International Journal of Reconfigurable and Embedded Systems (IJRES)
Vol. 13, No. 2, July 2024, pp. 441~449
ISSN: 2089-4864, DOI: 10.11591/ijres.v13.i2.pp441-449

A condition-based distributed approach for secured privacy preservation of nodes in wireless sensor networks IoT

Bharat Kumara, S. Anantha Padmanabhan
Department of Electronics and Communication Engineering, Gopalan College of Engineering and Management, Bangalore, India

Article Info

Article history:

Received Feb 20, 2023
Revised Dec 23, 2023
Accepted Jan 25, 2024

Keywords:

CDPP
Internet of things
Nodes
Secure data transmission
Wireless sensor network

ABSTRACT

The fast expansion of wireless sensor network-internet of things (WSN-IoT) in recent years has led to the adoption of a vital infrastructure. Adversaries who work together to carry out privacy-related attacks and capture sensitive information from critical infrastructure for a range of personal, political, and commercial purposes, thus security and node preserving have been one of the key areas of research in WSN-IoT. Existing security and privacy research work focuses on cryptography, either which is less efficient, or it majorly focuses on securing the network, which further leads to exposing the nodes to the vulnerability in terms of privacy in the network. This research develops condition-based distributed privacy-preserving (CDPP) approach to preserve the sensor node privacy; the CDPP algorithm develops a condition based on which the nodes' vulnerable information is preserved and not accessed by the compromised nodes. CDPP architecture is evaluated considering the amount of misclassified nodes for safeguarding the node in the network. CDPP is evaluated by inducing the corrupt nodes and further comparing the model with existing low energy adaptive clustering hierarchy (LEACH) based on classification, misclassification and throughput. Furthermore, comparative analysis proves the marginal improvisation in terms of discussed parameter against existing protocol.

Corresponding Author:

Bharat Kumara
Department of Electronics and Communication Engineering
Gopalan College of Engineering and Management (GCEM)
Bangalore, Karnataka, India
Email: bharatk_12@rediffmail.com

1. INTRODUCTION

To gather and share data, the internet of things (IoT) is a network or hub of machines, objects, and devices equipped with sensors and connectivity-enabled technologies. The technology intends to revolutionize human existence by boosting internet technology; consequently, its applications in a range of lifestyles are expected to increase substantially [1]. The IoT is a new paradigm that enables the internet connectivity of multiple smart objects. Actuators and sensors may independently manage and transmit data to a system. Wireless sensor networks (WSNs) are an integral component of the IoT and are regularly used to collect data from local devices and send it to a central controller for further processing. IoT can benefit from WSNs, which can incorporate a range of processing, communication, caching, and sensing smart device components [2], [3].

WSNs are at the forefront of business, smart home, and environmental monitoring communication systems. The small size, low cost, and ease of deployment of this technology give real-time applications far more possibilities [1], [2]. WSN application depends on several variables. Even if there is no energy constraint, the delivery packets are the most critical factor to consider when building a network for industrial

and home automation applications. In hazardous circumstances where batteries are not replaced or recharged, such as mines, the network's longevity is the most important design consideration. Nevertheless, the size of the deployed zone has a substantial effect on the WSN's design. In smaller regions, the base station or sink nodes may directly receive packets from the sensory nodes. In bigger regions, however, packets must pass through many intermediate nodes [3]. The IoT-enabled system may link a variety of "things" to provide effective data exchange and communication for a single network [4], [5]. Shortly, IoT technology will play a crucial role in several industries, including healthcare, manufacturing, logistics, and transportation, as well as organizations that support the IoT's critical infrastructure [6]. Nevertheless, sensor nodes have limited energy, processing power, transmission range, and onboard memory. Because of these constraints, sensor nodes are susceptible to manipulation. Frequently, threats to WSN security emerge from both the outside and the inside of the network, with legitimate network nodes being infiltrated and sometimes coerced to act maliciously. To guarantee the security of a WSN, malicious nodes must be rapidly recognized, separated, and removed. Resolving security issues has had a significant influence on the design and development trends of WSNs and attracted a great deal of attention in the literature.

Due to the increasing complexity of design, it is tough to identify, access, and manage a wide variety of device applications and privacy issues. Nonetheless, the rapidly rising complexity of IoT devices causes a surge of data. Since private and sensitive information is routinely sent between networks, privacy, and security are the fundamental design issues for the IoT [7]. Any attack on a permeable cyber infrastructure might endanger the security and confidentiality of huge quantities of sensitive data [8], [9]. Since the development of information technology has affected the privacy of individuals, privacy protection strategies have been a subject of interest throughout history. Despite the increasing use of edge computing and fog concepts for IoT [10], latency, position awareness, connectivity, real-time data sharing, and quality of service (QoS) have deteriorated [11]. Data-processing devices on the periphery of IoT pose privacy problems [12]. Security is another key element of WSN. Anyone can listen in on the conversation since the data of WSNs is transferred freely over the air and accessible through these wireless signals. The wide majority of WSN nodes to conduct operations independent side band (ISB) uses the license-free ISB protocol. In both commercial and military applications, security is essential to withstand hostile attacks, such as unauthorized access and denial-of-service attacks (DoS).

