International Journal of Safety and Security Engineering
Vol. 13, No. 6, December, 2023, pp. 1099-1108
Journal homepage: http://iieta.org/journals/ijsse

Digital Incontrovertible Multi Level Key Set Based Node Authentication Model for Malicious Node Detection for Secure Data Transmission in WSN

Doma Murli Krishna Reddy[1*], Rajendran Sathya[1], Veeravatnam V.A.S. Lakshmi[2]

[1] CSE Department, Annamalai University, Chidambaram, Tamil Nadu 608002, India
[2] CSE(AI&ML), Narasaraopet Engineering College, Narasaraopet 522601, India

Corresponding Author Email: murali.aucse32@gmail.com

https://doi.org/10.18280/ijsse.130613

Received: 9 September 2023
Revised: 16 November 2023
Accepted: 29 November 2023
Available online: 25 December 2023

Keywords:
wireless sensor networks, cryptography, sensors nodes, node authentication, malicious nodes, multi level key set, data security

ABSTRACT

Wireless sensor networks (WSNs) present a paradigm that is both innovative and complex, characterized by their autonomous operation and the deployment of diminutive, resource-constrained sensor nodes. Despite the promising prospects offered by their unique features, WSNs are inherently more susceptible to security threats compared to conventional networks, primarily due to their operational environment and reliance on wireless communication. The vulnerability of nodes to physical attacks is exacerbated by the typical deployment strategies and the intrinsic limitations of radio connections. Due to the resource-scarce nature of sensor nodes, which are often situated in adversarial settings, security measures are particularly challenging to implement. These nodes are generally equipped with limited energy, computational power, and communication capabilities, imposing significant constraints on the safeguarding of WSNs without compromising network efficiency. The identification and isolation of compromised nodes are critical to prevent adversaries from disseminating false data throughout the network. However, securing networks with a flat topology poses considerable difficulties, including limited adaptability and excessive communication overheads. Traditional security methods, which typically entail substantial overhead and computational requirements, are not viable in such resource-constrained environments. Authentication emerges as a critical security measure, serving as a means to discern authentic, forged, or altered messages. This study introduces a novel Digital Incontrovertible Multi-Level Key Set based Node Authentication Model (DIMLKS-NA-MND) that leverages cryptographic principles to enhance data transmission security in WSNs. Comparative analyses demonstrate that the proposed model outperforms existing models in securing data transmissions.

1. INTRODUCTION

Wireless sensor networks (WSNs) are comprised of a multitude of autonomous nodes, each a cost-effective and compact sensor [1]. These networked nodes are dispersed across extensive areas to monitor environmental parameters such as temperature, pressure, and humidity, serving an array of applications from habitat monitoring to advanced scientific exploration. It has been posited that to distill valuable insights from the voluminous raw data, significant processing and computational capabilities must be embedded within the nodes [2]. Communication within these networks is facilitated wirelessly among randomly placed sensor nodes, which are constrained by their limited energy, storage, and computational capacities [3]. A sensor node, designed as a small, low-power device, is tasked with data acquisition. The inherent limitations of their batteries render the nodes with finite storage, memory, and processing capabilities, thereby increasing their susceptibility to security breaches [4]. Energy conservation within WSNs is paramount, as the network lifetime — the duration from deployment until the depletion of the first node's energy - directly impacts the effectiveness and longevity of the network [5]. Hierarchical clustering has emerged as a prominent strategy to mitigate energy consumption and prolong the operational span of WSNs [6]. This technique involves segmenting expansive sensor networks into more manageable sub-units.

These nodes find utility in a spectrum of fields, including military surveillance, environmental monitoring, transport systems, smart home technologies, and disaster management. Each sensor node is equipped with an array of sensors, potentially including mechanical, biological, and magnetic types, along with a low-power battery, processor, radio, memory, and an actuator [7]. The remote and often hostile deployment environments elevate the risk of unauthorized access and attacks, presenting a significant security challenge [8].

1.1 Malicious actions in WSN

Despite the development of numerous security protocols and strategies designed to thwart attacks and malicious node

activities within WSNs, these networks remain susceptible to an array of security threats and weaknesses [9]. It has been observed that nodes which act selfishly or maliciously, contravening the established protocol norms, can disrupt the routing process. WSN attacks can be categorized broadly into internal and external types [9]. External attacks often target authentication and key management systems [10], and although cryptographic measures, authorization, and encryption are employed to counter these threats, their efficacy is compromised in the face of internal attacks. Such attacks include scenarios where an adversary compromises a node, inducing abnormal behavior and facilitating attacks such as black holes and sinkholes [11]. When dealing with network intrusions from within, conventional methods are useless. The malicious node detection in WSN is shown in Figure 1.

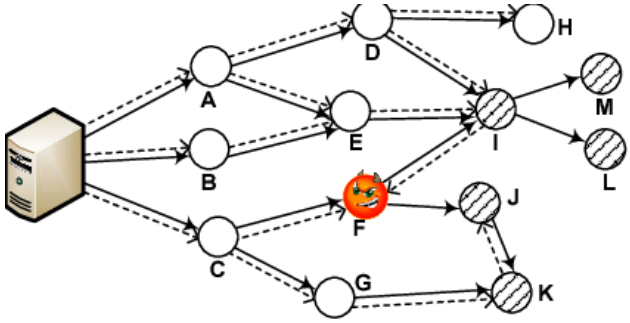

Figure 1. WSN malicious node detection

The ongoing quest for secure WSNs has yielded a plethora of strategies to protect against malicious nodes and other attacks. Predominantly, these strategies have centered on cryptographic and authentication measures, yet the absence of centralized management in WSNs presents a significant challenge to their implementation [12]. Cryptographic solutions demand substantial resources, and once a node is compromised, its credentials, including secret keys and memory contents, can be exploited [13]. The present study proposes a novel and practical key distribution method to secure communications within WSNs. It has been proposed that the operation frequency of a node correlates with its transaction volume, with nodes decelerating in dense network segments to facilitate universal connectivity, and accelerating in sparser areas to compensate for decreased key exchange demands [14]. WSNs maintain communication continuity even when mobile nodes are transiently outside the communication range of others. This continuity hinges on the trustworthiness of the keys exchanged among sensor nodes for the duration of a session [15]. The integrity of communication is preserved as long as it occurs within the designated temporal confines of the session, regardless of the node's immediate presence [16].

