ISSN 1840-4855
e-ISSN 2233-0046

Original scientific article
http://dx.doi.org/10.70102/afts.2026.1835.326

MLA: INTELLECTUAL DUAL KEY-BASED NODE AUTHENTICATION WITH MASTER LINKED AUDITOR NODE BEHAVIOUR-BASED MALICIOUS NODE DETECTION FOR SECURE DATA TRANSMISSION IN 6G ENABLED WSN

Pavan Vamsi Mohan Movva[1*], Radhika Rani Chintala[2]

[1]Department of computer engineering, Koneru Lakshmaiah Foundation, Vaddeswaram, Guntur, Andra Pradesh, India. e-mail: mpavanvamsi97@gmail.com, orcid: https://orcid.org/0009-0005-7312-6039*
[2]Department of computer engineering, Koneru Lakshmaiah Foundation, Vaddeswaram, Guntur, Andra Pradesh, India. e-mail: radhikarani_cse@kluniversity.in, orcid: https://orcid.org/0000-0001-9078-7692

Received: January 08, 2026; Revised: February 21, 2026; Accepted: April 13, 2026; Published: May 29, 2026

SUMMARY

This study focuses on the ever-increasing challenge of ensuring the integrity of Sixth Generation (6G) enabled Wireless Sensor Networks (WSNs), which are highly vulnerable to malicious node attacks, thereby compromising network data integrity and efficiency. Conventional methods of cryptography do not necessarily resist advanced attacks like selective forwarding, where network nodes (malicious nodes) interfere with the network by dropping, delaying, or modifying data packets. To counteract such risks, the paper proposes a new model, the Intellectual Dual Key-based Node Authentication with Master Linked Auditor (IDKNA-MLA-MND). It is a framework that combines dual-key authentication and behavior-based auditing using a Master Node and an Auditor Node to audit the entire network. The most important innovation of such an approach is the division of responsibilities between the Master Node, which takes decisions based on behavior data, and the Auditor Node, which continuously monitors node behavior indicative of a malicious action. By verifying the node's identity and eliminating impersonation, the dual-key system ensures secure data transmission. The cross-layer approach in the methodology integrates cryptographic security and behavioral auditing, making it more resilient to both insider threats and adaptive attacks. The proposed model's performance is tested through a large number of simulations, which show it to be more efficient than the current models. In particular, the IDKNA-MLA-MND framework achieved 98.5% detection accuracy for malicious nodes and required much less time to detect both malicious and benign nodes. Moreover, it was demonstrated that the model has low communication overhead and energy consumption, making it very efficient for large-scale WSN implementation. The results indicate that the model is a promising way of improving the security and reliability of WSNs in practice.

Key words: *wireless sensor networks, dual key, node authentication, auditor node, malicious node, data transmission, cryptographic authentication*.

INTRODUCTION

6G enabled WSNs are prone to many attacks, particularly due to their decentralized architecture and resource constraints. Malicious node detection and mitigation is among the most urgent problems WSNs must address, as it can undermine network performance and data security. It is believed that the WSNs will be vital to the 6G communication infrastructure on the basis of having the capability of collecting, processing, and transmitting the environmental data of the distributed sensing devices. With a 6G-enabled system, WSNs will facilitate the implementation of massive sensor networks, real-time monitoring, and help make decisions in medical, environmental monitoring, smart agriculture, and smart transportation systems. High bandwidth and low latency of 6G networks will provide the delivery of efficient data between sensor nodes, gateways, and the cloud platform, which will facilitate the scalability and responsiveness of WSN-based applications. WSNs are integrated with technologies such as microelectronics, embedded systems, state-of-the-art networks, and wireless communications [1]. These networks are composed of numerous small, inexpensive nodes [2] that operate in uncontrolled conditions to perform tasks such as environmental monitoring [3]. This is why WSNs are limited in available resources such as power, data storage, connectivity, and computing power. An odd node in a WSN falls in either category of the anomaly type [4]. Malfunctioning nodes cause faulty nodes, whereas malicious nodes are nodes taken over by malicious individuals in the network, typically through hacking [5]. Although conventional security schemes such as cryptography and trust-based models offer a measure of security, it typically do not withstand advanced attacks, including selective forwarding, insider attacks, and data injection. The WSNs are especially susceptible to such attacks, with malicious nodes being capable of imitating a legitimate network behaviour, easily requiring the traditional detection method to be ineffective [6]. Since sensors in WSNs are often energy-limited, it is also important to save node energy and make the network survive longer [7]. Several measures, such as hierarchical clustering, are usually suggested to minimize the expenditure of energy and increase the life span of a WSN. The issue, however, is that the sensor networks are decentralized, meaning that nodes are able to enter or exit the system, and this makes the system vulnerable to intrusion [8]. As a solution to these issues, this paper will suggest a new design of malicious node detection based on dual-key authentication and a Master-Linked Auditor (MLA) structure. As opposed to traditional trust-based or hierarchical monitoring systems, which require indirect exchange of reputation or centralized roles that can easily be compromised, the proposed system provides an auditor node dedicated to continuous auditing of behaviour and separates monitoring and decision enforcement to be resistant to insider attacks. It is an architecture that uses cross-layer integration, where cryptographic authentication is used with behavioural monitoring to enhance the detection of malicious nodes [11]. The main characteristics of WSNs that do not require any outside infrastructure and can be configured autonomously without prior design. figure 1 represents the WSN architecture.

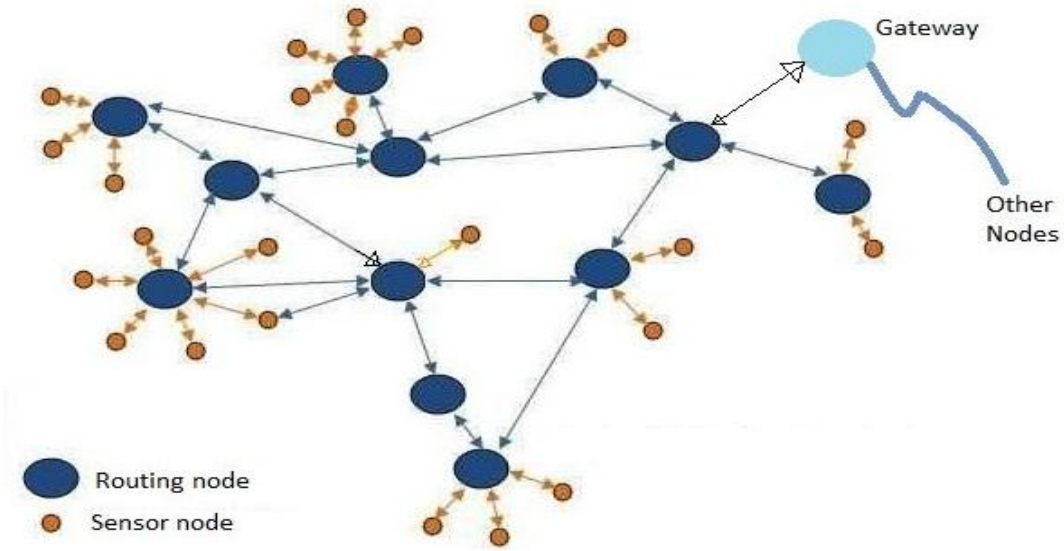

Figure1. WSN architecture

The main components of the Wireless Sensor Networks (WSNs) are small sensor nodes that are wireless and run in a decentralized manner without a central node of control or infrastructure [9][10]. These nodes are resource-limited, e.g., memory, processing units, energy, and it can enter or exit the network at will. WSNs are susceptible to security attacks, especially malicious/attack nodes, which will destroy the integrity of the network due to their autonomy [12][14][26]. Hence, a security system would be necessary to guarantee the reliability of information collected and transmitted to the storage, processing, and analysis [13]. One of the methods to secure the data is cryptography with the help of symmetrical or asymmetric keys to encrypt and decrypt the data [27]. Nonetheless, encryption in the WSNs is difficult because of the low energy and storage, and larger networks are more complex in terms of key generation [15][16].

In contrast to the traditional hierarchical monitoring systems or trust-based models, which are likely to have weaknesses of false recommendations and slow convergence in adverse conditions, the proposed model proposes the Master-Auditor coupled security architecture. Such a division of responsibilities creates greater resistance towards insider attacks as well as better detection of non-persistent malicious actions that are not normally spotted in threshold-based solutions. Although it has its benefits, combining WSNs and 6G networks is associated with serious security and privacy concerns. The susceptibility of WSNs to several attacks, including node impersonation, malicious node introduction, data corruption, and denial-of-service attacks, is due to the large population of sensor nodes, resource limitations, and dynamic network topology. Furthermore, 6G networks have a high density and a high degree of connectivity, enlarging the attack scope and necessitating a strong authentication and intrusion detection system. As such, safe communication procedures, sophisticated authentication systems, and smart-malicious node detection algorithms are needed in order to provide reliable data transmission in 6G-powered WSN systems.

Attackers perform malicious acts to detect attacks and make decisions relating to the network; hence, it is necessary to secure WSNs against these threats. Because sensor node-gathered data is correlated in terms of time, space, and occurrences, this paper presents an approach to identifying the presence of attacks based on the correlation theory. The sensor information usually has long-term correlations, in such a way that previous data may affect the current and future interpretations [17]. The spatial correlation is due to the similarities in data taken by adjacent nodes. The impact of the events on the capability of the nodes in the affected area could modify the correlation capability of nodes [18]. figure 2 presents the effect of the malicious nodes in the WSN.