Information confidentiality: when it is authorized by law, confidentiality implies the right to access information. The security of wireless networks is strongly constrained by the radio spectrum's openness and accessibility. An adversary may, for instance, recognize and modify the packet being sent. It is usual to only transfer data after it has been encrypted using a secret key that is only known to the intended recipients to ensure data secrecy.

Information integrity: a hacker who is familiar with the WSN protocol stack's packet architecture may also inject a fresh, deceptive packet into the network between nodes. The information in the packet is thus untrue or deceptive. Applications for surveillance, tracking, and environment monitoring are subject to compromise when such erroneous data is provided. To get around this issue, people frequently utilize message authentication codes, signatures, secret keys, and broadcasting authentication. WSNs are susceptible to faults because wireless transmission channels are unstable. Data that is traveling through an impacted electromagnetic medium need to be retransmitted due to signal fading, reflection, diffraction, scattering, and other types of noise. A considerable number of retransmissions in a WSN could be expensive in terms of energy consumption. Data integrity may be ensured via message integrity codes. There are several ways to safeguard privacy [13], including both traditional and present deep learning techniques. Existing deep learning approaches need expensive computation because they rely on fog/edge computing and the significance of their contributions to mission-critical information solutions.

To protect IoT data against Sybil attacks and DoS, various measures need to be carried out. The two types of access level-based cyber risks for IoT critical networks are passive and aggressive attacks [10]. Network connectivity is prevented by active attacks, also known as attacks with a security focus, which manage to get over the defenses put in place. On the other side, passive attacks aim for networks that ensure privacy to get unauthorized access to confidential data. IoT data is increasingly susceptible to hacking and organized crime due to its size and constant development. The rise in privacy hazards that target sensitive IoT data may be addressed in several practical ways. However, most proposed security measures are never implemented, whether because of logistical difficulties, high prices, or other pertinent circumstances. The research's contribution in light of the aforementioned issues is as:

- This research work designs a privacy-enabled secure mechanism named condition-based distributed privacy-preserving (CDPP) to protect the nodes' privacy; moreover, CDPP considers the dependability and security of the account along with reliability.
- CDPP is a condition based where the nodes aim to hide the vulnerable information regarding and cannot be accessed by compromised nodes.

- CDPP is evaluated considering the various compromised nodes to prove the CDPP model; further efficiency is proved by comparing with the existing low energy adaptive clustering hierarchy (LEACH) protocol for the detection of compromised and non-compromised nodes.

This research is organized as follows: i) the first section starts with a background of WSN along with the importance of security along with privacy, further, the section moves forward with research motivation and contribution; ii) the second section presents the existing security technique to preserve node privacy along with its shortcomings; iii) CDPP and its mathematical modelling are presented in the third section of the research work; and iv) CDPP is evaluated in the fourth section of the research.

2. RELATED WORK

Security and privacy have been one of the early issues raised in the research area concerning WSN; apart from energy efficiency, it is considered the major area for the researcher to focus on and develop a lightweight security model. This section of the research reviews the existing privacy and security aware framework developed. The star and tree topologies are combined in this work by Naghibi and Barati [12] to offer a safe data aggregation structure. The network is physically divided into four equal parts. A predictable and consistent informational star structure is known to each component. Pirbhulal *et al.* [13] offer a security- and dual-resource-aware architecture for internet of medical things (IoMT)-based remote medical systems. Medical data is secured using a biometrics-keys generation approach to assure consistency in IoMT and lower the system's resource needs. WSNs can benefit from the data aggregation technique created by Hasheminejad and Barati [14] based on a tree topology [15]. The plan aims to reduce energy consumption, increase network reliability, and prolong network life. This method yields a three-part binary tree as well as trustworthy data aggregation and verification. The routing dynamic data integrity (RDDI) approach enhances the data distribution and route-finding process [16].

Another option for securely sending data is to use a fuzzy hierarchical method. Efficient healthcare data aggregation (EHDA) technology makes data aggregation safe and portable [17]. The collecting node receives compressed health data from the sensor nodes. The secure and portable sharing of medical data is made possible by the use of symmetric key-based data encryption. Compression of healthcare data also lowers the cost of storage and transmission. Wang *et al.* [18] provide a binary tree-aided model for fog-based approaches. Sending processed data to the edge node is accomplished using the current method. Many IoT and industrial IoT applications employ WSNs, and in this case, the system works better while using fewer processing resources from the edge servers. The data aggregation methods employed in this study's industrial IoT (IIoT) are well known in WSNs for their capacity to lower energy usage, according to Li *et al.* [19]. Furthermore, these networks are exposed to a range of dangers due to their wireless connection. As a result, it is crucial to protect data while it is being collected. A novel technique for guaranteeing homogenous sensor devices in IoT-enabled WSNs is presented by Miao *et al.* [20], mobile-edge nodes are necessary for this technique.