1.2 Cryptography in WSN

In wireless sensor networks, the deployment of a robust encryption mechanism constitutes a critical facet of secure information handling. Cryptography is generally bifurcated into symmetric and asymmetric categories [17]. Initiatives for key generation have encompassed the use of random number generators and key derivation functions. The strength of the key is a pivotal factor at this juncture, necessitating the elimination of weak keys from the pool. Although it is acknowledged that lengthier keys typically confer enhanced security, they also impose a greater computational burden [18]. Subsequent to key generation, the dissemination of the key to all relevant entities is imperative. It must be transmitted with safeguards against interception, as exposure through plaintext transmission could precipitate key compromise [19]. Distinct from cryptography, there exists a gamut of systems for the detection of defects, abnormalities, and outliers within WSNs. Predicated on the assumption that the majority of sensor nodes function accurately, these systems predominantly focus on singling out malfunctioning sensor nodes or excising anomalous sensor data in a distributed framework [20].

Some studies have capitalized on the premise that measurement discrepancies arising from faults are likely to manifest as uncorrelated, whereas observations within a targeted region exhibit spatial correlation. This concept has been leveraged to distinguish between events and faults [21]. To demarcate event boundaries under adversarial conditions, a secure detection methodology has been proposed within this paradigm. Despite the ubiquity of malicious nodes within WSNs, their impact is frequently underestimated or insufficiently addressed [22]. Should malicious nodes generate spurious measurements that deviate from the prescribed fault model, the realized performance may be compromised. Moreover, if these nodes demonstrate sophisticated behavioral patterns, the challenge of discerning between genuine events and false alarms induced by such nodes is exacerbated. Conventional models tend to yield high false alarm rates, while existing cryptographic models lack robustness, thereby degrading network performance. This study introduces a novel approach: the Digital Incontrovertible Multi-Level Key Set based Node Authentication Model. Employing cryptography, this model is aimed at the detection of malicious nodes, thereby facilitating secure data transmission within WSNs.

2. LITERATURE SURVEY

2.1 Attack detection models

In spite of decades of study, developing an effective multi-factor user authentication strategy for WSN remains difficult. This is due to the fact that protocol designers have to deal with the age-old security versus efficiency conundrum: sensor nodes are small, low-powered devices with limited memory and processing power, while the security requirements are stringent because WSNs are typically used for sensitive tasks. The same errors are made over and over again, despite the fact that hundreds of proposals have been made. Smart card loss attacks and node capture attacks are two of the most typical security lapses. While the former has been studied extensively, node capture attacks have received very little academic interest. Wang et al. [2] made a significant contribution in systematically exploring node replication attacks versus multi-factor user authentication techniques for WSNs, which would go a long way towards mitigating this unfavourable condition. First, the author looked into the numerous factors that contribute to node capture attacks, and then categorized them into 10 distinct varieties based on the nodes targeted, the skills of the adversary, and the vulnerabilities that are exploited.

Many different types of gadgets and objects can now connect to the internet thanks to the IoT. With this network in place, data may be sent via a wide variety of state-of-the-art techniques; this advances the possibility of intelligent

identification. Wireless sensor networks (WSNs) are an essential part of the Internet of Things (IoT), and they have found applications in many fields. Researchers have paid particular attention to data security concerns and challenges including leaking of personal data as a direct result of the rapid proliferation of WSNs and remote health monitoring sensor networks (WMSNs), etc. Several of the novel authentication mechanisms developed by researchers for WMSNs suffer from serious security problems. Saleem et al. [3] conducted an extensive security analysis of the protocol and found that it does not safeguard user privacy against sensor node impersonation attacks.

Defense, smart healthcare, smart transportation, and even space exploration are just some of the many applications seeing increased use of WSNs. However, WSNs are more vulnerable to cyber assaults because they authenticate users and deliver messages across an open channel, unlike traditional networks. WSNs lack the capacity for a typical authentication scheme, which is essential for ensuring network security. That's why it's so important for WSNs to have a solid authentication scheme. The Dynamic Authentication Credential (DAC) has been the subject of extensive study in recent years due to its proven ability to increase authentication security. A secure authentication approach for WSNs was devised by Liu et al. [4] using DAC and Intel Software Guard Extensions (SGX). Since DAC rotation is not provided by alternative DAC authentication methods, this one is essential for preventing the asynchronous update problem caused by packet loss. To protect against privileged user attacks and verification table leaking attacks, the author employed SGX, which can secure the data in use, as the trusted runtime environment in the gateway node and adopted SGX to store the master key for protecting the authentication table. Finally, the author confirmed the security of this authentication method using BAN logic, the simulation tool AVISPA, and informal security evaluation.

With the use of IoUT networks, it is easy to monitor environmental conditions in the water, including temperature, pressure, pollution levels, and more. In addition to collecting data regarding potential natural disasters, they are utilized for ocean weather forecasting. Yet, because they are typically deployed in unsupervised settings, they are highly vulnerable to compromise. Security in IoUT networks is necessary to prevent unwanted access and to ensure network credibility, which is essential for overcoming these challenges. To prevent hostile internal nodes and untrusted external nodes from accessing the network, respectively, Abbas et al. [5] suggested an authentication and harmful node detection technique. As an added layer of security and auditability, blockchain records credential hashes of registered sensor nodes. Simultaneously, a weighted trust evaluation technique is implemented for data aggregation and the detection of malicious nodes. In addition, before aggregating, the data from malicious nodes is verified by placing them in an intensive observation queue using an additive increase multiplicative decrease algorithm. Furthermore, sensor nodes are given weights according to their actions.

In times of emergency, the safety of supplies depends heavily on emergency logistics. Safety and efficiency are hallmarks of emergency logistics, which is an essential part of strategic material reserve and allocation. Given the severity of the consequences that would result from unauthorized access to the IoT-based emergency logistics system, its protection is of paramount importance. Authentication is a cornerstone of any reliable security system. Current certificate less authentication techniques, which are often based on bilinear pairings, do not meet the needs of emergency logistics networks, which require easy deployment and quick authentication of numerous nodes. Yang et al. [6] presented a lightweight certificate less authentication system (CL-LAP) that does not rely on bilinear pairings in this work. Elliptic curves' discrete logarithm problem is the deciding factor in their security. Energy efficiency and low computation costs are ensured through nonlinear pairings. To further address the issue of fast authentication in broadcast messages and lower the cost of authentication, the author employed batch verification. To prove that the proposed CL-LAP is secure enough for the perception layer, the author performed a security study on it using the random oracle model and show that it can survive typical security threats.

