A TRUSTED NODE FEEDBACK BASED CLUSTERING MODEL FOR DETECTION OF MALICIOUS NODES IN THE NETWORK

SIMHADRI MADHURI[1], DR. S VENKATA LAKSHMI[2]

[1]Research Scholar, GITAM (Deemed to be University), Department of CSE, Visakhapatnam,

Andhra Pradesh, India

[2]Asst. Professor, GITAM (Deemed to be University), Department of CSE, Visakhapatnam,

Andhra Pradesh, India

E-mail: [1]madhurisimhadri09@gmail.com, [2]svlakshmi2014@gmail.com

ABSTRACT

The study of malicious nodes is an interesting one, but it has had a negative impact on network performance characteristics. A degraded network response time may be caused by the attacker node's impact on network throughput. Analytical methods have been employed to combat the problem. The type of node is determined by analyzing the existing node's activity and its properties using behaviour based detection for malicious node detection. In the guise of machine learning, intelligent systems are devising new methods for locating and eradicating malicious nodes from the system. Lowering the severity of the data transmission degradation will be a difficult task because malicious nodes share many of the same properties as trusted nodes in the fixed region. Due to an increase in the number of malicious nodes, network performance will suffer. Malicious nodes in the network can affect metrics such as packet delivery ratio, performance, detection rate, energy consumption, accuracy value, and link failure. The proposed model calculates the trust factor of every registered node in the network. The trust factor is used in the process of node authentication and in detection of malicious nodes in the network. The proposed primary security module includes a dynamic authentication mechanism that allows current nodes to authenticate incoming new nodes, resulting in the development of secure links and disseminate authentication between surrounding nodes. The authentication strategy prohibits external hostile nodes from gaining access to the system. A Trusted Node Feedback based Clustering model for Malicious Node Detection (TNFC-MND) is proposed in this research for the detection and removal of malicious nodes in the network. Each node in the cluster receives the cluster key from the cluster head, and this key is used to exchange data with the cluster head. Every time a node sends data to the cluster, the cluster head verifies this key to see if it matches the cluster table. It will only acknowledge this node as a member of the cluster when the match is valid; otherwise, it will be deemed malicious. The proposed model is compared with the existing model, and the results exhibit better performance.

Keywords: *Network Nodes, Node Behaviour, Trusted Node, Network Cluster, Cluster Head, Malicious Node, Node Feedback, Data Loss*

1. INTRODUCTION

Wireless Sensor Network (WSN) is defined as a highly dispersed network created by a large number of small, lightweight sensor nodes for information gathering and maintaining at central level. Nodes that collect data and send it to a central location are called "sensor nodes" in a WSN [1]. The sensor nodes can sense, interpret data, and interact with each other over a wireless link, and they are typically placed in challenging locations [2]. Through hop-by-hop transmissions, the sensor nodes relay data to the base station, the network's center. At the aggregator node, all of the data is added together, and then just the totals are sent to the base station [3]. By reducing network traffic through aggregation, the overall energy needs of the network can be lowered.

Different nodes connected by a wireless route comprise wireless networks. Only a small number of networks are directly linked to the network by a single hop [4]. A few examples are the cellular voice, data, and IP (Internet Protocol) networks on sensor devices [5]. Desktop computers have transformed into networked agents that rely mostly on separate workstations within the last half a decade. Some of the unique educational and business services provided include email, cloud services [6], and access to the world wide web. Mobile computing on devices like tablets and laptops is also growing. Recent decades have seen an increase in research on digital advertising networks due to the increasing availability and demand for wireless communication services [7]. A WSN is a wireless infrastructure-connected, sensor device network. Because of their flexibility, self-governance, rapid deployment, and low-cost infrastructure [8], WSNs can be used for a variety of tasks, including environmental monitoring, disaster relief, and military communications [9]. The multi-hop data transmission technique of a decentralized system makes it more robust than network output [10].

Due to the several channels that data might take in a WSN, the likelihood of one failure point is greatly lowered. WSNs are able to overcome difficulties such as network fragmentation or disconnection because of their evolution over time [11]. Communications and security in a collaborative communications environment can only be improved with proper routing. However, because of the dynamic topology of the network [12], wireless connections media, and resource constraints, WSN faces extra safety and performance challenges. Because of this, the WSNs research community has been highly interested in developing a secure and efficient routing protocol [13]. A connection can be recognized by observing the behaviour of evaluated nodes with dimensional attributes and aggregating this information so that the original function of a network can be validated [14]. The behaviours of a contender router and its validation status are taken into account when a node makes a routing decision using a trusted multi-authenticated routing protocol [15]. The Reliable Validation metric quantifies this point of view. Trust measures are used to evaluate the best path to take from one point to another. In order to protect network performance and resources from unwarranted use, trust-based routing is essential [16].

Many WSN applications are critical to national security and public services, such as for army and healthcare purposes. WSN infested with misbehaving nodes that cause information loss by misrouting traffic with misinformation or by not passing packets to their intended destinations [17]. A reliable routing protocol can protect data transfer, offer safety data, and secure the value of data. There are, however, certain fundamental drawbacks to the traditional trust-based routing approaches [18]. There are inherent risks in wireless networks, but trust-based solutions introduce new ones that require extra care. The cluster head selection in WSN is shown in Figure 1.

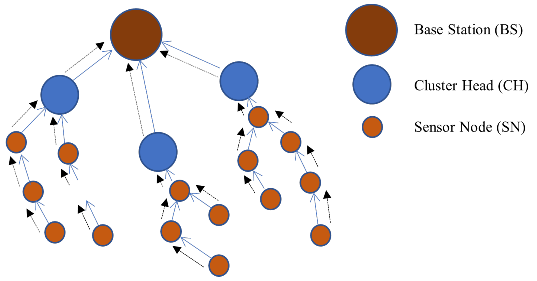

Figure 1: Cluster Head Selection

In WSNs, nodes work together in an uncontrolled external environment to do environmental monitoring. So, there are constraints on resources like power, data storage, connectivity, and processing power. This leaves them open to harm from both natural and man-made sources. According to the nature of the anomaly, a WSN classifies abnormal nodes as one of two categories [19]. Faulty nodes are network nodes that function incorrectly due to some sort of malfunction or accident. Malicious nodes are the opposite kind, and they are the ones that have been compromised by attackers [20]. Challenge collapse, distributed denial-of-service, fraudulent data injection (FDI), and witch assaults are all examples of such intrusions.

