithm Based on Chaos

This paper employs chaos theory and the chaotic tent map to create a highly effective algorithm for one-way hash function encryption (Amin et al., 2009). Chaos theory, together with a chaotic tent map, is aimed at providing a method of developing highly secure methods for one-way hash function encryption. Each block into which the input data is divided will be processed sequentially by the chaotic map to produce interim hash values. The final hash is the accumulation of these interim hashes. The tent map, as well as adjustable parameters governing chaotic behavior, contribute to this simple yet secure hash function. This has low complexity, so the simple tent map and secure adjustable parameters dictate chaotic behavior. Simulations confirm the anticipated hash properties and provide partial protection against common attacks such as birthday and meet-in-the-middle attacks. A Proof of Stake consensus algorithm is employed, in conjunction with First Come First Serve bid scheduling, to determine the cluster head responsible for generating and disseminating the subsequent block. This consensus mechanism guarantees distributed trust and transparency by employing equal selection probability and avoiding centralized control. Subsequently, the cluster head node that has been chosen through an election process transmits the recently formed block to all peer nodes in order to undergo validation. After receiving the block, each node generates the hash code again using the specialized chaos-based circuit that is present in every node. The regenerated hash is compared to the received current hash. In addition, the previous hash contained in the current block is authenticated against the existing blockchain ledger at every node. If both tests are successful, the node will vote in favor of incorporating the new

block into the blockchain. Once it is approved by a majority consensus, it is added to the blockchain structure and remains stored in the ledger of every node.

3.3 Network Behavior

Figure 3 explains the behavior of a node to accept a block upon receiving a block from another node. Validation takes place by regenerating cryptographic hashes and contrasting them (Amin et al., 2009).

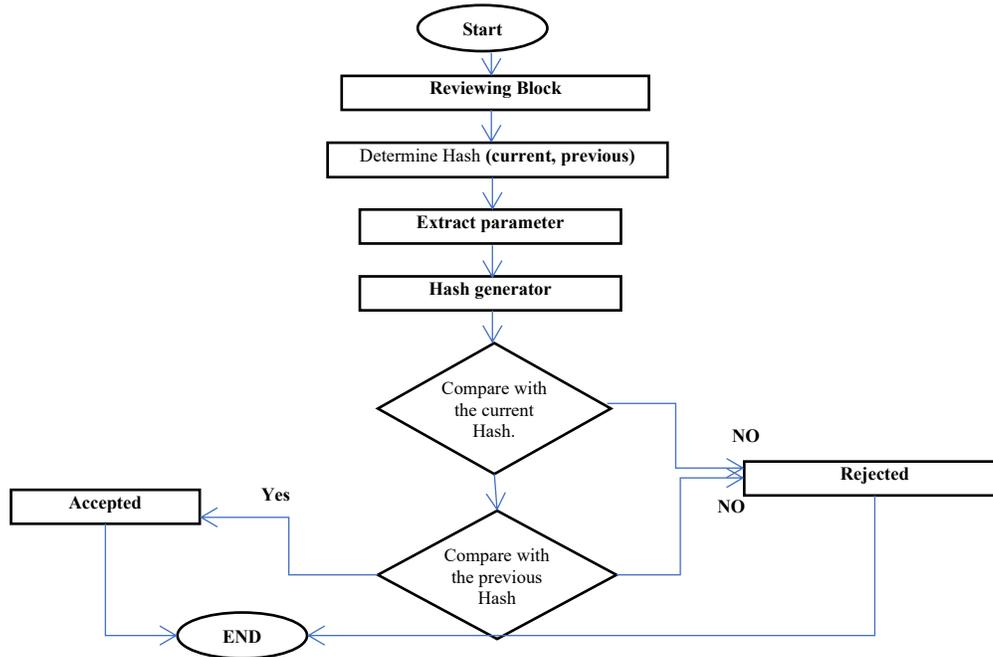


Figure 3: Network Behavior

In particular, the CH node retrieves the cluster parameters from the block data, so that they were initially hashed to produce the current hash encoded in the received block. With these parameters, the cluster head node recomputes the hash as it has been given out. Assuming the new hash agrees with the old one, this verifies the integrity of the block contents by ensuring the data has not been altered. Meanwhile, the CH node matches the previous hash in the received block with the most recent hash saved on it. They will do so for a while, and then it means that the received block, too, is connected in chronological succession to the cluster head's existing blockchain dataset without interruption. Before it is accepted, the reproduced has and previous hash checks are both omitted. The validity of the received block is the only thing that is guaranteed before accepting it, enhancing security as shown in Figure 3. The dual hash verification technique permits network nodes along the way to check out new data in the blockchain that comes from others in a decentralized manner without necessarily having to rely on central trusted authorities.