2.2 Cryptography models

The open nature of nodes in a WSN makes them vulnerable to many threats, including dishonest recommendation attacks, which provide the attacker an advantage by offering misleading trust values. Pang et al. [7] offered an approach to malicious node detection using the artificial bee colony algorithm (ABC) and a fuzzy trust model (FTM-ABC). To better detect dishonest recommendation attacks, the ABC method is used to optimize the trust model, and the fuzzy trust model (FTM) is used to calculate the indirect trust. In addition, the fitness function incorporates the departure from the recommended value and the interactions index deviation to improve performance.

WSN are self-configuring Wireless Ad hoc Networks (WANET) for the Internet of Things and are made up of a large number of Sensor Nodes (SN) with limited capabilities. Both energy efficiency and security are crucial for WSN. An adversary can disseminate false information with the use of Malicious Nodes (MNs). Therefore, identifying and isolating certain MNs is essential for reducing vulnerability to security threats. Therefore, Kumar et al. [8] suggested a method for recognizing MNs in WSN that exploits the distinctive characteristics of each SN. This research takes into account security and provides energy-efficient data transmission (DT) by picking the Cluster Head (CH) based on the sensor's remaining energy. The Malicious Nodes (MN) are identified by the Improved Deep Convolutional Neural Network (IDCNN) and added to the malicious list box in the Malicious Nodes Detection (MND) phase. The t-Distribution based Satin Bowerbird Optimization (t-DSBO) algorithm selects a CH for each cluster based on the residual energy of the nodes in that cluster after the Trusted Nodes (TN) have been grouped using the Extended K-Means (EKM) algorithm. It is the CH's job to transmit cluster information to the BS. The t-DSBO will automatically switch to a new CH if the power on the current CH suddenly goes out.

In order to manage node registration with credentials and other security issues, Nouman et al. [9] presented a concept in which blockchain is implemented on the BSs and CHs. Histogram Gradient Boost (HGB) is a Machine Learning (ML) classifier used by the BSs to detect if the nodes in question are malicious. The node's membership in the network will be revoked if it is found to be malicious. In contrast, information from legitimate nodes is saved in an extrasolar database (IPFS). With IPFS, information is kept in bite-sized pieces, each of which is given its own unique hash before being appended to

the blockchain. In addition, Verifiable Byzantine Fault Tolerance (VBFT) is used to achieve consensus and validate transactions as opposed to Proof of Work (PoW). Full simulations additionally make use of the WSN dataset (abbreviated WSN-DS). Both the original data and the rebalanced data were put through the author's proposed model's paces. In addition, several established classifiers are compared to HGB across a range of performance metrics; these include Adaptive Boost (AdaBoost), Gradient Boost (GB), Linear Discriminant Analysis (LDA), Extreme Gradient Boost (XGB), and ridge.

WSN sensors are often placed in unfriendly environments. Unfortunately, most sensors have limited energy, computational resources, and communication channels. Thus, it is difficult to guarantee the safety of WSN without negatively impacting the efficiency of the network. Network coding (NC) shows promise as a means of enhancing WSN communications capabilities like throughput, robustness, and energy efficiency. Nonetheless, malevolent assaults can compromise network coding. Nowadays, several secure detections have been presented to deal with a single type of attack, such as information theoretic-based or cryptographic-based techniques, but they are unable to withstand the joint attacks, such as the union of pollution attacks and replay attacks. In this work, Zhai et al. [10] introduced a protected detection service. It is installed on every WSN node to track and handle all incoming and outgoing communications. Using Exclusive OR network coding, the service creates a lightweight timestamp-based message authentication code called TMAC. To simultaneously prevent pollution assaults and replay attacks, a joint detection based on TMAC and time synchronization technique has been created. The detecting service's accuracy has been demonstrated.

Wireless sensor networks are dispersed at will and tasked with performing widespread monitoring. Due to its limited power and computing capabilities, data aggregation in WSN is quite complicated. The data may be sent on malicious node, which is a problem in data aggregation. The transfer of such a massive amount of data poses a security risk for all of the currently available data aggregation methods. The WSN is a multi-hop wireless network that incorporates several sensor nodes placed in a self-organized fashion. Typically used in unmonitored settings, where malicious actors might compromise sensor nodes and skew detection results by inserting fake data. In order to stop fault data injection attacks, the authors of this study offer a correlation-theory based approach for identifying rogue nodes.

3. PROPOSED MODEL

A method for identifying malicious nodes in wireless sensor networks based on their proximity to other nodes is performed in this research. By monitoring for faults and events, malicious nodes can be identified without compromising healthy ones. They are represented as malfunctioning nodes with the ability to manipulate sensor data and engage in deceptive behaviour to avoid detection [23]. During typical operations, the reliability of sensor nodes is estimated using confidence levels. Each sensor node takes these into account while making a judgement. As long as their behaviour is distinct from that of regular nodes, two parameters for updating the confidence levels are used to identify malicious nodes [24]. In order to eventually isolate malicious nodes, despite their slightly different behaviour from normal nodes, the ratio between them must be carefully chosen [25]. In the presence of faults and events, the detection rate is kept high while the false positive rate is kept low. As a result, false alarm rates are maintained to a minimum without sacrificing precision while detecting events [26]. The reliable and secure key distribution center in this system is the base for key generation and distribution. In order for two sensor nodes to successfully interact, a key set is generated for both the nodes that must be kept in the memory of both nodes. The benefit is that the sensor node's key set can't expose the entire network; it's just accessible to a specific node [27].

