International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Wireless Sensor Network Security with the Probability Based Neighbourhood Estimation

Dr. Nachaat Mohamed[*1] , K Sampath Kumar[2], Dr. Sanskriti Sharma[3], Dr. R. Dinesh Kumar[4], Shiv Mehta[5], Dr Isa Mishra [6]

Submitted: 25/08/2022 **Accepted:** 24/11/2022

Abstract: Wireless Sensor Network (WSN) is considered as the ad hic network environment in the resource-limited devices for the energy, storage, bandwidth, and computation. In WSN environment security is a significant contribution for more computation and power in the nodes. Sensor node comprises of the hostile environment for the remote management of network topology. The captured node exhibits the fundamental characteristics in the security of the WSN. The security constraints in the WSN derives significant attention towards the vast range of application for traffic monitoring in the network. Another challenge in the WSN is the mobility of the sensor nodes in which nodes are located far away between the nodes each other with the one-hop neighbors. In this paper proposed a Probability Neighbourhood Estimation (PNE) model for improved security in the WSN environment. The proposed PNE mode estimates the neighborhood estimation of the node. With the computation of the threshold value in the neighboring nodes, the probability features of the nodes are computed. The performance of the proposed PNE model is comparatively examined with the existing Pworm and RTT based approach. The analysis of the results expressed that the proposed PNE model achieves the effective performance for the throughput and PDF value of 0.99 which is a significantly higher value than the 0.91 and 0.98. The analysis expressed that the proposed model~6 – 7% than the existing models..

Keywords: *Wireless Sensor Network, Probability, Neighbourhood value, threshold value*

1. Introduction

Sensor nodes are distributed in a given area for monitoring real world environmental or physical conditions such as location, pressure, temperature, motion, sound etc [1]. It is widely used by military applications. Normally the environment is hostile or disaster area. Due to the presence of malicious nodes in the sensor network, it has to face various security problems [2]. Major research issues in wireless sensor networks include energy, self-management, hardware and software issues, MAC layer issues, data collection and transmission, deployment, decentralized management, multimedia communication, synchronization and real time operations [3] Due to the fundamental characteristics of sensor nodes, security is the important and crucial issue. This study focuses on security attacks in wireless sensor networks.

Each node in the wireless sensor network contains power supply (battery), radio transceiver, analog-to-digital converter and microprocessor [4]. Each node sends data to the neighboring nodes and the neighboring nodes forward it to the next neighboring nodes and at last it reaches to the sink node. Major applications of wireless sensor networks are divided into two parts: event detection applications and data collection applications [5]. Sensor nodes are deployed in the field. When any event occurs, the information is routed to the base station or sink node [6]. User can access base station through internet or satellite. Security is effective parameter in the resource constraint environment based on the fundamental operation. The

vulnerability of the WSN subjected to the different attacks such as wormhole, sinkhole, blackhole, selective forwarding, sybil and so on [7].

Among the different security model, the wormhole is challenging in the network with the consideration of the gateway model [8]. The gateway model comprises of the different attack parameters that are very difficult to handle without the implementation of the cryptographic process in the network. The malicious node attack computes the location traffic in the network based on the consideration of the different locations those are distributed in the routing process [9]. Recently, the wormhole network is considered as the more challenging to the WSN environment for the network security. This paper presented a probability-based neighbourhood estimation model in the network. The developed model PNE is estimated the neighbourhood estimation of the WSN variables for the prevention of the security in the network.

2. Related Works

In [10] developed a distance vector routing algorithm for the computation of the periodic node transmission in the routing table

[1] *Rabdan Academy, UAE Homeland Security, University Sains Malaysia Abu Dhabi, eng.cne1@gmail.com*
[2] *Professor, Department of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India, k.sampath@galgotiasuniversity.edu.in*
[3] *Electronics and telecommunication Manager @ Anshkriti Academy, Raipur, Chhattisgarh, India, sanskriti04sharma@gmail.com*
[4] *Dept. of Electronics and communication Engineering, PERI Institute of technology, Chenna, India*
[5] *Student, Dhirubhai Ambani International School, Mumbai, India shivmehta722@gmail.com*
[6] *KIIT Deemed to be University School of Management KIIT School of Management Bhubaneswar, India, isa.mishra@ksom.ac.in*
* *Corresponding Author Email: eng.cne1@gmail.com*

with the estimation of the neighbors. Every node in the network computes the routing table value with the computation of the neighbours with the periodic update of the values in the routing table through neighbourhood estimation in the routing table. The routing table evaluate the distance entries for the broadcast of the routing nodes. The neighboring nodes are estimated connected with the wormhole attack to update the value in the routing table based on the hop distance.