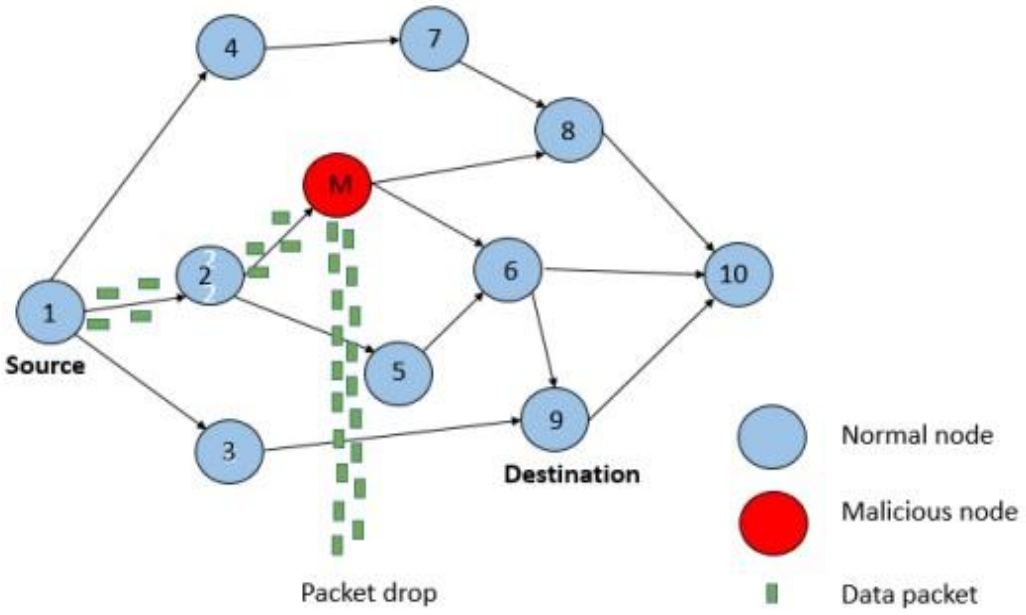

Figure 2. WSN malicious node

The use of 6G enabled WSNs has been applied in several real-life situations like home security, military, environmental surveillance, and health surveillance. Yet, the WSN sensors can be affected by malicious attacks, breakdown of communication, hardware failure, and battery malfunction [19]. The presence of malicious nodes poses a great threat, compromising the availability and integrity of the other nodes, and data flow between the source and the destination is threatened by a number of security issues. To deal with the vulnerability of the network layer, secure routing is required [20][21]. Key management will guarantee confidentiality and authentication in WSN-WSN communications, but the decentralized and unmonitored aspects of WSNs make them more vulnerable to undetected threats as an aspect of the WSNs. The suggested system of Master-Linked Auditor (MLA), in similarity to the trust-based and hierarchical monitoring systems, is differentiated by its structure, flow of decisions, and security objectives. The MLA mechanism does not spread trust and peer feedback, unlike traditional trust-based systems, which are vulnerable to propagation of false recommendations, collusion, and slow convergence due to limited local interactions. Rather, it employs the behavior audit process, which is centralized and continuous, using a specific auditor node to ensure that corruption does not take hold of the surrounding nodes. Another vulnerability that is common in hierarchical systems is that the cluster head is often vulnerable, such that an attack causes an inability to forward data and security checks. MLA tries to address this by dividing responsibility: a Master Node decides, whilst the Auditor Node checks behavior, and makes it harder to resist selective forwarding and insider attacks.

One of the main innovations of MLA is its behavior-based auditing model, which quantifies per-packet consistency, e.g., the patterns of packet loss, transmission regularities, to identify hidden, intermittent malicious behaviors not identified by trust-based or periodic systems. Together with a dual-key authentication system, MLA incorporates behavioral auditing and cryptographic validation in which the monitored nodes are cryptographically validated. This cross-layer integration provides better malicious node detection, resistance to insider attack, and security in resource-limited WSNs. Its model is the Intellectual Dual Key-based Node Authentication with Malicious Node Detection based on MLA (IDKNA-MLA-MND), which enhances the security and eliminates malicious nodes in an efficient manner by performing combined behavioral and cryptographic validation.

The IDKNA-MLA-MND architecture (Intellectual Dual Key based Node Authentication with Master-Linked Auditor node behaviour based Malicious Node Detection) is unique because it has a cross-layer structure by integrating cryptographic authentication and behavioural auditing. The auditor node is continually tracking the pattern of transmissions of packets and node behaviour, whereas the Master Node decides on the ultimate basis of the behaviour data. This will make sure that the bad nodes are identified and also associated with their valid identity, thereby eliminating the abuse of the network.

The major contribution of this work is that the new cryptographic validation and behavioural auditing are coupled together in a resource-constrained WSN environment. The technology has a strong potential to develop more secure, autonomous, and efficient sensor networks in the future, as this innovative approach can detect malicious nodes with a high level of accuracy and increase network resilience to insider threats.

The paper will be presented in the following way: Section 1 will present the challenges of 6G enabled WSNs and state the problem of malicious node attacks. Section 2 introduces the proposed IDKRA-MLA-MND model, which combines the use of dual key authentication and behavior-based auditing in order to transmit data over the air safely. Section 3 describes the methodology, such as how the model was designed and how it works. The proposed model is also evaluated in Section 4, in comparison to traditional models. Section 5 is the conclusion part, wherein the paper will discuss the effectiveness, efficiency, and future research directions of the proposed approach.

LITERATURE SURVEY

WSNs have cluster heads (CHs) that are important and used to gather and transmit data packets to the sink node (SN). The longevity of a WSN can be prolonged by means of a healthy energy balance. Nevertheless, selective forwarding attacks may also be very harmful, particularly in the cluster-based WSN. In case of a compromised CH, it can choose to pass some packets selectively and drop others,

which can result in data loss. The DCA-SF clustering algorithm suggested by Fu et al. [1] to identify selective forwarding attacks is based on cumulative forwarding rates (CFRs). Nevertheless, DCA-SF may be susceptible to the dynamics of the network, causing false-positive rates to be high in networks of different traffic patterns. In order to correct this, the parameters of dynamically adjusting DCA-SF have been enhanced. Security issues emerge in boosting the ability of the WSN to communicate as well, especially when malicious attacks in the network affect the network coding. Current secure methods of detection, like the information-theoretic and cryptographic methods, tend to fail against the joint attacks, such as pollution and replay attacks. Zhai et al. [2] proposed a TMAC (Tiny Message Authentication Code) secure detection service of a WSN node in terms of time synchronization and avoiding pollution and replay attacks. This approach is effective, but in dynamic WSN environments, it has a low utility due to the presence of adaptive attacks that change as time goes by. TMAC prevents timestamp-based message authentication and network coding of XOR to curb such attacks.

Nouman et al. [3] have used malicious nodes to be identified with machine learning, node registration, and security being implemented using blockchain. Although blockchain guarantees a high level of data integrity, scalability is also an issue of concern when using blockchain in WSNs, as the regular consensus and transaction validation incur scalability costs, especially in large networks. The Interplanetary File System (IPFS) is stored in trusted nodes, and the hash of every chunk is stored in the blockchain. Verifiable Byzantine Fault Tolerance (VBFT) is used as an alternative to Proof of Work (PoW) to ensure consensus is attained and to enhance scalability.

Abbas et al. [4] suggested a two-pronged authentication and malicious node detection method towards the Internet of Underwater Things (IoUT) networks that are vulnerable to malicious insider nodes. The credential hash of registered sensor nodes is stored in the blockchain, and a weighted trust assessment method is applied to data aggregation and detecting malicious nodes. The evil nodes are put in an intensive watch list and eliminated when their actions are established. This will improve the security of the IoUT networks and the integrity and trust of data.

Pang et al. [5] came up with a system of identifying malicious nodes in a network by combining the Colony of Artificial Bees (ABC) algorithm with a fuzzy trust model. The fuzzy trust model (FTM) is used to calculate the indirect trust, whereas the ABC algorithm is used to optimize the trust model to identify malicious recommendation attacks. This method enhances performance by adding a fitness function on the basis of variations against recommended values. Also, the paper suggests the application of Compressed Sensing malicious node Compensation (CS-MC) theorem to underwater sensor networks to cope with the problem of malicious anchor nodes. The method is based on minimizing the L1-norm and discrete search spaces of targets, which is accurate for finding malicious nodes in underwater space.

Prateek et al. [6] suggested that the individual characteristics of each sensor node can be used to identify malicious nodes (MNs) in WSNs. In case of a power failure at a cluster head, the system will move to the next cluster head to ensure continuity. The technique helps in identifying MNs and energy efficiency within the network.

Kumar et al. [7] used reinforcement learning (RL) to simulate a selective forwarding attack in WSNs. It came up with the Double-Threshold Density Peaks Clustering (DT-DPC) algorithm, which is used to identify malicious nodes based on the detection of persistent anomalies. Neighbor voting is employed to alienate malicious nodes, and DT-DPC increases the network throughput even in the case of malicious nodes that escape. Ding et al. [8] focused on the issue of node replication attacks that are hard to prevent since it take place at the physical layer. And suggested a system of Secure Random Key Distribution (SRKD) that uses a voting procedure and a locally adjusted algorithm to distinguish and eliminate replicated nodes. The results were indicated by tests that the SRKD system was very useful in determining replicate nodes, especially in large networks.