Previous studies on both traditional wired networks and ad hoc wireless networks have determined that cryptographic protection of messages sent between nodes is necessary for securing the operations of communication. They typically necessitate authentication at the source, security of message integrity, and private communication. There have been various attempts to develop key cryptography systems despite the constrained resources available in WSNs [28]. Different communication keys, such as unicast, broadcast, multicast, etc., are needed for different WSN application types. When sending data to the sink node, a unicast key is necessary, whereas a broadcast key is needed for intermediate routing nodes and for sending control packets to all nodes. Many recent studies have looked into preloading keys, but they have been found to have poor scalability for big networks and high overhead. It has trouble accommodating new nodes that join the system since the existing nodes can't tell the difference between malicious and lawful additions.

Unattended sensor networks are more vulnerable to attacks, which can introduce malicious nodes into the network. Many assaults have been demonstrated that can be launched against a sensor network. Most studies have focused on head-on assaults on the networks themselves, proposing various methods for detecting and thwarting such attacks. In this paper, zero in on indirect attacks, in which malicious nodes appear to be acting normally but are actually sending out false sensor readings to their neighbours is considered in an effort to trick the network into making a bad choice with potentially disastrous results or to waste resources by generating unnecessary computation and communication. Noise, malfunctions, and unexpected occurrences can potentially affect sensor readings in unexpected ways. Given the prevalence of faults and events, it is imperative that malicious nodes be identified. The malevolent nodes are handled by considering them defective nodes with the ability to arbitrarily alter their readings. If no fault-tolerance mechanisms are adopted, users reporting their own readings might swiftly bring the network to a halt. Each sensor node is presumed to be familiar with the typical range of measurements and to be able to ascertain whether or not the measured values fall within that range. In this context, normal range refers to the interval throughout which no events would cause a deviation from the expected sensor data. The proposed model framework is shown in Figure 2.

In the proposed model, initially node information is consideres and to each node a immutable token allocation is performed. The proposed model generates incontrovertible multi level key set that is distributes to all the nodes in the network and these keys are used for node authentication. The node which needs to transmit the data has to provide the authentication key to complete the node authentication process. The nodes after successful authentication only will allow for

communication. The node actions are considered and the malicious nodes can be detected.

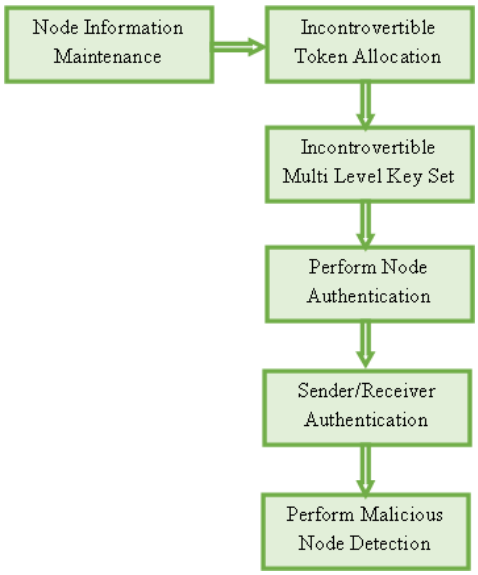

Figure 2. Proposed model framework

In order for nodes in a WSN to communicate with one another wirelessly, a system for managing keys is required. WSNs are more susceptible to assaults from malicious nodes than wired networks. This research presents a digital incontrovertible multilevel key management system to address the limitations of current key management systems by allowing keys to be produced on the fly and distributed among wireless network nodes for strong node authentication and malicious nodes detection. The proposed method uses a unique digital token system for key management, which allows for easy differentiation between potential attackers. Node capture attacks have been successfully tested against the proposed scheme. Security in communications relies heavily on authentication. This feature guarantees that information has been gathered from reliable resources. When two nodes exchange information, the sending node wants to verify that it is a valid network node and that the information it is sending is accurate. Other nodes can check to see if the source of a message or data is reliable. In this research, Digital Incontrovertible Multi Level Key Set based Node Authentication Model for Malicious Node Detection (DIMLKS-NA-MND) using cryptography is proposed for secure data transmission in WSN.

Algorithm DIMLKS-NA-MND
{

Step-1: The nodes information in the network is maintained for monitoring the nodes behavior in the network. The node information is gathered as

$$NInfo[M] = \sum_{i=1}^{M} \lim_{i \to M} \left(maxNetsize(M) + \frac{getNode(i)}{netLimit(M)} \right) + TiIns(i) + nodeAddr(i) + \mu$$

Here μ is the node transmission range capability, node address is considered for maintain the node information and network limit is considered to store the network size. TiIns() is the time instant of the node during registration. maxNetsize() model considers the maximum limit of the network size,nodeArr() model considers each node address, netLimit() model considers the network limit of nodes.

Step-2: The nodes in the network will be allotted with the Digital Incontrovertible Token that is used to identify the nodes during data transmission. The Digital Incontrovertible Token is a security number that is used by nodes for authentication and recognition. The Digital Incontrovertible Token allocation is performed as:

$$DigT(NInfo[M]) = \prod_{i=1}^{M} \frac{NodeAddr(i)}{\mu} + getRand\big(node(i)\big) + \max\big(NInfo(i)\big) + Th$$

Here getRand() is used generate a random value in calculation of digital token. Th is the threshold value considered in digital token calculation. The digital token is a secret value generated for every node that is used for node authentication to enter into network.

Step-3: The proposed model generates Incontrovertible Multi Level Key Set that is used for node authentication during data transmission. The sender node and receiver node has to provide the keys from the key set to complete the authentication process. The Incontrovertible Multi Level Key Set generation is performed as:

$$IntValM = \sum_{i=1}^{M} \frac{getPrime(i)}{Th} + getRand(i)$$

$$IntValN = \sum_{i=1}^{M} getRand(i) + nodeAddr(i)$$

$$KeyM = \prod_{i=1}^{M} \frac{IntValM(i) \oplus \text{IntValN}}{Th} \ll 2$$

$$PriKey[M] = \sum_{i=1}^{M} \left(\frac{(KeyM || IntValM)}{getRand(i)} \oplus (\text{IntValN} \&\& IntValM) \right) \ll 4$$

$$IKset[M] = \sum_{i=1}^{M} \left[\frac{KeyM(i) \oplus \text{PriKey(i)}}{IntValN(i)} : \frac{PriKey(i) \&\& IntValN(i)}{KeyM(i)} \right]$$

The IKset is a key set that contains two keys that are represented as K1 and K2. Here IntValM, IntValN are the intermediate key generation values, Key M is the model key that is generated from the intermediate values. PriKey is the private key generated and IKset is the key set generated for all the nodes.