With the demand routing protocol integrated with the Dynamic Source Routing (DSR) and Ad Hoc on Demand Distance Vector Routing (AODV) presented in [11]. Based on the on demand routing the RREQ packet is incorporated for the forwarding of the RREQ messages to reach the destination. Upon the reception of the RREQ message the destination nodes are transmitted for the RREP for the path reverse. Upon the reception of the RREP node the path is established between source to destination for the transferred data packet from source to destination in the route. This approach detects neighbors which are not within the transmission range but are remotely connected [12]. When node A sends RREQ packet to the next node, that is node B, it promiscuously monitors the behavior of node B. If node A transmitted overhead data packet by node B, then it identifies that RREQ is not affected by wormhole. If node A does not transmit data packet overhead by node B, then it identifies that RREQ is affected by wormhole.

In [13] presented mobile beacon-based wormhole detection in wireless sensor networks. Attackers are localized accurately and eliminated. The intersection point of the chords' perpendicular bisector is found when the communication properties are violated between mobile and static beacon. The wormhole attacker is localized as the center of the communication disk. For communication with the static beacon, mobile beacon moves in the network. The authors have presented location-based compromise tolerant security approach which uses location-based keys for wormhole detection. Each node has a unique private key which is bound to both location and ID of the node. A node-to-node authentication protocol is presented in [14]. It is based on location-based keys. It is an efficient countermeasure for wormhole. If the node is within the communication range and has the location-based keys, then it is accepted as a real neighbor. If the node is outside the communication range, then the authentication process is denied.

The authors have proposed mitigation of wormhole in mobile multi hop wireless networks using secure localization and key distribution approach [15]. Communication keys are loaded in every sensor node. If two sensor nodes are within the communication range of each other, then they can share a communication key. If the nodes are not within the communication range, then they cannot share a communication key. A node does not process the message received from the neighbor connected through tunnel because the node does not have the shared key used for decryption. The authors have presented secure range independent localization approach for wormhole detection in [16]. The locators transmit the beacon information. Based on the beacon information, each sensor node computes its location. This method is range independent and distributed. Wormhole is detected if the transmission range violation property and the sector uniqueness property are satisfied.

3. Probability Neighbourhood Estimation

All sensor nodes are assumed to be static. It is also assumed that for some initial interval malicious nodes are not present and every node safely establishes neighbor information. Two malicious nodes create high speed tunnel. One malicious node is located in one area and second malicious node is located in different area. One malicious node attracts traffic from one part and tunnels the traffic to another malicious node located in different area. The goal of an adversary is to disturb routing with the flow chart is presented in figure 1.

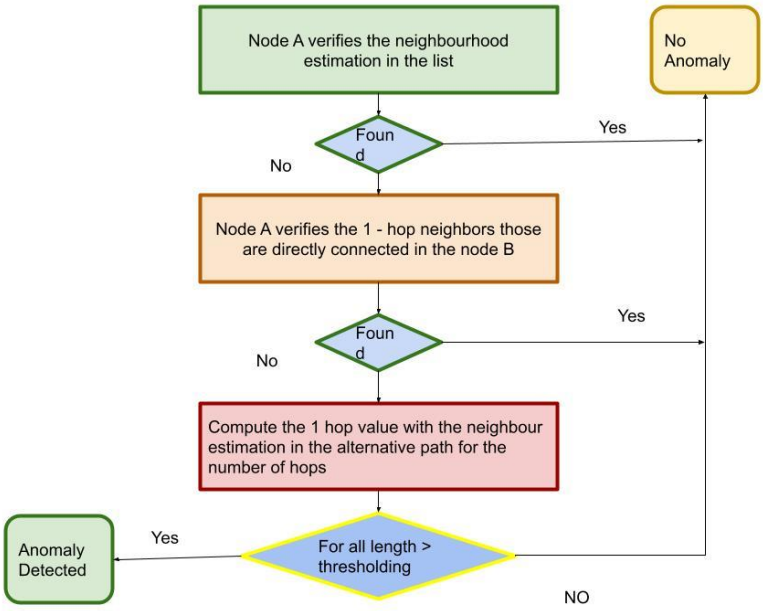

Figure 1: Flow Chart of the PNE

Node A first verifies that one of its neighbors is included in the neighbor list of node B. To do this, node A finds the intersection of neighbors of its own with the neighbors of node B. If any common neighbor is found, then attack is not present. If not found, then node A verifies that one of its one hop neighbors is directly connected to one of the one hop neighbors of node B. To