4 Mathematical Model of Proposed Method

The following are the steps that describe the mathematical model representation of the proposed model:

1. The mathematical framework integrates chaotic encryption, traditional encryption, chaos-driven hashing, and blockchain technology into a holistic model for improving the security of wireless sensor networks. This multifaceted mathematical approach facilitates automatic threat detection and response in wireless sensor networks through coordinated encryption, data compression,

integrity checks, and decentralized monitoring. Chaos theory-based encryption relies on chaotic maps (Alwan & Hussain, 2019):

$$X_{n+1} = a X_n(1 - X_n) \dots \dots (1)$$

In equation (1), x_n represents the initial condition, while a is a control parameter that regulates the features and behavior of the logistic map (Ashish et al., 2018).

1. The sparse signal x and measurement vector y have a relationship through the sensing matrix Φ in CS encryption as established in equations (2) (Cho & Yu, 2019):

$$y = \Phi x \dots \dots (2)$$

For each measurement, the sensing matrix is adapted according to equations (3):

$$\Phi' = \Phi + \Delta \dots \dots (3)$$

The symbol Δ represents the alteration that is affected by the encryption key k .

2. Equation (4) defined the chaos-based hash functions (Amin et al., 2009):

$$H_n = K_{n-1} \oplus H_{n-1} \dots \dots \dots (4)$$

The value K_n denotes the initial state of the tent map.

3. The process of connecting a series of linked blocks is known as Blockchain Integration (Meidute-Kavaliauskiene et al., 2021):

$$B_i \rightarrow B_{i+1} \rightarrow \dots \rightarrow B_n \dots \dots (5)$$

A nonce for cryptographic validation, data B_i , and the hash of the preceding block are all contained in each block B_i . Verifying the legitimacy for every block maintains the blockchain's integrity.

4. Network Behavior and Attack Detection mechanism of the model $\delta(\text{parameters}) \rightarrow \{\text{malicious, benign}\}$. Although it seems complex and unfathomable at truth are individual qualities expressed via network feedback to evaluate benign and malignant nodes on the basis of specific quantities. In wireless networking, many distinct factors come together to provide efficient and secure rule enforcement for finding the bad ones.

This model integrates various components into a cohesive whole, helping to make an efficient and robust method for detecting malicious nodes in WSN. With the aid of advanced encryption algorithms and the use blockchain technology, both data transmission and data protection are secure. This componentry, working together, form strong measures of defense against malicious entities at the network level. In order to better understand our mathematical model, we first define the sequential actions and the corresponding symbols:

1. Chaos Theory-Based Encryption (CTE): Represented by CTE (x_0, k, t) which outputs the encryption key K .
2. CS Encryption: Represented by $CS(x, \Phi, K)$ which outputs the encrypted data y .
3. CHF: Represented by $CHF(m, K)$ which outputs the hash value H .
4. BC: Represented by $BC(D, H)$ which integrates data D and hash H into the blockchain.
5. Network Behavior and Attack Detection (NBAD): is a system that examines parameters and identifies the status of a node.

The integrated representation can be conceptualized as a function that processes data x through these steps, ultimately resulting in a decision on the node's status:

$$\text{System } (x, x_0, k, t, \Phi, \text{parameters}) \\ = \text{NBAD} (BC(CS(x, \Phi, CTE(x_0, k, t))), CHF(CS(x, \Phi, CTE(x_0, k, t))), CTE((x, \Phi, CTE(x_0, k, t)))) \dots \dots (6)$$

Where:

- $CTE(x_0, k, t)$ Utilizes chaos theory to derive the encryption key k .
- $CS(x, \Phi, K)$ encrypts the data x utilizing Φ and the cryptographic key k .
- $CHF(m, K)$ generates a hash of the encrypted data m leveraging the key k .
- $BC(D, H)$ incorporates the encrypted data D and its corresponding hash H into the blockchain.
- NBAD evaluates the blockchain and additional metrics to identify malicious nodes.

5 Results and Discussion

The effectiveness of our proposed approach is evaluated in this section, with a focus on its ability to identify malicious nodes during a single-node attack. A comparative analysis will be conducted between our blockchain-enabled WSNs and versions without blockchain integration. Furthermore, we will implement an authentication mechanism for improved efficiency. The proposed approach will be tested and appraised using MATLAB R2019b. We will provide the simulation findings for the network structure put forth in this research.

