Capacity trust assessment for multi-hop routing in wireless sensor networks

Sowmya Gali [1*], *Madhusudhana Reddy* Y [2], *Alekya Himabindu* B[1], *Nagamani* V[1,]
Jayamangala S[1], *Munawwar* S[1], *Mallikarjuna Rao* Y[1], *A. Hussien* Abbas[3]

[1] ECE Department, Santhiram Engineering College, Nandyal, Andhra Pradesh, INDIA
[2] ECE Department, RGM College of Engineering and Technology, Nandyal, Andhra Pradesh, INDIA
[3] Computer Technical Engineering Department, College of Technical Engineering, The Islamic University, Najaf, Iraq

Abstract: This paper proposed a newIntrusion Detection mechanism based on Multiple Trust Attributes in Wireless Sensor Networks (WSNs). Mainly this work concentrated to assess the trust in ems of capacities of the sensor nodes. The capacity of a node is formulated based on two trusts namely Fault Tolerance Trust and Stability Trust. Every SN checks the trustworthiness of its neighbour SNs based on the Capacity Trust and confirms their trustworthiness. If any node is discovered as malicious, such type of node is called as intrusion or outlier and isolated from network.Extensive Simulations are conducted over the proposed intrusion detection mechanism and the performance is evaluated through Malicious Detection Rate, and False Positive Rate.

Keywords: Intrusion Detection, Capacity Trust, Stability Trust, Malicious Detection Rate.

1 Introduction

WSNs are increasingly witnessing novel applications in diverse fields [1], [2]. Many of these are futurist in nature, although a large proportion of these are currently in use. Even though there is a huge prospect for WSNs in real time applications, many challenges like inter-operability, resource constraints, scalability, mobility, privacy and security are raised during the connection of sensor nodes. Many different type of architectures are developed for WSNs [3] to provide the solutions for these challenges. Major challenges are solved by changing the architectures except security and privacy. So, this security posing great hurdle to WSN architectures. As a result, there are numerous possible security and privacy issues, from the internet to the real world, and there is a chance that people could be harmed. For example, a compromised sensor node may lead to attack on the other nodes or on the entire network.A compromised node may potentially enable the leaking and misuse of personal information, depending on the attack method.

[*] Corresponding author: Sowmya.ece@srecnandyal.edu.in

A communication breakdown may have an impact on the outside world and put people's physical safety at danger. Since the WSN is a more prone to several security threats, there is a necessity of an efficient routing design such that the Sensor Nodes in WSN will get protected. Once any of the node is compromised in network, it consequences to several problems such as information loss, control over the connected devices, hacking etc. A serious communication between two sensor nodes can be hacked easily if it is going on through free communication channel because of so many adversaries. A more serious concern in the WSN is that the attacked nodes starts misbehaving and can drop the packets or can manipulate the packets. Due to the nature of openness of transmission and deployment, the WSN suffer from several serious attacks like sink-hole, black-hole, worm-hole, replay, Distributed Denial of Service (DDOS), Sybil selective forwarding, DoS, data tampering, hijack attacks. Thus there is a necessary to design an effective security framework to make the IoT more secure and resilient to all these attacks. Since the WSN is an infrastructure less network, for data transmission to base station, the sensor nodes look for the service of remaining nodes for an information transfer and effective communication [4]. Due to this co-operative nature, the WSN has become vulnerable to several types of security threats.

1.1 Problem Identified:

In the WSN, the interconnected sensor nodes are heterogeneous in nature and every node has its own aspects by which they can be compromised more easily. Design of a trust based security framework just by considering few aspects makes the WSN network less resilient to different attacks. For example, if the trust design is addressed towards the tampering attacks, then the network can be compromised through remaining attacks like DoS attack, sinkhole attacks etc.

To achieve more resilience towards different types of attacks in WSNs, this work proposes a new intrusion detection mechanism based multiple attributes. Under this objective, multiple trust metrics are combined together to help the node in the selection of a more trustworthy next hop node. 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.

Rest of the paper is organized as follows; section II explores the details of literature survey. Section III explores the details of proposed methodology. Section IV explores the results and section V concludes the paper.

2 Related work

S.M. Sajjad et al., [6] 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 [7] 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.

F. Shang et al. [5] 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.

Some authors focused on the layer level security provision and towards such methodology, Umashankar G et al., [8] 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[11] 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)” [9]. 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.