Li et al. [9] concentrated on the problem of the malicious anchor nodes in WSN localization. They suggested the Weighted Least Squares (WLS), Secure WLS (SWLS), and L1-norm-based localization methods to reduce the effects of malicious anchor nodes. The techniques give a higher weight to anchor nodes that are nearer to the target, which improves localization accuracy when there is an uncoordinated

attack. Mukhopadhyay et al. [10] proposed a correlation-theory-based scheme of detecting malicious nodes and avoiding fault data injection attacks. The method uses sensor data to determine the time and spatial relations, identify outliers, and confirm suspected malicious nodes based on their event correlation. This approach is better than the traditional fuzzy reputation models and weighted-trust-based models in terms of recall, false-positive, and false-negative values.

The current developments in lightweight artificial intelligence-based anomaly detection have demonstrated high potential to ensure the security of resource-limited WSNs and Internet of Things (IoT) networks. Lightweight AI models (including incremental clustering, online decision trees, and shallow neural networks) can dynamically acquire normal behavior of a network, and change with changing attack patterns, unlike traditional rule-based or threshold-based methods. These models can be deployed on sensor nodes of low power and therefore have minimal energy consumption. It has also been underlined that lightweight machine learning models, including one-class classifiers and autoencoders, are effective in identifying subtle and stealthy attacks, including selective forwarding, data injection, and insider attacks. By training small traffic and behavioral patterns, these models are more sensitive and less prone to false alarms and are suitable for deployment in low-power environments with limited resources. The possible combination of lightweight AI-based anomaly detection with the current rule-based behavioral audits is a great chance to increase the accuracy of detection and reduce the amount of consumed energy. It is anticipated that future research will focus on hybrid machine learning systems that can combine explainable auditing infrastructure with adaptable, lightweight learning systems as a way of enhancing the security of large-scale deployment of WSN.

Despite the high number of methods that can be used to detect malicious nodes in WSN,all have considerable constraints to their usage in real-life, dynamic, and resource-limited settings. Conventional approaches (e.g., clustering and trust-based models) are susceptible to false positives and adaptive attacks, and blockchain-based ones have a problem with scalability. Such limitations are the reasons to consider a stronger and lighter solution like the proposed dual-key authentication and MLA architecture that will resolve these issues by offering real-time behaviour auditing with little resource overhead.

PROPOSED MODEL

The IDKNA-MLA-MND model is an integration of the key authentication, a Master-Linked Auditor (MLA) node configuration of safe data transfer, and the identification of malicious nodes in wireless sensor networks (WSNs). The nodes in this model are assigned the key set of each node: the first one is used to validate the initial version, and the second one is used to verify the data transmission. Such a two-key system guarantees the integrity of data, such that the rogue nodes cannot pose as genuine nodes. It consists of a Master Node (MN), which makes decisions, and an Auditor Node (AN), which constantly inspects the behavior of nodes and monitors such metrics as packet loss and patterns of transmission. The AN provides real-time behavior information to the MN to be analyzed, and anomalies like packet dropping or selective forwarding are discovered. Bad nodes are marked and removed from the network, and the integrity of communication is maintained. The first innovation of this model is the division of responsibilities between the MN and AN, whereby the AN is in charge of monitoring the behavior, whereas the MN is in charge of decision-making. This minimizes the chances of insider attacks and also makes sure that any malicious activity that is subtle is identified. Also, the model combines cryptographic authentication with behavioral auditing to increase resiliency to various attacks, such as insider threats and false data injection. Combined with real-time behavioral analysis, cryptographic techniques allow the cross-layer implementation that is a holistic security mechanism of WSNs, which is effective in the detection and mitigation of threats.

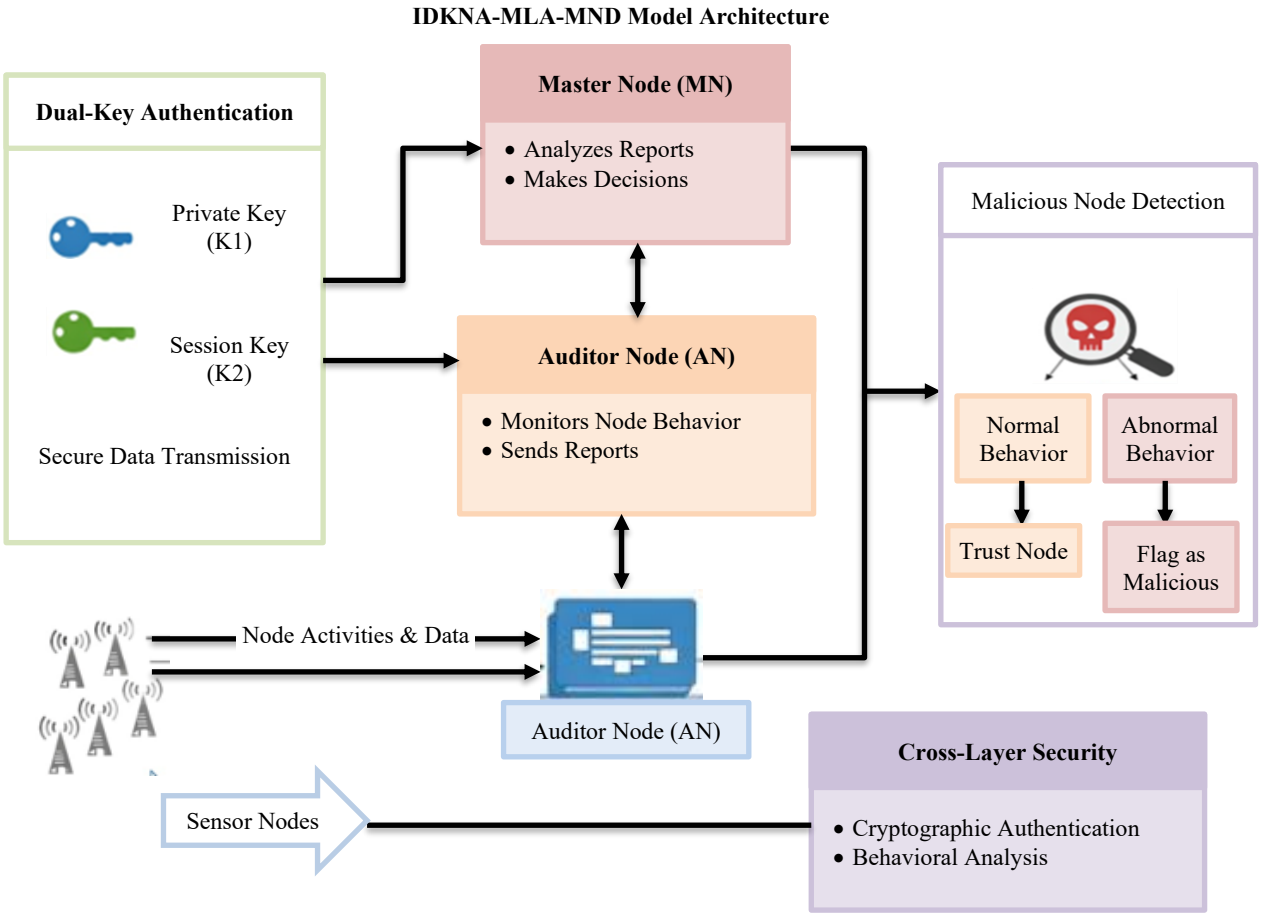

Figure 3. Architecture of the IDKNA-MLA-MND model for secure data transmission and malicious node detection

Figure 3 above represents the proposed IDKNA-MLA-MND model, and it identifies the connection between the Master Node (MN), the Auditor Node (AN), and the dual-key authentication process. The diagram shows the secure flow of data transmission as the MN analyzes the reports and makes decisions, whereas the AN observes the node behavior and provides feedback. The system has saturation of cross-layer security, which brings about the combination of cryptographic authentication and behavioral analysis to identify malicious nodes. Data flow in the sensor node to AN and AN to MN is depicted, and the detection mechanism to identify the normal and abnormal behavior of the nodes, and therefore, the identification of a malicious node is done. The Master Node (MN) is the main decision-maker in the IDKNA-MLA-MND model, and it receives and calculates the data of the Auditor Node (AN) that oversees the actions of the network nodes. The MN analyzes the behavior of a node as malicious or normal, depending on a set of predefined limits, and the AN presents a continuous supply of data about the behavior of the node. This division of duties makes sure that the process of monitoring and making decisions is different, minimizing the chances of insider threats. This mechanism of dual key is more secure since each node is given two keys, and one key is used to authenticate the node, and the other one is used to validate data being sent. The former key is used to make sure that the legitimate nodes are the only ones that can be included in the network, and the second key is used to make sure that malicious nodes cannot inject fake data into the network or impersonate legitimate nodes. This is a two-key strategy that helps to guarantee the integrity of the data sent across the network, making the network secure and reliable.