5.1 Description MATLAB Simulation of Model

The following is a summary of the MATLAB simulation scenarios used in the paper:

- Sensor nodes were randomly distributed within a square region.
- Because each node in a social network had a unique identification number and was limited in energy, social network was distinguished by their uniformity.
- The, BS, was located at the center of the region and had a fixed position.
- Nodes communicate with their neighbors through a direct connection.
- The wireless transmitter's power can be adjusted. Table 1 enumerates the fundamental parameters.

Table 1: Simulation Parameters (Jabor et al., 2023)

Parameters	Value
Network area size	100 × 100
Round	500
Nodes number	100
Initial energy	0.5 J
Maximum block size	1000 bits

5.2 Malicious Nodes Detection

The key objective of implementing a blockchain platform in WSNs is to detect malicious attacks while assessing the network's performance and resilience when facing security threats. Important metrics for assessing WSN performance encompass the quantity of packets dispatched by a node and received at the target without failure, as well as throughput and packet delivery ratio per cycle. The suggested

blockchain framework can identify the approximate location of a malicious node within a $100\text{m} \times 100\text{m}$ zone, as depicted by the red indicator estimating the whereabouts of the detrimental node in Figure 4.

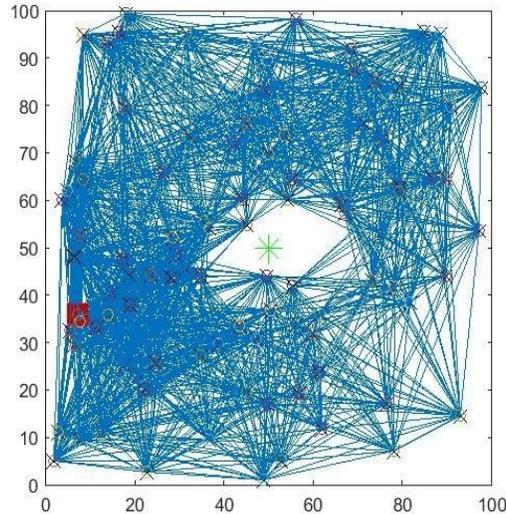


Figure 4: Blockchain Model to Detection Node

This capability to determine the general vicinity of attacks targeting either sensor node data or cluster head blockchain data could prove valuable for security response. Overall, the blockchain-enabled WSN aims to identify threats and quantify impact on vital network operation metrics to evaluate effectiveness against attacks and make informed improvements to system resilience (Guo et al., 2010). Pinpointing the approximate location of the malicious node can help uncover compromised sensor nodes if the attack is corrupting sensor data. If the threat instead manipulates cluster head blockchain records, the location still provides useful clues indicating a potentially vulnerable network region warranting further inspection. However, additional investigation is necessary in either case to accurately determine the exact malicious node from the estimated vicinity area. While not precise, the capability to broadly localize attacks provides an initial focal point to aid in isolating threats and assessing any sensor nodes that may require quarantining or other mitigation steps. But more targeted forensic analysis of the suspicious network segment would still be vital to conclusively identify the singular compromised node enabling the malicious activity.

5.3 Throughput

Throughput, defined as the rate of successful packet delivery to the intended destination, is a crucial parameter for assessing network performance during an attack. By quantifying throughput, the number of legitimate packets correctly received can be used to measure the efficacy of the attack detection scheme.

To calculate the throughput for a given simulation run with a fixed total runtime, the following equation can be utilized:

$$\text{Throughput (avg.)} = (\text{Total valid packets received} / \text{Total simulation time}) \quad (7)$$

Throughput is derived using Equation 7 (Al-Majmaie, 2019), and the simulation involves evaluating this metric along with other performance measures. As delineated in Table 2, during the attack-free scenario the system sustains an average throughput of 10.5502 packets per unit time, denoting consistent

transmission stability in normal conditions. Conversely, under attack conditions, throughput varies more clearly relative to the no-attack case. With attacks, the average throughput undergoes a minor decline to 10.2863 packets per unit time, indicating a lowered transmission rate.

Between rounds, throughput changes marginally based on the attack severity, however the suggested detection system can sufficiently uphold a relatively stable transmission pace during assaults, as divergences are minor. The slight throughput decrease could originate from the overhead of detection processes. Between rounds, throughput fluctuates marginally depending on severity of attack, however the proposed detection method can adequately uphold a relatively stable pace of transmission amid the attack, as discrepancies are negligible. The minor throughput decrement could originate from demands of detection processing overhead. The notable reduction in throughput could potentially be attributed to the supplementary overhead induced by the attack detection system. Conducting thorough analysis and detection of potential attacks necessitates extra time and resources, leading to a minor decline in productivity.