While acknowledging the high level of consumer spending, Li *et al.* [21] addresses the problem of user privacy and security on two levels. The unique lightweight approach for privacy protection presented in Zheng *et al.* [22] is used to construct two non-colluding cloud platforms and develop a homomorphic cryptosystem. Li *et al.* [23] presents a novel strategy to disguise-based data poisoning attack (DDPA). It is determined to use a method in which the negative characteristics are masked to conceal the processes used to uncover the truth. In addition, the limitation of maximizing the attack's efficacy is automatically overcome by producing optimization issues at the bi-level, which are subsequently addressed by a separate optimization approach. Information-theoretical privacy (SEITP) is a unique semantic awareness for the protection of privacy in the progression of online location sharing, as outlined in [24], [25]. The highest level of protection is offered for both data privacy and semantic awareness.

3. PROPOSED METHOD

Secure data aggregation has been one of the efficient approach for securing the WSN, especially when the consensus-based protocol is adopted; in previous work, efficient secure aggrigated data (ESAD) and integrated data model (IDM) has been developed which solely focuses on the securing the aggregation approach while being efficient. However, while securing the data, it is important to preserve the privacy of the node especially in consensus-based protocol. This research work adopts the secured data aggregation from the previous work and develop a CDPP algorithm that aims at hiding the vulnerable information to the compromised nodes.

3.1. Preliminary analysis and network design

The network considered here for ($nodes \geq 2$), for communicating nodes with various neighbours, the communication topology is captured by a graph known as a communication digraph. A graph here is defined as $H_d = (X, Y)$, here $X = \{x_1, x_2, x_3 \ldots\ldots, x_n\}$ with cardinality $nodes = |K| \geq 2$ is the set of nodes and $C \subseteq X \times X - \{(x_b, x_b) | x_b \in X\}$ is the set of edges whose value is depicted by $g = |C|$. An edge connected from the node x_a to x_b that is denoted as $g_{ba} \triangleq (x_a, x_b) \in Y$, this captures the node x_b that receives the information from the node x_a. The given digraph $H_d = (X, Y)$ connected through the nodes $x_b, x_a \in X$, $x_b / = x_a$, there exists a directed route from x_a to x_b. The subset nodes are responsible for directly transmitting information to the node x_b is called the set of neighbours of x_b depicted as $\beta_b^- = \{x_a \in X | (x_b, x_a) \in Y\}$, the subset of nodes directly receive information from node x_b for a set of neighbours of x_b and denoted by $\beta_b^+ = \{x_{len} \in X | (x_{len}, x_b) \in Y\}$. The cardinality of β_b^- is called the in-degree of x_b denoted by α_b^-, $(\alpha_b^- = \beta_b^-)$, whereas the cardinality of β_b^+ is called the in-degree of x_b denoted by α_b^+, $(\alpha_b^+ = |\beta_b^+|)$.

3.2. Designing sensor nodes operation

At each time step $v \in S_{\geq 0}$, for each node $x_b \in Y$ retains the state variables $g_b^h[v], p_b^h[v], e_b^h[v]$, here $g_b^h[v] \in S$ and $p_b^h[v] \in S_{\geq 0}$. Here e^h is a memoryless function for the states g^h and p^h. By assuming each node aware of its neighbors to directly transmit messages to all of them. This cannot necessarily receive messages from them. The distributed protocols here, each node x_b allocates a unique order in the set $\{0,1, \ldots\ldots, \alpha_b^+ - 1\}$ for each of the outgoing edges f_{len_b} here $x_{len} \in \beta_b^+$, specifically to the link (x_{len}, x_b) for node x_b depicted by T_{len_b}(where $\{T_{len_b} | x_b \in \beta_b^+\} = \{0,1, \ldots\ldots, \beta_b^+ - 1\}$). The pre-determined order for execution of the proposed algorithm in a way for allowing the node x_b to transfer the messages to the neighbors in a round-robin fashion. Each node x_b in the network has an initial state $g_b[0] \in S$. At each step v for each node $x_b \in X$ retains the parameters $g_b[v] \in S$ and $p_b[v] \in S_{\geq 0}$ and state variables $g_b^h[v] \in S$ and $p_b^h[v] \in S_{\geq 0}$ and $e_b^h[v] = g_b^h[v] / p_b^h[v]$. The values of mass variables are updated as (1) and (2),

$$g_b[v+1] = g_b[v] + \sum_{x_a \in \beta_b^-} 1_{ba}[v] g_a[v] \quad (1)$$

$$p_b[v+1] = p_b[v] + \sum_{x_a \in \beta_b^-} 1_{ba}[v] p_a[v] \quad (2)$$

here $1_{ba}[v] = 0$ if no message is received at the node x_b from the neighbor x_a at iteration [v], the following cases are encountered.