The limited computational, storage and communication capabilities of individual sensor nodes in WSNs make them vulnerable to compromise. Malicious nodes pose a serious threat to the integrity of the network because they can be used to launch a wide range of internal and external attacks including, but not limited to, eavesdropping on sensitive data as it travels through the network [21], flooding sensor networks with fake readings, disrupting the data aggregation process, and launching a variety of denial-of-service (DoS) attacks. Because malicious nodes in multipath will send false data or pollution data to access points in multiple paths at once, it is easy to cause the smog data to continue to spread [22], consuming a large number of valuable assets of intermediate routing nodes and ultimately shortening the life cycle of the entire wireless sensor network. As a result, it is crucial to detect, locate, and disassociate the malicious nodes in the routing process [23]. The malicious node in the cluster group involved in communication is shown in Figure 2.

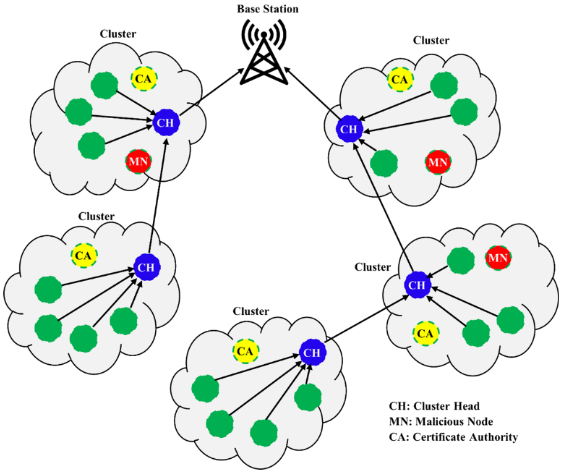

Figure 2: Malicious Node in Cluster Group

Malicious node detection has long been a focus of research in wireless sensor networks, and numerous credible methods have been developed by academics [24]. However, many sensor data in wireless sensor networks are conveyed by multipath for the sake of reliability, and existing detection systems of malicious nodes mostly focus on how to detect and locate malicious nodes in a single path [25]. A Trusted Node Feedback based Clustering model for Malicious Node Detection is proposed in this research for the detection and removal of malicious nodes in the network, which allows for the detection and localization of malicious nodes via different paths.

2. LITERATURE SURVEY

Khan et al.[2] proposed a model for developing trust among sensor nodes that is essential for improving security, dependability, and successful cooperation in WSNs, which have several applications in domains such as monitoring systems, army monitoring, healthcare, and intrusion detection. For large-scale WSN, conventional trust management systems have ended in failure due to their low consistency, greater communication, as well as memory overhead. By detecting malevolent sensor nodes with lower resource consumption, the author introduced a general and exhaustive trust forecasting model for large-scale WSNs that makes use of clustering to promote cooperation, trustworthiness, and security. On two levels, intra-cluster and inter-cluster, the proposed technique uses distributed and centralized approaches to make accurate trust decisions for sensor nodes with minimal overheads. One of the most notable characteristics is its strong trust estimate function that is attack-resistant, as well as its efficient trust aggregating at the cluster level. In dealing with hostile nodes, data and communication trust are critical. Even more importantly, statistical dispersion is used to eliminate malicious nodes.

Xia et al. [3] proposed a model that is concerned about the security of routing in automotive ad hoc networks. While cryptography-based solutions are seen as a potential approach, trust-based solutions, which primarily specify two activities: trusted computing and security application, are deemed more accepted as a promising approach. First, the author investigated trust qualities and develops a unique trust inference model, which uses two trust attributes, namely subjective trust and suggestion trust, to quantify the level of trust in a certain vehicle. Based on fluctuation recognition, a new evaluation approach for determining suggestion credibility is developed, which uses the SCGM weighted Markov predictive model to accurately quantify subjective trust. As a result, the author designed a light-weight trusted multichannel routing mechanism that can secure and reliably communicate by selecting trustworthy relay vehicles. Two approaches, including a forwarding node reuse mechanism and a trust-aware route handoff mechanism, are presented to further increase routing efficiency that avoid malicious actions.

Zhou et al. [6] proposed a model in light of the increasing rise of electronic social media platforms (OSNs), attackers have found OSNs to be a lucrative target. It's important to note the Sybil attack, in which a large number of harmful operations are carried out using Sybil accounts. Preconditions or assumptions, such as lowering the amount of attacking edges, are common in existing Sybil detection techniques. However, in the real world, only a few of these assumptions hold true. These methods operate badly when the hypothesis is not established. In this paper, the author suggested a solution to increase Sybil detection capability by using victim prediction. Senders don't need to make any assumptions to come up with a solution. A victim classifier was first developed to help identify potential victims. As a result of this prediction [34] process, the graph model's edge weights are tweaked accordingly. On the graph model, trust propagation is then carried out. All of the accounts are now sorted.

Gong et al. [8] proposed a model to provide feedback control, the sensor networks in smart city captures and transmits a massive volume of time and space sensitive data. In a way, it connects the digital world to the actual world. The trustworthiness and security of the Internet of Things are heavily reliant on the reliability of the data it collects. As a result, sensing nodes must be identified and proven to be trustworthy as the collection of data and transmission entity. In contrast, the existing studies were unable to identify and measure the trustworthiness of sensing nodes in real time. There is no viable way to protect the most sensitive information using existing methods of trust-proof security. First, this research presents a multifunctional and fine-grained dynamic measuring method in a trusted computing system to overcome these issues. This is followed by the presentation of an approach to classifying the trustworthiness of sensor nodes, and a grouping technique to identify faulty nodes. An authentication technique for data sources is proposed that relies on threshold ring signatures. The attestation node's privacy is fully protected, and the system is completely anonymous and untraceable. Because of its small signature and excellent computational efficiency, the technique is also well-suited to sensing nodes with constrained computer resources.