Step-4: A malicious network node is one that intentionally interferes with other network nodes. The malicious node impedes communication between the sender and the recipient, replaying older information. The estimated locations of the unidentified nodes are inaccurate because they are based on historical information. To bring down a whole network, all a replay attack needs is access to a single node. The node authentication to enter into the network is performed as:

$$NodeAuth[M] = \sum_{i=1}^{M} getDigT\big(Node(i)\big) + getTime(i) \begin{cases} 1 & if\ getDigT(i) == NInfo(DigT(i)) \\ 0 & otherwise \end{cases}$$

The node if successfully authenticated, allocated with a label 1, and 0 if not authenticated in case of malicious node. The node labeling helps in consideration of nodes into network. $getDigT()$ models retrieves the digital token of each node during authentication process.

Step-5: The sender and the receiver in the network, before data transmission into the network and before receiving the data, the nodes need to get authenticated using the key set keys. The malicious nodes can be easily detection with the strong authentication scheme. The sender and receiver node

authentication process is performed as:

$$SourceAuth[M] = \coprod_{i=1}^{M} \lim_{i \to M} \left(NodeAuth(i) + \frac{getNode(i)}{nodeAddr(i)} \right) + getIKset(K1) + getTime(i) \begin{cases} 1 & if\ getIKset(K1) == IKset(Node(K1(i))) \\ 0 & otherwise \end{cases}$$

$$DestAuth[M] = \coprod_{i=1}^{M} \lim_{i \to M} \left(NodeAuth(i) + \frac{getNode(i)}{nodeAddr(i)} \right) + getIKset(K2) + getTime(i) \begin{cases} 1 & if\ getIKset(K2) == IKset(Node(K2(i))) \\ 0 & otherwise \end{cases}$$

Here 1 represents authenticated and 0 represents not authenticated.

Step-6: Any network node with the intent to disrupt operations to other nodes is considered malevolent or malicious. The malicious actions in the network degrade the network performance. The proposed model accurately detects the malicious nodes in the network and the process is performed as:

$$MaliciousN[M] = \frac{\sum_{i=1}^{M} getSourceAuth(i) + getDestAuth(i)}{NodeAuth(i)} \begin{cases} 1 & if\ \left(SourceAuth(i) \&\& \ and\ DestAuth(i) \right)! = 1 \\ 0 & otherwise \end{cases}$$

Here 1 is allocated to the nodes that has malicious properties and such nodes will be removed from the network and 0 is allocated for the nodes that are normal and can be involved in communication.

}

4. RESULTS

A WSN is a collection of interconnected sensors that work together to accomplish a common goal. Multi-hop networks are a common way for these nodes to communicate with one another. The environmental, medical, industrial, and many other types of monitoring are just some of the many uses for WSNs. While the potential uses for wireless sensor networks are many, the same high standard of security is required on the receiving end. One of the most effective ways to secure a sensor network is through authentication. The proposed authentication method protects sensitive data without exposing it to potential breaches. If the zero-knowledge protocol is utilized for repeated challenges, the entire network's security will be bolstered. As no intensive calculations are needed, the computational burden of this method also appears to be low. As a result, the sensor node's power and storage needs will be diminished.

Efforts should be made to provide similarly robust authentication methods. Here, secure communication in wireless sensor networks that might move from place to place is monitored. Strong encryption and authentication protocols among sensor nodes are necessary for achieving security in WSNs. Extreme resource limitations in common WSNs prevent them from concluding crucial agreements. In this research, Digital Incontrovertible Multi Level Key Set based Node Authentication Model for Malicious Node Detection (DIMLKS-NA-MND) using cryptography is proposed for secure data transmission in WSN. The proposed model is compared with the traditional Automated Labeling and Learning for Physical Layer Authentication Against Clone Node and Sybil Attacks in Industrial Wireless Edge Networks (ALL-PLACN-SA) and the results represent that the proposed model performance in node authentication and malicious node detection is high.

In the proposed model, the nodes in the network information is maintained that is used for establishing communication and monitoring the nodes. Each node will be allocated with a Incontrovertible Token that is used for node identification and monitoring that helps in security levels in the network. The Node Incontrovertible Token Allocation Time Levels of the existing and proposed models are shown in Table 1 and Figure 3.

Table 1. Node incontrovertible token allocation time levels

Nodes in the Network	Models Considered	
	DIMLKS-NA-MND Model	ALL-PLACN-SA Model
50	12	19.4
100	13	19.6
150	14	19.8
200	15	20
250	16	21
300	17	22

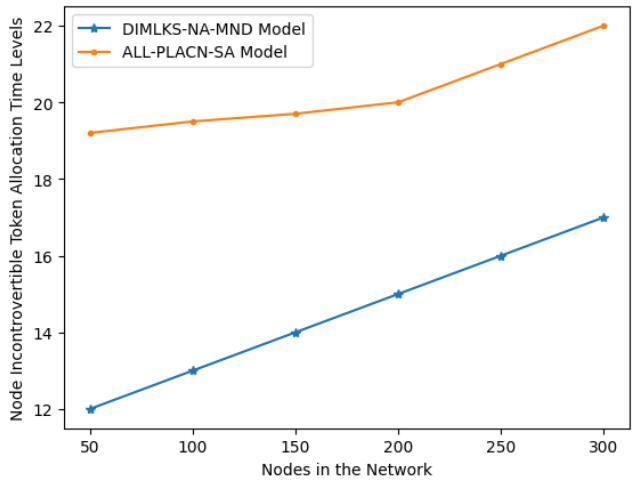

Figure 3. Node incontrovertible token allocation time levels

In WSNs, there are numerous issues, such as the reciprocal interfering of wireless links, military applications and nodes are subjected to weak physical protective medium. All of these factors increase the sensor nodes' susceptibility to assault and compromise. Given that sensors in WSNs are typically power constrained, it is always fundamental to conserve the node energy and increase the network's lifetime.

The Digital Incontrovertible Multi Level Key Set Generation is performed that is used for Node authentication at every transaction. The key set keys are used by each node in the network to get validated. The key set contains two keys that are used for one time and the Digital Incontrovertible Multi Level Key Set Generation Time Levels of the proposed and existing models are shown in Table 2 and Figure 4.