Table 2 : Throughput Outcomes in Malicious Node Identification

No. Round	Throughput without Attack	Throughput with Attack
100	10.5272	10.0656
200	10.5339	10.2661
300	10.5346	10.3375
400	10.5297	10.3750
500	10.5243	10.3874
Average	10.5502	10.2863

As shown in Figure 5, the proposed system's average throughput per round is contrasted under both non-attack and attack scenarios.

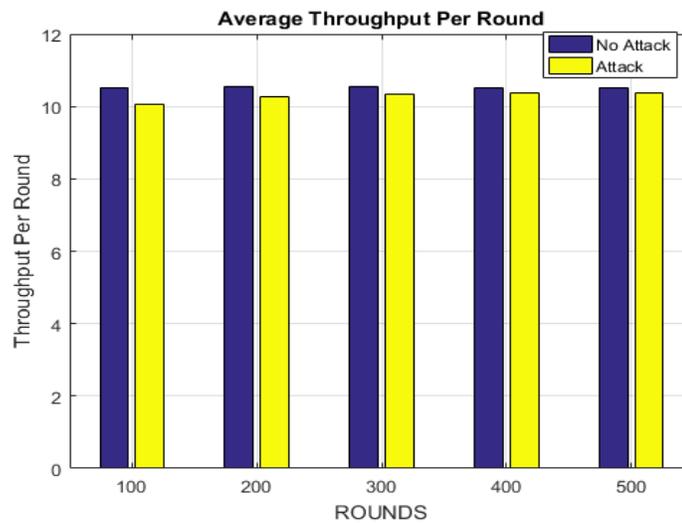


Figure 5: Throughput Average/Round

5.4 Packet Delivery Fraction

An extremely valuable indicator of the efficiency of any intrusion detection system is "packet delivery ratio." This ratio measures the percentage of packets originating from a cluster head which actually reached their intended destinations without any failure. To calculate the packet delivery ratio, it is necessary to have two pieces of information: how many packets were successfully transmitted from the

source to the destination and also how many packets the source cluster head produced and intended for delivery the parcel delivery share can give us even more interesting angles to consider. Throughput measures the general speed at which valid packets are received, while delivery score specifically quantifies the number of original packets that were successfully delivered. Using both the throughput and the packet delivery scores as benchmarks allows us to better determine the reliability of an intrusion detection system for transporting data safely in the presence of malicious nodes. There are times when a given transmission rate might indicate a system's ability to maintain stable data transfer, but that will not always mean efficient delivery. It is possible to infer the quantity of packets dropped or re-transmitted from the delivery fraction metric. During this step, we are going to compare the network performance of our proposed system during the attack and normal performance standard. Let us specifically consider packet transmission.

As shown in Table 3, denoting that, on average, all transmitted packets are received correctly. Contrasting the packet delivery ratios between the attack and no-attack cases validates the proposed system's efficacy in mitigating the adverse impact of intrusions on packet transfers. The consistent packet delivery performance across attack rounds further exhibits the intrusion detection system's steady ability to obstruct malicious packets at a uniform rate.

This test case examines packet transmission between a cluster head CH and base station BS within a network clear of malicious attacks. To ensure consistency, the CH creates block size 1000 bits per round as maximum for the BS (Jabor et al., 2023). Without intrusions, as shown in the revised Table 3, the quantity of packets sent and obtained per round is held at a fixed. The steady packet transmission aligns with the consistent data flow absent attacks. The analysis utilizes controlled tests with a sole CH for gaining insights into the system's capacity to reliably safeguard data exchange between a key CH and BS, packet delivery ratio. Outcomes show the detection system's robustness at sustaining packet delivery and throughput despite attack persistence, fundamentally. It is worth mentioning that due to the large size of the produced data in both tables, i.e., Tables 3 and Tables 4, we calculate the average for each 100 rounds for both sent and received packets. After that, we calculate the average for all averages.

Based on Table 4, network attacks influence packet delivery. On the other hand, Table 4 depicts the packet delivery ratio for a continuous network environment.

The research reveals that the packet delivery rate is only slightly lower under attack than under no attack conditions. During the attack, the average packet delivery rate was about 99.4631, showing a very small decrease in the successful transmission of packets as a result of deliberate attacks (Lara-Niño et al., 2018). From Table 4, we can see that the average number of transmitted packets is more or less constant, but the average number of received packets has dropped slightly. This indicates that the intrusion detection system can efficiently discover and stop specific packets that are classified as malicious or intruding. The decrease in received packets offers further proof of this system's success in identifying and blocking these packets. The mean packet delivery ratio without attacks is 100.4270.