A number of studies have demonstrated that cluster Wireless Sensor Network are more efficient in terms of balancing energy consumption and battery life. As a result of their vulnerability to assault, clustered WSNs are vulnerable to attack. It is extremely difficult to detect a selective forwarding attack. During selective forwarding attacks, malicious sensor nodes drop some or all of the data packets they receive. A technique for identifying selective forwarding attacks (NB-DPC) is proposed in this paper by Ding et al. [10]. Clustering [32] of the Continuous Feeding Frequencies of all sensors enables it to detect assaults that only transmit certain packets. For quicker identification, the Density Peak Clustering (DPC) steps in the NB-DPC technique have been deleted and noise points developed specifically for spotting malicious behaviour.

WSN nodes are vulnerable to several threats because of their openness, including dishonest recommendation attacks, which provide fake trust values in the attacker's favour. A malicious node detection technique based on the fuzzy trust model and an artificial bee colony algorithm (ABC) is proposed in this paper by Pang et al. [12]. For the purpose of calculating indirect trust, the imprecise granting credit is presented, and the ABC method is used to optimize [33] the trust model. The suggested variation and interactions index deviation are both included in the fitness function.

Open communication and distribution in unsupervised places that make WSNs particularly vulnerable to a variety of attacks. For two reasons, the node capture operation is among the most hard inside assaults to detect. Malicious nodes commonly get away from detection because the unit in a tough environment must drop certain data packets. Reinforcement learning (RL) is used in this paper by Ding et al. [13] to describe a node capture attack against smart malicious nodes. The double-threshold densities peak clustering (DT-DPC) algorithm is designed to identify selective forwarding attacks in a hostile environment. Continual anomalies identify anomalous nodes as dangerous and isolate them. The neighbour voting method is used to identify suspicious nodes since malicious behaviour appears in discrete episodes, and harsh conditions disrupt aggregate nodes across all environments. Even if malicious nodes are able to evade identification by an RL methodology, DT-DPC increases the network's performance.

Hassan et al. [14] proposed an approach that considers the trust factor, neighbour feedback, and multi-level authentication while creating a secure data transfer path. In order to prevent malicious network behaviour, the proposed approach analyses authenticated nodes to find the secure path. Packet delivery is improved, and latency is reduced, with the proposed model's implementation. The provided model has a very low packet drop rate when compared to standard models. Node overhead can be reduced and performance increased by changing the processes for non - linear and non-identification and trust factor computation.

3. PROPOSED MODEL

Wireless sensor networks are dispersed at will and tasked with performing widespread monitoring. The restricted resources of a WSN and malicious users make data aggregation a challenging task. The data may be sent on malicious node, which is a problem in data aggregation. Because of the sensitive nature of such a huge data transfer, all current methods of data aggregation are vulnerable to intrusion. The malicious node detection method is based on the correlation detection principle, which allows us to identify malicious nodes. Sensor data is first analysed for temporal correlations that can reveal any irregularities. The effects of an abnormal event on a single node in a WSN will show up in the perception data for that node as a time series.

By comparing the node's historical data with the changes in the perceived data at the next time slot, the node's operational status can be determined. Spatial correlations can be used to identify malicious nodes. Since the same kinds of data transmission occurrences tend to have similar effects on neighbouring sensing nodes, it is possible to use their spatial correlation to ascertain their respective operational statuses. Finally, malicious nodes may be verified with the help of event correlation. Event correlations can aid in the first two steps of verifying malicious nodes because of the changes in node correlation that occur when events like data integrity violations and packet loss occurs.

When an adversary injects false data, it can have an effect on all of the system's sensors. In order to locate aberrant nodes, correlation between nodes is considered to find pairs with a low correlation. Spatial correlation between malicious nodes is analysed to identify them. When an assault occurs in a WSN, a cluster head's correlation fusion value will diverge from the values of other cluster heads, making it easier to spot malicious nodes. To identify malicious nodes, their anomalous situations are analyzed and compute the corresponding fusion value. The abnormal conditions of the nodes are first obtained by fusing the abnormal circumstances of each attribute datum by the cluster head. Node probability ranges can be used to convey the degree of uncertainty associated with a research problem. As a result, it is frequently applied to issues involving ambiguity. The cluster header determines the corresponding fusion value by calculating the degree of similarity between nodes based on each aberrant condition. A Trusted Node Feedback based Clustering model for Malicious Node Detection is proposed in this research for detection and removal of malicious nodes in the network. The process of trusted node feedback clustering model is clearly represented in algorithm. The proposed model framework is shown in Figure 3.

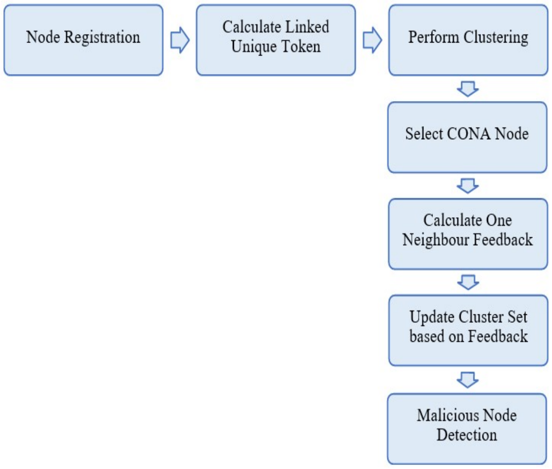
Node Registration
Calculate Linked Unique Token
Perform Clustering
Select CONA Node
Calculate One Neighbour Feedback
Update Cluster Set based on Feedback
Malicious Node Detection

Figure 3: Proposed Model Framework

Algorithm TNFC-MND

{

Step-1:

The nodes in the network will be considered to involve in data communication. Each registered node will be allocated with a linked unique token for easy identification in data transmission. The node behaviour is considered and the nodes which has best transmission levels in previous communications is considered and such nodes only will be registered. The node analysis and linked unique token is calculated as

$$Net(Node(i)) = \sum_{i \in Nset} \frac{nodeID(i)}{Th} + gettime[N(i)]_N + ener(i) + Th$$

$$LUToken\big(Node(i)\big) = \sum_{i=1}^{M} \max\big(Net(i)\big) + \max(PDR) * \frac{Th}{\max\,(ener(i))}$$

$$TFval(Node(i)) = \sum_{i=0} max(\,Net(i)) * \frac{Th}{count(Net)} + max(\,PDR) - min(\,Loss)$$

Here Th is threshold value considered at the node registration and the PDR is the packet delivery rate, Loss is the data loss rate in the previous transmissions.

