Received: September 2, 2020. Revised: November 13, 2020.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Multi-Strategic Trust Evaluation for Intrusion Detection in Wireless Sensor Networks

Putty Srividya[1] **Lavadya Nirmala Devi[1]**

[1]*Department of Electronics and Communication Engineering, University College of Engineering, Osmania University, Hyderabad, India*
* Corresponding author's Email: puttysrividya8@gmail.com

Abstract: Wireless Sensor Networks (WSNs) have gained a huge research interest due to their nature of deployment and widespread applicability in several applications. However, the distributed deployment nature of WSNs poses several security challenges. In this paper, an Intrusion (Outlier) detection system is proposed based on multi-strategic trust metrics, which is flexible for constantly varying WSN characterized by changes in the variations in direct trust value, recommendations and capacities. Under the multiple strategic trust metrics, this approach considered three trust metrics; they are subjective trust, witness trust and Capacity trust. Furthermore, the capacity trust is modeled as the combination of fault tolerance trust and stability trust. Each node in the network measures the overall trust of its neighbor nodes based on these three metrics and decides whether it is malicious or not. Similarly, among the available routes, one route is finalized which has more Route Trust. Extensive Simulations are conducted over the proposed intrusion detection mechanism and the performance is evaluated through Malicious Detection Rate, False Positive Rate and Packet Delivery Ratio. From the results, we have noticed that the average Malicious Detection Rats of proposed model is 93.4012% while the False Positive rate and Packet Delivery Ratio are observed as 5.5000% and 74.1745% respectively. The obtained metrics indicate that the proposed method shows an outstanding performance in Intrusions detection and packet deliveries.

Keywords: Intrusion detection, WSNs, Witness, Capacity, Stability, Fault tolerance, Malicious detection, Packet delivery.

1. Introduction

In recent years, WSNs have been gaining a huge interest due to its widespread applicability in both public and industry related applications. According to Akyildiz et al., [1] the WSN can be applied in Home related applications, health care application, environmental monitoring, military applications and some other commercial applications. WSNs are composed of numerous cheap and tiny nodes that cooperate with each other to achieve the complex requirement of several applications. Unlike the nodes cooperation in wired networks (like intranet and internet), the cooperation between nodes in WSN faces several problems because the nodes have limited access, limited resource availability and several security concerns. Further the nodes in WSNs won't have any centralized administration to observe and regulate the risks. The Sensor Nodes (SNs) has flexibility to deploy even in an unattended environment and hence they are susceptible to several attacks and threats. Further the wicked actions from malicious nodes can threaten the nodes and may prevent from achieving their goals. Hence, for appropriate functioning, the security of nodes is the prime concern in WSNs [2].

Similar to the computer related environment in which the computers are protected from several viruses, the WSNs also need a security provision system. Generally, there are two types of security provision systems; they are detection based system and prevention based system. The prevention based security provision systems usually employs key management, cryptography, data fusion and secure routing etc. These mechanisms prevent the malicious activities based on pattern matching, key sharing etc. Hoverer, the prevention is the first line of defense, which is not sufficient for WSNs because the nodes which are already connected in the network may turn into malicious. Hence there is a need of run time detection which can detect the malicious entities even after the starting of process. This task is done by Detection based security provision system, Intrusion (Outlier) Detection System (IDS) the best example [3]. The main objective of malicious nodes is to maximize the damage by disrupting the operations in WSNs and consequently wasting the resources of senor nodes. Once any node in the network is compromised then the entire network needs to face so many challenges and this is due to the flexibility of cooperation. A node which was intended to cooperate must be more trustworthy and before choosing any node for cooperation, its trustworthiness must be checked in several viewpoints. Recently, Security provision based on IDS has been recommended as an effective security provision appliance to improve the reliability by mitigating several security threats or attacks within the network. Based on the analysis of node's behavior, the decisions regarding node selection can be made by checking the trust features those are derived through subjective or objective impressions. Based on this strategy, the malicious sensor nodes are detected and isolated from network. Generally, the Intrusion Detection in WSNs is modeled as a two phase model; in the first phase, the node checks the neighbor node's events while in the second phase, it decides whether the event is normal or not. This dynamic situation is an interaction between malicious node and checking node at which the IDS is installed. The main problem in IDS is the features based on which the node is deciding other node either malicious or not. Since there are so many attacks models, considering only a few set of features won't make the system resilient to all types of attacks. Even though several intrusion detection approaches [4] are proposed in earlier for the malicious node detection in WSNs, they have considered limited set of features. Most of the approaches are considered only communication interactions as a main metric to decide whether the node malicious or not. However, there may exist some malicious interactions, resulting in a less Malicious Detection rate [5], [6].

To solve this problem, we have proposed a new Intrusion Detection mechanism based on Multiple Strategies, called as Multi-Strategic Approach for Trust Aware Routing and Intrusion Detection. The proposed approach totally considers three types of trusts, namely Subjective Trust, Witness Trust and Capacity Trust for Intrusion (Malicious Node) detection in WSNs. A composite trust factor is formulated by combining all these trusts. Every node checks the trustworthiness of its neighbor nodes based on the composite trust factor and decides whether the node is trustworthy or not. If any node is discovered as malicious, such type of node is called as intrusion or outlier and isolated from network.

The organization of Remaining paper is done as follows; the particulars of literature survey are explained in section II. Section III explores the complete particulars of proposed approach. Section IV explores the particulars of simulation experiments and the obtained performance metrics. At last section V provides the conclusions.

2. Literature survey

Several approaches are developed in earlier for intrusion detection in WSNs. In all these approaches, the node which is turned as malicious is considered as the intrusion and that node is detected when a source node trying to establish a secure route towards destination. Similar to the standard IDS methodology which was generally employed through machine learning algorithms, in WSNs, the intrusion is detected based on its characteristics. Since the malicious behavior of a node is too much deviated with its normal behavior, another monitoring node is can identify it. During the detection process, another node compares the malicious node's behavior with its earlier behavior based on past experience. If the node found to be malicious, then it is simply removed from network. Based on this methodology, so many authors tried to develop an efficient intrusion detection mechanism to prevent the network from several attacks [12].

Bao et al., [6] proposed a hierarchical trust management framework [11] for the detection of intrusion detection in WSNs. In this approach, multiple trust attributes are considered and the trust value is measured through QoS trust as Social trust. Under QoS trust, this approach considered unselfishness, energy, honesty, and intimacy; meanwhile the objective and subjective trusts were taken into consideration. However, this approach assumed that the nodes which have maximum number of interactions are considered as more trustworthy. This assumption is not correct because in some attacks, like flooding, the nodes communicate more times. Hence our method considered the witness trust based on which the sensor node seeks the help of common nodes for trust evaluation.

M. Riecker et al., [7] proposed an energy efficient and light weight intrusion detection mechanism to make the network secure from Denial of Service

(DoS) Attack, i.e., Flooding attack. This approach used the energy consumption as a reference metric to detect the intrusion nodes. The energy consumption of a node is estimated bas on linear regression model. However, the single energy based analysis won't have much significance in the evaluation of trustworthiness. If a node is working as relay for more sensor nodes, then the energy depletes quickly. Unlike this method, our method considered three metrics for trustwortniness evaluation.

Next, the intrusion detection mechanism proposed by Gerrigagoitia K [8] considered the reputation and trust of the different nodes for decision making and to determine the possible sources of malicious attacks. If any node suspects about the confidence of any other node, then that node can ask other common nodes about the reputation of suspected node. Based on most shared opinions the trustworthiness is confirmed. However, some attacks are there which effects on the stability of node which was not considered here.