- Scenario 1: $p_b[v+1] > p_b^h[v]$,
- Scenario 2: $p_b[v+1] > p_b^h[v]$ and $g_b[v+1] \geq g_b^h[v]$ is satisfied, the node x_b updates the state variables as (3),

$$p_b^h[v+1] = p_b[v+1],$$

$$g_b^h[v+1] = g_b[v+1],$$

$$e_b^h[v+1] = \frac{g_b^h[v+1]}{p_b^h[v+1]}. \quad (3)$$

it then transmits $g_b[v+1]$, $p_b[v+1]$, to an out-neighbor $x_{len} \in \beta_b^+$ and set the value $g_b[v+1]$=0 and $p_b[v+1] = 0$.

3.3. Problem definition for securing the vulnerable information of nodes

A connected digraph $H_d = (X, Y)$, where $|X| \geq 3$. Here each node $x_b \in X$ has an initial state of $g_b[0]$. The nodes here calculate the exchange of information. The information transfer takes place between the nodes aligned with H_d, which represents the system topology.

$$g = \frac{\sum_{len=1}^{k} g_{len}[0]}{k} \quad (4)$$

Any node in this set X, which means that it tries to identify the initial states g [0] for all the subsets of nodes in the network. The set X is segmented in two different ways: i) a subset of nodes $X_O \subseteq X$ to ensure privacy, the node $x_b \in X_O$ to retain its initial state $g_b[0]$ for other nodes remaining nodes in the set are $X_k = X \backslash X_O$ are indifferent to privacy and ii) a subset of nodes $X_c \subseteq X$to gather among them in identifying the

initial values of various nodes. The nodes herein X_c are responsible for not caring about the privacy to share the initial state with different nodes in X_c.

3.4. Condition based distributed approach

The main objective in the system is to evaluate g whilst ensuring the nodes follow the protocol, the approach is focused on the event-triggered deterministic algorithm with some alterations. The main issue is the approach deployed that focuses on an offset of the mass variable for each node $x_b \in X_O$, to preserve the privacy of its initial state $g_b[0]$. In the existing system, the node x_b for the initial state to $g_b[0]=g_b[0]+s_b$, here $s_b \in G$. The offset is initially given as d_b is a negative number shown as $d_b \in S_{\geq 0}$, henceforth to lead the calculations to the initial average after a few finite steps. Each node x_b ensures that privacy values like $d_b[v] \in S_{\geq 0}$ to add the steps, $A_b \in S_{\geq 0}$, for the offset added to the counter $a_b \in S_{\geq 0}$ and the transmission counter as $l_b \in S_{\geq 0}$. The value of the initial offset d_b to select greater neighbors β_b^+ to node x_b. For initial purpose each node selects steps a_b whereas the offsets as $d_b[v] \in S_{\geq 0}$ and $d_b[l_b] \in S_{>0}$ for all $a_b \in \{0,1,2 \ldots., a_b\}$.

In (5), the offset is added is A_b for each node x_b which is greater than or equal to the node x_b outer degree such that each neighbor x_a out-degree such that each of its neighbor $x_a \in \beta_b^+$ that receives a single value of $d_b[l_b]$ from node x_b.

$$A_b \geq \beta_b^+ \tag{5}$$

In (6) determines the accumulated offset integrated with the computation by the node x_b is equal to zero and the exact average of the nodes' initial state is determined without any error.

$$d_b = -\sum_{a_b=0}^{A_b} d_b[l_b] \tag{6}$$

In (7), the offset $d_b[l_b]$ is injected into the network for each node x_b when the event condition is triggered that needs to be non-negative to hold for each node after a few steps. The average value of the initial state is evaluated.

$$d_b[l_b] \geq 0, l_b \in [0, A_b] \tag{7}$$

In (8), the node x_b stops the offset in the network so that the accurate average of the initial states is estimated without any error.

$$d_b[l_b] = 0, l_b \in [0, A_b] \tag{8}$$

The above choice state that the offset d_b for each node x_b injects the network to be selected which is negative and satisfies $d_b \leq -\beta_b^+$. Henceforth ensuring the operation of the proposed mechanism. The event-triggered conditions do not hold on to the proposed protocol failing to evaluate the average of the initial state. The proposed algorithm has a value transfer process in which each node has a connected digraph $H_d = (X, Y)$, which performs executions according to a set of the event- triggered conditions. Each node here $x_b \in X_O$ to ensure privacy in these steps.