Guleria and Verma [10] projected a novel ant colony meta-heuristic based unequal clustering for the selection of CH. The fusion of data from CH node to that of the intermediate node termed Rendezvous node in turn decreases the transmission of energy and thus the consumed energy by the nodes were minimal. The phase of neighbor node recognition and the maintenance of link by meta-Heuristic Ant colony optimization technique in turn choose the optimal path among the nodes that enhances the delivered packet to the destination nodes. The initialization of population needs excess time at this stage. Therefore, the Haversine distance was estimated between the nodes that too decreases the message transmission dimensionality over the nodes. The optimal path prediction and the selection of CH with the use of ant colony optimization Meta-Heuristics [12] and the unequal clustering process thus reduce the consumption of energy effectively.

3 Proposed Methodology

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;

3.1 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

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

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.

3.2 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;

$$Q_T(s_i,s_j) = \begin{cases} \frac{|T_w|}{|T_e|}, & if\ P = 0 \\ \delta \times \frac{|T_w|}{|T_e|}, & if\ P \neq 0 \end{cases} \qquad (2)$$

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. $\delta$is mathematically derived as;

$$\delta = \beta^{\left(1-\frac{1}{P+1}\right)} \qquad (3)$$

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

$$C_T(s_i,s_j) = \frac{1}{2} \times \left[\left(w_1 \times F_T(s_i,s_j)\right) + \left(w_2 \times Q_T(s_i,s_j)\right)\right] \qquad (4)$$

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.

4 Simulation 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, and FPR.

Here, 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) [6] 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 [7], 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 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.

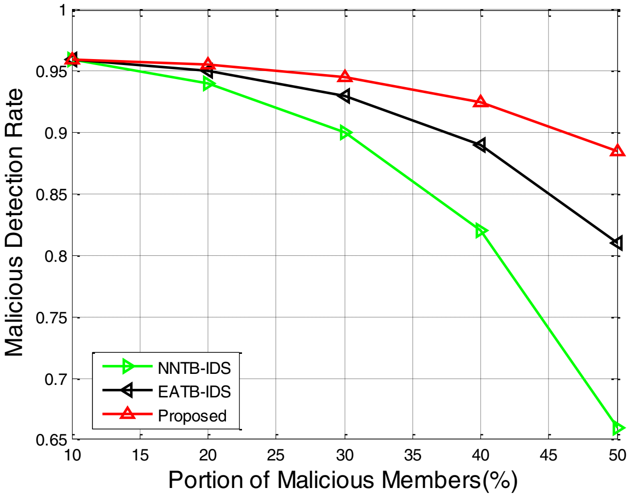

Fig.1 MDR vs. portion of malicious members

Fig.1 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.

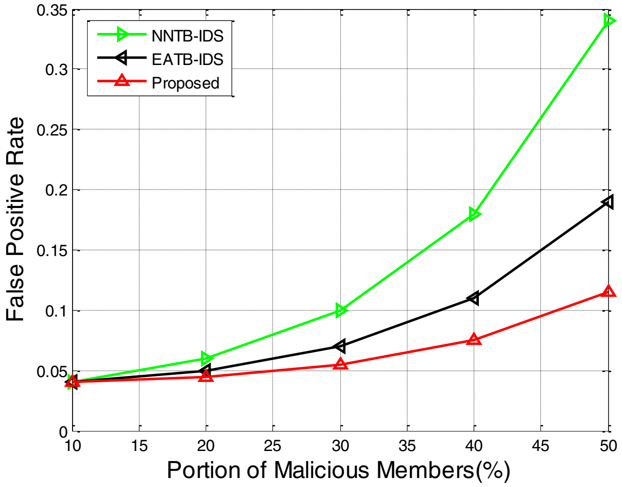

Fig.2 FPR vs. portion of malicious members

Fig.2 shows the FPR comparison between proposed and existing approaches. As shown in this figure, the FPR is increasing with an increase in the 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.

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 through capacity trust. Under capacity trust, we have further considered two sub-trusts; they are fault tolerance trust and stability trust.Experimental validations are accompanied on the proposed approach 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 robust and effective than the existing approaches. In summary, the approximate MDR, and FPR of proposed approach is noticed as 93.4012%, and 5.5000% respectively

References

1 Sohraby, K., Minoli, D., Znati, T. "*Wireless sensor networks: technology, protocols, and application*," JWsons, 203–209,(2007).