Next, Xie Jinhui et al. [9] proposed an intrusion detection model for the detection of Hybrid DoS in WSNs. A power series correlation check is proposed based on the energy consumption estimation algorithm. However, the energy parameter is not sufficient for trust calculation. Hence we have considered interaction between nodes in both direct and indirect fashion.

An "Efficient and Light weight Intrusion Detection (ELID)" mechanism is proposed by Sedjelmaci H, and Senouci S M [10]. In this approach, the malicious nodes are detected by observing the characteristics of nodes in the same cluster by assuming that the nodes in the same cluster have similar behavior. This approach mainly intended to detect DoS attack, Wormhole attack, Sink-hole attack, Black hole attack and Selective Forward attack. However, the assumption may not correct because generally the clustering is accomplished based on distances. Even though it was able to detect multiple attacks, the stability and fault tolerance is not considered which also have significant impact on the security in WSNs.

Li et al., [13] proposed a "Lightweight and Dependable Trust System (LDTS)" for clustered WSNs. In the process of trust evaluation, LDTS considered only successful and unsuccessful interactions for trustworthiness calculation. A self-adaptive weighting mechanism is proposed for trust calculation at cluster head level. However, this approach has less robustness in the attacks that effect on the stability and fault tolerance, for example jamming attack.

One more light weight trust management mechanism is proposed by He et al., [14] called as ReTrust for intrusion detection in "Medial Sensor Networks (MSNs)". ReTrust is a hierarchical trust management approach in which the cluster heads stores the trust values of all of its cluster members. In this approach, the trust evaluation is considered both the direct and indirect trust value. However the main drawback is storage overhead incurs due to the storage of direct and indirect trust values.

A one more trust evaluation method is proposed by He et al., [15] for MSNs. The authors focused on the identification of node's misbehavior based on some unique features like data rate and leaving time. Data rate is very much effective and helps in the detection of DoS attack but for a node with multi-hop communication, this is a not recommendable metric. Because a single node receives and transmits more packets by which the data rate may get abnormal. Dhakne and Chatur [16] proposed a "Distributed Trust based Intrusion Detection (DTBID)" system for the detection of malicious nodes in WSNs. DTBID considered multiple attributes like communications, data and energy and evaluated direct trust, recommended trust and indirect trust for the detection of malicious nodes. However, the stability and fault tolerance of senor nodes is not considered which is essential for the improvisation of network lifetime as well as for the detection of tampering and spoofing attacks.

Recently, Z. Zhang et al., [17] proposed an intrusion detection approach based on hierarchical trust and dynamic state of nodes in WSNs. A hierarchical trust evaluation is employed to derive the trustworthiness of Sensor nodes and Cluster heads based on multiple trust attributes; they are Content trust, honesty trust and interactive trust. A self-adaptive dynamic trust threshold is employed through which the applicability and flexibility of clustered WSNs can be improved. However, it is essential to consider the witness trust to measure the trust of nodes which are not directly connected.

F. Shang et al. [18] proposed Cumulative Summation based Hybrid Intrusion Detection model for the detection of sink hole attack and Dos Attacks in WSN. This approach considered two metrics for trust evaluation; they are link quality and majority rule. However, this approach not focused on the basic properties of nodes through which the trust is simply measured and malicious nature is identified.

S.M. Sajjad et al., [19] focused only on the detection of Selective forwarding attack, Jamming attack and Hello Flood attack. Towards such detection, the authors considered two metrics; they are Received Signal Strength (RSS) and Packet

Forwarding Rate (PFR) and every node measures the trustworthiness based on these two factors. Based on the obtained trust, the nodes are declared as trustworthy, malicious or risky. The PFR metric is much effective but not RSS, because for maximum number of attacks, the data rate will vary but not RSS. However, without the consideration of interactions, the trust evaluation is inefficient.

A "Trust Based Adaptive Acknowledgment (TRAACK)" is proposed by G. Rajeshkumar and K. R. Valluvan [20] in which the trust of a node is evaluated based on Kalman filter and Successful packet deliveries. Based on the entire trust of a route, an acknowledgment is initiated for the selection of packets such that the control overhead will get reduced. However, the only successful packet deliveries are not sufficient for intrusion detection. Non-successful packet deliveries have more significance in the detection of several attacks, because for DoS attack there exists more number of successful packet deliveries.

Some authors focused on the layer level security provision and towards such methodology, Umashankar G et al., [21] proposed a "physical layer based intrusion detection system (PL-IDS)". In PL-IDS, the trust value of a node is calculated based on the deviation of important factors at physical layer. The abnormal nodes mainly attack the physical layer through DoS attack and use jamming attacks to consume the resources of trustworthy nodes. Further PL-IDS is enhanced by adding two more layers (Network layer and Medium Access Layer) for intrusion, called as "Protocol Layer Trust Based Intrusion Detection System (LB-IDS)" [22]. At physical layer, two metrics namely Energy and Number of messages received are considered for trust calculation. Next, MAC layer, numbers of successful transmissions and Back off time are considered and finally at network layer, only number of hops is considered for trust evaluation. Finally, the overall trust value of senor node is estimated by combining these individual trust metrics. LB-IDS mainly focused on the detection of jamming attack, sink-hole attack and back-off manipulation attack. Even though this method is able to detect more number of attacks but the computational burden is too high because every time, the node has to check the trustworthiness at three layers. This excessive time introduces a time delay for packet at base station.

3. Proposed approach

3.1 Overview

In this section, we discuss about the newly proposed secure routing mechanism, called as Multi-Strategic Approach for Trust Aware Routing and Intrusion Detection. Under this multi-strategy, the trustworthiness of a sensor node is measured in three orientations; they are (1) Trust evaluation based on direct interactions, called as Subjective Trust (ST), (2) Trust evaluation based on neighbor node's critical reviews, called as Witness Trust (WT) and (3) Trust evaluation based on capacity of node, called as Capacity Trust (CT). Under the capacity trust, we have considered two more trust metrics; they are fault tolerance trust and stability trust. Based on these three trust measures, a composite trust factor is modeled and used for next-hop node selection followed by trustworthy route.

3.2 Network model & assumptions

In this paper, we consider the WSN as a randomly deployed network with N number of nodes and they are distributed in an area of size $M \times N$, where M is length of network and N is the width of network. Initially all the sensor nodes are assumed to have similar characteristics such as node status, energy and trust value. There exists only one base station and the energy of base station is infinite. Next, the sensor nodes are assumed to have static nature, i.e., they can't move. Every Sensor node is equipped with a GPS and it can sense the location information of current node. The sensor node can adjust is energy mode dynamically according to the transmission distance. Further we also assume every node can obtain past data like other node's opinions, working history and earlier decisions, from their neighbor nodes. One senor node can be a member of more than one routing paths, i.e., a single node can serve for multiple communities. The communication range of every sensor node is assumed to be constant and let it be R. The source node follows multi-hop routing if it was found that it was very far from the base station. Every node in WSN maintains a trust list in which the past records will store and it can be updated based on the other nodes and their recommendations. The trust list has nodes and their trustworthiness factors such as Subjective trust, Witness trust and Capacity trust.

3.3 Subjective trust

Subjective trust is derived based on the past experiences, interactions and observations. Subjective trust [23] is a trust of a node towards

Received: September 2, 2020. Revised: November 13, 2020.

another node and it is computed based on past as well as direct experiences. For instance a sensor node can capture the opinions of other sensor nodes after the completion of its interaction with other nodes. Based on this perception, the subjective trust is measured by the accumulation of earlier or past opinions between sensor nodes and can be updated based on recent experiences. Subjective trust denotes the direct opinion of nodes those are connected directly and have direct interactions. The subjective trust is obtained based on historical opinions which are available only if the sensor nodes are interacted with each other at least once in the past.