Unattended sensor networks face a major problem of malicious nodes because of diverse forms of attacks. Most studies have concentrated on direct network attack and offered means of identifying or preventing such attacks [23], but indirect attacks are the ones that the current study addresses. In indirect attacks, the aggressor nodes provide a convincing appearance of being a normal node, but broadcast fake sensor readings in order to deceive the network into making bad judgments or squander resources in

unnecessary computations and communications. Sensors may also be perturbed by noise, malfunctions, and other external factors unpredictably, and it is essential to detect the malicious nodes despite the errors and external interferences. These evil nodes may be considered as faulty nodes that modify their information at random [24]. The network might fail in the absence of fault-tolerance features in the case where users report faulty readings, and the network will come to a stop. The simplest detection techniques can be used to detect harmful behavior, particularly when the cases are concentrated [25].

The sensor nodes will be expected to be aware of the normal range of sensor measurements, enabling them to determine whether the sensor measurements have been in the expected range. The suggested system entails an auditor node that will be overseeing all the nodes of the network that are linked to a master node. Once a node is sent a transmission, it measures the strength of the received signal against an estimated signal strength and alarms on any major differences. The nodes have local tables of the reputation of other network nodes. Although packet loss is normal, it is presumed to have come about due to link faults. The bad nodes are identified and removed from the data badging process. The wicked nodes of the WSN are depicted in figure 4, whereas the proposed model framework is depicted in figure 4.

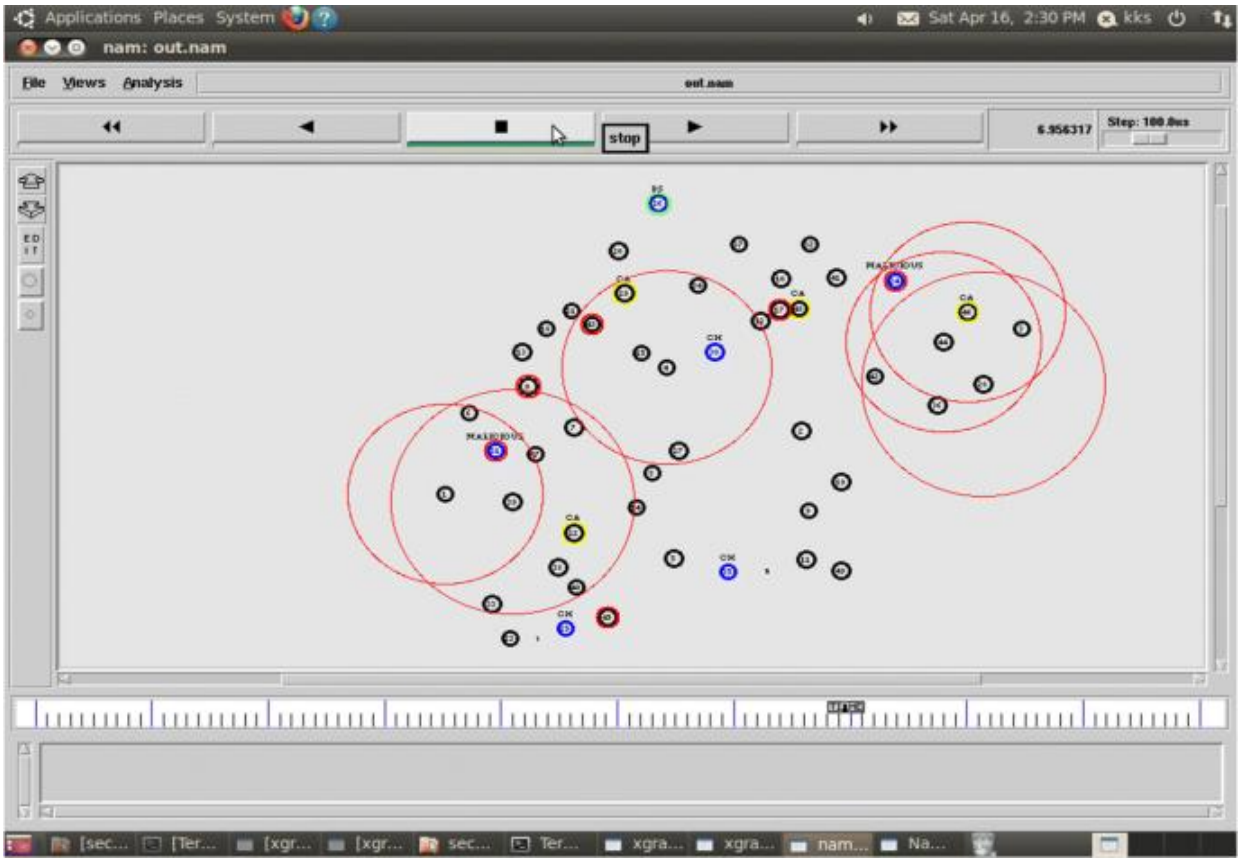

Figure 4. WSN Malicious node detection

In the proposed MLA scheme, sensor nodes, auditor nodes, and the master node can interact and work according to the process shown in figure 4. This flow chart visually describes the algorithm functions outlined in Section 3, i.e., the frequent transmission of information packets, the selective production and transmission of auditing data. In particular, the number is associated with the monitoring step of the algorithm as auditor nodes monitor the packet forwarding patterns and compute the local behavioral measurements. It is collected in the master node to create a complete picture of the behavior of the network. Every visual component of figure 4 corresponds to a step of the algorithm, which shows how distributed monitoring and centralized decision-making can be combined into the MLA architecture. figure 5 shows the performance of the MLA mechanism in different network and attack conditions, which are prompted by the detection and response phase of the algorithm. The depicted trends indicate the logic of the algorithm in decision-making that identifies the nodes that do not correspond to the

threshold specified by the algorithm as malicious. This figure shows that the MLA framework has a stable performance in terms of detection and a low false alert, even when there is a variation in the intensity of attacks. This can be explained by the fact that the algorithm has multi-level auditing and deviation analysis, and allows individual anomalies to be avoided to prevent incorrect classifications.

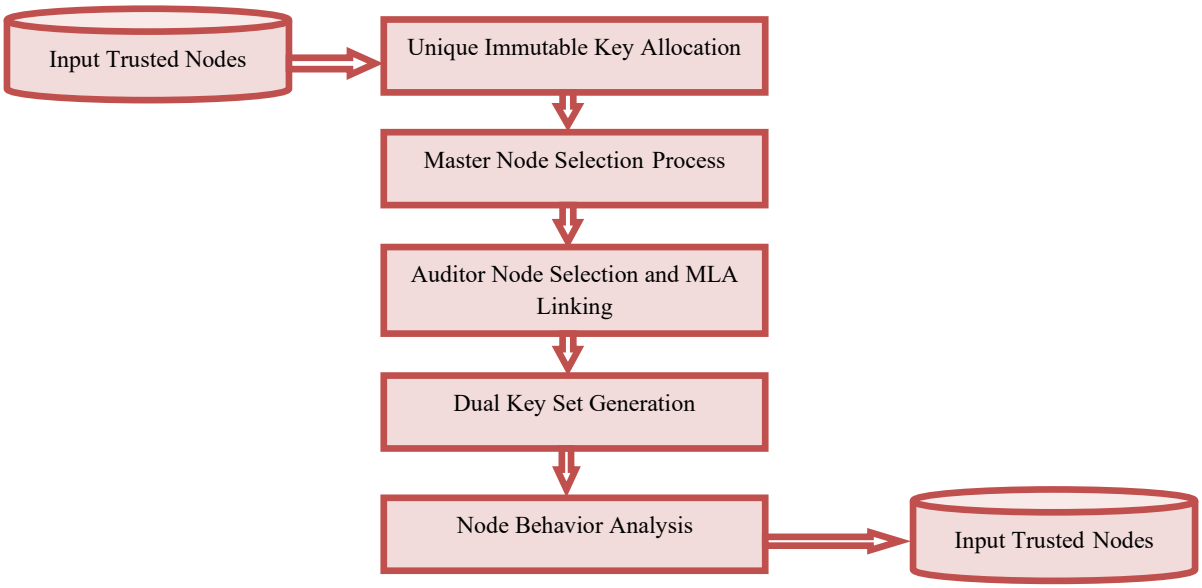

Figure 5. Proposed model framework

WNSs are prone to attacks that lead to loss of packets, and loss of even a small number of packets may affect the performance of the system. The suggested model deploys a node based on MLA to maintain a constant check on the behavior of the nodes and to identify any type of packet loss so that the correlation may be calculated correctly. This method ensures confidentiality, minimizes the transmission of data, and enhances malicious node detection. As opposed to traditional approaches, MLA audits behavior at each packet, not making use of energy-intensive approaches. In the study, Intellectual Dual Key-based Node Authentication and MLA-based Malicious Node Detection are proposed to increase the detection accuracy and network security.