Malicious nodes in distributed wireless sensor networks provide a difficult problem since they might compromise a large number of sensors and are always accompanied by damaging threats. Therefore, sensor networks require an authentication service to verify the authenticity of sensors before allowing them to transmit data. In addition, sensor security appliances always have intrusion detection and prevention strategies to improve network security by

identifying hostile or compromised nodes. This study proposes adaptive security modules to promote secure communication of cluster-based sensor networks. The proposed primary security module includes a dynamic authentication mechanism that allows existing nodes to authenticate new incoming nodes, which then causes secure linkages to be established and broadcast authentication to take place between surrounding nodes. This core security architecture uses authentication to block access from potentially harmful external nodes.

Table 2. Digital incontrovertible multi level key set generation time levels

Nodes in the Network	Models Considered	
	DIMLKS-NA-MND Model	ALL-PLACN-SA Model
50	4	14
100	4.6	14.6
150	5	15
200	5.7	15.4
250	6	15.8
300	7	16

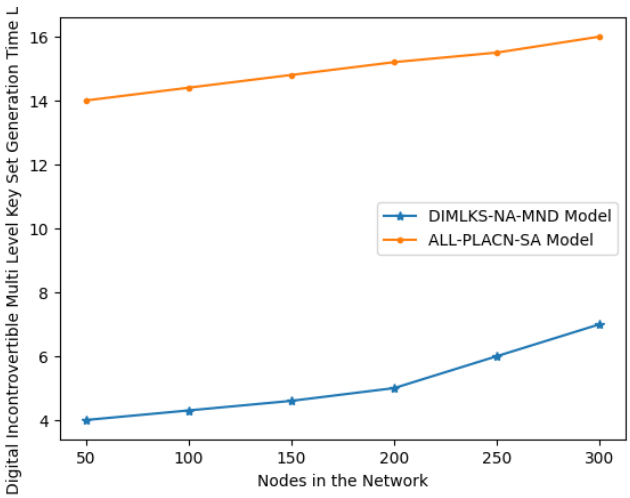

Figure 4. Digital incontrovertible multi level key set generation time levels

The proposed model performs detection of malicious nodes in the network. The node authentication helps in detection of normal and malicious nodes in the network. The nodes have to provide a allocated key from the key set for accurate authentication. The Node Authentication Accuracy Levels of the proposed and traditional models are shown in Table 3 and Figure 5.

Table 3. Node authentication accuracy levels

Nodes in the Network	Models Considered	
	DIMLKS-NA-MND Model	ALL-PLACN-SA Model
50	94	90.2
100	94.7	90.5
150	95.2	91
200	95.6	91.6
250	96	92
300	97.2	93

The sender initially sends the data by initiating the communication in the network. The sender needs to get authenticated to transmit the data. This data initiation authentication helps in authorization of nodes ate entry level for securing the network. Data Initiation Authentication Accuracy Levels of the existing and proposed models are shown in Table 4 and Figure 6.

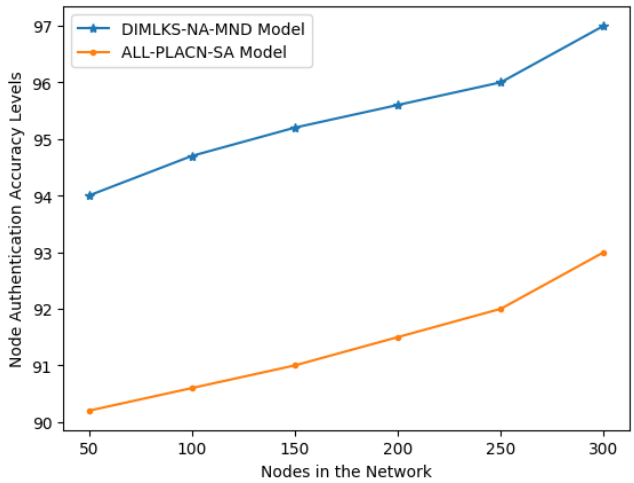

Figure 5. Node authentication accuracy levels

The data receiver needs to get authentication before receiving data in order to avoid malicious actions in the network. In order to receive data, the receiver must first prove their identity. This data receiver identification aids in authorizing nodes at the gateway, which is a crucial step in ensuring the safety of the network. Accuracy levels of existing and proposed models for data receiving authentication are displayed in Table 5 and Figure 7.

Table 4. Data initiation authentication accuracy levels

Nodes in the Network	Models Considered	
	DIMLKS-NA-MND Model	ALL-PLACN-SA Model
50	95	92
100	95.7	92.4
150	96.3	93
200	96.5	93.6
250	96.9	94
300	97.8	94.2

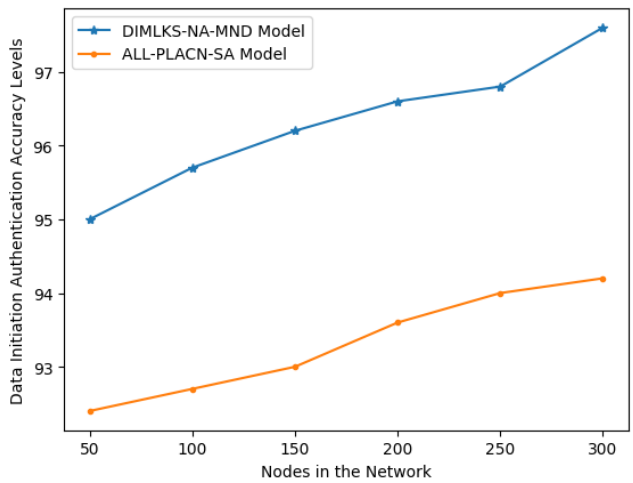

Figure 6. Data initiation authentication accuracy levels

Table 5. Data receiving authentication accuracy levels

Nodes in the Network	Models Considered	
	DIMLKS-NA-MND Model	ALL-PLACN-SA Model
50	96	93
100	96.4	93.6
150	96.8	94.2
200	97	94.7
250	97.5	94.8
300	97.9	95