Step-2:

The nodes registered will be considered for data transmission in the network and the nodes will be grouped as clusters. The clustering process will be performed by grouping nodes of similar location and properties for handling data transmission operations. The process of clustering is performed as

$$ClusterSet(DS(i)) = \left(\frac{\delta(TFval)}{2}\right)^2 + \sqrt{\left[\left(\frac{simm(Node(i,i+1))}{(1-F(i+1,i))}\right)^2 + \left(\frac{max(LUToken(i))}{Th}\right)^2\right]}$$

Here δ is the function that considers the best trust value, simm function identifies the similarity of node location to perform clustering. F is the function considering the tokens of the node and one neighbour node.

Step-3:

The trusted nodes only will be considered for communication and among the trusted nodes a Cluster One Node Appraiser (CONA) is selected that exhibits better cluster communication performance. The CONA node is considered as

$$CONA(Node(i)) = \sum_{i=1} max(TFval(Node(i)) + \frac{max(G(i,i+1)) + max(PDR)}{max(ener(Node(i))} + Th$$

Here G is the function considering the maximum computational capabilities and the packet delivery rate PDR and energy levels.

Step-4:

The cluster nodes will be frequently monitored by the CONA node for malicious behaviour analysis. The CONA node will take feedback from one neighbour feedback node and verifies the trust of a node and the cluster group will be updated. The one neighbour node feedback is considered and analyzed as

$$Feed(CONA(i)) = \sum_{i=1}^{M} PDR(Node(i+1)) - Loss(Node(i)) + \frac{availener(Node(i-1))}{allocener(Node(i-1))} + G(Node(i-1)) + \frac{\max\,(ClusterSet(i-1))}{LUToken(Node(i-1))}$$

Step-5:

In order to connect normal nodes, the CONA node will assess the feedback it receives from one neighbour node and then execute clustering based on self-feedback and one node feedback. Clustering using feedback from one node and self node and the cluster is updated as

$$CUpdate(Feed(CONA(i))) = \frac{\min\,(DUToken(i)}{\max\,(TFval(Node(i)))} + \max\,(PDR(Node(i))) + \frac{\max\,(\mathrm{Feed(Node(i))}}{sizeof(Net)}$$

$$FCset(Node(i)) = \sum_{i=1}^{M} \frac{max(Simm(ClusterSet(i),Cupdate(i)))}{G(i)} + LUToken(Node(i))$$

Step-6:

The malicious node detection is performed by analyzing the traffic flow in the network by the CONA node and the intrusion causing list is generated. The nodes causing more traffic than regular and nodes causing packet loss is considered and the list is generated as

$$MNodeset(Node(i)) = \frac{min(Loss)}{Th} + (\textstyle\sum_{i=1}^{M} min(FCset(i))). + \left[\sum_{i=1}^{M} \left(\frac{max(Loss)+max(ener(i))}{min(Feed(Node(i))}\right)^2\right]$$

}

4. RESULTS

Since several issues arise in the data processing technique referred to by each correlation module, correlation theory can be used to effectively identify malicious nodes. Inaccurate temporal correlation prediction models, data, node association fusion value calculations in spatial correlation verification, and the detection of malicious nodes are all considered in the model.

WSNs play a crucial role in understanding environmental features, hence protecting the accuracy of the data they collect is essential. Spoofing of identity and location by hostile nodes is one of the biggest threats to the safety of WSNs. During a phase of discovery, an empirical path loss model is produced at each node. This strategy takes into account a wide range of contextual elements, including mobility, channel characteristics, and network density and neighbour node feedback. Furthermore, the new method may pinpoint the discovered node to a relatively limited region. The high detection rate of the approach is highlighted by the simulation results under different settings. The proposed Trusted Node Feedback based Clustering model for Malicious Node Detection (TNFC-MND) model is compared with the traditional heterogeneous cluster based secure routing protocol (HCBS) model, Game-Theoretic Actor–Critic-Based Intrusion Response Scheme (GTAC-IRS) for Wireless SDN-Based IoT Networks,Identify Selective Forwarding Attacks Using Danger Model: Promote the Detection Accuracy in Wireless Sensor Networks (ISFA-DM). he proposed model when contrasted with the existing model exhibits better performance in malicious node detection.

It has been suggested that the integrated attributes model for delivering the security, dependability, privacy with respect to mobility is called trust in WSN. Trust in WSN must be established and evaluated so that nodes can communicate with one another in a safe, trustworthy manner. As a solution to access control, privacy, a safe routing strategy, and dependable communication in wireless sensor networks, trust is a crucial issue. The Figure 4 and Figure 5 shows the Node Trust Factor Calculation Accuracy Levels of and Table 1 gives the accuracy values of the nodes in network of the proposed and existing models.

Table 1: Node Trust Factor Calculation Accuracy Levels

Nodes in the Network	Node Trust Factor Calculation Accuracy Levels			
	TNFC-MND	*HCBS*	*GTAC-IRS*	*ISFA-DM*
50	91	87	83	80
100	93	88.5	84.5	82.5
150	94	90	87	87
200	95.5	90.5	88.5	89.5
250	97	91	89.5	92.5
300	97.5	93.5	90.5	94

