A novel and distributed three phase consensus based secured data sharing in internet of things environment

Rashmi H. Chamarajappa[1], Guruprakash C. Dyamanna[2]
[1]Department of Information Science and Engineering, Sri Siddhartha Institute of Technology,
Sri Siddhartha Academy of Higher Education, Tumkur, India
[2]Department of Computer Science and Engineering, Sri Siddhartha Institute of Technology,
Sri Siddhartha Academy of Higher Education, Tumkur, India

Article Info

Article history:

Received Jan 4, 2023
Revised Mar 3, 2023
Accepted Mar 12, 2023

Keywords:

Internet of things
Internet of things environment
Secure routing
Three-phase consensus based secured data sharing
Wireless sensor networks

ABSTRACT

The most essential part of any internet of things (IoT) model is the wireless sensor networks (WSN); latest technologies are combined with the applications of WSN results in fast, efficient, flexible as well as economical models. These networks are highly prone to attacks considering their characteristic nature, which includes self-organization, a topology that is dynamic, large-scale and constrained on the resources. Various models have been proposed for the detection of attacks in these wireless sensor networks. This research work proposes three-phase consensus based secured data sharing (TCSDS) in IoT environment. TCSDS adopts the consensus-based protocol for designing the security model in this research. Furthermore, TCSDS comprises three distinctive phases, each phase consisting of novel algorithm. First phase includes the setting up threshold value for sensor nodes. Second phase includes the efficient data packet transmission and third phase includes the efficient and secure routing, which tends to discard the unsecured nodes. TCSDS is evaluated considering the different parameter like energy consumption, malicious packet detection and throughput. Further comparison with the existing model is carried out based on the classified and misclassified packet; through the comparative analysis, it is observed that the TCSDS approach simply outperforms the existing model.

Corresponding Author:

Rashmi H. Chamarajappa
Department of Information Science and Engineering, Sri Siddhartha Institute of Technology
Sri Siddhartha Academy of Higher Education
Tumkur, India
Email: rashmihc_12@rediffmail.com

1. INTRODUCTION

Internet of things (IoT) network mainly deals with the collection of various devices over a network, which involves the transfer of data to and from the devices to the cloud or the transfer of data amongst the devices themselves. IoT in wireless sensor networks (WSN) is the crucial part of which involves various devices like sensors to monitor the changes across the environment and record the changes as smart cities [1], [2], healthcare sector in building a smart home, and giving disaster warning [3], [4]. The figure depicts a WSN architecture that consists of a base station, cluster head, and nodes; the information is sensed through the base station (BS) across the clouds. Figure 1 shows the architecture of WSN.

By nature, WSNs are susceptible to several attacks following their distinguishing nature that accommodates self-organization, a dynamic topology that are large-scale and constricted over the resources. The malicious attacks on the network are subjected to anomalies when the information is collected in the network. Information relevant to the security is collected known as security data utilized for detecting various types of intrusion threats, and attacks in the security domain. The data generated for applications relevant to WSN are used in the healthcare domain, smart home, and smart city. By taking into account various detection methods the security is sensory data, which includes the strength for receiving signals, acknowledgement, and various types of security data such as special data including the biometrics that is extracted appropriately. To detect the attack which supports the defense for security measures to resist malicious packets as well as threats to assure the security of WSN. Hence, it is an essential task in WSN for security purposes. The networks here are exposed either to accommodate the faults or attacks relevant to cyber which results in malicious packets in the sensory data which are categorized into degradation, precision, spike, drift, outlier, offset and stuck-at [5]. These anomalies are further classified as anomalies of short-term involving degradation, anomalies, spike precision, drift, outlier, and offset. Long-term anomalies are classified as drift, stuck-at as well as offset anomalies [6]. The attacks are detected based on their methods related to measuring the security at each point has been accommodated, however, the sink trust is missing. The literature survey is missing a holistic approach to the detection of attacks that is mainstreamed in WSN that is extremely essential for measuring security. The parameters considered here are our efficiency; the node energy is restricted to the resources for WSN being constricted. A threshold value is set for detecting an attack that has not been researched appropriately.