Table 3: Average Packet Delivery in Non-Attack Scenarios

No. Round	Average Sent Packets	Average Received Packets
100	100.8081	100.8081
200	100.7035	100.7035
300	100.2676	100.2676
400	100.2005	100.2005
500	100.1603	100.1603
Average	100.4280	100.4270

Table 4: Average Packet Delivery under Attack Conditions

No. Round	Average Sent Packets	Average Received Packets
100	100.9092	99.9092
200	100.5527	99.5527
300	100.3343	99.3377
400	100.2505	99.2532
500	100.2604	99.2626
Average	100.4615	99.4632

6 Conclusion

Historically, centralized modalities performed malicious node detection in wireless sensor networks, lacking monitoring and verification of original sensor data. Blockchain has materialized as a promising decentralized technology for intrusion detection through consensus and manipulate-evident logging. This research introduces a tailored blockchain framework to pinpoint and obstruct data manipulation attacks in wireless sensor networks aiming to manipulate stored sensor measurements. The results show that the system is able to handle attacks effectively, identify which nodes are sending out malicious signals, and put appropriate measures in place. This article studies standard attack modes and defense methods of principal ways, focusing mainly on hash algorithms, block composition of messages, and the data-manipulation detection in blockchain. The streamlined blockchain approach is even able to categorically identify and bypass malevolent packets in the data stream, which can make a traditional way of doing so seem complex. Its resilience to intrusion is shown by its performance in packet delivery and throughput, maintaining reliable functionality without compromising service during attacks. Data integrity is maintained, and the intrusion detection system upholds security through its effective monitoring of all data packets from source to destination points, as well as returning refuse on unauthorized forms or content. On gain also for current efforts, reducing detection overhead now becomes a priority target. Future work might well mean that large scopes are added to the attack landscape and testing for effect on such methods narrow-band networks, done compared with an alternative in order of sequence non-blockchain technologies. In conclusion, this paper emphasizes how tailored blockchain solutions can be effective for detecting intrusions into wireless sensor networks.

References

- [1] Almaiah, M. A. (2021). A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In Y. Maleh, Y. Baddi, M. Alazab, L. Tawalbeh, & I. Romdhani (Eds.), *Artificial intelligence and blockchain for future cybersecurity applications* (Vol. 90, pp. 243–258). Springer. https://doi.org/10.1007/978-3-030-74575-2_12
- [2] Almaiah, M. A. (2021). A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In *Artificial intelligence and blockchain for future cybersecurity applications* (pp. 217-234). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-74575-2_12
- [3] Al-Majmaie, S. M. A. (2019). *A comprehensive approach on impacts of grayhole, blackhole and Sybil attack based on AODV protocol in wireless sensor networks*.
- [4] Alwan, N. A., & Hussain, Z. M. (2019). Compressive sensing with chaotic sequences: an application to localization in wireless sensor networks. *Wireless Personal Communications*, 105(3), 941-950. <https://doi.org/10.1007/s11277-019-06129-z>
- [5] Amin, M., Faragallah, O. S., & Abd El-Latif, A. A. (2009). Chaos-based hash function (CBHF) for cryptographic applications. *Chaos, Solitons & Fractals*, 42(2), 767-772. <https://doi.org/10.1016/j.chaos.2009.02.001>