Subjective trust is similar to the human behavior in which a person can gain an opinion or understating if he/she is interacted with other person at least once in the past. However, the main problem arises if the nodes are not interacted even at least once in the past. At this situation, the nodes can obtain subjective trust (initially it is called as initial trust) by aggregating the past experiences of nodes those have similar characteristics. If we assume the trust evaluating node as source node and evaluated node as target node, at the initial phase the source node have no interaction with target node. In the starting phase, the target node can be called as stranger node. At this situation, the source node aggregates the past experiences of its neighbor nodes those have similar characteristics wit stranger node. Hence nodes can build initial trust with a stranger node based on the past opinions of the nodes which have similar characteristics with Stanger node. Since there exists M number of such type of nodes, the initial trust is obtained by averaging the past opinions.

Consider two sensor nodes s_i and s_j are directly connected to each other and the node s_j was interacted with node s_i P times in the past. At every interaction, the node s_i generates an opinion, let it be $o_p(s_j)$ regarding the communication behavior of node s_j. Here we assumed to have the range of opinion lies in between 0 and 1, i.e., $o_p(s_j) \in [0\ 1]$. Further assume that there are Q opinions, given by node s_i, regarding the malicious behavior of node s_j. Let's consider there are M nodes which have similar characteristics of node s_j and also interacted with node s_j directly in the past. In such condition, they have past opinions reading the behavior of node s_j. These M opinions are considered to evaluate the initial trust of node s_j by node s_i. Let the opinion of node s_m regarding the behavior of node s_j is denotes as $o_m(s_j)\ \forall m \in M$, the subjective rust is evaluated as

$$S_T(s_i, s_j) = \begin{cases} \alpha \times \frac{\sum_{m=1}^{M} o_m(s_j)}{M}, & If\ P = 0 \\ \beta \times \frac{\sum_{p=1}^{P} o_p(s_j)}{P}, & If\ P \neq 0 \end{cases} \tag{1}$$

Where $S_T(s_i, s_j)$ is subjective between nodes s_i and s_j, $o_m(s_j)$ is the opinion of senor node s_m regarding the behavior of node s_j and $o_p(s_j)$ is the opinion of node s_i at p^{th} interaction regarding the behavior of node s_j, β is an observation factor and α is impact factor.

According to Eq. (1), the subjective trust is evaluated in two phases; i.e., before interactions ($P = 0$) and after interactions ($P \neq 0$). At the former phase, i.e., there are no interactions between two nodes; the obtained subjective trust is nothing but the average trust of past opinions of similar type nodes which are interacted with node s_j in the past. Once the interaction is started between nodes, then the node s_j directly comes into the picture and the second condition ($P \neq 0$) comes into exist. At the p^{th} interaction, the subjective trust is evaluated based on the opinions observed at interactions starting from 1 to P-1. Among these P opinions, there may exist some opinions in which the node s_i has given a malicious opinion. Hence we need to consider this fact and we introduced a new factor called as observation factor (β), it is derived as

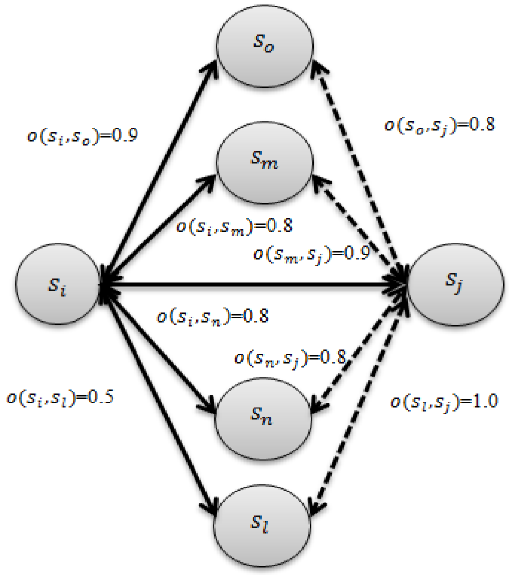
$$\beta = \left(\frac{P-Q}{P}\right)^{\left(\frac{1}{P-Q}\right)} \tag{2}$$

Where P is the total number of past opinions and Q is the total number of malicious opinions. Based on the malicious opinions into the observation factor followed by subjective trust, we can understand that the subjective trust leads to reduction, i.e., trust value is reduced. As the number of malicious opinions increases, the subjective trust reduces. This observation is in resemblance with human behavior at where the human beings try to maintain the relationship by communicating with others continuously. And if any interaction is gone wrong, the entire relation will get damage.

3.4 Witness trust

Witness trust is derived based on the past experiences, and observations of other nodes. If any node is not directly connected to other node, then it can pursue the trust based on critical reviews of its most trustable neighbor nodes. Witness trust is nothing but an indirect subjective trust. In WSNs, it is somewhat normal that a node may have no direct

Received: September 2, 2020. Revised: November 13, 2020.



$$W_T(i,j) = \frac{(0.9 \times 0.8) + (0.8 \times 0.9) + (0.8 \times 0.8)}{(0.9 + 0.8 + 0.8)} = 0.832$$

Figure. 1 Witness trust evaluation

connection with other node or target node. In such situation, the node considers can take the reviews of its most trustworthy nodes to measure the trustworthiness of target node. This type of trust evaluation is called witness trust because the nodes, from which the trust is measured, are the witnesses (evidences). The witness trust is completely depends on the strength of relationships between source node and witness nodes as well as between witness nodes and target node. Witness trust infers an indirect trust from third party nodes which are more trustable neighbors. Hence we have considered a trust threshold during the selection of trustable neighbors.

Consider two sensor nodes s_i and s_j which don't have a direct connection. Let s_i^k be the k^{th} neighbor node of senor node s_i which have a direct connection with the target senor node s_j. Then there exists a trust opinion with node s_j, means the neighbor node have an individual opinion regarding the behavior of target node s_j. Let $o(s_i^k, s_j)$ be the opinion of k^{th} neighbor node of senor node s_i regarding the behavior of target node s_j and $o(s_i, s_i^k)$ be the opinion of node s_i regarding the behavior of its k^{th} neighbor node s_i^k, then the witness trust is evaluated as;

$$W_T(s_i, s_j) = \frac{\sum_{k=1}^{K}(\, o(s_i, s_i^k) \times o(s_i^k, s_j))}{\sum_{k=1}^{K}(\, o(s_i, s_i^k))} \tag{3}$$

S. to

$$o(s_i, s_i^k) \geq T_T \tag{4}$$

Where $W_T(s_i, s_j)$ is the witness trust between nodes s_i and s_j, T_T is the thrust threshold and K is the total number of neighbor nodes of source senor node s_i.

Here T_T is used to select the most trustworthy nodes and the condition in Eq. (4) denotes that the opinion value which is greater than the trust threshold is only considered as witness and the respective node is considered as most trustworthy node. According to Eq. (3), the node s_i initially selects witness nodes through T_T. Then the witness opinions $o(s_i^k, s_j)$ are aggregated according to the weighted average method for the calculation of $W_T(s_i, s_j)$. The main advantage of witness trust evaluation is it less computational complexity. Further, the witness trust evaluation considers only the opinions of most trustable nodes; the probability of risk is less. An Example demonstration of witness trust evaluation is shown in Fig. 1.