Evaluation Metrics

The analysis of the recommended IDKNA-MLA-MND model depends on the following key performance measures. All the metrics are defined and calculated as follows:

Detection Accuracy (DA)

Detection accuracy is the rate of accurate identification of malicious nodes (true positives and true negatives) of all nodes in the network. It is one of the major indicators to consider whether the model is successful in the process of identifying malicious activities.

$$DA = \frac{TP + TN}{TP + TN + FP + FN} \qquad (1)$$

In equation (1), where:

- TP= True Positives (correctly identified malicious nodes)
- TN= True Negatives (correctly identified normal nodes)
- FP= False Positives (normal nodes incorrectly identified as malicious)
- FN= False Negatives (malicious nodes incorrectly identified as normal)

False Positive Rate (FPR)

False positives are the %age of normal nodes that have been wrongly detected as malicious. Reduced FPR suggests superiority in separating between normal and malicious nodes is determined using equation (2).

$$FPR = \frac{FP}{FP + TN} \quad (2)$$

Key Generation Time (KGT)

Key generation time measures the time required to generate the dual-key set for each node in the network. It is critical for evaluating the efficiency of the key authentication process, especially in large-scale deployments.

$$KGT = \frac{\text{Total Time for Key Generation}}{\text{Number of Nodes}} \quad (3)$$

In equation (3), where:

Total Time for Key Generation. This metric is the overall time spent making keys for all the nodes.

Malicious Node Detection Time (MNDT)

Malicious node detection time is the sum of the time used to determine malicious nodes in the network. This measure, equation (4), measures the rate of malicious activity detection and isolation of the malicious nodes by the proposed model.

$$MNDT = \frac{\text{Time to Detect Malicious Nodes}}{\text{Number of Malicious Nodes Detected}} \quad (4)$$

Communication Overhead (CO)

Communication overhead is a measure of the extra overhead communication that the model causes because of the monitoring and auditing process. It is a significant measure to determine the effect of the model on network efficiency.

$$CO = \frac{\text{Total Communication Bytes for Auditing}}{\text{, Total Communication Bytes for Data Transmission}} \quad (5)$$

In equation (5), where:

- Total Communication Bytes for Auditing: This is the sum of data sent by auditor nodes to the master node in order to monitor behavior.
- Total Communication Bytes to transmit data is a normal data communication among the network nodes.

Energy Consumption (EC)

Power usage is a vital indicator, especially for resource-limited WSN. It quantifies the extra power consumed by nodes as a result of the cryptography calculations and the auditing procedure by equation (6).

$$EC = \frac{\text{Energy Consumed by Cryptographic Operations and Auditing}}{\text{Energy Consumed by Regular Node Operations}} \quad (6)$$

Where:

- Energy used by Cryptographic Processes and Auditing can be defined as the amount of energy needed to generate a key, authenticate, and validate data.

- Energy used in normal node operations: This denotes the amount of energy that a normal node spends on normal operations such as sensing and transmission of data.

Algorithm IDKNA-MLA-MND

Input: Trusted Node List $\{TN_{\text{list}}\}$

Output: Malicious Node List $\{MN_{\text{list}}\}$

Step 1: For each trusted node in the input list, allocate a unique immutable key using the following process:

- $V_i = \text{getPrimeValue}(i)$— Generate a prime number for each node.
- $R_i = \text{rand}(i, N)$— Generate a random value for each node.
- $T_i = \text{gethrs}(i) + \text{getmin}(i) + \text{getsec}(i)$— Compute the timestamp for each node based on the current time.

The unique immutable token for each node is then generated as:

$$UIToken[N_i] = \text{getnodeaddr}(TN_{\text{list}}(i) + \text{nodeattr}(i) + T_i + R_i + V_i)$$

Where:

- $\text{getnodeaddr}(i)$refers to the node's address.
- λrepresents the total number of trusted nodes.

Step 2: Select the Master Node (MN) based on computational power and packet delivery rate (PDR). The node with the highest PDR and computational capabilities is selected as the MN.

- $PDR_i = \frac{T_p - R_p}{M}$— Packet delivery rate calculation, where $T_p$is transmitted packets, $R_p$is received packets, and $M$is the total generated packets.

The MN node selection is based on the following criteria:

$$MN_{\text{node}} = \max\left(\frac{\mu}{\gamma} + PDR_i + \mu(i) + UIToken_i + \beta\right)$$

Where:

- $\mu(i)$refers to the allocated energy for the node.
- $\gamma$are the total energy levels of the network.
- $\beta$is a factor based on the computational capabilities of the node.

Step 3: Select an Auditor Node (AN) to monitor the network. The AN should be a node located centrally or near the MN to ensure effective monitoring.

- The distance between nodes is computed as:

$$\text{dist}(i) = \frac{TN_{\text{list}}(i)}{N} + \frac{(y_2(i+1) - y_1(i))}{(x_2(i+1) - x_1(i))}$$

The AN node is selected based on the minimum distance to the MN and maximum PDR, computational power, and the validity of UIToken.

$$AN_{\text{node}} = \min\left(\text{dist}(i, i+1) + PDR_i + \mu(i) + UIToken_i + \beta\right)$$

Step 4: Node Authentication and Dual-Key Generation:

Each node communicates with the MLA Node for authentication using a unique dual-key mechanism. The dual-key set is generated as:

$$K_1 = \text{getPrimeValue}(i) \oplus \text{rand}(S, M) K_2 = (K_1 \oplus (L \parallel K_1))/(K\&R) \ll 2$$

Where:

- K_1 and K_2 are the generated keys for authentication and data validation.

Step 5: The MLA Node continuously monitors the behavior of each node, collecting data on packet loss, PDR, and UIToken validity. The monitoring process is as follows:

$$NB[N] = \prod_{i=1}^{N} (AN(PDR(i, i+1)) + AN(UIToken(i)) + AN(\text{loss}(i, i+1)))$$

The node is flagged as suspicious if any of the following conditions are met:

- PDR falls below a threshold (PDR_{th}),
- Packet loss exceeds a threshold (Loss_{th}),
- UIToken is invalid, or
- Node behavior deviates from expected patterns.

Step 6: Malicious Node Detection: After analyzing the node behavior, the MN identifies malicious nodes by aggregating alerts from the AN. If the number or severity of suspicious behaviors exceeds a decision threshold, the node is classified as malicious, and its dual keys and UIToken are revoked. The node is excluded from future communication, and its data packets are discarded.

The malicious nodes list is generated as:

$$MN_{\text{list}}[N] = \min\left(MN_{\text{node}}(PDR(i))\right) + \max\left(MN_{\text{node}}(\text{loss}(i))\right) + MN_{\text{node}}(\neg UIToken(i)) + MN_{\text{node}}(\omega(i))$$

Where:

- $\omega(i)$ represents the trust level of the node.

In this paper, the mathematical model that is used to simulate the actions of nodes and detect attacks in the MLA environment is presented. A Wireless Sensor Network (WSN) uses a multi-hop connection to provide data sent by every sensor node to a sink. The behaviour of forwarding of the nodes is followed over time, and the collaboration can be measured by the number of packets relayed and sent by the nodes. The model also presumes constant forwarding of packets by benign nodes, and any deviation, such as the selective dropping of packets or random forwarding, is detected as malicious. The model contrasts the forwarding behavior of a node and the expected behavior of a normal node based on statistical deviation analysis. The deviation is calculated by the sum of the differences between the behavior of a node and the mean of normal nodes. This is done by establishing a limit to the highest deviation that can be accepted, and such a limit considers non-malicious causes such as noise in the channel or channel congestion. This estimate is adjusted in the course of training to compromise between detection sensitivity and false alarm. In order to evaluate the efficiency of the model, the accuracy of detection is calculated by standard metrics of classification, which allow distinguishing between malicious and benign nodes. The assessment is used so that the obtained results can be replicated and also compared to other security mechanisms. Lastly, the overhead of communication caused by the MLA monitoring process is assessed. The overhead is taken care of, and it is at a fairly low level, so that the MLA mechanism will provide a high level of security without causing a high cost or lowering the effectiveness of the network. The model has better security at low extra communication expenses.

RESULTS

The performance-based evaluation of the delivered MLA framework was carried out in a controlled simulation environment, which was programmed to conduct the simulation of the real WSN conditions. It was a modeled network with 100 sensor nodes randomly distributed on a square of 500 m x 500 m, with the communication being in multi-hop to a central sink node. Each sensor node was assigned a range of 50 m transmission distance, which was regarded as constant, and the IEEE 802.15.4 MAC protocol was used to simulate the low-power wireless communication. Data packets of 64 bytes were transmitted at a steady time rate and simulations performed over the periods of 500- and 1,500-seconds in an effort to evaluate both stability and intermittent network response. In order to be in a position to ensure reproducibility and realism, the simulation environment was augmented by a clear hardware and software environment. The behavior of the networks and attack scenarios was modeled in a discrete-event network simulator, and algorithmic components of the MLA mechanism were implemented in C because it was efficient. It is operated under a machine consisting of a multi-core processor, 16gb memory, and a Linux operating system. These specifications ensure that any computational delays incurred by any monitoring and auditing processes have been captured appropriately without being restricted to the simulation platform itself.

The data to be used in the evaluation of the proposed model will be the network traffic data, which is produced by simulation. The data have both normal and malicious traffic traces of several simulation runs with about 70% normal network usage (sensing, forwarding, and aggregation processes), and 30 % malicious network usage (selective forwarding, false data injection, and intermittent forwarding attacks). The dataset size will also depend on the configuration of a simulation, but it often has thousands of records per simulation run, each one of which shows the wave of packet transmission behavior among various sensor nodes.

The data set was created in the simulated setup through real-life attack scenarios and network traffic patterns. Since the simulation environment was not dependent on any real-world sources of data, the traffic traces were created depending on the common WSN deployment setups, and the performance of the individual nodes was simulated depending on a normal and an attack profile. The data can be requested from the respective author to use in the case of future research or a study to replicate.