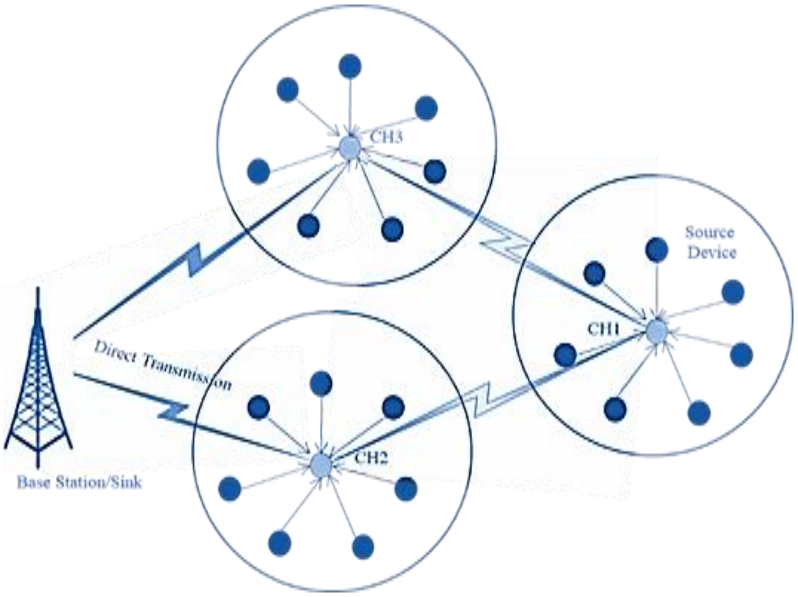

Figure 1. WSN architecture

The relevant attacks to ensure the security of WSN are categorized into two classes, one is passive attacks and the other is active attacks. The types of passive attacks are grouped into network interruptions, failure of the server, eavesdropping, analysis of traffic, and degradation of the network. Active attacks deal with activities and roles of the network, which is targeted. The main aim goal of the attacker here is to cause remarkable damage such that the security is not able to detect easily. Attacks like flooding; denial of service (DoS), black hole, jamming, Sybil, sinkhole and wormhole are classified as active attacks. The survey was performed by grouping the issues relevant to security as stated in. In paper the malicious attacks in an IoT environment an intrusion detection system (IDS) approach is proposed. The proposed mechanism here deals with two techniques known as reducing the dimensions and reducing the number of features that are used [7]-[9]. The complexity of this method is reduced by using a component principle and analyzing the linear discrimination. Further, there exist two types of methods known as naïve Bayes, and K-nearest neighbor (KNN) for these activities, which are malicious as well detected. In paper, an intrusion detection system based on a blockchain signature collaboration mechanism is used for IoT networks. In this proposed model, an attacker uses signatures or rules for detecting malicious attacks. The nodes share the data through a network to update the database, as well as improve overall detection. However, the possibility of an attack in a network is increased because the nodes may be malicious or consist of fake signatures that reduce the performance of combined IDS. To solve this methodology by blockchain, which is, used in intrusion detection systems databases. A lightweight detection system is proposed for usage in an IoT network (HADES-IoT) [10]-[13].

This method is applicable based on devices, and various methods, which are active and developed in Linux. The unique feature that differentiates this is likely to load this kernel into the OS. The usage of this method is increased in Linux for the installation of HADES-IoT. An approach for a client-based attention detection system is proposed for detecting the anomalies that are termed E-spion. There exist many players for security measures at each level, as the security is enhanced leads to a rise in overhead. In the first module, we have considered there exists a comparative analysis of the system for the processes, which execute IDS; this phase is carried out as a learning process for malicious process detection.

The data aggregation is a technique that minimizes the communication of nodes and the energy of each node for secure transmission of data; the security methods have a negative impact on the efficiency for data aggregation techniques. The approaches designed here satisfy the security requirements for security purposes that has a negative impact on the efficiency for energy of data aggregation approaches. Techniques designed here satisfy the requirements for security wherein the communication overhead is reduced. WSN layers have a combination more than a single attack predefined and launched in the stack of a protocol [14]. These attacks are DoS, jamming and man-in-the-middle (MITM) attacks. Attacks, which involve the physical layer known as jamming attack, have initial jamming whereas the data link layer has intelligent jamming attack. In the physical layer, the replay attack for network layer is grouped under MITM attack. The passive attacks are not responsible for sensing the missing emissions of radio adversaries as well the privacy is breached. The attacker's camouflaged. This research adopts a consensus-based technique for malicious packet detection, further the research contribution is stated by the given points.

- This research work presents three phases secured and consensus based data transmission approach; three-phase consensus based secured data sharing (TCSDS) comprises three phase each phase presenting a novel algorithm.
- First phase includes the Initialization phase where the threshold data range for the purpose to detect the any unsecured data packets.
- Second phase includes the efficient data packet transmission algorithm to enhance the network lifetime.
- Third phase includes the secured and efficient routing algorithm, which also identifies the malicious packet if any. Furthermore, consensus based approach is develop for data transmission.
- TCSDS is evaluated considering the different parameter like energy consumption for network lifetime evaluation, malicious packet identification and misidentification for security evaluation and throughput evaluation for TCSDS efficiency in term of security.

The research work is classified as following: the section 1 of the research work deals with the background introduction of the WSN concerned over the security, and this section further focuses on various security features and needless for various malicious packet detection techniques according to the security perspective. In the section 2 the advantages and disadvantages of the model of malicious packet detection. The section 3 presents a proposed methodology with mathematical formulation and algorithm; the performance evaluation is carried out in the section 4.

2. RELATED WORK

WSNs connected via IoT is prone to various attacks that damage critical security issue throughout the network. WSN attacks are categorized into two types; passive attacks and active attacks. Passive attacks are categorized as resultant of failure of the server, the attacker is responsible for the activities as well as the network whose motive is targeted at the attacker is to create an issue of the security of the network which detects conveniently. The attacks that as flooding, DoS, black hole, jamming, Sybil, sinkhole, and wormhole attacks are categorized as active attacks. The essential survey for classification of the issues, which pertain to the security model, is published in [15]-[18]. An intrusion detection system is proposed for different types of malicious attacks, which are detected in an IoT environment [19]. The proposed methodology deploys two methods for the detection of dimensions like decreasing the number of characteristics that are to be used. The complexity of this method is reduced as the component of the application principle and thorough analysis with linear discrimination. The two methodologies are distinguished as naïve Bayes and KNN for the detection of malicious nodes. A detection mechanism for intrusion based on blockchain-driven signature collaborated with IoT networks [20]. The proposed work here states that the intruder utilizes signatures or rules, which detect malicious activities. The nodes share the data via the network for updating the database as well as improvising the detection rate. The improving the rate of detection.