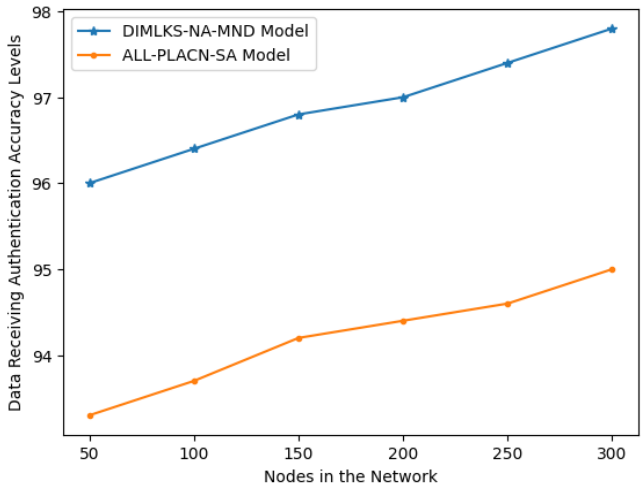

Figure 7. Data receiving authentication accuracy levels

Table 6. Malicious node detection accuracy levels

Nodes in the Network	Models Considered	
	DIMLKS-NA-MND Model	ALL-PLACN-SA Model
50	96.2	92.5
100	96.3	93.2
150	97	93.4
200	97.4	93.7
250	97.8	93.9
300	98.2	94

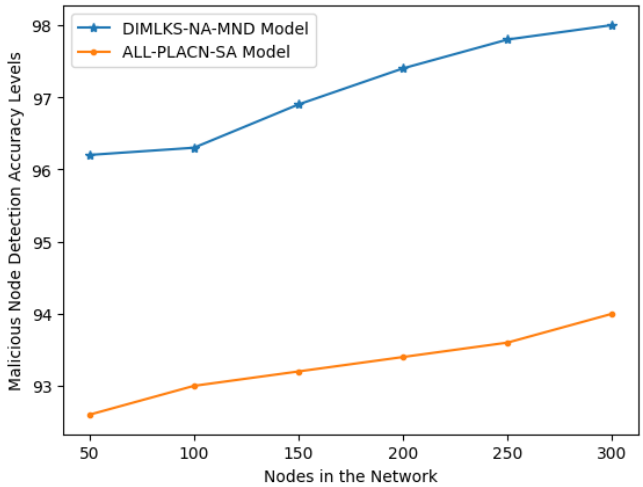

Figure 8. Malicious node detection accuracy levels

Any network node with the intent to disrupt service to other nodes is considered malevolent. The malicious node slows down the data stream between the transmitter and the receiver, and then plays back the out-of-date data. The unknown nodes' position estimates are incorrect since they are based on out-of-date data. Replay attacks are unique in that they only need to compromise a single node to bring down the entire network. The Malicious Node Detection Accuracy Levels of the existing and proposed models are shown in Table 6 and Figure 8.

5. CONCLUSION

It is crucial to authenticate nodes in wireless sensor networks. Most sensor network uses cases necessitate that data be kept secret from attackers. There are a number of approaches to authenticating sensor networks; however, they all have some sort of downside, be it a cumbersome communication or processing demand, a large storage requirement, a high battery drain, or a difficult manner of key management. In this paper, we present a system for user authentication using key distribution. When the proposed algorithm is implemented, its security and robustness are verified. For wireless sensor networks, this research also proposes a malicious node identification method for safe data transfer. By dividing the network space into square grids, a distributed system is able to locate malicious nodes in their immediate vicinity. When the event zone spans multiple adjacent grids but is still relatively small, inter-grid communication is employed to improve the accuracy of event detection. The weights given to pieces of data represent how confident one is in the accuracy of the data presented by sensor nodes. If a node's weights fall below a specific level, it is effectively severed from the rest of the network. The criteria have been carefully chosen to ensure accurate detection of malicious nodes while sparing benign ones. In this paper, we suggested a method for identifying malicious nodes in wireless sensor networks based on their proximity to other nodes. By monitoring for faults and events, malicious nodes can be identified without compromising healthy ones. They are represented as malfunctioning nodes with the ability to manipulate sensor data at will and engage in deceptive behavior to avoid detection. In this research, Digital Incontrovertible Multi Level Key Set based Node Authentication Model for Malicious Node Detection using cryptography is proposed for secure data transmission in WSN. Each sensor node takes these into account while making authentication. The multi level key set that is immutable cannot be altered by attackers and reused that maintains strong security levels. In addition to improving network performance, the proposed model is 98% accurate at authenticating nodes and detecting malicious nodes. The detection rate is maintained at a high level while the false positive rate is maintained at a low level in the presence of faults and malicious events. This guarantees accurate event detection with little false alarms. In the future, the network's security can be improved by taking into account the nodes' trust factors and the feedbacks of the remaining nodes and the cluster head.

REFERENCES

[1] Chen, S., Pang, Z., Wen, H., Yu, K., Zhang, T., Lu, Y. (2020). Automated labeling and learning for physical layer authentication against clone node and sybil attacks in industrial wireless edge networks. IEEE Transactions

on Industrial Informatics, 17(3): 2041-2051. https://doi.org/10.1109/TII.2020.2963962

[2] Wang, C., Wang, D., Tu, Y., Xu, G., Wang, H. (2020). Understanding node capture attacks in user authentication schemes for wireless sensor networks. IEEE Transactions on Dependable and Secure Computing, 19(1): 507-523. https://doi.org/10.1109/TDSC.2020.2974220

[3] Saleem, M.A., Shamshad, S., Ahmed, S., Ghaffar, Z., Mahmood, K. (2021). Security analysis on "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems". IEEE Systems Journal, 15(4): 5557-5559. https://doi.org/10.1109/JSYST.2021.3073537

[4] Liu, X., Guo, Z., Ma, J., Song, Y. (2021). A secure authentication scheme for wireless sensor networks based on DAC and Intel SGX. IEEE Internet of Things Journal, 9(5): 3533-3547. https://doi.org/10.1109/JIOT.2021.3097996

[5] Abbas, S., Nasir, H., Almogren, A., Altameem, A., Javaid, N. (2022). Blockchain based privacy preserving authentication and malicious node detection in Internet of Underwater Things (IoUT) networks. IEEE Access, 10: 113945-113955. https://doi.org/10.1109/ACCESS.2022.3216850