do this, node A finds the intersection of its one hop neighbor list with the one hop neighbor list of node B. If any common neighbor is found, then no attack is present in the network. If not found, then node A asks all its one hop trusted neighbors to find shortest path to node B. This path cannot be direct path and does not pass-through node A and report the number of hop count. If for any path, no of hop count is less than or equal to the threshold value then attack is not present in the network

The steps of the proposed PNE protocol are as follow:

Step 1: Node A verifies that whether node A and node B share any one hop common neighbor. Two fake neighbor nodes will not compute the neighbour node with the one hop count. Two genuine neighbor nodes generally share a common one hop neighbor node among them. If found then go to step (4), otherwise go to the next step.

Step 2: Node A verifies that any neighbor of A is directly connected to any neighbor of node B. Node A visits its entire neighbor's neighbor table to verify that if any of B's neighbor is present. Then go to step (4) else go to the next step.

Step 3: Based on the trusted neighbor value the shortest path is computed based on the suspicious node B. The path is formed based on the direct path those are not passes through the node A. If any length is computed based on the threshold than the value is minimal, otherwise go to step (6)

Step 4: Eliminate the suspicious entry in the node based on the trusted list value. The identified route from the source A to B is computed based on the estimated values. This illustrate the wormhole attack is not present in the network.

Step 5: Stop.

Step 6: The identified route in the data transmission between A to B is computed with the estimation fo the fake route in the network.

Step 7: Stop.

The proposed PNE model is estimated based in the neighbourhood values in the network nodes for the radius R between the node value of P and Q. The transmission probability in the occurrence node for the transmission is estimated as in the equation (1) – (3)

$$Sector\ Area\ (PASB) = \left(\frac{1}{2}\right) * R * S = \left(\frac{\theta}{2}\right) * R^2 \quad (1)$$

$$\cos\left(\frac{\theta}{2}\right) = \frac{\left(\frac{D}{2}\right)}{R} = D/2R \quad (2)$$

$$\left(\frac{\theta}{2}\right) = Cos^{-1}\left(\frac{D}{2R}\right) \quad (3)$$

Based on the computation of the deployed sensor nodes in the network the PNE compute the estimated neighbouring values using the equation (4) – (10)

$$PASB = R^2 * Cos^{-1}\left(\frac{D}{2R}\right) \quad (4)$$

$$Area\ of\ Triangle\ (PAB) = \left(\frac{1}{2}\right) * AB * PO = \left(\frac{1}{2}\right) * OA * D/2 \quad (5)$$

$$R^2 = PO^2 + OA^2 = \frac{D^2}{4} + OA^2 \quad (6)$$

$$OA^2 = R^2 - \frac{D^2}{4} \quad (7)$$

$$OA = \sqrt{R^2 - \left(\frac{D^2}{4}\right)} * \left(\frac{D}{2}\right) \quad (8)$$

$$Overlapping\ Area\ A(D) = 2(PASB - PAB) \quad (9)$$

$$A(D) = 2 * \left(\left(RCos^{-1}\left(\frac{D}{2R}\right)\right) - \sqrt{R^2 - \left(\frac{D^2}{4}\right)} * \left(\frac{D}{2}\right)\right) \quad (10)$$

The PNE model overlapping area in the node are computed as in equation (11)

$$= e^{-\delta.A(d)} \quad (11)$$

The maximal probability distance computed between the variables are computed using P and Q is R as in equation (12)

$$P(D) = \left(\frac{1}{R^2}\right) * \left(\frac{\partial D^2}{\partial D}\right) = \frac{2D}{R^2} \quad (12)$$

Trough the consideration of the proposed PNE mode the algorithm 1 is presented as follows:

Algorithm 1: PNE in the WSN Security

Input: - the number of nodes in the network, length of the grid in the network, Cluster centre, Area of the network, radius of communication, density of the grid

1. Classify the network into partition in the grid plane defined as $P(D)$rwith the equal cluster values $\frac{2D}{R^2}$, with the transmission radius
2. Compute the each grid in the network, those are computed $PASB$
3. Evaluate the probability value of th every grid in the network based on the density level in the cluster as in equation (6)
4. Calculate the area of the network as$P(D) = \left(\frac{1}{R^2}\right)$, the cluster grid number is calculated as (12)
5. Elect the neighbour node in the selected cluster groups as $A(D)$
6. Compute the cluster probability grid number using the equation (!0)

The probability value of the nodes are computed.