The possibility of attack within a network that increases due to the node within is malicious or fake signatures, which reduce the performance of the combined IDS method. Based on solving this methodology, a blockchain is proposed which is used for databases that are distributed widely across intrusion detection systems. A detection mechanism for the lightweight-based host is proposed and used in an IoT framework

(HADES-IoT) [21], [22]. This technique is based on a proactive model, which is deployed in Linux. The unique characteristics of this technique are responsible to load the kernel of operating system (OS). The useability is enhanced for the installation process of HADES-IoT. The machine learning techniques employed here are used at the level of nodes makes this approach effective in performance. An IDS approach here is proposed here to design a system that is depicted in two steps. In the first step, IDS uses a random model for a neural network for the anomaly [23], [24]. In the second step, a new system is proposed for designing a system, which is connected to the memory of the model [25]. A unique machine learning technique is proposed for IDS-based systems for detection of attacks the proposed paper the design phase of IDS initiates the data gathered until the models are built [24]. The proposed results are shown via the experiments stating that the proposed IDS method is responsible for analyzing the features of trained models built. The result produced here shows that IDS is capable of detecting four various models required for training.

3. PROPOSED METHOD

Existing systems for security purposes are discussed here in detail that tends to detect any kind of malicious activity. The existing systems are divided into two categories protecting and restricting the data, which leads to modification of information, and designing the access control. However, this requires alteration of the application or the network. This research adopts a lightweight consensus protocol that displays and detects the malicious packet and then creates a consensus based security model.

3.1. Energy model and preliminary analysis

The sensor nodes are connected through a cluster; the clustering approach is carried out thoroughly which is previously developed in consensus-based malicious packet detection. The proposed approach has a huge count of sensory nodes T , which is widely spread, across hospitals. For each node, a range for transmission is denoted by S_{max} that implements the network as depicted as a graph without providing the appropriate direction as given by a graph throughout its direction as $V = (G, H)$ to group the nodes given by $G = \{ g_1, g_2, \dots, g_T\}$ and H is the distance given in between two nodes g_a, g_b, the link of this data is transmitted across various nodes that has the edge of the node g_a, g_b here the data transmitted across any two different nodes having edge nodes g_a, g_b that belong to H do not accommodate similar capability. The capability of it to transmit this packet as depicted by J_{g_a, g_b} from the nodes g_a, g_b . Each node is responsible for data transfer of data packets communicating that is multi-hop for the base station, our proposed model here mainly deals with the consumption of energy in the first phase. A data message is transmitted from one node to another that has ∂ bits which are transmitted across each node placed at a distance d from each other, hence the consumption of energy is stated by (1).

$$EC_{G=}\begin{cases} \partial EC_{val} + \partial a_b x^2 & x \leq x_0 \\ \partial C_{val} + \partial e_{amp} x^2 & x \geq x_0 \end{cases} \tag{1}$$

Here in the equation given above the loss due to the transmission is denoted as EC_{val} , the energy power is given as a_b, the distance threshold is denoted as x_i. The message of ∂ bits is transmitted there exists energy consumption, the amplification of energy is depicted based on dissipation of network for transmission is given as (2).

$$EC = \partial EC_{val} \tag{2}$$

The rate at which the data packet is transmitted is shown as v_b to node n_b, so as the rate at which the null node is not working. The graph here is F_w=(G, H, W) for a graph based on an IoT network that is wide enough to forgo the bandwidth of the network. The packet of information is clustered up which leads to malicious data packets, the information packets are sent from one node to another $n_b\ to\ n_c$. The sending rate of the sending node n_b is greater than that of the receiving node n_c. This results in clustering and gathering the cache nodes in a network which leads to malicious data packets.

The main aim of the proposed model is that it effectively detects malicious data packets in the network. Other parameters detect the working of a network. The energy consumption during this process, the packet transmission and discarding the anomalies is the main focus of the paper on an IoT resulting in healthcare, the lifetime of the network is increased and opted as well. The network lifetime is split into different stages such that $[R_i, R_1, R_2, \dots, R_{q-1}, R_q]$, initially, the first node is considered which works and ends its working by the end stage R_i by the time the stage R_q is reached the node breaks down. The network is considered to frame the objective of the proposed model to detect malicious data packets. The parameter of traffic consumption of energy is considered at each stage of the network, the malicious data packets are detected under these conditions. The main goal of this section of our proposed model is to detect the malicious data packet through the IoT network by considering the healthcare systems for WSNs that are spread across the network lifetime. A few aspects are considered here which involve packet transmission, energy consumption, network traffic, discarding malicious data packets. The network traffic considered is of two types that are either sensitive or non-sensitive. Our proposed model consists of three phases; the initiation phase, packet transmission, detection of a malicious packet and discarding it. The IoT applications consist of various stages in which each stage exhibits the priority for IoT devices in the network, our proposed model consists of various nodes based on their importance. Before transmission of data packets, each node in this process is transmitted based on the priority status. Here exist two main types of nodes; one is the transmitter node and the other is the receiver node, the intermediate nodes here are transmitted based on the priority.

3.1.1. First phase

The lifetime of this phase is that it operates only once when the network process is initiated. For each node and its surrounding nodes, a single hop process is detected; after which the nodes are divided into various stages. At the initial phase, the value is given as $I_{st} = 1$ a packet is transmitted to the nodes in the range C_{Max}. Each packet has its ID, $I_{st} = 1$ and relevant data about the location. Once the node receives the packet with an initial phase value, its value is incremented by one other than the initiation phase, $(n\_b\ ) = I\_st + 1$. The nodes of the network, twice their Max range enhance the initiation phase value and increment a value at their initiation stage determined as the parent stage. The algorithm explains the process in detail. Algorithm 1 shows the malicious packet detection.