- [6] Aminanto, M. E., Wicaksono, R. S. H., Aminanto, A. E., Tanuwidjaja, H. C., Yola, L., & Kim, K. (2022). Multi-class intrusion detection using two-channel color mapping in IEEE 802.11 wireless network. *IEEE Access*, *10*, 36791-36801. <https://doi.org/10.1109/ACCESS.2022.3164104>
- [7] Arifeen, M. M., Al Mamun, A., Ahmed, T., Kaiser, M. S., & Mahmud, M. (2021). A blockchain-based scheme for Sybil attack detection in underwater wireless sensor networks. In M. S. Kaiser, A. Bandyopadhyay, M. Mahmud, & K. Ray (Eds.), *Proceedings of International Conference on Trends in Computational and Cognitive Engineering* (Vol. 1309, pp. 431-442). Springer. https://doi.org/10.1007/978-981-33-4673-4_37
- [8] Ashish, Cao, J., & Chugh, R. (2018). Chaotic behavior of logistic map in superior orbit and an improved chaos-based traffic control model. *Nonlinear Dynamics*, *94*(2), 959-975. <https://doi.org/10.1007/s11071-018-4403-y>
- [9] Asqui, O. P., Marrone, L. A., & Chaw, E. E. (2020, January). Evaluation of TEEN and APTEEN hybrid routing protocols for wireless sensor network using NS-3. In *International Conference on Information Technology & Systems* (pp. 589-598). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-40690-5_56
- [10] Butun, I., Morgera, S. D., & Sankar, R. (2014). A survey of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, *16*(1), 266-282. <https://doi.org/10.1109/SURV.2013.050113.00191>
- [11] Cho, K., & Cho, Y. (2020). HyperLedger fabric-based proactive defense against inside attackers in the WSN with trust mechanism. *Electronics*, *9*(10), 1659. <https://doi.org/10.3390/electronics9101659>
- [12] Cho, W., & Yu, N. Y. (2019). Secure and efficient compressed sensing-based encryption with sparse matrices. *IEEE Transactions on Information Forensics and Security*, *15*, 1999-2011. <https://doi.org/10.1109/TIFS.2019.2953383>
- [13] Dai, H.-N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal*, *6*(5), 8076-8094. <https://doi.org/10.1109/JIOT.2019.2920987>
- [14] Farooq, M. O., Dogar, A. B., & Shah, G. A. (2010). MR-LEACH: Multi-hop routing with low energy adaptive clustering hierarchy. In *2010 Fourth International Conference on Sensor Technologies and Applications* (pp. 262-268). IEEE. <https://doi.org/10.1109/SENSORCOMM.2010.48>
- [15] Gad, A. H., Abdalazeem, S. E. E., Abdelmegid, O. A., & Mostafa, H. (2020, October). Low power and area SHA-256 hardware accelerator on Virtex-7 FPGA. In *2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES)* (pp. 181-185). IEEE. <https://doi.org/10.1109/NILES50944.2020.9257922>
- [16] Guo, X., Huang, S., Nazhandali, L., & Schaumont, P. (2010). On the impact of target technology in SHA-3 hardware benchmark rankings. *Cryptology ePrint Archive*.
- [17] Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on wireless communications*, *1*(4), 660-670. <https://doi.org/10.1109/TWC.2002.804190>
- [18] Hossain, M., Muslima, U., & Islam, H. (2015). Security analysis of a literature review. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, *2*(1), 393-403.
- [19] Hsieh, S.-H., Hung, T.-H., Lu, C.-S., Chen, Y.-C., & Pei, S.-C. (2018). A secure compressive sensing-based data gathering system via cloud assistance. *IEEE Access*, *6*, 31840-31853. <https://doi.org/10.1109/ACCESS.2018.2844184>
- [20] Jabor, M. S., Azez, A. S., Campelo, J. C., & Bonastre Pina, A. (2023). New approach to improve power consumption associated with blockchain in WSNs. *Plos one*, *18*(5), e0285924. <https://doi.org/10.1371/journal.pone.0285924>
- [21] Javaid, N. (2022). A secure and efficient trust model for wireless sensor IoTs using blockchain. *IEEE Access*, *10*, 4568-4579. <https://doi.org/10.1109/ACCESS.2022.3140401>