- A counter a_b is set to zero and sets the total number of offset-added steps A_b such as $A_b \geq \beta_b^+$ and the set of $(A_b + 1)$ with a positive offset $d_b[a_b] > 0$, here $a_b \in \{0,1,2 \ldots., a_b\}$. The initial negative offset value d_b injects the initial state value $g_b[0]$ to $d_b = -\sum_{a_b=0}^{A_b} d_b[a_b]$. The node x_b consists of four-out neighbors.
- To select the $v_{len} \in \beta_b^+$ in the order H_{lenb} to transmit $p_b[0]$ and $g_b[0] + d_b + d_b[0]$ to the out-neighbor. Then it sets the value to $g_b[0] = 0$, $p_b[0] = 0$, and $a_b = a_b + 1$.
- The algorithm is executed, at each step v, node x_b to receive a set of mass variables $g_a[v] = 0$ and $p_a[v] = 0$ for each-in neighbor $x_a \in \beta_b^-$. The node x_b updates the variables with $g_a[v]$ to check if the events-triggered condition holds. If true then $d_b[a_b]$ to $g_a[v + 1]$ and enhances the offset counter a_b by one. It then sets the variables $p_b^h[v + 1]$ and $g_b^h[v + 1]$ irrespective of $p_b^h[v + 1]$ and $g_b^h[v + 1]$. Then it transmits to an out-neighbor $p_b[v + 1]$ and $g_b[v + 1]$ to an out-neighbor in pre-trained order. Here x_b holds the $p_b[v + 1]$ and $g_b[v + 1]$. No message is received from any of –its neighbors, and with no transmission, the mass variable retains the same. Algorithm 1 presents the conditional approach for hiding the vulnerable information for securing the sensor nodes privacy.

Algorithm 1. Condition based privacy preserving

Input: A digraph, $H_d = (X, Y)$ with nodes $= |x|$ and $C = |Y|$ edges, each node $x_b \in X$ here has an initial state of $g_b[0] \in$

Step 1. Initialize each node $x_b \in X_O$

Step 2. A unique ID is assigned H_{lenb} in the set $\{0,1,\ldots..,\alpha_b^+ - 1\}$ for each of its neighbors $x_{len} \in \beta_b^+$

Step 3. This sets the counter value $q_b$to 0 and priority index w_b to q_b

Step 4. Set the counter a_b to 0, selecting $A_b \in Z_{>0}$, here $A_b \geq \beta_b^+$, and $d_b[v] \geq 0$ for $v \in \{0,1,\ldots,A_b\}$ and $d_b[v'] = 0$ for $v' > A_b$. To set the value $A_b = -\sum_{a_b}^{A_b} d_b[a_b]$

Step 5. This sets the value $g_b[0] = g_b[0] + d_b$, $p_b[0] = 1$, $p_b^h[0] = 1$, $g_b^h[0]$=$g_b[0]$

Step 6. It then picks the neighbor $v_{len} \in \beta_b^+$ such that $H_{lenb} = w_b$ and transmits $p_b[0]$ and $g_b[0] + d_b[0]$ to this out-neighbor. It sets the value $g_b[0] = 0, p_b[0], a_b = a_b + 1$

Step 7. Set the value $q_b = q_b + 1$ and $w_b = q_b \bmod \alpha_b^+$

Iteration: For $v = 0,1,2, \ldots\ldots$, each node $x_b \in Vp$ does the following

This receives $g_a[v]$, $p_a[v]$ in at least one-neighbor $x_a \in \beta_b^-$ updates the value accordingly. If either of the conditions holds;

This sets $g_a[v+1] = d_b[a_b] + g_b[v+1]$ and $a_b = a_b + 1$

This sets $p_b^h[v+1] = p_b[v+1], g_b^h[v+1] = g_b[v+1]$

and $e_b^h[v+1]$=$\frac{g_b^h[v+1]}{p_b^h[v+1]}$

this transmits $p_b[v+1]$ and $g_b[v+1]$ to out-neighbor

$\delta_\gamma \in \beta_b^+$ for which $\vartheta_{\gamma b} = w_b$ to set the value $g_b[v+1] = 0$,

$g_b[v+1] = 0$ and $p_b[v+1] = 0$;

This sets the value $q_b = q_b + 1$ and $w_b = q_b \bmod \alpha_b^+$

else it stores $g_b[v+1]$ and $p_b[v+1]$

Output: $e_b^h[v]$, for each $x_b \in X$

4. PERFORMANCE EVALUATION

When the data is aggregated, it is important to preserve the privacy of the nodes especially its initial information; thus to preserve the privacy of these nodes, this research develops CDPP mechanism which aims to preserve the model's node privacy. CDPP mechanism seeks to safeguard the privacy of sensor nodes and the integrity of the data. Additionally, CDPP is analyzed in consideration for classification and misclassification of sensor nodes. It is evaluated with a 2 TB hard drive, 16 GB of RAM, and 2 GB of NVidia CUDA-capable graphics. The model provided here analyses an inaccurate identification of a node that leads to network inequalities by including many parts, including the classification of the correct node, the misclassification of the node, and the computation of the throughput for 10, 15, 20, and 25 nodes. In addition, a comparison study between the proposed model and the existing model is undertaken to ensure the model's security and efficiency and to conclude that the proposed system outperforms the existing system.