Algorithm 1. Malicious packet detection

```
Steps     Initiation Phase Detection Algorithm
Input     Sensory nodes
Step 1    $I_{st} = 1$ // the initiation stage value = 1
Step 2    A packet $I_{Stage}$ is transmitted within the $C_{Max}$
Step 3    For every node $n_t$
Step 4                   If the distance of the initiation stage to the node $n_t$ is $C_{Max}$
Step 5                          Then, I= $I_{st} + 1$
Step 6                          And, the value of their initiation stage as the parent stage
                                               $Parent = I_{st}$
Step 7                  End if;
Step 8    End for;
Step 9    For the range 2$C_{Max}$ the node $n_t$ transmits a packet for modification
Step 10   If node $n_b$ receives the packet
Step 11         And $I(n_b) > I(n_t)$ then
Step 12                         $I(n_b) = I(n_t) + 1$
Step 13                         $Parent(n_b) = n_t$
                                $Child\ (n_b) = n_t$
Step 14   Else discard packet
Step 15   End if;
Step 16   Every node $n_t$has and sends ID, $I_{st}$and the data regarding the location.
Step 17   End for;
Output    an initiation stage value has been set to all the nodes
```

3.1.2. Second phase: efficient data packet transmission

Once the data packet is received in the Initiation stage, the initiation node distributes the essential requirements for the nodes used to match the essential requirements. Algorithm 2 shows the secure and efficient packet transmission. In IoT applications, the information transmitted across is highly essential to be transferred while data collection. However, few parameters have sensitive information and data. During the transmission phase, the initiation node detects the stage along the location of the nodes from the data collected and determines the packet lifetime in the network. The lifetime of the packet that is transmitted to the level of transmission reliability and the packet overhead is decreased. The evaluation is given by (3).

$$I_{DP\_LS} = \sum_{1}^{des\_Stage}(R_r + R_g)\ I_r \tag{3}$$

In (3), the destination node value is given as des_stage, and the delay in the transmission is given as R_r, however, the delay in receiving the data packet is stated as R_g and the delay is calculated by R_g, the processing delay is given as I_r.

In the IoT network, multiple packets are received at the initial node end for varied or similar IoT devices connected through a network. The simultaneous transmission of packets results in network traffic, which results in malicious data packets in the IoT network. Our proposed model works on the priority of the data, the time request for the packets received is taken into consideration when the data packets are transmitted.

Algorithm 2. Secure and efficient packet transmission

```
Steps      Packet Transmission Algorithm
Step 1     Input: Packets from initial devices
           Output: Response to these Packets
Step 2     The initiation stage node receives data packets from the devices in the network
Step 3     Initialize response to these packets as per priority
Step 4     If the packets required are unavailable; then
Step 5           The stage is identified by the initial node and ID of a node $n_b$
Step 6           The packet lifespan is evaluated using (3)
Step 7           The life of the packet is set
Step 8           Send the $Response\_Packet$ with single-hop
Step 9     For every node $u_M$
Step 10           If the $u_M$ node ID= $u_a$ node ID
Step 11                     Then response packet is sent to the initial node
Step 12            end if;
Step 13            If $S(u_M) \neq S(u_a)$ then
Step 14                            The response packets are sent to the $Child$ nodes
Step 15            end if;
Step 16    If the lifespan of the packet $S_{Packet\_lifespan} = 0$ and $S(u_M) < S(u_a)$
Step 17           The packet is discarded
Step 18    end if;
Step 19    end for;
```

3.2. Consensus leverage and data aggregation

In this paper, the proposed work considered here is the detection of consensus of the anomalies for management of incidence of these malicious packets. The nodes spread wide across an IoT environment are capable to avoid anomalies by choosing various transmission paths for transferring the data packets. The anomalies are completely not avoided they are reduced in each step. The irrelevant anomalies are identified based on the consensus. The proposed approach consists of a classifier that consists of different packets as well as transmission. This is established for the given sections for transmission of packets that occur based on priority. The priorities are divided into three types: packets consisting of high priority, packets of low priority, and control management packets. The kind of packet mentions that for each packet in its header. The classifier is responsible to detect and classify the packet and arrange them in different queues according to the classifications and their priority. A scheduling system based on a priority queue is proposed according to various types of packets. The priority queue medium consists of low priority data that is processed and high priority data enters the queue. The data packets are transmitted in the queue, which stops the transmission path of various data packets. The anomalies are not avoided completely they are decreased. The rate at which the packets are received exceeds the transmission rate for high-priority packets. The packets of high priority are transferred across the priority queue that restarts transmission. Abnormal behavior is detected at the rate at which the packets are transferred exceeds the transmission of the packet. The packets are transmitted across the $Child$ nodes leads to an issue of missing packets or packet loss; these issues are not resolved via a different transmission route selected by the malicious packet that reaches a peak value. At a specific time, the $Child$ node sends the packet to the node, which is a response by an acknowledgement packet. The change in the path is decided by the $Parent$ node when the peak value is reached. The queue is filled approximately by 95% of this packet. Further, the data aggregated by (4).

$$Z_m^i = \sum_{h \; belongs \; to \; y_i} Z_h^i \tag{4}$$

Further, it is stated here that $Z^i = [Z_1^i, Z_2^i, Z_3^i, \ldots\ldots, Z_h^i]$ belongs to M^K that represents the data packet, which is detected when consensus is leveraged, and data aggregation is shown as (5).

$$Q_i(R_i) = S\left(\sum_{h=1}^{S} S_h\right)^{-1} \tag{5}$$

3.3. Third phase: efficient routing and malicious packet detection

This phase deals with packet transmission, the end node transmits a packet that updates the data to the initial node or this base station that utilizes an energy link that is efficient in a network. A high-priority data packet is transferred by a node to the initial node transformed across the specifications. The packets consist of the essential parametric values that the initial node provides the necessary response packets. In this section the data packet related to high-priority information is transmitted to the initial node, hence the initial node captures the data packet, that is related to the anomalies. This occurrence is sent to the parent node at the adjacent using the transmission link. This node may consist of many $Parent$s given in the initial stage that results in different paths of transmission to the initial node.