3.5 Capacity trust

Capacity trust is one of the most significant aspects of evidence that manifests the trustworthiness of sensor nodes. Capacity trust is derived based on the node's capability that includes the performance of a node in the earlier communication interactions. Under this trust, we have considered two sub-trusts; they are fault tolerance trust and stability trust. Fault tolerance ensures the robustness against node failures from several technical reasons. Next the stability trust ensures the capacity of a sensor node with respect to its stability. Further details are explored in the following subsections;

3.5.1. Fault tolerance trust

In WSNs, the sensor nodes are tiny devices which are very sensitive to operating environments like breakages, electrical surges, and damages etc. If any node was break down, then it can't work properly, i.e., it can't perform even its basic operations like sensing, processing and transmitting. Even though if these nodes are recovered quickly, they can't properly as they work before break down. The recovery time of these tiny devices is very small because the sensor nodes won't have much complex circuitry. Moreover, there is an availability of alternate circuits or processors through which the damaged circuits can be replaced. However, it is probable that some nodes may not recommence the normal operation. A sensor node which has frequent breakages is considered to be not reliable. Hence we considered to evaluate the trustworthiness of a node through its fault tolerance. For this purpose, we have considered three factors through which the fault tolerance can be modeled; they are (1) Pass Rate, (2) Failure Rate and (3) Recovery Rate. The pass rate is defined as the total successfully completed instances by the target node to the total instances given by source node. For a given task, if the target node exists until the completion of task, then it is considered as pass and the pass rate counts such types of instances. As the pass rate is high, the fault tolerance is high. Next, the failure rate is defined as the total number of failure instances to the total number of instances. Further, the recovery rate is measured based on the node's regaining from the breakage. Some instances are possible at which the node can't recover. Based on this fact, the recovery rate is defined as the ratio of total number recovered instances to the total number instances. For any node, a less failure rate, more pass rate and recovery rate denotes good fault tolerance and such type of nodes are only preferred for communication process. All these rates are obtained based on past working experience in the trust list without heavy data communication.

Consider two sensor nodes s_i and s_j, let the pass rate of node s_j is $P_r(s_j)$, failure rate is $F_r(s_j)$ and the recovery rate is $R_r(s_j)$. Based on these three rates, the fault tolerate trust is evaluated as

$$F_T(s_i, s_j) = \left(P_r(s_j)\right)^{\left(1-F_r(s_j)\right)} \times \left(R_r(s_j)\right)^{F_r(s_j)} \tag{5}$$

Where $F_T(s_i, s_j)$ is the fault tolerance trust between sensor nodes s_i and s_j, lies in the range of 0 and 1, where 0 denotes the node s_j have less fault tolerance trust and 1 denotes the higher fault tolerance trust. Among the available senor nodes, one final node is selected as final which has higher fault tolerance.

3.5.2. Stability trust

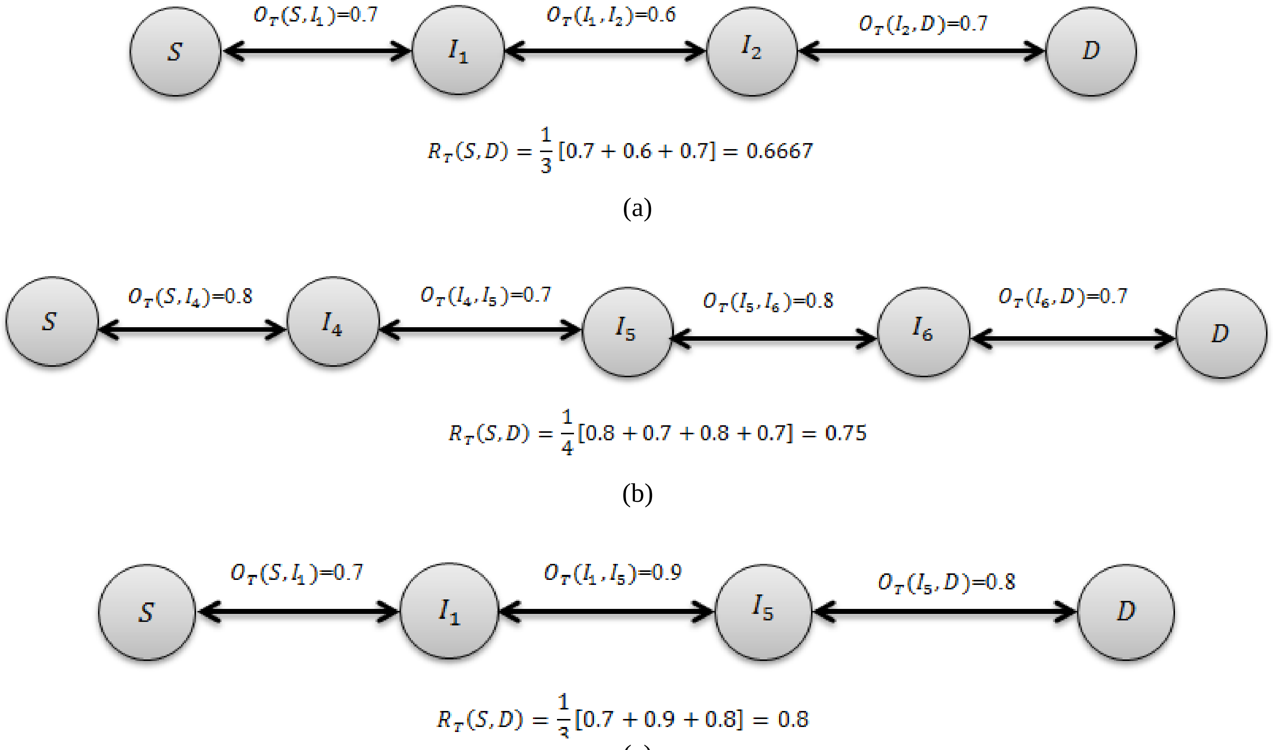
In WSNs, the topology of the network changes dynamically. Consequently, the nodes join and leave the network dynamically. There are so many reasons behind this dynamic topology variation, for example minor movements (done by external things), energy depletion, additional node deployment, resource constraints etc. Since the nodes in WSN have frequent departures and arrivals, we have considered these facts to analyze the node's stability. Hence a more stable node can gain more trust because it can provide more benefit to the network. To model the stability trust, we have considered its lifecycle because the lifecycle gives information about the node's departures and arrival times. Under the lifecycle concept, we have defined the entire lifecycle of a node through two time periods; they are working time and existing time. Here the existing time is defined as the time period up to which the node has present in the same position (no departure or no arrival) or simply the entire lifecycle. Next, the working time is defined as time period up to which the node is present in the working mode (sensing, processing and transmitting). Generally, a greater value of working time denotes the higher stability. Hence we define the stability trust as the ratio of working time to existing time. Consider two sensor nodes s_i and s_j, and let T_w and T_e be the working time and existing time respectively, where $|T_w|$ denotes the length of working time and $|e|$ denotes the length of existing time of node s_j. Further assume that the node s_j has interacted with node s_i P times, the stability trust is expressed as;

$$Q_T(s_i, s_j) = \begin{cases} \frac{|T_w|}{|T_e|}, & if\ P = 0 \\ \delta \times \frac{|T_w|}{|T_e|}, & if\ P \neq 0 \end{cases} \tag{6}$$

Where $Q_T(s_i, s_j)$ is the stability trust of node s_i over node s_j, δ is a penalizing parameter which has been modeled with respect to the total number of interactions happened between two sensor nodes. δ is mathematically derived as;

$$\delta = \beta^{\left(1-\frac{1}{P+1}\right)} \tag{7}$$

Where β is an arbitrary constant, lies in the range of 0 and 1, and P is the total number of interactions



(a)

(b)

(c)

Figure. 2 An example for route selection based on route trust

incurred between two sensor nodes.

For a node which has frequent departures from the network, the penalizing parameter is high, means that particular will get penalized heavily. As we discussed that that a node which has frequent departures is not reliable, hence the stability trust of such node is very less and it can't be considered for communication process. Since the length of working time as well as existing time is recorded by nodes, the computational cost of stability trust is not considerable.