- [22] Kavitha, T., & Sridharan, D. (2010). Security vulnerabilities in wireless sensor networks: A survey. *Journal of Information Assurance and Security*, 5(1), 31-44.
- [23] Khan, A. U., Javaid, N., & Othman, J. B. (2021, September). A secure authentication and data sharing scheme for wireless sensor networks based on blockchain. In *2021 IEEE Symposium on Computers and Communications (ISCC)* (pp. 1-5). IEEE. <https://doi.org/10.1109/ISCC53001.2021.9631439>
- [24] Kim, T. H., Goyat, R., Rai, M. K., Kumar, G., Buchanan, W. J., Saha, R., & Thomas, R. (2019). A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks. *IEEE Access*, 7, 184133-184144. <https://doi.org/10.1109/ACCESS.2019.2960609>
- [25] Kuldeep, G., & Zhang, Q. (2020, May). Revisiting compressive sensing based encryption schemes for IoT. In *2020 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1-6). IEEE. <https://doi.org/10.1109/WCNC45663.2020.9120785>
- [26] Lara-Niño, C. A., Morales-Sandoval, M., & Díaz-Pérez, A. (2018). Small lightweight hash functions in FPGA. In *2018 IEEE 9th Latin American Symposium on Circuits & Systems (LASCAS)* (pp. 1-4). IEEE. <https://doi.org/10.1109/LASCAS.2018.8399948>
- [27] Li, W., Tug, S., Meng, W., & Wang, Y. (2019). Designing collaborative blockchained signature-based intrusion detection in IoT environments. *Future Generation Computer Systems*, 96, 481-489. <https://doi.org/10.1016/j.future.2019.02.064>
- [28] Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017, June). Blockchain based data integrity service framework for IoT data. In *2017 IEEE International Conference on Web Services (ICWS)* (pp. 468-475). IEEE. <https://doi.org/10.1109/ICWS.2017.54>
- [29] Liu, G., Zhao, H., Fan, F., Liu, G., Xu, Q., & Nazir, S. (2022). An enhanced intrusion detection model based on improved kNN in WSNs. *Sensors*, 22(4), 1407. <https://doi.org/10.3390/s22041407>
- [30] Mansour, R. F. (2022). Blockchain assisted clustering with intrusion detection system for industrial internet of things environment. *Expert Systems with Applications*, 207, 117995. <https://doi.org/10.1016/j.eswa.2022.117995>
- [31] Marchang, J., Ibbotson, G., & Wheway, P. (2019, April). Will blockchain technology become a reality in sensor networks? In *2019 Wireless Days (WD)* (pp. 1-4). IEEE. <https://doi.org/10.1109/WD.2019.8734268>
- [32] Mbarek, B., Ge, M., & Pitner, T. (2022). An adaptive anti-jamming system in HyperLedger-based wireless sensor networks. *Wireless Networks*, 28(2), 691-703. <https://doi.org/10.1007/s11276-022-02886-1>
- [33] Meidute-Kavaliauskiene, I., Yıldız, B., Çiğdem, Ş., & Činčikaitė, R. (2021). An integrated impact of blockchain on supply chain applications. *Logistics*, 5(2), 33. <https://doi.org/10.3390/logistics5020033>
- [34] Mishra, S., & Tyagi, A. K. (2019, December). Intrusion detection in Internet of Things (IoTs) based applications using blockchain technology. In *2019 third international conference on I-SMAC (IoT in social, mobile, analytics and cloud) (I-SMAC)* (pp. 123-128). IEEE. <https://doi.org/10.1109/I-SMAC47947.2019.9032557>
- [35] Mo, J., Hu, Z., & Shen, W. (2022). A provably secure three-factor authentication protocol based on chebyshev chaotic mapping for wireless sensor network. *IEEE Access*, 10, 12137-12152. <https://doi.org/10.1109/ACCESS.2022.3146393>
- [36] Moreau, I., & Sinclair, T. (2024). A Secure Blockchain-Enabled Framework for Healthcare Record Management and Patient Data Protection. *Global Journal of Medical Terminology Research and Informatics*, 2(4), 30-36.
- [37] Moubarak, J., Filiol, E., & Chamoun, M. (2018, April). On blockchain security and relevant attacks. In *2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)* (pp. 1-6). IEEE. <https://doi.org/10.1109/MENACOMM.2018.8371010>