Consider, a set of nodes $\{n_1, n_2, n_3, \ldots., n_i\}$ the nodes considered here belong to the $Parent\{n_j\}$. By assuming the nodes, a high-priority packet is transmitted, and the evaluation of the energy consumption of the $Parent$ node is carried out by the node considered n_i the as shown in (6).

$$\alpha(n_y) = \frac{\sum_{g=1}^{i} EC_p(n_t)}{V} \tag{6}$$

Considering this equation, the current energy condition is stated as EC_p, the number of nodes in $Parent(n_y)$ is given as V. The energy of the $Parent$ is given as $L = \{l_1, l_2, l_3, \ldots, l_i\}$ which is equalized to the value of $\alpha(n_y)$. The node (n_y) transmits the packet to the $Parent$, in this section of the process there exists a likability for malicious packet detection. It is necessary for the proposed algorithm wherein the malicious packets are detected as well as discarded. The detailed Algorithm 3 for this section is explained.

Algorithm 3. The malicious packets are detected as well as discarded

```
Steps     Malicious Packet Detection
Step 1    Input: Malicious Packet Detection by the nodes
Step 2    For each node $n_i$
Step 3          For each node $S_h \in Parent\ (n_i)$
Step 4                $var = var + EC_p(S_h)$
Step 5          End for;
Step 6        $\alpha(n_y) = \frac{var}{Parent\ (n_i)}$
Step 7                For each node $S_h \in Parent\ (n_i)$
Step 8                            If $EC_p(S_h) = \alpha(n_y)$
Step 9                                  A= $A \cup n_1$
Step 10                           End if;
Step 11                End for;
Step 12   For each node $n_h \in A$
Step 13       If $Max\ EC_p(n_i)$ and $Min\ (dis(n_o, n_i))$
Step 14                $Max = EC_p(n_i)$
Step 15               The node $n_o$ is detected as a Malicious packet
Step 16        End if;
Step 17   End for;
Output    A malicious Packet detected is transmitted to the initial node or base station
```

4. PERFORMANCE EVALUATION

IoT applies to human beings in a wide variety of convenient measures; the attackers steal the configuration susceptibilities of the device that controls the service, steal data, hijack devices and operate illegally. However, these, restrictions not only lead to major security risks but also possess a serious risk to infrastructure services. These issues are resolved based on infrastructure service. The issues are not solved by detecting a malicious packet detection within the data packets. The simulation here is carried out using a sensoria simulator. The model requires 2 TB of hard disk embedded with 8 GB of random access memory (RAM), which is packed, with 2 GB of graphics. The performance evaluation here involves malicious packet detection by introducing different nodes. Evaluation is performed on malicious packet detection by comparative analysis of the malicious packet detection.

4.1. Energy consumption

Figure 2 depicts the energy consumption of the proposed model for varying numbers of different malicious nodes in response to malicious packet detection. Energy consumption for the TCDS model while considering case of 5, 10, 15 malicious nodes is stated below. From the figure we can conclude that once the malicious packet detection results in an optimal value for energy consumption.

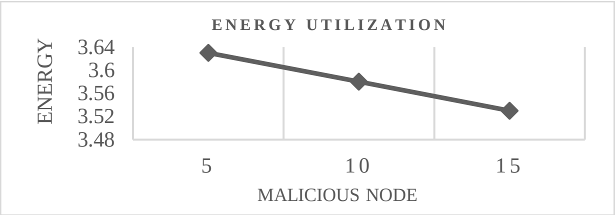

Figure 2. Energy consumption

4.2. Malicious packet detection

Generally, any abnormal behaviour in the sensor results in a malicious packet; evaluation is carried out for different malicious nodes as 5 nodes, 10 nodes, and 15 nodes. Figure 3 shows the malicious data packet detected for 5 malicious nodes, the sensed range is given as 25 to 30, value above this is considered a malicious data packet. Figure 4 shows the malicious data packet detection for 10 malicious nodes, this shows that the increase in malicious no nodes is directly proportional to the increase in malicious data packet detection. Figure 5 depicts the malicious data packet detected for 100 nodes where 15 nodes are malicious.