Based on these two sub-capacity trusts, the final capacity trust is modeled as;

$$C_T(s_i,s_j)=\frac{1}{2}\times\left[\left(w_1\times F_T(s_i,s_j)\right)+\left(w_2\times Q_T(s_i,s_j)\right)\right] \qquad (8)$$

Where w_1 and w_2 are two weight factors, signifies the weight of Fault tolerance trust and stability trust respectively. From Eq. (8), we can understand that the stability trust is an average of Fault tolerance trust and stability trust. With respect to the capacity trust, among the available neighbor nodes, the source node chooses one node which has higher capacity trust.

Next, the composite trust factor is formulated by integrating the three trusts such as Subjective Trust $\left(S_T(s_i,s_j)\right)$, Witness Trust $\left(W_T(s_i,s_j)\right)$ and Capacity Trust $\left(C_T(s_i,s_j)\right)$. Mathematically the composite trust factor is expressed as;

$$O_T(s_i,s_j)=\frac{1}{3}\times\left[\left(\omega_1\times S_T(s_i,s_j)\right)+\left(\omega_2\times W_T(s_i,s_j)\right)+\left(\omega_3\times C_T(s_i,s_j)\right)\right] \qquad (9)$$

Where $O_T(s_i,s_j)$ denotes the overall trust or composite trust factor, lies in the range of 0 and 1. ω_1, ω_2 and ω_3 are the three weight parameters assigned to signify the importance of Subjective trust, witness trust ad capacity trust respectively. The values of ω_1, ω_2 and ω_3 are need to be assigned in such a way they have to satisfy the following condition, i.e., $\omega_1+\omega_2+\omega_3=1$. In this paper, we have assigned an equal value for every weight, means we have given equal importance for every trust.

Consider a route $rt(S,I_1,I_2,\ldots,D)$, where S is the source node, D is the destination node and $I_1,I_2,\ldots,I_Z$ are intermediate nodes. Based on the above specified trust measures, the complete trust of a route is modeled as

$$R_T(S,D)=\frac{1}{length\ (route)}\left[O_T(S,I_1)+\sum_{z=1}^{Z}O_T(I_{z-1},I_z)+O_T(I_Z,D)\right] \qquad (10)$$

Where $O_T(S,I_1)$ is the overall trust between source node and first intermediate node, I_1 and

$O_T(I_Z, D)$ is the overall trust of last intermediate node and destination node. The middle term denotes the summation of overall trust of intermediate trust. Since there exists Z number of intermediate nodes between source and destination, we considered the trust between them also. A simple example about this demonstration is shown in Fig. 2.

As shown in the Fig. 2, there are totally three available routes between Source (S) and Destination (D) nodes. In Fig. 2 (a), the there are two intermediate nodes between source and destination, and the route trust is measured as 0.667. Next, in Fig. 2 (b), there are three intermediate nodes between source and destination, and the route trust is measured as 0.75. The final route shown in Fig. 2 (c) has also two intermediate nodes between source and destination and the route trust is measured as 0.80. Among these routes, the third route has highest route trust hence it is selected as optimal route.

4. Simulation experiments

In this section, we demonstrate the particulars of experimental simulations conducted over the proposed approach and the observed performance measures. Initially we discuss about the details of simulation setup and then discussed about the performance measures through the performance of proposed approach is analyzed. Simultaneously, we also demonstrated the comparative analysis done between proposed and existing approaches.

4.1 Simulation set up

Under the simulation setup, the WSN is considered as a randomly deployed network with P number of nodes in the area of size MXN, where N is width and M is the length of the network. All sensor nodes are assumed to be stationary. To realize the proposed concept of intrusion detection, among the available nodes, some nodes are declared as malicious and then the proposed as well as existing approaches are applied over the network to find out the malicious nodes. Based on the obtained detection results, the performance is evaluated through several performance metrics. Here the portion of malicious is varied with respect to the total number of node deployed in the network. For example, if we considered the total number of nodes is 200 and portion of malicious members are 20%, and then the total number of malicious nodes present in the network is 40. In this manner, the simulation experiments are conducted for varying portion of malicious members and at every phase the performance is analyzed. Further, according to the assumptions, we also vary the total number of interactions such that we can analyze the impact of observation factor. Table. 1 shows the details of simulation parameters considered for simulation experiments.

Table. 1 Simulation parameters

Parameter	Value
Network area	100×100 m^2
Number of nodes	100
Communication Range (R)	¼ of network area
% of malicious behavior	15%, 30% and 45% of total nodes
Trust threshold (T_T)	0.6
Nodes Deployment	Random
w_1 and w_2	0.500
Number of Interactions (P)	100-1000
ω_1, ω_2 and ω_3	0.3333
α, β	[0 1]
Number of Malicious Interactions (Q)	10-20% of P

4.2 Performance metrics

Packet Delivery Ratio (PDR): It is defined as the ratio of total number of packets delivered at destination node to the total number of packets transmitted from source node.

$$PDR = \frac{P_r}{P_s} \tag{11}$$

Where P_r is the total number of packets received and P_s is the total number of packets sent. A lower value of PDR denotes bad performance while high value denotes good performance.

Malicious Detection Rate (MDR): MDR is defined through a fraction of nodes which are detected as malicious when they are malicious to the original malicious nodes.

$$MDR = \frac{TP}{TP+FN} \tag{12}$$

Where TP is True Positives and FN is False Negatives. Here the TP means the total number of malicious nodes those are detected as malicious and FN is the total number of malicious nodes those are detected as normal. Lower MDR denotes bad performance while higher MDR denotes good performance.

False Positive Rate (FPR): FPR is defined through a fraction of nodes which are detected as malicious when they are non-malicious to the sum of malicious and non-malicious nodes.

$$FPR = \frac{FP}{TP+FP} \tag{13}$$

Where TP is True Positives and FP is False Positives. Here the TP means the total number of malicious nodes those are detected as malicious and FP is the total number of non-malicious nodes those are detected as malicious. Lower FPR denotes good performance while higher FPR denotes bad performance.

False Negative Rate (FNR): FNR is defined through a fraction of nodes which are detected as non-malicious when they are malicious to the sum of malicious and non-malicious nodes.

$$FNR = \frac{FN}{TP+FN} \tag{14}$$

Where TP is True Positives and FN is False Negatives. Here the TP means the total number of malicious nodes those are detected as malicious and FN is the total number of malicious nodes those are detected as normal. Lower FNR denotes good performance while higher FNR denotes bad performance.

4.3 Results

During the simulation, we have varied the number of interactions and the portion of malicious members. The interactions are varied from 100 to 1000 and the portion of malicious members is varied as 15%, 30% and 45% of total number of nodes present in the network. For example, consider an instance of 200 interactions. At this instance, we have varied the portion of malicious members as 10%, 20%, 30%, 40% and 50%, and a every phase the performance is measured through MDR, FRP and FNR. The obtained performance metrics are plotted in the following figures.

Fig. 3 demonstrates the average rust value of normal nodes as well as malicious nodes. From the above Fig. 3, we can observe that the average trust of malicious node is 0.45 whereas the average trust value of malicious nodes is observed as 0.75. In the detection process, we have fixed the trust threshold as 0.6. Based on the proposed intrusion detection mechanism, the normal nodes and malicious nodes can be identified more accurately. Since we have considered three types of trusts, we can observe that the average trust value of malicious nodes is not decreased sharply. Generally a sharp decrease can be observed in such a scenario where the trust evaluation considered only one reference metric. But in the case of multiple strategies or reference metrics, a sharp decrease couldn’t observe because there exists a mutual effect between reference trusts.