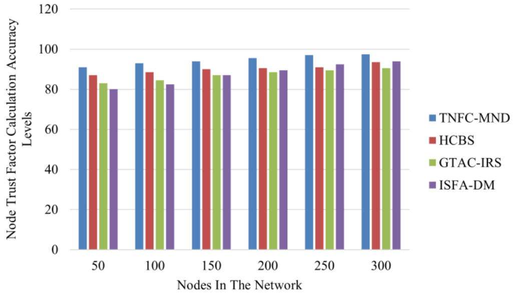

Figure 4: Node Trust Factor Calculation Accuracy Levels

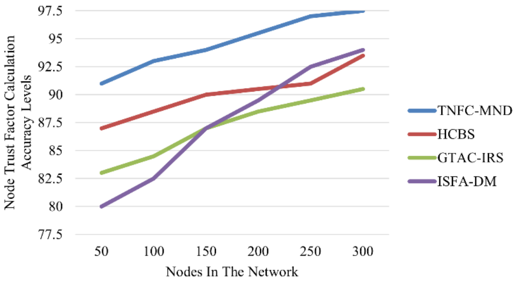

Figure 5: Node Trust Factor Calculation Accuracy Levels

As with the trust framework, the direct trust calculation requires three models: the node's security model, mobility model, and reliability model. Every node model's trustworthiness is calculated by the node itself. Along with the direct trust, indirect trust is calculated from neighbouring nodes. Trust can be labelled as low trust, medium trust, high trust, and extremely high trust, or it can be represented as a continuous variable across a defined range. When a node in a network receives a communication request from another node, it begins determining how much trust to put in the requesting node before establishing a secure connection. Table 2 gives the Trust Factor Calculation Time Levels of the existing and proposed models and are also shown in bar and line graphs in Figure 6 and Figure 7.

Table 2: Trust Factor Calculation Time Levels

Nodes in the Network	Trust Factor Calculation Time Levels				
	TNFC-MND	*HCBS*	*GTAC-IRS*	*ISFA-DM*	
50	10	17	23	30	
100	11	19	25	34	
150	12	19	27	36	
200	13	21	28	40	
250	16	22	30	42	
300	17	23	31	45	

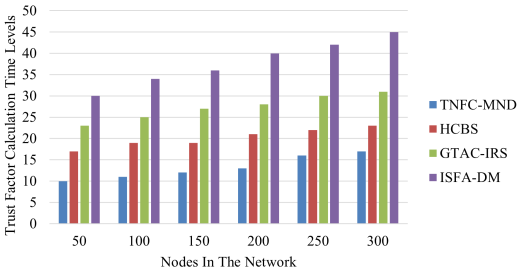

Figure 6: Trust Factor Calculation Time Levels

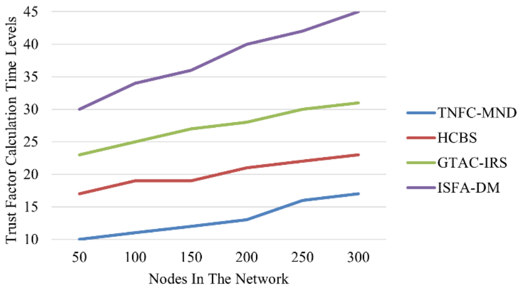

Figure 7: Trust Factor Calculation Time Levels

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Node variables of the system are represented by nodes in cluster-based network models, which then repeat the resulting dynamics on a directed network. High-order direct transfer functions identified from the data provide the basis for the transition attributes between the nodes. Because of its ability to perform network node trust calculation. The trusted nodes will be considered for cluster generation so that the entire network is divided into clusters for communication. Each node inside a cluster will talk to the cluster head to compile data. The information gathered by each cluster is sent back to the main hub. The Network Cluster Generation Accuracy Levels of the proposed and existing models are illustrated in Table 3 and are depicted in Figure 8 and Figure 9.

Table 3: Network Cluster Generation Accuracy Levels

Nodes in the Network	Network Cluster Generation Accuracy Levels			
	TNFC-MND	*HCBS*	*GTAC-IRS*	*ISFA-DM*
50	89	87	83	82
100	91	90	85	85
150	92	92	86	86
200	94	92.5	87.5	89.5
250	95.5	93.5	89.5	91.5
300	98	95	92	93.5

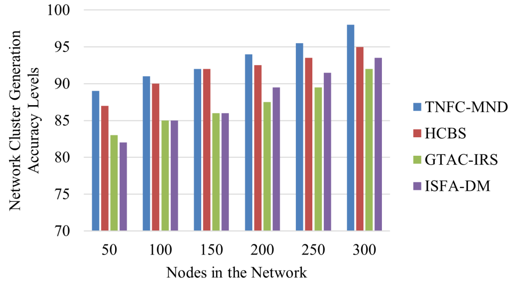

Figure 8: Network Cluster Generation Accuracy Levels

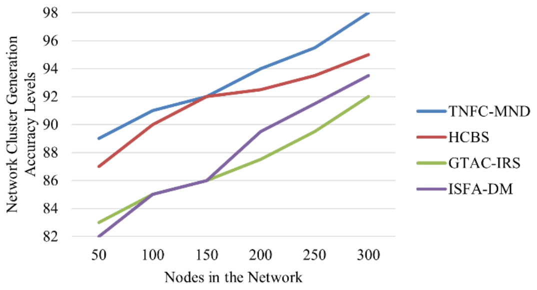

Figure 9: Network Cluster Generation Accuracy Levels

Clustering is a crucial procedure to extend the lifetime of the network in WSN. One type of node in a cluster is the cluster head, which is responsible for relaying information from the cluster's sensors to the main hub. The heads of each cluster might be chosen at random or according to certain criteria. The ideal cluster head selected in the proposed model has a high residual energy, a large number of neighbour nodes, and a short distance to the base station. The Cluster Head Selection Accuracy Levels of the proposed and traditional models are given in the Table 4 and also shown in Figure 10 and Figure 11.