4.1. Nodes classification

In this section, the classification of the sensor nodes is carried out wherein a comparison is made between the existing system and the proposed system by evaluating the correct identification of nodes with 10, 15, 20, and 25 nodes. Figure 1 shows the comparison of the stated above; in the context of 10 compromised nodes, the existing system detects 91 sensor nodes and the proposed model identifies 100 nodes. Consequently, in the context of 15 sensor nodes, the existing system identifies 91 nodes whereas the proposed model identifies 98 nodes. For 20 sensor nodes, the existing system identifies 87 nodes whereas the proposed model identifies 91 nodes for 25 nodes the existing system identifies 82 nodes whereas the proposed model identifies 97 nodes.

4.2. Nodes misclassification

Figure 2 depicts the misclassified nodes for 10, 15, 20, and 25 sensor nodes. In 10 nodes context, the existing model misclassifies 10 wrong nodes whereas the proposed model misclassifies 1 node. In 15 nodes, the existing model misclassifies 10 nodes whereas the proposed model misclassifies 3 nodes. In 20 nodes context, the existing model misclassifies 14 wrong nodes whereas the proposed model wrongly identifies 10 nodes for 25 nodes the existing system misclassifies 18 nodes and the proposed model misclassifies only 13 nodes.

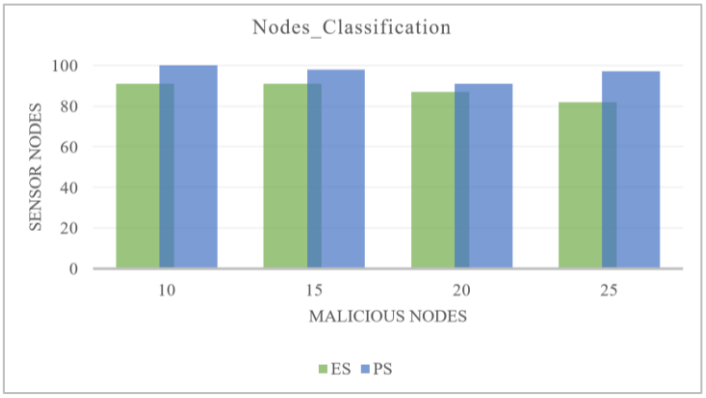

Figure 1. Nodes classification

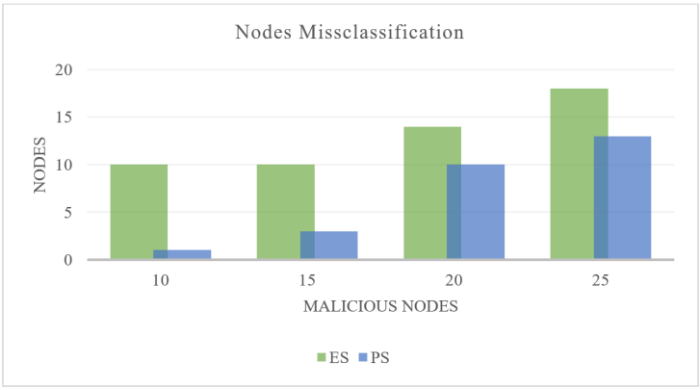

Figure 2. Nodes misclassification

4.3. Throughput

Throughput is defined as the amount of work done in a specific amount of time, it displays the models' efficiency; further depicted in Figure 3. In the case of 10 compromised nodes, the throughput of the existing model is 0.819 and for the proposed model, it is 0.989010989. In the case of 15 compromised nodes, the throughput of the existing model is 0.7735 and for the proposed model, it is 0.915384615. In the case of 20 compromised nodes, the throughput of the existing model is 0.696 and for the proposed model, it is 0.83781609 whereas for 25 nodes, the throughput of the existing model is 0.615 and for the proposed model, it is 0.887195122.