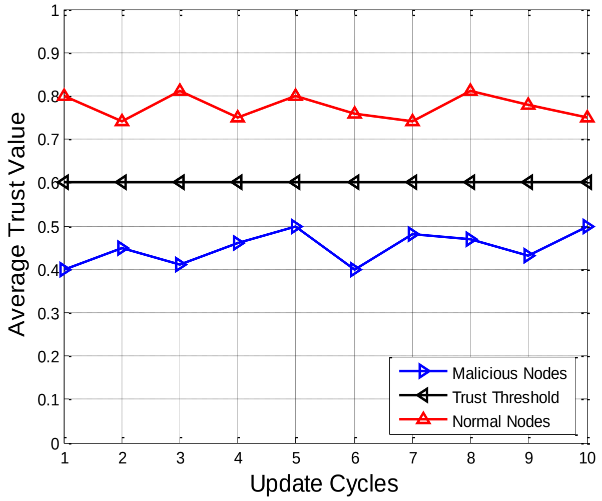


Figure. 3 Average trust value for malicious and normal nodes

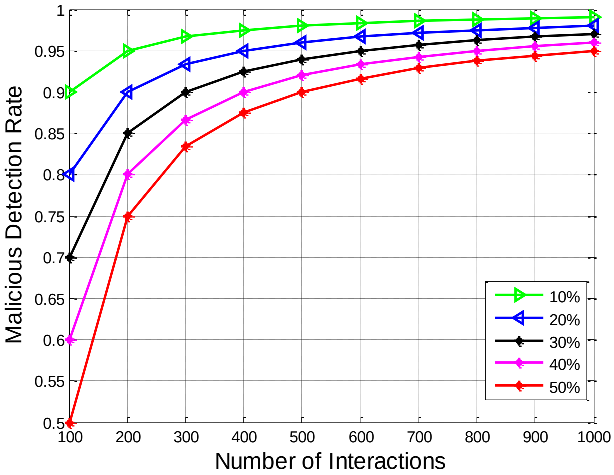


Figure. 4 MDR vs. number of interactions for varying malicious portion

Generally, the sensor nodes in the Network perform more communication interactions to maintain a trustworthy relationship. This is in resemblance with human behavior where the persons try to maintain the relationship by maintaining a continuous communication. However, this relationship is very sensitive and it will end up r collapse even if single malicious interaction is happened. Based on this inspiration, we have modeled the subjective trust based trustworthiness evaluation and the relation between the malicious nodes detection rate and number of interactions is shown in Fig. 4. Generally the MDR is evaluated as the ratio of total number of nodes detected as malicious to the total number of original malicious nodes. As shown in Fig. 4, MDR is increasing with an increase in the number of interactions, but the MDR is decreasing with an increase of portion of malicious members from 10% to 50%. For instance

Received: September 2, 2020. Revised: November 13, 2020.

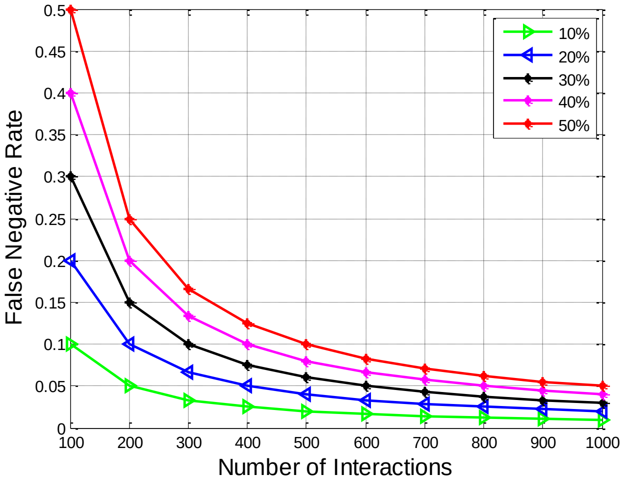


Figure. 5 FNR vs. number of interactions for varying malicious portion

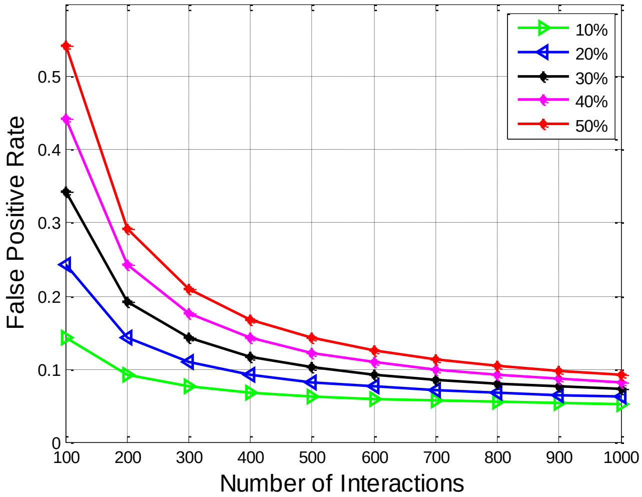


Figure. 6 FPR vs. number of interactions for varying malicious portion

let's consider the MDR at the number of interactions 200. It is varied as 0.95, 0.90, 0.85, 0.80, and 0.75 for the portion of malicious members 10%, 20%, 30%, 40% and 50% respectively. The main reason behind this decrement is that we have included the number of malicious interactions in the observation factor β (Eq. (2)) which has a direct relation with subjective trust. As the number of malicious interactions increases, the nodes will lose the trust over the respective nodes and consequences to less MDR. Since there are so many types of attacks, all the malicious interactions won't be same which creates confusion for the nodes there by it can't detect the malicious node effectively.

FNR has a simple inverse relation with MDR, as MDR increases, the FPR decreases and vice versa. On the other hand the FNR can also be measured as the ratio of total number of malicious nodes those are detected as non-malicious nodes (i.e., normal nodes) to the total number of original malicious nodes. Let's consider the original malicious node count is 20, the total number of malicious nodes those are detected as malicious nodes are 15, then the total number of malicious nodes those are detected as non-malicious nodes are obtained as 20-15 = 5. Here 15 is called as True Positive and 5 is called as False Negative and FNR is obtained as 5/(15+5) = 5/20 = 0.25. Similar to MDR, the FNR also have a relation with number of interactions, as the number of interactions increase, the FNR decreases, as demonstrated in Fig. 5. Let's consider the portion of malicious members at 50%, the FNR is varied as 0.2517, 0.1255, and 0.0757 for the number of interactions 200, 400 and 600 respectively. Simultaneously, we can observe that the FNR has inverse relation with portion of malicious members. Consider the instance of 200 interactions from Fig. 5, the FNR is varied as 0.0500, 0.1008, 0.1523, 0.2028, and 0.2530 for the portion of malicious members 10%, 20%, 30%, 40% and 50% respectively.

FPR also have inverse relation with MDR but not linearly related. On the other hand the FPR can also be measured as the ratio of total number of non-malicious nodes those are detected as malicious nodes (i.e., normal nodes) to the total number of detected malicious and non-malicious nodes.

For example, consider the original malicious node count is 20, the total number of malicious nodes those are detected as malicious nodes are 15, and the total number of non-malicious nodes those are detected as malicious nodes are 8. Here 15 is called as True Positive and 8 is called as False Positive and the FPR is obtained as 8/(15+8) = 8/23 = 0.347. For the same example, we have obtained 0.25 FNR while 0.347 FPR. Since there exists more number normal nodes in the network, there is a possibility that some normal nodes which have Overall trust nearer to trust threshold can be declared as malicious. Similar to MDR and FNR, the FPR also have a relation with number of interactions, as the number of interactions increase, the FPR decreases, as demonstrated in Fig. 6. Let's consider the portion of malicious members at 50%, the FPR is varied as 0.1002, 0.0752, and 0.0653 for the number of interactions 200, 400 and 600 respectively. Simultaneously, we can observe that the FPR has inverse relation with portion of malicious members. Consider the instance of 200 interactions from Fig. 6; the FPR is varied as 0.1514, 0.2522, 0.3537, 0.4509, and 0.5522 for the portion of malicious members 10%, 20%, 30%, 40% and 50% respectively.