Table 4: Cluster Head Selection Accuracy Levels

Nodes in the Network	Cluster Head Selection Accuracy Levels			
	TNFC-MND	*HCBS*	*GTAC-IRS*	*ISFA-DM*
50	86	88	82	84
100	89	90	84	89
150	91	91	84.5	91
200	93	92	86.5	92
250	95	94	91	93
300	98	95	91.5	95

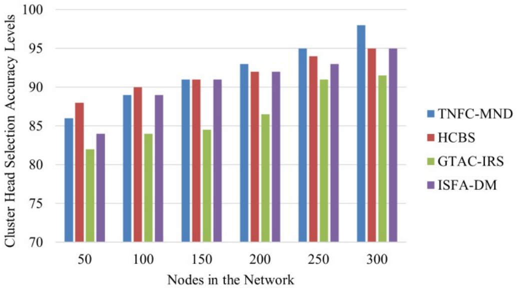

Figure 10: Cluster Head Selection Accuracy Levels

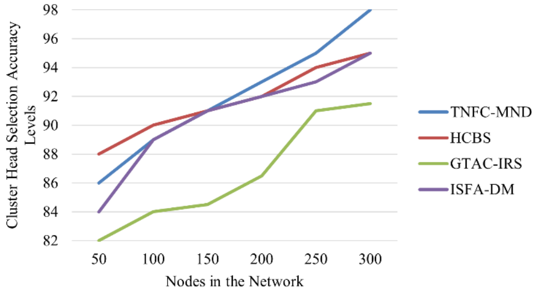

Figure 11: Cluster Head Selection Accuracy Levels

To keep track of information gathered during earlier communications in a network, the neighbour nodes are used for considering the feedbacks of other nodes. The status information from the previous execution can be stored in the feedback set to analyze the node behaviour. The trusted nodes in the WSN only will be considered for considering the feedback. The node feedback will helps the WSN to accurately identify the malicious action in the network. The Trusted Node Feedback Collection Accuracy Levels of the existing and proposed models are shown in Figure 12 and Figure 13. Table 5 illustrates the values of 6 nodes in the network.

Table 5: Trusted Node Feedback Collection Accuracy Levels

Nodes in the Network	Trusted Node Feedback Collection Accuracy Levels			
	TNFC-MND	*HCBS*	*GTAC-IRS*	*ISFA-DM*
50	88	89	84	84
100	90	90	87	85
150	93	91	89.5	87
200	93.5	91.5	90.5	87.5
250	95	93	93	89.5
300	97	94	95	90.5

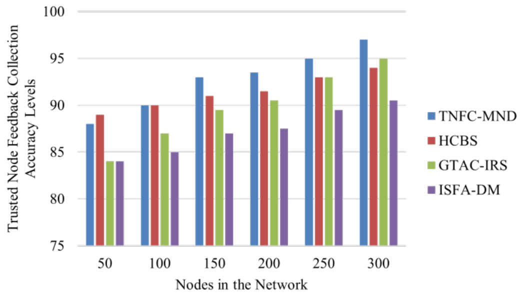

Figure 12: Trusted Node Feedback Collection Accuracy Levels

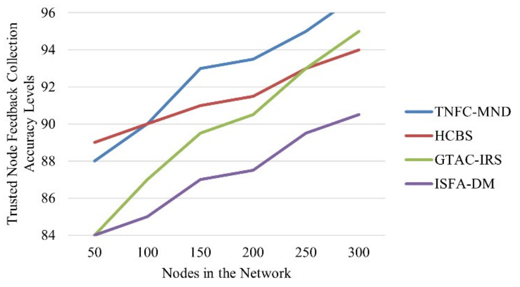

Figure 13: Trusted Node Feedback Collection Accuracy Levels

The feedback of the node in the network helps in node behaviour analysis. The malicious nodes need to be detected and avoided to improve the network performance. The nodes causing packet loss will be detected and nodes causing traffic in the network are identified to avoid such nodes in communication. The values of the Trusted Node Feedback Collection Time Levels of the proposed and existing models are given in Table 6 and shown in Figure 14 and Figure 15.

Table 6: Trusted Node Feedback Collection Time Levels

Nodes in the Network	Trusted Node Feedback Collection Time Levels			
	TNFC-MND	*HCBS*	*GTAC-IRS*	*ISFA-DM*
50	5	27	18	20
100	10	29	21	23
150	14	31	22	24
200	15	32	23	26
250	16	33	24	27
300	17	36	25	28

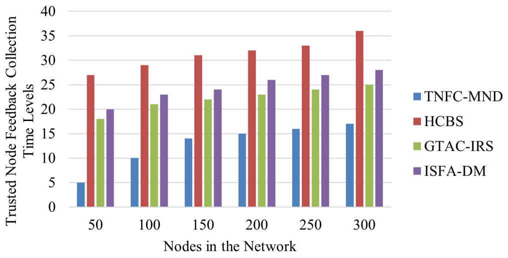

Figure 14: Trusted Node Feedback Collection Time Levels

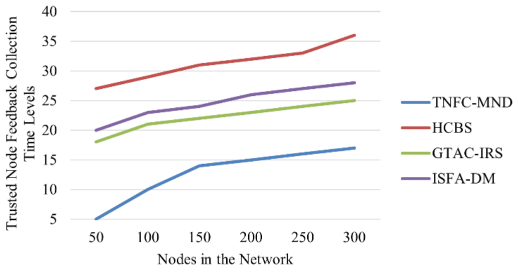

Figure 15: Trusted Node Feedback Collection Time Levels

Monitoring the activities of the assessed nodes with multidimensional attributes and combining this data allows for the detection of malicious nodes in a network, ensuring the network's integrity and proper functioning. A malevolent node is described as one seeking to refuse access to other nodes within the network. A malicious node is a node that tampers with data either before, during, or after transmission. WSN features a mathematical function that enables to set the calculations required and set the threshold level. A node is considered harmful if its count is higher than the allowed maximum threshold. Table 7 represents the Malicious Node Detection Accuracy Levels of the proposed and traditional models and are also depicted in Figure 16 and Figure 17.