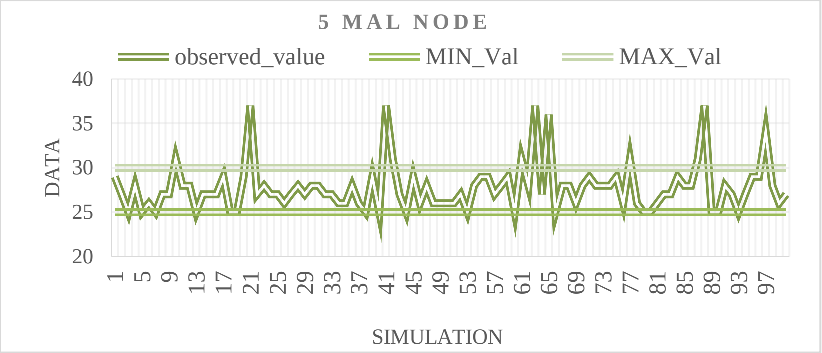

Figure 3. 5 malicious nodes

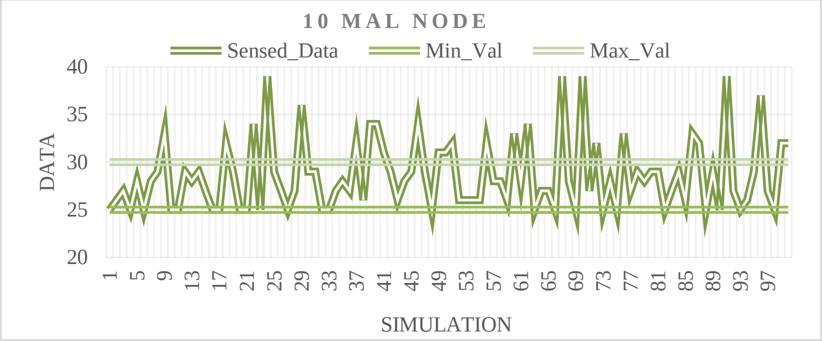

Figure 4. 10 malicious nodes

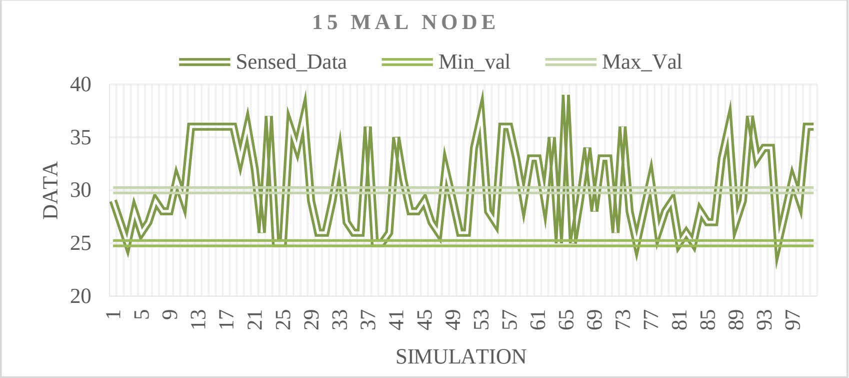

Figure 5. 15 malicious nodes

4.3. Classification and misclassification of the data packet

The malicious data packet is essential in terms of security; however, for various reasons as mentioned, there exists a possibility of detection of the normal data packet as malicious data packet, which leads to a major concern. In this section, the existing comparison of the existing system with the proposed system is carried out to analyze the correct identification of malicious data packets and normal data. Figure 6 classification and misclassification comparison of 5 malicious nodes induced. The proposed model is capable of detecting correct packets whereas the existing model fails to identify 9 packets. Figure 7 here depicts the classification and misclassification comparison of 10 malicious nodes induced. The proposed model classifies the model efficiently into normal data and indicates misclassified data packets whereas 1 indicates correctly classified packets. Figure 8 depicts the classification and misclassification of when 15 nodes are induced, through observation, the TCSDS model classifies each packet, as well as malicious data packets wherein the existing system, misclassifies 35 packets.