Received: September 2, 2020. Revised: November 13, 2020.

4.4 Comparison

Under this sub-section, we have demonstrated the effectiveness of proposed approach by comparing its performance with some existing approaches. We have compared with Nearest Neighbor Trust based Intrusion Detection System (NNTB-IDS) [19] and Energy Aware Trust Based Intrusion Detection System (EATB-IDS) [20]. NNTB-IDS considered two metrics for the trust evaluation of nodes; they are Received Signal Strength (RSS) and Packet Forwarding Rate (PFR). Based on the obtained trust, the nodes are declared as trustworthy, malicious or risky. However, the RSS is a perfect metric for the evaluation of distance between while it has less contribution in the detection of malicious nodes. Next, under the Packet Forwarding Rate, they have considered packet generation rate and packer receiving rate only. These factors perform well in the detection of only one attack, i.e., flooding attack. This approach didn't consider the basic criterion, i.e., communication interactions which are a generalized theme for the detection of several attacks. Hence NNTB-IDS is not robust. Meanwhile they didn't consider the fault tolerance trust as well as stability trust.

Next, in EATB-IDS [20], the trust of a node is evaluated based on Kalman filter and Successful packet deliveries. Based on the entire trust of a route, an acknowledgment is initiated for the selection of packets such that the control overhead will get reduced. In this approach the Kalman filter is employed for the trust evaluation. The Kalman filter is a generalized filter which works based on the concept of Minimum Mean Square error (MMSE). MMSE is evaluated between current and previous states (i.e., Packets send and acknowledgments received) of a node. If it observes a greater MMSE, then that node is declared as malicious otherwise normal. The Successful packet deliveries are evaluated based on TWOACK [24, 25] scheme. However, they didn't consider the communication interactions and recommendations for the trust evaluation. Moreover, they didn't discuss about the trust evaluation when there is no direct link between nodes. Meanwhile the fault tolerance trust and stability trust are also not considered.

Fig. 7 shows the MDR comparison between proposed and existing approaches. As shown in this figure, the MDR is decreasing with an increase in the portion of malicious members. However, for a particular instant of portion of malicious members, the MDR of proposed approach is high compared to the both existing approaches. For example, at portion of malicious members 20%, the MDR of proposed approach is observed as 0.9556 while for NNTB-IDS and EATB-IDS it is observed as 0.9302 and 0.9415 respectively. Further at 30% portion of malicious members, the MDR of proposed approach is observed as 0.9489, while for NNTB-IDS and EATB-IDS it is observed as 0.9003 and 0.9213 respectively. From these values we can observe that the MDR at higher portion of malicious members (30%) is much deviated with MDR at lower portion of malicious members (20%). But this deviation is less in the case of proposed approach. The main reason is that the proposed approach considered multiple strategies to measure the trustworthiness of a node while the conventional approaches are considered only few strategies that too they are oriented in only one orientation. The NNTB considered RSS and the EATB considered Kalman filter and these don't have much significance in the trust estimation in WSNs.

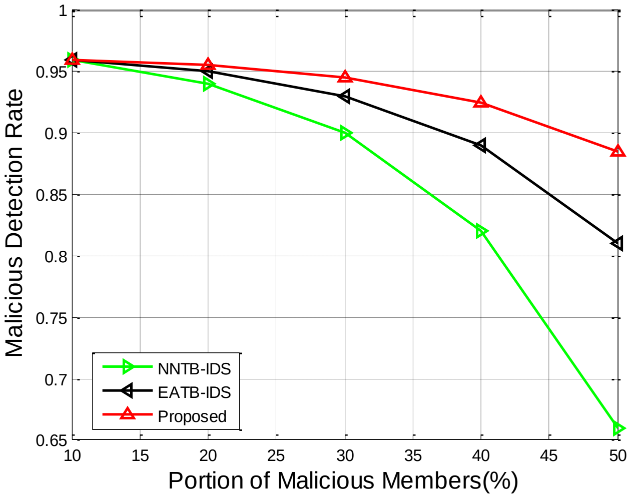


Figure. 7 MDR vs. portion of malicious members

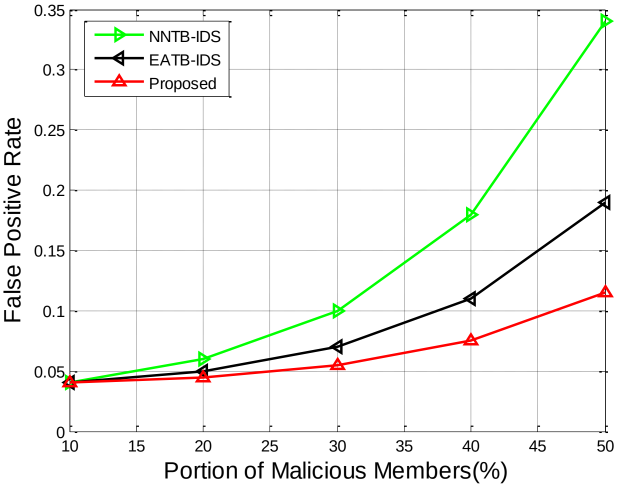


Figure. 8 FPR vs. portion of malicious members

Fig. 8 shows the FPR comparison between proposed and existing approaches. As shown in this figure, the FPR is increasing with an increase in the

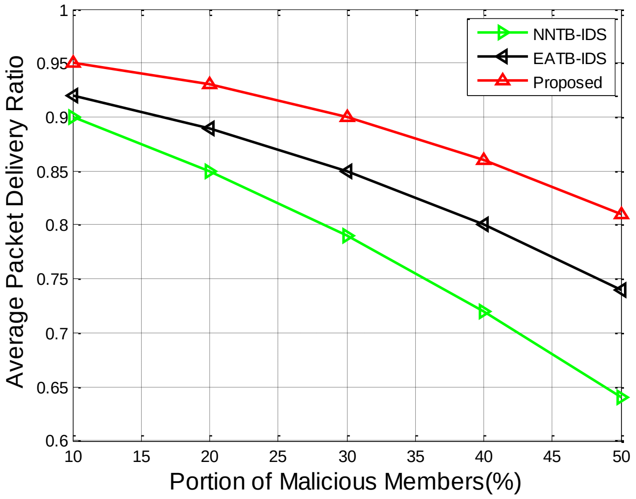


Figure. 9 APDR vs. portion of malicious members

portion of malicious members. However, for a particular instant of portion of malicious members, the FPR of proposed approach is less compared to the both existing approaches. For example, at portion of malicious members 20%, the FPR of proposed approach is observed as 0.0402 while for NNTB-IDS and EATB-IDS it is observed as.0654 and 0.0586 respectively. Further at 30% portion of malicious members, the FPR of proposed approach is observed as 0.0555, while for NNTB-IDS and EATB-IDS it is observed as 01547 and 0.775 respectively. This deviation is increasing for further increment in the portion of malicious members. At 50% portion of malicious members, the FPR of proposed approach is noticed as 0.11 while for NNTB-IDS and EATB-IDS, it is observed as 0.1998 and 0.3489 respectively. Means the FPR is observed as very high for higher portion of malicious members. The main reason is that the conventional approaches didn't focus on the communication interactions as well as recommendations during the trust evaluation of nodes.