Table 7: Malicious Node Detection Accuracy Levels

Nodes in the Network	Malicious Node Detection Accuracy Levels			
	TNFC-MND	*HCBS*	*GTAC-IRS*	*ISFA-DM*
50	93	87	87	81
100	93.5	89	91	83
150	94.5	90.5	91.5	85
200	96	92.5	92	85.5
250	96.5	93	94	86
300	98	95.5	95.5	90

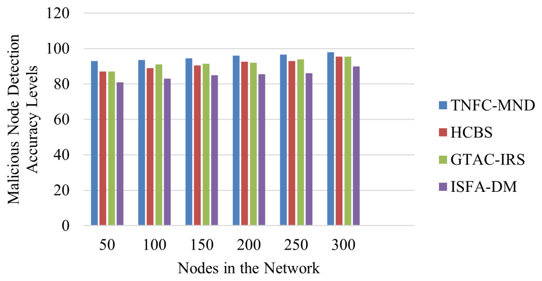

Figure 16: Malicious Node Detection Accuracy Levels

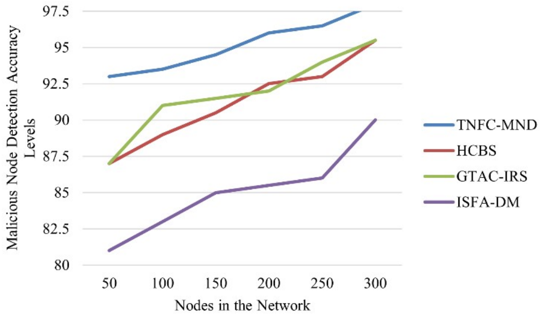

Figure 17: Malicious Node Detection Accuracy Levels

5. CONCLUSION

The security of WSN, a crucial information-transmission channel, has been recently compromised by a number of malicious nodes. The WSN is an autonomous, self-organized collection of sensor nodes that form a multi-hop wireless network. It is typically used in unmonitored settings where attackers can quickly compromise sensor nodes and skew detection outcomes by introducing fake data. A WSN is a collection of nodes/sensors that can considered across a network dynamically in order to exchange data. Sensor mobility, speed, direction and residual energy are used to build more stable intermediate routes between destination node in the sender and receiver node paths. A wide range of operational scenarios and situations have been tested to show that the methods offered are effective. For WSNs, an efficient and safe model for malicious node identification based on a mixed clustering network that makes use of both mobile trustworthy nodes and one cluster head is proposed. A Trusted Node Feedback based Clustering model for Malicious Node Detection model is proposed in this research for detection and removal of malicious nodes in the network. An efficient method for detecting and localising malicious nodes in WSNs is suggested that considered the trusted node feedback for accurate detection of malicious nodes in the WSN. The findings demonstrated that a greater detection rate is achieved by collecting a larger number of samples during the detection phase. In addition, it is observed that having more nodes take part in the detection process improves its precision. In future, multi cluster heads can be considered and the neighbour feedbacks also can be taken into consideration for the improvement of malicious node detection rate.

REFERENCES:

[1] Gomathy, Dr & Padhy, Dr. Neelamadhab & Samanta, Debabrata & Sivaram, M. & Jain, Vishal & Sadegh Amiri, Iraj. (2020). Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks. *Journal of Ambient Intelligence and Humanized Computing*. 11. 10.1007/s12652-020-01797-3.

[2] T. Khan et al., "A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks," in *IEEE Access*, vol. 7, pp. 58221-58240, 2019, doi: 10.1109/ACCESS.2019.2914769.

[3] H. Xia, S. Zhang, Y. Li, Z. Pan, X. Peng and X. Cheng, "An Attack-Resistant Trust Inference Model for Securing Routing in Vehicular Ad Hoc Networks," in *IEEE Transactions on Vehicular Technology,* vol. 68, no. 7, pp. 7108-7120, July 2019, doi: 10.1109/TVT.2019.2919681.

[4] K. A. Awan, I. U. Din, A. Almogren, H. Almajed, I. Mohiuddin and M. Guizani, "NeuroTrust—Artificial-Neural-Network-Based Intelligent Trust Management Mechanism for Large-Scale Internet of Medical Things," in *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15672-15682, 1 Nov.1, 2021, doi: 10.1109/JIOT.2020.3029221.

[5] S. Chen, Z. Pang, H. Wen, K. Yu, T. Zhang and Y. Lu, "Automated Labeling and Learning for Physical Layer Authentication Against Clone Node and Sybil Attacks in Industrial Wireless Edge Networks," in *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 2041-2051, March 2021, doi: 10.1109/TII.2020.2963962.

[6] Q. Zhou and G. Chen, "An Efficient Victim Prediction for Sybil Detection in Online Social Network," in *IEEE Access*, vol. 8, pp. 123228-123237, 2020, doi: 10.1109/ACCESS.2020.3007458.

[7] C. Ge, L. Zhou, G. P. Hancke and C. Su, "A Provenance-Aware Distributed Trust Model for Resilient Unmanned Aerial Vehicle Networks," in *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12481-12489, 15 Aug.15, 2021, doi: 10.1109/JIOT.2020.3014947.

[8] B. Gong, J. Liu and S. Guo, "A Trusted Attestation Scheme for Data Source of Internet of Things in Smart City Based on Dynamic Trust Classification," in *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 16121-16141, 1 Nov.1, 2021, doi: 10.1109/JIOT.2020.3006349.

[9] M. Debe, K. Salah, R. Jayaraman, I. Yaqoob and J. Arshad, "Trustworthy Blockchain Gateways for Resource-Constrained Clients and IoT Devices," in *IEEE Access*, vol. 9, pp. 132875-132887, 2021, doi: 10.1109/ACCESS.2021.3115150.

[10] J. Ding, H. Zhang, Z. Guo and Y. Wu, "The DPC-Based Scheme for Detecting Selective Forwarding in Clustered Wireless Sensor Networks," in *IEEE Access*, vol. 9, pp. 20954-20967, 2021, doi: 10.1109/ACCESS.2021.3055026.

[11] Y. Yengi, A. Kavak and H. Arslan, "Physical Layer Detection of Malicious Relays in LTE-A Network Using Unsupervised Learning," in *IEEE Access*, vol. 8, pp. 154713-154726, 2020, doi: 10.1109/ACCESS.2020.3017045.

[12] B. Pang, Z. Teng, H. Sun, C. Du, M. Li and W. Zhu, "A Malicious Node Detection Strategy Based on Fuzzy Trust Model and the ABC Algorithm in Wireless Sensor Network," in *IEEE Wireless Communications Letters*, vol. 10, no. 8, pp. 1613-1617, Aug. 2021, doi: 10.1109/LWC.2021.3070630.