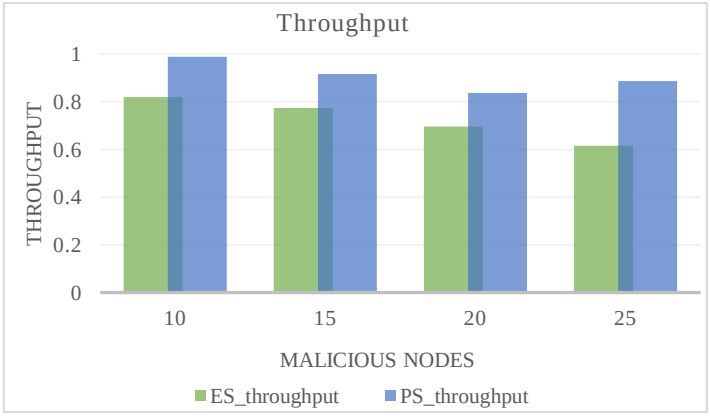

Figure 3. Throughput

4.4. Comparative analysis

This section displays the comparative analysis and shows the percentage improvisation for the proposed model from the existing model. The improvisation is carried out for 10, 15, 20, and 25 sensor nodes the improvisation for 10 nodes is 20.75836252%, improvisation for 15 nodes the improvisation is 18.34319527% for 20 nodes the improvisation is 20.22724% whereas, the improvisation for 25 nodes is 44.25936942%. Table 1 shows the improvisation of the CDPP model over the existing mechanism.

Table 1. Improvisation of the CDPP model over the existing mechanism

Nodes	Improvisation over the existing
10	20.75836252
15	18.34319527
20	20.22724
25	44.25936942

5. CONCLUSION

Sensor node security has been an integral part of any security framework of WSN-IoT; however, due to the development of the lightweight protocol, nodes face the exposing of its information, which could lead to the compromising position for the data transmission and result in violation of security protocol. This research work aims at securing the privacy of sensor nodes deployed in the network; CDPP adopts the secure data aggregation from previous work discussed earlier and develops certain conditions to meet the criteria that can protect the nodes against compromised nodes. Thus, if the specified conditions are satisfied, transmission to neighboring nodes continues; otherwise, transmission terminates. In addition, the CDPP architecture is evaluated for misclassification of nodes for 10, 15, 20, and 25 nodes. After calculating throughput and comparing the CDPP model to the current aggregation method, it is found that the CDPP model comparatively works better with the improvisation of 20.75%, 18.34%, 20.22%, and 44.25% for compromised nodes 10, 15, 20, and 25 in a respective manner. In a recent development to the growth of attack models based on deep learning, the future of research will involve the adoption of data integrity solutions such as blockchain.

REFERENCES

[1] T. A. Ahanger and A. Aljumah, "Internet of things: a comprehensive study of security issues and defense mechanisms," *IEEE Access*, vol. 7, pp. 11020–11028, 2019, doi: 10.1109/ACCESS.2018.2876939.
[2] L. Zhou, C. Ge, S. Hu, and C. Su, "Energy-efficient and privacy-preserving data aggregation algorithm for wireless sensor networks," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3948–3957, May 2020, doi: 10.1109/JIOT.2019.2959094.
[3] A. Li, W. Liu, L. Zeng, C. Fa, and Y. Tan, "An efficient data aggregation scheme based on differentiated threshold configuring joint optimal relay selection in WSNs," *IEEE Access*, vol. 9, pp. 19254–19269, 2021, doi: 10.1109/ACCESS.2021.3054630.
[4] B. A. Begum and S. V. Nandury, "Component based self-healing approach for fault-tolerant data aggregation in WSN," *IEEE Access*, vol. 10, pp. 73503–73520, 2022, doi: 10.1109/ACCESS.2022.3190004.
[5] N. A. El-Mawla, M. Badawy, and H. Arafat, "Security and key management challenges over WSN (a survey)," *International Journal of Computer Science & Engineering Survey*, vol. 10, no. 01, pp. 15–34, Feb. 2019, doi: 10.5121/ijcses.2019.10102.
[6] K. Ramasamy, M. H. Anisi, and A. Jindal, "E2DA: energy efficient data aggregation and end-to-end security in 3D reconfigurable WSN," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 2, pp. 787–798, Jun. 2022, doi: 10.1109/TGCN.2021.3126786.
[7] R. Goyat *et al.*, "Blockchain-based data storage with privacy and authentication in internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14203–14215, Aug. 2022, doi: 10.1109/JIOT.2020.3019074.
[8] F. Mukamanzi, M. Raja, T. Koduru, and R. Datta, "Position-independent and section-based source location privacy protection in WSN," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 5, pp. 6636–6646, May 2023, doi: 10.1109/TII.2022.3183804.
[9] C. Peng, M. Luo, P. Vijayakumar, D. He, O. Said, and A. Tolba, "Multifunctional and multidimensional secure data aggregation scheme in WSNs," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2657–2668, Feb. 2022, doi: 10.1109/JIOT.2021.3077866.
[10] L. Xiong, T. Peng, F. Li, S. Zeng, and H. Wu, "Privacy-preserving authentication scheme with revocability for multi-WSN in industrial IoT," *IEEE Systems Journal*, vol. 17, no. 1, pp. 38–49, Mar. 2023, doi: 10.1109/JSYST.2022.3221959.
[11] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion detection protocols in wireless sensor networks integrated to internet of things deployment: survey and future challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020, doi: 10.1109/ACCESS.2019.2962829.
[12] M. Naghibi and H. Barati, "SHSDA: secure hybrid structure data aggregation method in wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 12, pp. 10769–10788, 2021, doi: 10.1007/s12652-020-02751-z.
[13] S. Pirbhulal, O. W. Samuel, W. Wu, A. K. Sangaiah, and G. Li, "A joint resource-aware and medical data security framework for wearable healthcare systems," *Future Generation Computer Systems*, vol. 95, pp. 382–391, Jun. 2019, doi: 10.1016/j.future.2019.01.008.
[14] E. Hasheminejad and H. Barati, "A reliable tree-based data aggregation method in wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 2, pp. 873–887, Mar. 2021, doi: 10.1007/s12083-020-01025-x.
[15] A. Seyfollahi and A. Ghaffari, "Reliable data dissemination for the internet of things using Harris hawks optimization," *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 1886–1902, Nov. 2020, doi: 10.1007/s12083-020-00933-2.