Fig. 9 shows the APDR comparison between proposed and existing approaches. As shown in this figure, the APDR is decreasing with an increase in the portion of malicious members. However, for a particular instant of portion of malicious members, the APDR of proposed approach is high compared to the both existing approaches. The main reason is that the proposed approach modeled the trust by considering the stability and fault tolerance which are key parameters in the determination of Quality of Service. A node which has more fault tolerance and stability can cooperate to other nodes to forward the data destination nodes. Due to this fact, the packets which are passing through the more stable and fault tolerant nodes will reach the destination without any fail. Hence the APDR is high for proposed approach when compared to conventional approaches. On an average the APDR of proposed approach is observed as 89.1245% while for NNTB-IDS and EATB-IDS it is observed as 78.2241% and 84.4152% respectively.

5. Conclusion

In this paper, we have developed a new Multi-strategic intrusion detection mechanism to identify and isolate the malicious node sin the WSN. Under the multi-strategic principle, we have modeled the total trust of anode with respect to three trust metrics; they are subjective trust, witness trust and capacity trust. Under capacity trust, we have further considered two sub-trusts; they are fault tolerance trust and stability trust. The first two trusts measures the communication trust between nodes while the last one measure the capacity of sensor nodes. The Subjective trust and witness trust ensures the robustness of proposed approach in such type of attacks where the communication process is tampered. Flooding attack is an example for such kind of attack. Next the capacity trust ensures that the proposed approach is robust for such kind of attacks in which the resources are wasted. DoS and Selective forwarding attack are the best example for such kind of attacks. Simulation experiments are conducted over the proposed model by varying the network parameters like number of interactions and portion of malicious members. At every phase of simulation, the performance is measured through MDR and APDR and they had proven that the proposed approach is more robust and effective when compared to existing methods. From the results, we have noticed that the average Malicious Detection Rats of proposed model is 93.4012% while the False Positive rate and Packet Delivery Ratio are observed as 5.5000% and 74.1745% respectively.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks a survey", *Computer Networks*, Vol. 38, No.4, pp.393–422, 2002.

[2] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks", *Communi*cations, Vol. 47, No. 6, pp. 53–57, 2007.

[3] Z. M. Fadlullah, T. Taleb, A.V. Vasilakos, M. Guizani, N. Kato, "DTRAB: combating against attacks on encrypted protocols through traffic-feature analysis", *IEEE/ACM Transactions on Networking*, Vol. 18, No.4, pp. 1234–1247, 2010.

[4] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks", *IEEE Communications Surveys & Tutorials.*, Vol. 16, No. 1, pp. 234-241, 2014.

[5] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, "Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges", *IEEE Access,* Vol. 8, pp. 3343-3363, 2019.

[6] F. Bao, I. R. Chen, M. Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection", *IEEE Transactions on Networking Service Management*, Vol. 9, No. 2, pp. 169-183, 2012.

[7] M. Riecker, Biedermann S, Hollick M., "Lightweight energy consumption-based intrusion detection system for wireless sensor networks", *International Journal of Information Security,* Vol. 14, No. 2, pp. 155–67, 2015.

[8] K. Gerrigagoitia, R. Uribeetxeberria, U. Zurutuza, I. Arenaza, "Reputation-based intrusion detection system for wireless sensor networks", In: *Proc. of International Conf. On Complexity in Engineering,* Aachen, Germany, pp. 11–13, 2012.

[9] X. Jinhui, T. Yang, Y. Feiyue, P. Leina, X. Juan, and Hou Yao, "Intrusion detection system for Hybrid DoS attacks using Energy Trust in Wireless Sensor Networks", In: *Proc. of 8th International Congress of Information and Communication Technology (ICICT-2018*), Coimbatore, India, pp. 1188-1195, 2018.

[10] H. Sedjelmaci, S. M. Senouci, "Efficient and lightweight intrusion detection based on nodes' behaviors in wireless sensor networks", In: *Proc. of IEEE Conf. on Global Information Infrastructure Symposium,* Trento, Italy, pp. 1–6, 2013.

[11] M. S. Islam, R. H. Khan, and D. M. Bappy, "A hierarchical intrusion detection system in wireless sensor networks", *Computer Science Network Security*, Vol. 10, No. 8, pp. 21–26, 2010.

[12] A. Ghosal, and S. Halder, Intrusion Detection in Wireless Sensor Networks: Issues, Challenges and Approaches, *Book chapter in Wireless Networks and Security*, Springer, Berlin, Heidelberg, pp. 329–367, 2013.

[13] X. Li, F. Zhou, and J. Du, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks", *IEEE Transactions on Information and Forensics Security,* Vol. 8, No. 6, pp. 924-935, 2013.

[14] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: Attack-resistant and lightweight trust management for medical sensor networks", *IEEE Transactions on Information Technology in Biomedicine*, Vol. 16, No. 4, pp. 623-632, 2012.

[15] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "A distributed trust evaluation model and its application scenarios for medical sensor networks", *IEEE Transactions on Information Technology in Biomedicine*, Vol. 16, No. 6, pp. 1164-1175, 2012.

[16] A. Dhakne and P. Chatur, "Distributed trust based intrusion detection approach in wireless sensor network", In: *Proc. of IEEE International Conf. on Communication Control Intelligent Systems,* Mathura, India, pp. 96-101, 2015.

[17] Z. Zhang, H. Zhu, S. Luo, Y. Xin, and X. Liu, "Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks", *IEEE Access*, Vol. 5, pp. 12088-12102, 2017.

[18] F. Shang, D. Zhou, C. Li, H. Ye, and Y. Zhao, "Research on intrusion detection model based on improved cumulative summation and evidence theory for wireless sensor networks", *Photon Newton communication,* Vol. 37, No. 4, pp. 212-223, 2019.

[19] S. M. Sajjada, S. H. Boukb, and M. Yousa, "Neighbor Node Trust Based Intrusion Detection System for WSN", In: *Proc. of 6th International Conf. on Emerging Ubiquitous Systems and Pervasive Networks,* Berlin, Germany, pp. 183–188, 2015.

[20] G. Rajesh kumar and K. R. Valluvan, "An Energy Aware Trust Based Intrusion Detection System with Adaptive Acknowledgement for Wireless Sensor Network", *Wireless Personal Communications*, Vol. 94, No. 5, pp. 1993–2007, 2017.

[21] U. Ghugar, J. Pradhan, S. K. Bhoi, R. R. Sahoo, and S. K. Panda, "PL-IDS: physical layer trust based intrusion detection system for wireless sensor networks", *International Journal of Information Technology,* Vol. 10, No. 4, pp. 489–494, 2018.

[22] U. Ghugar, J. Pradhan, S. K. Bhoi, and R.R. Saho, "LB-IDS: Securing Wireless Sensor Network Using Protocol Layer Trust-Based Intrusion Detection System", *Hindawi Journal of Computer Networks and Communications* Vol. 2019, Article ID 2054298, pp. 1-13, 2019.

[23] A. R. Alfarez and S. Hailes, “Supporting trust in virtual communities”, In: *Proc. of the 33rd Annual Hawaii International Conf. on System Sciences*, Maui, HI, USA, p. 9, 2000.

[24] H. Chenguang and S. Xuejun, “An energy-efficient message passing approach in MAC design for wireless sensor networks”, In: *Proc. of 4th IEEE International Conf. on Circuits and Systems for Communications*, Shanghai, China, pp. 550–554, 2008.

[25] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehavior in MANETs”, *IEEE Transactions on Mobile Computing*, Vol. 6, No.5, pp.536–550, 2007.