2 Tummala, S.K., Kosaraju, S. & Bobba, P.B. Optimized power generation in solar using carbon substrate for reduced greenhouse gas effect. Appl Nanosci 12, 1537–1543 (2022).

3 Xia, Feng, Tian, Yu-Chu, Li, Yanjun, Sun, Youxian, "*Wireless Sensor/Actuator Network Design for Mobile Control Applications*". Sensors, **7** ,2157–2173,(2008).

4 Vikash Kumar, Anshu Jain and Barwa P N, "*Wireless Sensor Networks: Security Issues, Challenges and Solutions*", Int Jour of Info & C.Tech, **4**, 859-868 ,(2014).

5 J. Srinivas Rao, Suresh Kumar Tummala, Narasimha Raju Kuthuri, Comparative investigation of 15 Level and 17 level cascaded h-bridge MLI with cross h-bridge MLI fed permanent magnet synchronous motor, Indonesian Journal of Electrical Engineering and Computer Science, 21(2), pp: 723-734, (2020)

6 Oladayo Olufemi Olakanmi and Adedamola Dad, "*Wireless Sensor Networks (WSNs): Security and Privacy Issues and Solutions*", (2020)

7 Shang .F, Zhou .D, Li.C, Ye.H, and Zhao.Y, "*Research on intrusion detection model based on improved cumulative summation and evidence theory for wireless sensor networks*", Photon Newton communication,**37**,212-223(2019) .

8 Tummala, S.K., Indira Priyadarshini, T., Morphological Operations and Histogram Analysis of SEM Images using Python, Indian Journal of Engineering and Materials Sciences, 2022, 29(6), pp. 794–798.

9 Sajjada S. M, Boukb S. H., Yousa M., "*Neighbor Node Trust Based Intrusion Detection System for WSN*", In: Proc.of 6th In Conf. On EUSPN,.183–188, (2015).

10 Suresh Kumar Tummala, Phaneendra Babu Bobba & Kosaraju Satyanarayana (2022) SEM & EDAX analysis of super capacitor, Advances in Materials and Processing Technologies, 8:sup4, 2398-2409

11 Rajesh kumar G., and Valluvan K. R., "*An Energy Aware Trust Based Intrusion Detection System with Adaptive Acknowledgement for Wireless Sensor Network*", Wireless Per Comm, **94**,1993–2007,(2017).

12 Ghugar U, Pradhan. J, Bhoi S. K.,. Sahoo R. R, and Panda S. K., "*PL-IDS: physical layer trust based intrusion detection system for wireless sensor networks*", IJIT, **10**, , 489–494(2018).

13 Davu, S.R., Tejavathu, R. & Tummala, S.K. EDAX analysis of poly crystalline solar cell with silicon nitride coating. Int J Interact Des Manuf (2022).

14 Ghugar U, Pradhan. J, Bhoi S. K.,. Sahoo R. R, "*LB-IDS: Securing Wireless Sensor Network Using Protocol Layer Trust-Based Intrusion Detection System*", Hindawi J.of Comp Net and Comms ,**19**,1-13,(2019).

15 M. Kavitha, P. B. Bobba and D. Prasad, "Effect of coil geometry and shielding on wireless power transfer system," 2016 IEEE 7th Power India International Conference (PIICON), Bikaner, India, 2016, pp. 1-6

16 Guleria, K. and. Verma A. K "*Meta-heuristic ant colony optimization based unequal clustering for wireless sensor network*" WirePers Comm **105,** 891-911, (2019).

17 Gali, S., Nidumolu, V, "*Multi-context trust aware routing for internet of things*" Int. J. Intell. Eng. Syst. **12**, 189–200 (2018)

18 Satyanarayana Kosaraju, Swadesh Kumar Singh, Tanya Buddi, Anil Kalluri & Ahsan Ul Haq (2020) Evaluation and characterisation of ASS316L at sub-zero temperature, Advances in Materials and Processing Technologies, 6:2, 365-375

19 Gali, S., Nidumolu, V.: "An intelligent trust sensing scheme with metaheuristic based secure routing protocol for Internet of Things". Clust. Comput. (2021).

20 Karthik Rao, R., Bobba, P.B., Suresh Kumar, T., Kosaraju, S., Feasibility analysis of different conducting and insulation materials used in laminated busbars, Materials Today: Proceedings, 2019, 26, pp. 3085–3089.