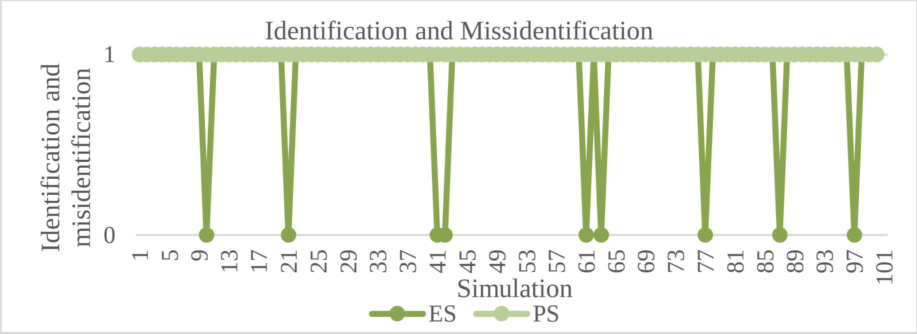

Figure 6. Classification and misclassification when 5 nodes are induced

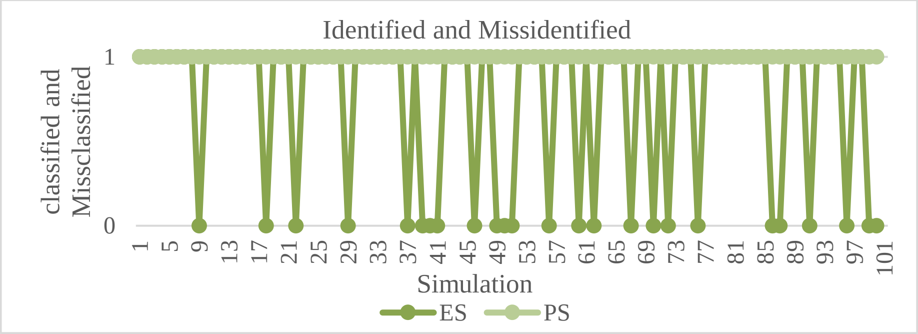

Figure 7. Classification and misclassification when 10 nodes are induced

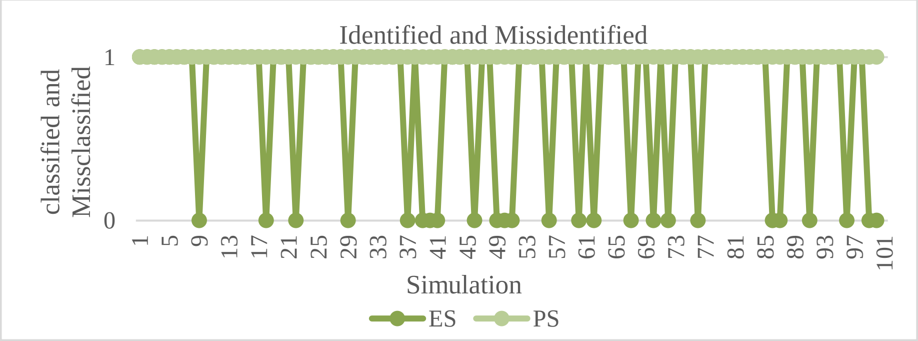

Figure 8. Classification and misclassification when 15 nodes are induced

4.4. Comparative analysis

In this section the research is carried out that performs the thorough analysis based on the throughput as depicted and given in Figure 9, the improvement in the proposed model over the existing system by variation in the malicious nodes as 5, 10, and 15. Throughput is stated as the total work done in a given period, by considering various metrics for efficient evaluation of proposed algorithm. In the case of 5 malicious nodes, the existing approach achieves a throughput of 80.99% whereas the TCSDS model achieves a throughput of 81.81%. in the context of 10 malicious nodes, the existing model observes a throughput of 96.15%. In the end, by considering the 15 malicious nodes, the existing model shows an increase in throughput of 27.95% whereas the proposed model observes a throughput of 81.39%. As shown in Figure 9, the proposed model for 5 different malicious nodes improves the throughput by 0.82%. The proposed model observes a 40.62% improvement over the existing model. For 15 malicious nodes, the proposed model results in an increase in the number of malicious packet detection, and the performance of the existing model depreciates wherein the proposed model enhances the throughput or remains steady.

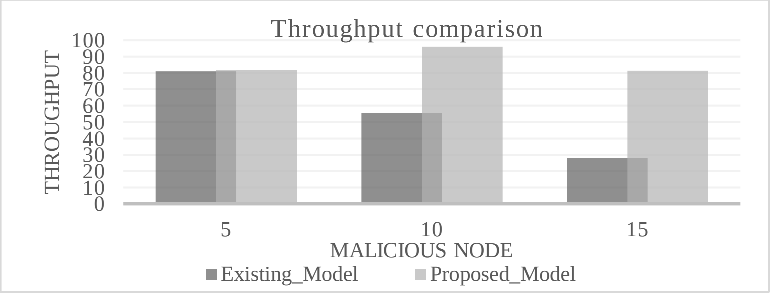

Figure 9. Comparison of existing and proposed model

5. CONCLUSION

IoT has been facing various security challenges in various application such as smart homes, smart city, military application and so on; security challenges occur due to various reason discussed in earlier section which mainly aims to compromise the data packets. Hence malicious data packet detection is effective to avoid risk. This research develops a mechanism TCSDS which is three phases secured and efficient data transmission model in IoT and each phase includes the particular algorithm; also, collectively TCSDS aims to process the secured and efficient routing through distribution model and identifying the malicious data packets. Consensus based approach has been adopted for performing the security protocol. Evaluation of the model is carried out in several steps; at first malicious data, packet detection on different malicious nodes is observed. Further thorough analysis is carried out in comparison with the classification and misclassification of data packets concerning the existing model. In last, a comparative analysis is carried out that states that a proposed model outperforms the existing model. The comparison analysis is carried out by considering the throughput of model efficiency. The comparison shows that the proposed model outperforms the existing system. The consensus-based malicious packet detection observes marginal improvement, by considering the susceptibility to which WSN is exposed along various security measures considered by an implementation based on a blockchain-based mechanism.

REFERENCE

[1] X. Miao, Y. Liu, H. Zhao, and C. Li, “Distributed online one-class support vector machine for anomaly detection over networks,” *in IEEE Transactions on Cybernetics*, vol. 49, no. 4, pp. 1475-1488, Apr. 2019, doi: 10.1109/TCYB.2018.2804940.

[2] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, “Data collection for security measurement in wireless sensor networks: a survey,” in *IEEE Internet of Things Journal,* vol. 6, no. 2, pp. 2205-2224, Apr. 2019, doi: 10.1109/JIOT.2018.2883403.

[3] T.-B. Dang, D.-T. Le, T.-D. Nguyen, M. Kim, and H. Choo, “Monotone split and conquer for anomaly detection in IoT sensory data,” *in IEEE Internet of Things Journal*, vol. 8, no. 20, pp. 15468-15485, 2021, doi: 10.1109/JIOT.2021.3073705.

[4] S. Jiang, J. Zhao, and X. Xu, “SLGBM: An intrusion detection mechanism for wireless sensor networks in smart environments,” in *IEEE Access,* vol. 8, pp. 169548-169558, 2020, doi: 10.1109/ACCESS.2020.3024219.

[5] K. Islam, W. Shen, and X. Wang, “Wireless sensor network reliability and security in factory automation: a survey,” in *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews),* vol. 42, no. 6, pp. 1243-1256, Nov. 2012, doi: 10.1109/TSMCC.2012.2205680.

[6] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, “An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security,” in *IEEE Internet of Things Journal,* vol. 7, no. 10, pp. 10250-10276, Oct. 2020, doi: 10.1109/JIOT.2020.2997651.

[7] N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande, “A review of security standards and frameworks for IoT-based smart environments,” in *IEEE Access*, vol. 9, pp. 121975-121995, 2021, doi: 10.1109/ACCESS.2021.3109886.

[8] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, “IoT: internet of threats? a survey of practical security vulnerabilities in real IoT devices,” *in IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8182-8201, Oct. 2019, doi: 10.1109/JIOT.2019.2935189.