[6] Yang, J., Fan, J., Zhu, X. (2023). Perception layer lightweight certificateless authentication scheme for IoT-based emergency logistics. IEEE Access, 11: 14350-14364. https://doi.org/10.1109/ACCESS.2023.3243624

[7] Pang, B., Teng, Z., Sun, H., Du, C., Li, M., Zhu, W. (2021). A malicious node detection strategy based on fuzzy trust model and the ABC algorithm in wireless sensor network. IEEE Wireless Communications Letters, 10(8): 1613-1617. https://doi.org/10.1109/LWC.2021.3070630

[8] Kumar, M., Mukherjee, P., Verma, K., Verma, S., Rawat, D.B. (2021). 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, 9(5): 3272-3281. https://doi.org/10.1109/TNSE.2021.3098011

[9] Nouman, M., Qasim, U., Nasir, H., Almasoud, A., Imran, M., Javaid, N. (2023). Malicious node detection using machine learning and distributed data storage using blockchain in WSNs. IEEE Access, 11: 6106-6121. https://doi.org/10.1109/ACCESS.2023.3236983

[10] Zhai, Z., Lai, G., Cheng, B., Qian, J., Zhao, L., Wu, J., Wan, Z. (2022). Lightweight secure detection service for malicious attacks in WSN with timestamp-based MAC. IEEE Transactions on Network and Service Management, 19(4): 5299-5311. https://doi.org/10.1109/TNSM.2022.3194205

[11] Fan, Q., Chen, J., Deborah, L.J., Luo, M. (2021). A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain. Journal of Systems Architecture, 117: 102112. https://doi.org/10.1016/j.sysarc.2021.102112

[12] Xu, H., Qiu, X., Zhang, W., Liu, K., Liu, S., Chen, W. (2021). Privacy-preserving incentive mechanism for multi-leader multi-follower IoT-edge computing market: A reinforcement learning approach. Journal of Systems Architecture, 114: 101932. https://doi.org/10.1016/j.sysarc.2020.101932

[13] Kumar, P., Gupta, G.P., Tripathi, R. (2021). TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. Journal of Systems Architecture, 115: 101954. https://doi.org/10.1016/j.sysarc.2020.101954

[14] Li, K., Lau, W.F., Au, M.H., Ho, I.W.H., Wang, Y. (2020). Efficient message authentication with revocation transparency using blockchain for vehicular networks. Computers & Electrical Engineering, 86: 106721. https://doi.org/10.1016/j.compeleceng.2020.106721

[15] Samuel, O., Javaid, N., Almogren, A., Javed, M.U., Qasim, U., Radwan, A. (2022). A secure energy trading system for electric vehicles in smart communities using blockchain. Sustainable Cities and Society, 79: 103678. https://doi.org/10.1016/j.scs.2022.103678

[16] Panda, S.S., Jena, D., Mohanta, B.K., Ramasubbareddy, S., Daneshmand, M., Gandomi, A.H. (2021). Authentication and key management in distributed IoT using blockchain technology. IEEE Internet of Things Journal, 8(16): 12947-12954. https://doi.org/10.1109/JIOT.2021.3063806

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

[18] Yahaya, A.S., Javaid, N., Javed, M.U., Almogren, A., Radwan, A. (2022). Blockchain-based secure energy trading with mutual verifiable fairness in a smart community. IEEE Transactions on Industrial Informatics, 18(11): 7412-7422. https://doi.org/10.1109/TII.2022.3141867

[19] Abbas, S., Javaid, N., Almogren, A., Gulfam, S.M., Ahmed, A., Radwan, A. (2021). Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things. IEEE Access, 9: 139739-139754. https://doi.org/10.1109/ACCESS.2021.3118948

[20] Jain, U., Hussain, M. (2021). Security mechanism for maritime territory and frontier surveillance in naval operations using wireless sensor networks. Concurrency and Computation: Practice and Experience, 33(17): e6300. https://doi.org/10.1002/cpe.6300

[21] Krishnaswamy, V., Manvi, S.S. (2021). Trusted node selection in clusters for underwater wireless acoustic sensor networks using fuzzy logic. Physical Communication, 47: 101388. https://doi.org/10.1016/j.phycom.2021.101388

[22] Muthukkumar, R., Manimegalai, D. (2021). Secured transmission using trust strategy-based dynamic Bayesian game in underwater acoustic sensor networks. Journal of Ambient Intelligence and Humanized Computing, 12: 2585-2600. https://doi.org/10.1007/s12652-020-02418-9

[23] Ahmad, B., Jian, W., Enam, R.N., Abbas, A. (2021). Classification of DoS attacks in smart underwater wireless sensor network. Wireless Personal Communications, 116: 1055-1069. https://doi.org/10.1007/s11277-019-06765-5

[24] Qin, Z., Ye, J., Meng, J., Lu, B., Wang, L. (2021). Privacy-preserving blockchain-based federated learning for marine Internet of Things. IEEE Transactions on Computational Social Systems, 9(1): 159-173. https://doi.org/10.1109/TCSS.2021.3100258

[25] Javaid, U., Aman, M.N., Sikdar, B. (2020). A scalable protocol for driving trust management in internet of vehicles with blockchain. IEEE Internet of Things Journal, 7(12): 11815-11829. https://doi.org/10.1109/JIOT.2020.3002711

[26] Isife, O.F., Okokpujie, K., Okokpujie, I.P., Subair, R.E., Vincent, A.A., Awomoyi, M.E. (2023). Development of a malicious network traffic intrusion detection system using deep learning. International Journal of Safety and Security Engineering, 13(4): 587-595. https://doi.org/10.18280/ijsse.130401

[27] Narayana, V.L., Midhunchakkaravarthy, D. (2021). Secured resource allocation for authorized users using time specific blockchain methodology. International Journal of Safety and Security Engineering, 11(2): 201-205. https://doi.org/10.18280/ijsse.110209

[28] Shaik, K.S., Thumboor, N.S.K., Veluru, S.P., Bommagani, N.J., Sudarsa, D., Muppagowni, G.K. (2023). Enhanced SVM model with Orthogonal Learning Chaotic Grey Wolf Optimization for cybersecurity intrusion detection in Agriculture 4.0. International Journal of Safety and Security Engineering, 13(3): 509-517. https://doi.org/10.18280/ijsse.130313