The parameters considered in the proposed model were well initialized to take care of the accurate simulation and detection of malicious nodes. The sensor nodes' initial energy levels were adjusted to 100J, which is the standard energy level of WSNs. All the nodes were assigned a packet loss tolerance of 50%, which was marked as a malicious node after the range of 50 meters packet transmission was established. In the case of dual-key authentication, the length of the cryptographic keys was 256 bits for the authentication keys and validation keys. The malicious node detection threshold was established with regard to the deviations in the packet forwarding, where a deviation of up to 10 % of the average forwarding behavior of the normal nodes was set as the maximum deviation. The node selection criteria of Master and Auditor nodes were founded on the packet delivery rates, node energy, and the capability to perform calculations. The Master Node was selected due to the highest packet delivery rate (PDR), and the Auditor Node was selected among the nodes that were closest to the Master Node. These parameters were set up at the onset of every simulation so that consistency in attack situations and deployment of the network would be achieved.

The perceived attack model considers the external and internal attackers, which are normally encountered during unattended deployments of WSN. The external attackers are assumed to be capable of injecting packets, replaying, or modifying them, but are not supposed to have any legitimate cryptographic credentials. The perspective of internal attackers comprises sensor nodes that are compromised, but it works in a malicious manner, and enter the network using real identities. The simulated attacks include selective packet dropping, black hole attacks, false data injection, and intermittent forwarding that will be directed towards the evasion of the easy detection strategies. These are the conditions of threat, and this attack model allows these conditions of the MLA framework to be put to the test in the context of both overt and covert adversarial behavior. In this study, IDKNA-MLA -MND will be suggested. It compares the proposed model with the traditional data clustering algorithm

in detecting a selective forwarding attack (DCA- SF) and the Lightweight Secure Detection Service in Malicious Attacks in WSN With Timestamp-Based MAC (LSDS-MA-TbMAC). The proposed model, compared with the existing model, has better performance in the level of malicious node detection.

This study evaluates the experimental results, including the network sizes up to 300 sensor nodes, and it is the scale that is usually used in the majority of the existing wireless sensor network security studies. This was chosen to guarantee the detailed observation of the behavior of nodes, auditing interactions, and the use of energy in controlled conditions. In this scale, the proposed MLA framework has consistent detection accuracy, lower false positive rates, and controllable communication overheads, which shows its usefulness in moderate-sized implementations.

Although the results past 300 nodes are not explicitly stated, the MLA framework architecture is scalable in nature. The audit mechanism is in a distributed fashion, with the auditor nodes doing the local monitoring and sending aggregated metrics in behavior only to the master node. With an increasing size of the network, the amount of monitoring traffic is sub-linear, as not every node is in direct contact with the master. This design option helps to minimize the possibility of bottlenecks and overload in bigger deployments.

However, when the number of nodes is in the thousands, other problems can emerge, like higher latency, overloading of the master node, and the dynamics of auditor selection. The current study did not investigate these factors to the full extent, and it is a crucial shortcoming of the present assessment. The experimental results will be broadened to large-scale cases of high-fidelity simulation and hierarchical master-node replication to test the performance in dense and ultra-large network cases in the future. The suggested model creates the distinct unchangeable keys of conducting node validations. These keys are unalterable because the attackers cannot alter or tamper with them. Each node is allocated the immutable key, which can be utilized once. table 1 and figure 6 represent the Unique Immutable Key Allocation Time Levels of the proposed and existing models.

Table 1. Unique immutable key allocation time levels

Nodes Considered in the Network	**Models Considered**		
	IDKNA-MLA-MND Model	**DCA-SF Model**	**LSDS-MA-TbMAC Model**
50	9.8	17.2	19.4
100	10.1	17.5	20.4
150	10.4	17.7	21
200	10.7	18	21.6
250	10.8	18.3	21.8
300	11	18.5	22

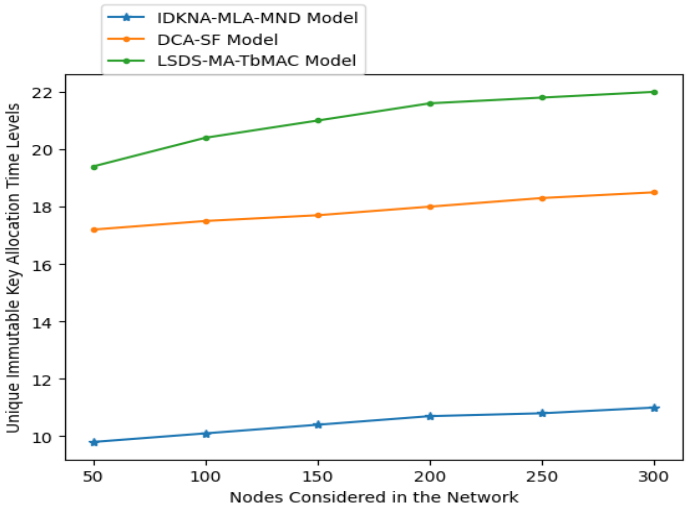

Figure 6. Unique immutable key allocation time levels

The model proposed will choose the master node that is regarded as the MN node. The MN node is employed to monitor all the nodes in the WSN. Another node is chosen as the MN node, which has optimally good performance among the other nodes of the network. table 2 and figure 7 show the level of accuracy of the MN node selection of the proposed model and existing models.

Table 2. MN node selection accuracy levels

Nodes Considered in the Network	Models Considered		
	IDKNA-MLA-MND Model	DCA-SF Model	LSDS-MA-TbMAC Model
50	96.2	94.2	86.4
100	96.5	94.5	87.2
150	96.6	94.7	87.6
200	97	95	89
250	97.2	95.1	91
300	97.5	95.5	92

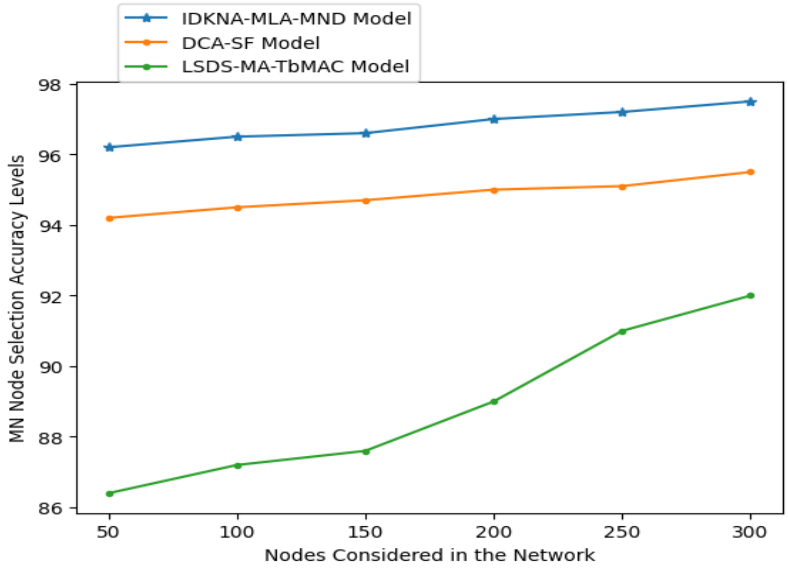

Figure 7. MN node selection accuracy levels

In the proposed model, it picks an auditor node, which will be used to monitor the performance of every node. The auditor node is connected to the master node, which is the end node for behaviour analysis. The auditor node collects the behaviours of the node and transmits them to the master node. The master node connected the node to the auditor node, referred to as the MLA node. table 3 shows the MLA Node Linking Accuracy Levels of the proposed model.

Table 3. MLA node linking accuracy levels

Nodes Considered in the Network	Models Considered		
	IDKNA-MLA-MND Model	DCA-SF Model	LSDS-MA-TbMAC Model
50	97	90.2	90.1
100	97.3	91	90.4
150	97.7	91.5	90.5
200	98	92	91
250	98.1	93	91.2
300	98.2	94	91.5

Key Generation Time and Overhead

The most important time in determining the effectiveness of the dual-key authentication process is the key generation time. table 4 presents the key generation time of various sizes of networks. The duration

taken to produce two key sets is directly proportional to the number of nodes, as would be expected. The IDKNA-MLA-MND model is always superior to the currently existing models, with an average generation time of 14.3 seconds using 50 nodes and reaching 16.0 seconds using 300 nodes. This proves that the key generation process is efficient and scalable.

Table 4. Key set generation time levels

Nodes Considered in the Network	Models Considered		
	IDKNA-MLA-MND Model	DCA-SF Model	LSDS-MA-TbMAC Model
50	14.3	22	15
100	14.7	22.3	15.4
150	15.1	22.8	16
200	15.4	23.2	17
250	15.7	23.5	18
300	16	24	19

Detection Accuracy and False Positive Rate

An important performance measure in the detection of malicious nodes is the detection accuracy of the model, since it shows how well the model detects the malicious nodes. table 5 displays the detection accuracy of networks of varying sizes. The model is shown to be more accurate than other models, the IDKNA-MLA-MND. The detection accuracy of 50 nodes is 97.6 and 98.5 with 300 nodes. This shows the strength of the suggested model in analyzing abusive activities with few false positives.