- [38] Narayana, V. L., & Midhunchakkaravarthy, D. (2020, July). A time interval based blockchain model for detection of malicious nodes in manet using network block monitoring node. In *2020 Second, International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 852-857). IEEE. <https://doi.org/10.1109/ICIRCA48905.2020.9183256>
- [39] Nematillaev, O., Turdiev, K., Kenjayev, T., Kilicheva, K., Sapaev, I., Axmadaliyeva, X., Yusubov, J., & Menglikulov, U. (2025). Integrating AI-Based Information Services in Legal Systems: Opportunities and Challenges. *Indian Journal of Information Sources and Services*, *15*(2), 406–412. <https://doi.org/10.51983/ijiss-2025.IJISS.15.2.49>
- [40] Nesa, N., Ghosh, T., & Banerjee, I. (2019). Design of a chaos-based encryption scheme for sensor data using a novel logarithmic chaotic map. *Journal of Information Security and Applications*, *47*, 320-328. <https://doi.org/10.1016/j.jisa.2019.05.017>
- [41] Ofoghi, R. (2015). Technical and structural analysis of the wireless networks, safety and security analysis of wireless and cable networks. *International Academic Journal of Science and Engineering*, *2*(1), 39-44.
- [42] Ojaghloo, M., & Jannesary, A. (2015). Investigate all attacks on Mobile Wireless Networks and Finding security solutions. *International Academic Journal of Innovative Research*, *2*(11), 1-11.
- [43] Ponuma, R., & Amutha, R. J. M. T. (2019). Encryption of image data using compressive sensing and chaotic system. *Multimedia Tools and Applications*, *78*(9), 11857-11881. <https://doi.org/10.1007/s11042-018-6745-3>
- [44] Quy, V. K., Nam, V. H., Linh, D. M., & Ngoc, L. A. (2022). Routing algorithms for MANET-IoT networks: a comprehensive survey. *Wireless Personal Communications*, *125*(4), 3501-3525. <https://doi.org/10.1007/s11277-022-09722-x>
- [45] Radice, P. (2022). Blockchain Technology in China and Its Application in the Chinese Accounting Sector.
- [46] Ramasamy, L. K., KP, F. K., Imoize, A. L., Ogbemor, J. O., Kadry, S., & Rho, S. (2021). Blockchain-based wireless sensor networks for malicious node detection: A survey. *IEEE Access*, *9*, 128765-128785. <https://doi.org/10.1109/ACCESS.2021.3111923>
- [47] Rhea, B. K., Harrison, R. C., Whitney, D. A., Werner, F. T., Muscha, A. W., & Dean, R. N. (2019). Hardware implementation of chaos control using a proportional feedback controller. In V. In, P. Longhini, & A. Palacios (Eds.), *Proceedings of the 5th International Conference on Applications in Nonlinear Dynamics. Understanding Complex Systems* (pp. 163–173). Springer. https://doi.org/10.1007/978-3-030-10892-2_16
- [48] Shanthi, S., & Rajan, E. G. (2016). Comprehensive analysis of security attacks and intrusion detection system in wireless sensor networks. In *2016 2nd International Conference on Next Generation Computing Technologies (NGCT)* (pp. 426–431). IEEE. <https://doi.org/10.1109/NGCT.2016.7877454>
- [49] She, W., Liu, Q., Tian, Z., Chen, J. S., Wang, B., & Liu, W. (2019). Blockchain trust model for malicious node detection in wireless sensor networks. *IEEE Access*, *7*, 38947-38956. <https://doi.org/10.1109/ACCESS.2019.2902811>
- [50] Shin, S. J., Park, Y., & Shin, S. U. (2024). Decentralized Fair Data Trading Scheme based on mCL-ME Primitive. *Journal of Internet Services and Information Security*, *14*(4), 569-589. <https://doi.org/10.58346/JISIS.2024.I4.036>
- [51] Sudhakar, R., Rajakumari, J., Poornima, S., & Ramya, V. (2019). A Security Threats and Authentication Approaches in Wireless Sensor Networks. *International Journal of Communication and Computer Technologies (IJCCTS)*, *7*(2), 1-3.
- [52] Teh, J. S., Tan, K., & Alawida, M. (2019). A chaos-based keyed hash function based on fixed point representation. *Cluster Computing*, *22*(2), 649-660. <https://doi.org/10.1007/s10586-018-2870-z>
- [53] Wu, Q. (2015, September). A chaos-based hash function. In *2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (pp. 1-4). IEEE <https://doi.org/10.1109/CyberC.2015.13>

- [54] Wu, Z., Zhang, H., Wang, P., & Sun, Z. (2022). RTIDS: A robust transformer-based approach for intrusion detection system. *IEEE Access*, 10, 64375-64387. <https://doi.org/10.1109/ACCESS.2022.3182333>
- [55] Yang, Z., Yan, W., & Xiang, Y. (2014). On the security of compressed sensing-based signal cryptosystem. *IEEE Transactions on Emerging Topics in Computing*, 3(3), 363-371 <https://doi.org/10.1109/TETC.2014.2372151>
- [56] Zhang, P., Wang, S., Guo, K., & Wang, J. (2018). A secure data collection scheme based on compressive sensing in wireless sensor networks. *Ad Hoc Networks*, 70, 73-84. <https://doi.org/10.1016/j.adhoc.2017.11.011>
- [57] Zhang, Y., Xiang, Y., Zhang, L. Y., Rong, Y., & Guo, S. (2018). Secure wireless communications based on compressive sensing: A survey. *IEEE Communications Surveys & Tutorials*, 21(2), 1093-1111. <https://doi.org/10.1109/COMST.2018.2878943>

Authors Biography



Maytham S Jabor received a bachelor's degree in software engineering from Al-Mansour University College Iraq in 2007, and MSc.IS degree from Osmania University, India, 2012, respectively, where he is teaching in AlKafeel University. He is also a Ph.D. student of the Universitat Politècnica de València (UPV), Spain, ITACA Institute. His research interests include the Internet of Things and wireless sensor network security.



Aqeel Salman Azez received a bachelor's degree in software engineering from Al-Mansour University College Iraq in 2007, and MSc.IS degree from Osmania University, India, 2013, respectively, where he is teaching in AlKafeel University. He is also teaching in Al-Sadiq University. His research interests include the Internet of Things and wireless sensor network security