[13] J. Ding, H. Wang and Y. Wu, "The Detection Scheme Against Selective Forwarding of Smart Malicious Nodes With Reinforcement Learning in Wireless Sensor Networks," in *IEEE Sensors Journal*, vol. 22, no. 13, pp. 13696-13706, 1 July1, 2022, doi: 10.1109/JSEN.2022.3176462.

[14] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan and A. Aldegheishem, "Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and Connected Vehicles," in *IEEE Access*, vol. 8, pp. 199618-199628, 2020, doi: 10.1109/ACCESS.2020.3034327.

[15] T. Khan et al., "A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks," in *IEEE Access*, vol. 7, pp. 58221-58240, 2019, doi: 10.1109/ACCESS.2019.2914769.

[16] N. I. Mowla, N. H. Tran, I. Doh and K. Chae, "Federated Learning-Based Cognitive Detection of Jamming Attack in Flying Ad-Hoc Network," in *IEEE Access*, vol. 8, pp. 4338-4350, 2020, doi: 10.1109/ACCESS.2019.2962873.

[17] T. Li, J. Ma, Q. Pei, H. Song, Y. Shen and C. Sun, "DAPV: Diagnosing Anomalies in MANETs Routing With Provenance and Verification," in *IEEE Access*, vol. 7, pp. 35302-35316, 2019, doi: 10.1109/ACCESS.2019.2903150.

[18] F. Li, Z. Guo, C. Zhang, W. Li and Y. Wang, "ATM: An Active-Detection Trust Mechanism for VANETs Based on Blockchain," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4011-4021, May 2021, doi: 10.1109/TVT.2021.3050007.

[19] L. Liu, X. Xu, Y. Liu, Z. Ma and J. Peng, "A Detection Framework Against CPMA Attack Based on Trust Evaluation and Machine Learning in IoT Network," in *IEEE Internet of Things Journal*, vol. 8, no. 20, pp. 15249-15258, 15 Oct.15, 2021, doi: 10.1109/JIOT.2020.3047642.

[20] S. -H. S. Huang and Z. Cao, "Detecting Malicious Users Behind Circuit-Based Anonymity Networks," in *IEEE Access*, vol. 8, pp. 208610-208622, 2020, doi: 10.1109/ACCESS.2020.3038141.

[21] Y. Hao, Q. Lu and X. Chen, "A Graph Representation Learning Algorithm for Approximate Local Symmetry Feature Extraction to Enhance Malicious Device Detection Preprocessing," in *IEEE Access*, vol. 10, pp. 53418-53432, 2022, doi: 10.1109/ACCESS.2022.3175581.

[22] U. Tefek, A. Tandon and T. J. Lim, "Malicious relay detection using sentinels: A stochastic geometry framework," in *Journal of Communications and Networks*, vol. 22, no. 4, pp. 303-315, Aug. 2020, doi: 10.1109/JCN.2020.000010.

[23] A. Tandon, T. J. Lim and U. Tefek, "Sentinel based malicious relay detection in wireless IoT networks," in *Journal of Communications and Networks*, vol. 21, no. 5, pp. 458-468, Oct. 2019, doi: 10.1109/JCN.2019.000049.

[24] W. She, Q. Liu, Z. Tian, J. -S. Chen, B. Wang and W. Liu, "Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks," in *IEEE Access*, vol. 7, pp. 38947-38956, 2019, doi: 10.1109/ACCESS.2019.2902811.

[25] K. Gu, X. Dong, X. Li and W. Jia, "Cluster-Based Malicious Node Detection for False Downstream Data in Fog Computing-Based VANETs," in *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 3, pp. 1245-1263, 1 May-June 2022, doi: 10.1109/TNSE.2021.3139005.

[26] K. Gu, X. Dong and W. Jia, "Malicious Node Detection Scheme Based on Correlation of Data and Network Topology in Fog Computing-Based VANETs," in *IEEE Transactions on Cloud Computing*, vol. 10, no. 2, pp. 1215-1232, 1 April-June 2022, doi: 10.1109/TCC.2020.2985050.

[27] M. Debe, K. Salah, M. H. U. Rehman and D. Svetinovic, "Blockchain-Based Decentralized Reverse Bidding in Fog Computing," in *IEEE Access*, vol. 8, pp. 81686-81697, 2020, doi: 10.1109/ACCESS.2020.2991261.

[28] M. Poongodi, M. Hamdi, A. Sharma, M. Ma and P. K. Singh, "DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET," in *IEEE Access*, vol. 7, pp. 183532-183544, 2019, doi: 10.1109/ACCESS.2019.2960367.

[29] Y. Li and Y. Wu, "Combine Clustering With Game to Resist Selective Forwarding in Wireless Sensor Networks," in *IEEE Access*, vol. 8, pp. 138382-138395, 2020, doi: 10.1109/ACCESS.2020.3012409.

[30] X. Xia, Y. Xiao and W. Liang, "SAI: A Suspicion Assessment-Based Inspection Algorithm to Detect Malicious Users in Smart Grid," in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 361-374, 2020, doi: 10.1109/TIFS.2019.2921232.

[31] S. M. P. Dinakarrao et al., "Cognitive and Scalable Technique for Securing IoT Networks Against Malware Epidemics," in *IEEE Access*, vol. 8, pp. 138508-138528, 2020, doi: 10.1109/ACCESS.2020.3011919.

[32] S Venkata Lakshmi, Valli Kumari Vatsavayi. Query optimization using clustering and Genetic Algorithm for Distributed Databases. *International Conference on Computer Communication and Informatics (ICCCI). IEEE*, 2016, doi: 10.1109/ICCCI.2016.7479934.

[33] S Venkata Lakshmi, Valli Kumari Vatsavayi. Teacher-Learner & Multi-Objective Genetic Algorithm Based Query Optimization Approach For Heterogeneous Distributed Database Systems, *Journal of Theoretical and Applied Information Technology*, April 2017.

[34] Sunita A Yadwad, Dr V. Valli Kumari and Dr S Venkata Lakshmi. Service Outages Prediction through Logs and Tickets Analysis. *(IJACSA) International Journal of Advanced Computer Science and Applications,* Vol. 12, No. 4, 2021, doi: 10.14569/IJACSA.2021.0120424.