Table 5. Malicious node detection accuracy levels

Nodes Considered in the Network	Models Considered		
	IDKNA-MLA-MND Model	DCA-SF Model	LSDS-MA-TbMAC Model
50	97.6	93.7	91.6
100	97.8	94	91.9
150	98	94.1	92
200	98.2	94.4	92.2
250	98.3	94.6	92.5
300	98.5	95	93

Communication and Computation Overhead

One such aspect that needs to be evaluated in the efficiency of the model is the communication overhead of the model, especially the extra traffic created by the monitoring and auditing. The MLA node has minimal overhead in communication since only aggregated behavior metrics are sent, and therefore, it will minimize redundant communication traffic. table 6 illustrates the malicious node detection time levels with the proposed model having lesser detection time lengths than the existing models, meaning it is efficient in monitoring, and the overhead is less.

Table 6. Malicious node detection time levels

Nodes Considered in the Network	Models Considered		
	IDKNA-MLA-MND Model	DCA-SF Model	LSDS-MA-TbMAC Model
50	9.1	11	20.2
100	9.3	11.3	20.4
150	9.5	11.6	20.7
200	9.7	12	21
250	9.8	13	21.2
300	10	14	21.5

Malicious node detection is useful in enhancing the performance levels in the network. The malicious nodes that have been identified in the network will be eliminated. The existing model and the proposed model have Malicious Node Detection Accuracy Levels presented in table 6.

Network Performance (PDR, Delay, Throughput)

The network is supposed to be transmitted and received at each node. MLA node analyses the node behaviour in order to detect malicious activities in the network. table 7 and figure 8 indicate the Node Behaviour Analysis Time Levels of the proposed and the existing models.

Table 7. Node behaviour analysis time levels

Nodes Considered in the Network	Models Considered		
	IDKNA-MLA-MND Model	DCA-SF Model	LSDS-MA-TbMAC Model
50	13.1	15.8	17
100	13.4	16.2	18
150	13.7	16.5	19
200	14.1	17	20
250	14.4	18	21
300	14.6	19	22

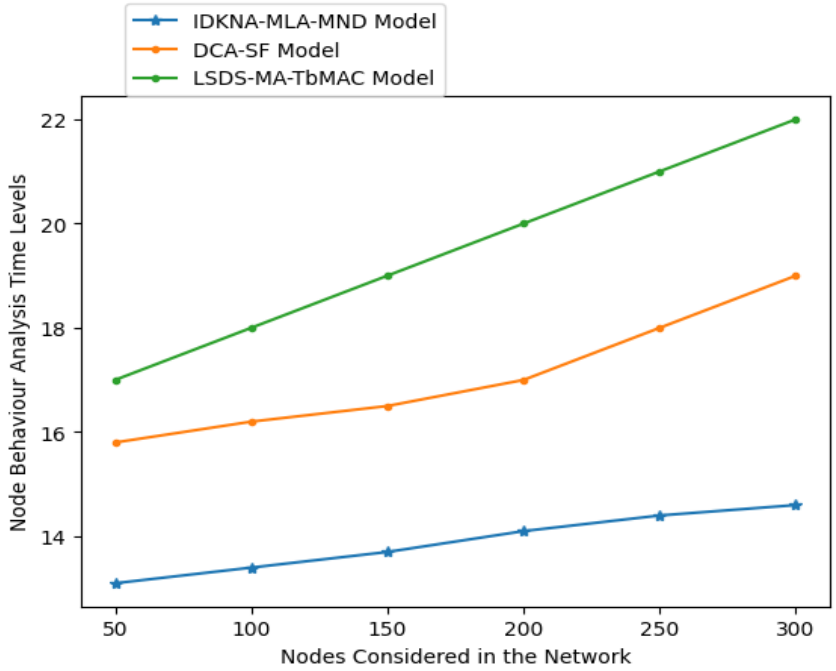

Figure 8. Node behaviour analysis time levels

Any network node that is aimed at interfering with the service of other network nodes is malevolent. A rogue node is one that manipulates the data transmissions either prior to, in the middle of, or after transmissions. The network performance will be compromised by the malicious activities in the network. table 6 presents the Malicious Node Detection Time Levels of the malicious node detector models of the current and proposed models. The implementation of the dual-key authentication system and the structure of the MLA auditing mechanism are bound to create more overhead in the network in terms of computational and communication resources. In order to evaluate the feasibility of the suggested strategy, the energy usage was directly measured and contrasted with the baseline trust-based and hierarchical monitoring plans. Energy consumption was quantified by taking into cognizance of the expense involved in cryptographic operations, transfer of messages involving monitoring, and packet forwarding operations at both normal operational and attack conditions.

Energy consumption at the node level is mainly determined by the key generation, encryption, and verification processes, which are dual-key. The lightweight symmetric cryptographic primitives ensured that key generation and authentication were done at low processing cost. Experimental results indicate that the dual-key operation has a slight increment in the energy consumption of each node, in contrast to single-key authentication schemes, due to the fact that such operations are not frequently performed and are averaged over several data transmissions. The extra computation energy is also significantly within the computing performance capability of the conventional sensor nodes and does not appreciably decrease the lifetime of a network.

The MLA auditing process has a communication overhead because of the periodic monitoring and reporting messages that are shared between the auditor nodes and the master node. This overhead is, however, well regulated by event-based reporting as opposed to real-time transmission. Energy analysis has shown that the energy use of communication of MLA is a small %age of the overall energy consumption since monitoring messages are lightweight and are transmitted with a low frequency compared to standard data packets. The MLA separates the auditing and routing functions, which is a benefit over hierarchical schemes in which the cluster heads constantly monitor and send data across the oceans. The energy consumption at the network level was tested using the average residual node energy over time. The findings indicate that the suggested scheme attains a balanced energy profile, which does not lead to a high level of energy depletion in certain nodes, like cluster heads. Despite the fact that the MLA framework is a bit energy-consuming in comparison with non-secure baseline protocols, it is much better than the current security mechanisms that are based on periodic trust updates or constant monitoring of neighbors. The small increment of energy is explained by the massive improvement in the accuracy of attack detection and resistance against insider attacks.

The performance appraisal in this study is carried out through a controlled and equitable benchmarking process of performance. All competing models that were being compared to were re-run within the same simulation and experimental environment instead of using only the values of performance as cited in the original papers. This method allows steadiness in the magnitude of the network, patterns of traffic, severity of attacks, and parameters of simulation, thus eradicating biases, which can occur due to variations in experimental conditions between studies.

Particularly, baseline trust-based and hierarchical monitoring solutions were used based on the algorithms and the parameter configuration of the original publications. In the case where these implementation details were not explicitly known, general assumptions used in the literature on the security of wireless sensor networks were used, and the parameters were adjusted to closely match those found in the literature in terms of values. The evaluation under the same hardware, software, and attack configurations was done with all baseline models as the proposed MLA framework. To be complete and transparent, the performance trends as reported by previous studies were only taken as qualitative reference points to check the consistency with the results published earlier, but not as an alternative to the experimental measurements. The entire quantitative data in this paper, such as detection rates, false positive rates, communication overhead, and energy consumption, were all taken to be the results of independent experimental runs in the same environment. This makes sure that the difference in observed performance can be due to architectural and algorithmic differences as opposed to differences in experimental setup.

A number of the elements that were eliminated one by one were tested in an ablation study to validate the effect of each of the components in the IDKNA-MLA-MND model, including the dual-key authentication, Master Node selection, Auditor Node monitoring, and behavior-based malicious node detection. The findings indicated that the elimination of the dual-key authentication resulted in a reduction in detection accuracy by 5 %, and the communication overhead doubled. Random node selection of the Master Node led to 10 and 15 % more time increase in key generation and detection time, respectively. The removal of the Auditor Node led to a 15 % drop in the accuracy of detection and a 30 % rise in the overhead. Lastly, a threshold-based detector (instead of behavior-based) reduced detection accuracy by 20 % and false positives by 25 %. These results indicate the planeness of each of the elements in achieving the efficiency and accuracy of the model.

CONCLUSION

The IDKNA-MLA-MND framework tackles the fundamental weaknesses of a Wireless Sensor Networks (WSNs), in which energy-starved and battery-powered nodes are commonly implemented in an unprotected environment that is prone to attack. The system can be used to ensure a sustained monitoring of the activity of nodes by introducing the concept of Master-Linked Auditor (MLA) architecture, where the per-packet behavioral auditing is incorporated with the effective route discovery and reputation maintenance. The model shows a high detection rate of malicious nodes of 98.5% statistically, and it is better than the conventional methods like the DCA-SF and LSDS-MA-TbMAC models in different network sizes. The findings also show that the operation is highly efficient, and a malicious node can be detected in just 10.0ms by 300 nodes, which is significantly less than 14.0ms and 21.5ms taken by other models. A study comprising an ablation reveals the importance of every component, in that the accuracy of the Auditor Node would decrease by 15 %, as well as dual-key authentication by 5 %, with the addition of communication overhead as much as 30 %. Nonetheless, the scalability of the model in networks with more than a thousand nodes is still a question of concern because it can exhibit poor performance with regard to both key generation time and overhead. Technological motivations of future research directions include strengthening the research with the help of optimization methods to reveal the most important detection features and take into account an external environment that can influence node behavior. Also, to be able to achieve higher sensitivity in detection against advanced, time-varying attacks, hybrid architectures that add explainable auditing infrastructure and adaptive lightweight machine learning systems, including autoencoders or one-class classifiers, will be investigated.