[9] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A survey on IoT security: application areas, security threats, and solution architectures,” in *IEEE Access,* vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[10] A. Ghosal and S. Halder, “Intrusion detection in wireless sensor networks: Issues, challenges and approaches,” in *Wireless Networks and Security (Signals and Communication Technology),* Germany: Springer, 2013, pp. 329-367, doi: 10.1007/978-3-642-36169-2_10.

[11] A. G. Finogeev and A. A. Finogeev, "Information attacks and security in wireless sensor networks of industrial SCADA systems," *Journal of Industrial Information Integration*, vol. 5, pp. 6-16, Mar. 2017, doi: 10.1016/j.jii.2017.02.002.

[12] K. Shabana, N. Fida, F. Khan, S. R. Jan, and M. U. Rehman, "Security issues and attacks in wireless sensor networks," *International Journal of Advanced Research in Computer and Communication Engineering Science Electronic Enggenering (IJARCSEE),* vol. 5, no. 7, p. 81, 2016, doi: 10.5829/idosi.wasj.2014.30.10.334.

[13] S. Bartariya and A. Rastogi, "Security in wireless sensor networks: Attacks and solutions," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 3, pp. 214-220, 2016.

[14] K. Sharma and M. Ghose, "Wireless sensor networks: An overview on its security threats," in *Special Issue on 'Mobile Ad-Hoc Networks' MANETs,* 2010, pp. 42-45, doi: 10.5120/1008-44.

[15] A. Abduvaliyev, A. K. Pathan, J. Zhou, R. Roman, and W. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," in *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 1223-1237, 2013, doi: 10.1109/SURV.2012.121912.00006.

[16] S. Yao, Z. Li, J. Guan, and Y. Liu, "Stochastic cost minimization mechanism based on identifier network for IoT security," in *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3923-3934, May 2020, doi: 10.1109/JIOT.2019.2961839.

[17] S. S. Desai and M. J. Nene, "Multihop trust evaluation using memory integrity in wireless sensor networks," in *IEEE Transactions on Information Forensics and Security,* vol. 16, pp. 4092-4100, 2021, doi: 10.1109/TIFS.2021.3101051.

[18] M. L. Laouira, A. Abdelli, J. B. Othman, and H. Kim, "An efficient WSN based solution for border surveillance," in *IEEE Transactions on Sustainable Computing,* vol. 6, no. 1, pp. 54-65, 2021, doi: 10.1109/TSUSC.2019.2904855.

[19] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K.-K.-R. Choo, "A two–layer dimension reduction and two–tier classification model for anomaly–based intrusion detection in IoT backbone networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 2, pp. 314-323, Apr. 2019, doi: 10.1109/TETC.2016.2633228.

[20] W. Li, S. Tug, W. Meng, and Y. Wang, "Designing collaborative blockchained signature-based intrusion detection in IoT environments," *Future Generation Computer Systems*, vol. 96, pp. 481-489, Jul. 2019, doi: 10.1016/j.future.2019.02.064.

[21] D. Breitenbacher, I. Homoliak, Y. L. Aung, N. O. Tippenhauer, and Y. Elovici, "HADES-IoT: A practical host-based anomaly detection system for IoT devices," *In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, Auckland, New Zealand*, 2019, pp. 479-484, doi: 10.1145/3321705.3329847.

[22] A. Mudgerikar, P. Sharma, and E. Bertino, "E-spion: A system-level intrusion detection system for iot devices," *In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security,* Auckland, New Zealand, 2019, pp. 493-500, doi: 10.1145/3321705.3329857.

[23] A. Saeed, A. Ahmadinia, A. Javed, and H. Larijani, "Intelligent intrusion detection in low–power IoTs," *ACM Transactions on Internet Technology (TOIT),* vol. 16, no. 4, pp. 1-25, Dec. 2016, doi: 10.1145/2990499.

[24] X. Huan, K. S. Kim, and J. Zhang, "NISA: node identification and spoofing attack detection based on clock features and radio information for wireless sensor networks," *in IEEE Transactions on Communications*, vol. 69, no. 7, pp. 4691-4703, Jul. 2021, doi: 10.1109/TCOMM.2021.3071448.

[25] M. Sharma, H. Elmiligi, and F. Gebali, "A novel intrusion detection system for RPL-based cyber–physical systems," *in IEEE Canadian Journal of Electrical and Computer Engineering,* vol. 44, no. 2, pp. 246-252, Spring 2021, doi: 10.1109/ICJECE.2021.3053231.

BIOGRAPHIES OF AUTHORS

Rashmi H. Chamarajappa received B.E degree in Information Science and Engineering from Vivesvaraya Technological University, Belgaum, Karnataka, India in 2009 and M. Tech. degree in Computer Science and Engineering from Sri Siddhartha Academy of Higher Education, Tumkur, and Karnataka in 2011. She has teaching experience of 12 years and published 03 Technical Papers in National, International Conference and Journal. She is working in the field of network security and internet of things. She is working as an Assistant Professor in Department of Information Science and Engineering from 2011 in Sri Siddhartha Institute of Technology, Tumkur. She can be contacted at email: rashmihc_12@rediffmail.com.

Dr. Guruprakash C. Dyamanna has completed doctoral degree from Kuvempu University in 2014. He has teaching experience of 21 years and research of 16 years. He published 35 Technical Papers in National, International Conference and Journals. He is a Life member of ISTE and working in the field of computer networks, and internet of things. He worked as Assistant Professor in Department of Computer Science and Engineering from 2001 to 2014 and as Professor from 2014 to till date in Sri Siddhartha Institute of Technology, Tumkur. He can be contacted at email: guruprakashcd@ssit.edu.in.