[16] T. Wang, Y. Mei, X. Liu, J. Wang, H.-N. Dai, and Z. Wang, "Edge-based auditing method for data security in resource-constrained internet of things," *Journal of Systems Architecture*, vol. 114, p. 101971,2021, doi: 10.1016/j.sysarc.2020.101971.
[17] M. S. Yousefpoor, E. Yousefpoor, H. Barati, A. Barati, A. Movaghar, and M. Hosseinzadeh, "Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: a comprehensive review," *Journal of Network and Computer Applications*, vol. 190, p. 103118, Sep. 2021, doi: 10.1016/j.jnca.2021.103118.
[18] T. Wang *et al.*, "Mobile edge-enabled trust evaluation for the internet of things," *Information Fusion*, vol. 75, pp. 90–100, Nov. 2021, doi: 10.1016/j.inffus.2021.04.007.
[19] Y. Li *et al.*, "An efficient two-layer mechanism for privacy-preserving truth discovery," in *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, New York, NY, USA: ACM, Jul. 2018, pp. 1705–1714. doi: 10.1145/3219819.3219998.
[20] C. Miao, L. Su, W. Jiang, Y. Li, and M. Tian, "A lightweight privacy-preserving truth discovery framework for mobile crowd sensing systems," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, Atlanta, GA, USA: IEEE, May 2017, pp. 1–9. doi: 10.1109/INFOCOM.2017.8057114.
[21] Z. Li, Z. Zheng, S. Guo, B. Guo, F. Xiao, and K. Ren, "Disguised as privacy: data poisoning attacks against differentially private crowdsensing systems," *IEEE Transactions on Mobile Computing*, pp. 1–1, 2022, doi: 10.1109/TMC.2022.3173642.
[22] Z. Zheng, Z. Li, H. Jiang, L. Y. Zhang, and D. Tu, "Semantic-aware privacy-preserving online location trajectory data sharing," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2256–2271, 2022, doi: 10.1109/TIFS.2022.3181855.
[23] S. Li, Z. Liu, Z. Huang, H. Lyu, Z. Li, and W. Liu, "DynaPro: dynamic wireless sensor network data protection algorithm in IoT via differential privacy," *IEEE Access*, vol. 7, pp. 167754–167765, 2019, doi: 10.1109/ACCESS.2019.2953470.
[24] S. Shin and T. Kwon, "A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated internet of things," *IEEE Access*, vol. 8, pp. 67555–67571, Apr. 2020, doi: 10.1109/ACCESS.2020.2985719.
[25] F. Rezaeibagha, Y. Mu, K. Huang, L. Zhang, and X. Huang, "Secure and privacy-preserved data collection for IoT wireless sensors," *IEEE Internet of Things Journal*, vol. 8, no. 24, pp. 17669–17677, Dec. 2021, doi: 10.1109/JIOT.2021.3082150.

BIOGRAPHIES OF AUTHORS

Bharat Kumara received his B.E. degree in electronics and communication engineering degree at VTU, Belagavi, and his M.Tech. in digital electronics and communication engineering from VTU, Belagavi. He is full-time professor in the Department of Electronics and Communication Engineering at MSRUAS, Bangalore. His research lines are sensor networks, multimedia communication, and digital processing. He can be contacted at email: bharatk_12@rediffmail.com.

Dr. S. Anantha Padmanabhan working as a professor in the Department of Electronics and Communication Engineering at Gopalan College of Engineering and Management, Bangalore. He also published many articles in reputed journals and international conference. He obtained Ph.D. from Anna University Chennai in the field of digital signal processing and his area of research are signal processing, control systems, field theory and electrical machines. He can be contacted at email: ananthu.padmanabhan@gmail.com.