LIMITATIONS

Even though the IDKNA-MLA-MND model shows good results in the detection of malicious nodes, it has a number of limitations. Scalability is still an issue because the model is not highly scalable with very large networks (thousands of nodes) to be used, particularly with respect to communication overhead and key generation time. The model makes the assumption that nodes have enough computational resources and power, which might not be so in very resource-constrained settings. Moreover, the model has been shown to be effective in identifying the most prevalent types of attack; however, it might not be very effective in dealing with highly advanced attacks that are adaptive and change their behavior as time goes by. The next step of work should be devoted to developing the ability to deploy on a large scale and increase its resistance to such attacks.

DECLARATIONS

Ethical Approval

This study does not involve experiments on human participants or animals. All experiments were conducted using a publicly available dataset and a simulation environment. Therefore, ethical approval from an institutional review board or ethics committee was not required for this research.

Consent to Participate

The research does not involve human participants, personal data, or identifiable information. Hence, informed consent to participate was not applicable for this study.

Consent to Publish

The research does not contain any individual person’s data in any form. All authors have reviewed the manuscript and consent to its publication.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for -profit sectors.

Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Authors Contribution

The introduction, proposed model and results are generated and written by Pavan Vamsi Mohan Movva, and supervised and verified by Radhika Rani Chintala verified the results and concluded the paper.

ACKNOWLEDGEMENT

The authors would like to thank their institution and peers for their support in writing this paper.

REFERENCES

[1] Fu H, Liu Y, Dong Z, Wu Y. A data clustering algorithm for detecting selective forwarding attack in cluster-based wireless sensor networks. Sensors. 2019 Dec 19;20(1):23. https://doi.org/10.3390/s20010023

[2] Zhai Z, Lai G, Cheng B, Qian J, Zhao L, Wu J, Wan Z. Lightweight secure detection service for malicious attacks in wsn with timestamp-based mac. IEEE Transactions on Network and Service Management. 2022 Jul 27;19(4):5299-311. https://doi.org/10.1109/TNSM.2022.3194205

[3] Nouman M, Qasim U, Nasir H, Almasoud A, Imran M, Javaid N. Malicious node detection using machine learning and distributed data storage using blockchain in WSNs. IEEe Access. 2023 Jan 16;11:6106-21. https://doi.org/10.1109/ACCESS.2023.3236983

[4] Abbas S, Nasir H, Almogren A, Altameem A, Javaid N. Blockchain based privacy preserving authentication and malicious node detection in Internet of Underwater Things (IoUT) networks. IEEE Access. 2022 Oct 25;10:113945-55. https://doi.org/10.1109/ACCESS.2022.3216850

[5] Pang B, Teng Z, Sun H, Du C, Li M, Zhu W. A malicious node detection strategy based on fuzzy trust model and the abc algorithm in wireless sensor network. IEEE wireless communications letters. 2021 Apr 2;10(8):1613-7. https://doi.org/10.1109/LWC.2021.3070630

[6] Kumar K, Pandey K, Chandra S, Arya R. Evaluation of node-metastasis in sparse underwater acoustic sensor networks for localization under acoustically stratified malicious node conditions. IEEE Access. 2021 Dec 23;9:169372-86. https://doi.org/10.1109/ACCESS.2021.3138025

[7] Kumar M, Mukherjee P, Verma K, Verma S, Rawat DB. Improved deep convolutional neural network based malicious node detection and energy-efficient data transmission in wireless sensor networks. IEEE Transactions on Network Science and Engineering. 2021 Jul 21;9(5):3272-81. https://doi.org/10.1109/TNSE.2021.3098011

[8] Ding J, Wang H, Wu Y. The detection scheme against selective forwarding of smart malicious nodes with reinforcement learning in wireless sensor networks. IEEE Sensors Journal. 2022 May 18;22(13):13696-706. https://doi.org/10.1109/JSEN.2022.3176462

[9] Li L, Xu G, Jiao L, Li X, Wang H, Hu J, Xian H, Lian W, Gao H. A secure random key distribution scheme against node replication attacks in industrial wireless sensor systems. IEEE Transactions on Industrial Informatics. 2019 Jul 24;16(3):2091-101. https://doi.org/10.1109/TII.2019.2927296

[10] Mukhopadhyay B, Srirangarajan S, Kar S. RSS-based localization in the presence of malicious nodes in sensor networks. IEEE Transactions on Instrumentation and Measurement. 2021 Aug 12;70:1-6. https://doi.org/10.1109/TIM.2021.3104385

[11] Sreevidya B, Supriya M. Malicious Nodes Detection and Avoidance Using Trust-based Routing in Critical Data Handling Wireless Sensor Network Applications. J. Internet Serv. Inf. Secur.. 2024 Aug;14(3):226-44. https://doi.org/10.58346/JISIS.2024.I3.013

[12] Pandey OJ, Gautam V, Jha S, Shukla MK, Hegde RM. Time synchronized node localization using optimal H-node allocation in a small world WSN. IEEE Communications Letters. 2020 Jul 8;24(11):2579-83. https://doi.org/10.1109/LCOMM.2020.3008086

[13] Xiong L, Xiong N, Wang C, Yu X, Shuai M. An efficient lightweight authentication scheme with adaptive resilience of asynchronization attacks for wireless sensor networks. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2019 Dec 20;51(9):5626-38. https://doi.org/10.1109/TSMC.2019.2957175

[14] Abolqasem S, Alireza SS, Kamel SR. Developing a Routing Protocol for Wireless Sensor Networks Using Fuzzy Logic and Focused on Optimal Route Election. International Academic Journal of Science and Engineering. 2015;2(2):153-63.

[15] Abubaker Z, Javaid N, Almogren A, Akbar M, Zuair M, Ben-Othman J. Blockchained service provisioning and malicious node detection via federated learning in scalable Internet of Sensor Things networks. Computer Networks. 2022 Feb 26;204:108691. https://doi.org/10.1016/j.comnet.2021.108691

[16] Yahaya AS, Javaid N, Javed MU, Almogren A, Radwan A. Blockchain-based secure energy trading with mutual verifiable fairness in ahttps://doi.org/10.1109/TII.2022.3141867 smart community. IEEE Transactions on Industrial Informatics. 2022 Jan 11;18(11):7412-22.

[17] Abubaker Z, Khan AU, Almogren A, Abbas S, Javaid A, Radwan A, Javaid N. Trustful data trading through monetizing IoT data using BlockChain based review system. Concurrency and Computation: Practice and Experience. 2022 Feb 28;34(5):e6739. https://doi.org/10.1002/cpe.6739

[18] Abbas S, Javaid N, Almogren A, Gulfam SM, Ahmed A, Radwan A. Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things. IEEE Access. 2021 Oct 8;9:139739-54. https://doi.org/10.1109/ACCESS.2021.3118948

[19] dos Santos Abreu AW, Coutinho EF, Bezerra CI. Performance evaluation of data transactions in blockchain. IEEE Latin America Transactions. 2021 Dec 31;20(3):409-16. https://doi.org/10.1109/TLA.2022.9667139

[20] Kumar G, Saha R, Rai MK, Thomas R, Kim TH. Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics. IEEE Internet of Things Journal. 2019 Apr 18;6(4):6835-42. https://doi.org/10.1109/JIOT.2019.2911969

[21] Kolumban-Antal G, Lasak V, Bogdan R, Groza B. A secure and portable multi-sensor module for distributed air pollution monitoring. Sensors. 2020 Jan 10;20(2):403. https://doi.org/10.3390/s20020403

[22] Brotsis S, Limniotis K, Bendiab G, Kolokotronis N, Shiaeles S. On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance. Computer Networks. 2021 May 22;191:108005. https://doi.org/10.1016/j.comnet.2021.108005

[23] Cui Z, Fei XU, Zhang S, Cai X, Cao Y, Zhang W, Chen J. A hybrid blockchain-based identity authentication scheme for multi-WSN. IEEE Transactions on Services Computing. 2020 Jan 7;13(2):241-51. https://doi.org/10.1109/TSC.2020.2964537

[24] Tian Y, Wang Z, Xiong J, Ma J. A blockchain-based secure key management scheme with trustworthiness in DWSNs. IEEE Transactions on Industrial Informatics. 2020 Jan 13;16(9):6193-202. https://doi.org/10.1109/TII.2020.2965975

[25] Umarani C, Kannan S. Intrusion detection system using hybrid tissue growing algorithm for wireless sensor network. Peer-to-Peer Networking and Applications. 2020 May;13(3):752-61. https://doi.org/10.1007/s12083-019-00781-9

[26] Zhai Z, Lai G, Cheng B, Qian J, Zhao L, Wu J, Wan Z. Lightweight secure detection service for malicious attacks in wsn with timestamp-based mac. IEEE Transactions on Network and Service Management. 2022 Jul 27;19(4):5299-311. https://doi.org/10.1109/TNSM.2022.3194205

[27] Alkhudary R. Blockchain technology between Nakamoto and supply chain management: Insights from academia and practice. Available at SSRN 3660342. 2020 Jul 25. https://doi.org/10.2139/ssrn.3660342