4. Simulation Setting

The proposed PNE model evaluate the probability value of the WSN model with the estimation of the neighbours. One can deploy more no. of nodes (200, 300 etc). But if more no. of nodes are considered for deployment then no. of neighbors of all nodes increase. It will increase the size of neighborhood table and increase the storage cost and also creates an overhead. If no. of neighbors of all nodes increases, then it will also consume more energy for route request packet broadcasting. In the table 1 the simulation setting for the proposed PNE model in the WSN mode is presented.

Table 1: Simulation Setting

Simulator	**Values**
No. of Nodes	14, 25, 50, 100
Simulation Time	500s
Area	1000 *1000 m2
Routing Protocol	AODV
Mobility Model	None (Static)
Attacker	1 pair
Traffic Model	CBR(UDP)
Channel Type	Wireless
Packet Size	512 bytes
MAC Protoco	IEEE 802.11
Antenna Type	Omni Antenna

The performance of the developed PNE model the detection accuracy is evaluated for the varying number of nodes such as 14, 25, 50 and 100. In the table 2 the detection accuracy is presented.

Table 2: Comparison of Detection Accuracy

No. of Nodes	P worm	RTT Based MDS	Proposed PNE
14	0.80	0.93	0.97
25	0.82	0.95	0.98
50	0.86	0.96	0.99
100	0.91	0.98	0.99

The proposed PNE model detection accuracy for the varying number of nodes are estimated. The proposed PNE model provides the overall detection accuracy of 0.99 for the 50 and 100 nodes in the network. Detection accuracy of our proposed approach is consistently maintained between 0.97 to 0.99 whereas that of Pworm falls down to 0.80 to 0.91 and RTT Based MDS to 0.93 to 0.98. The figure 2 provides the comparative analysis of the detection accuracy.

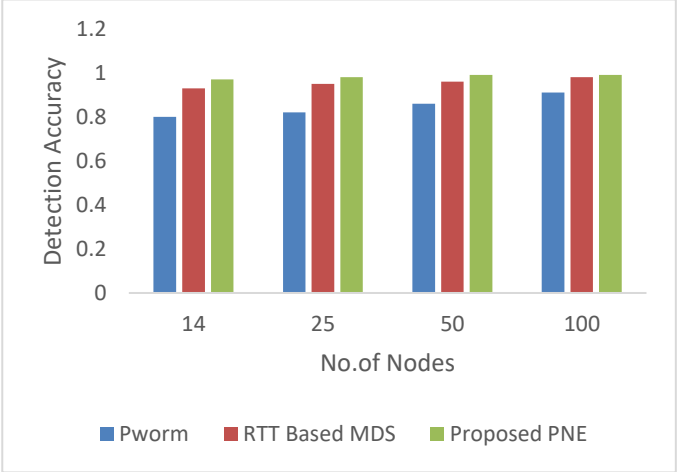

Figure 2: Comparison of Detection Accuracy

Table 3: PDF and throughput for sinkhole-based wormhole attack

No. of Nodes	Throughput (KBPS)		PDF (Percentage)	
	Without Attack	With Attack	Without Attack	With Attack
60	84	72.15	99.70	85.14
80	84.75	72.90	99.76	85.90
100	85.10	73.20	99.78	86.10

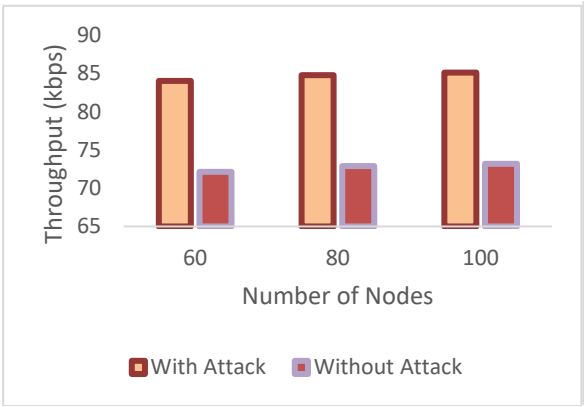

Figure 3: Comparison of Throughput

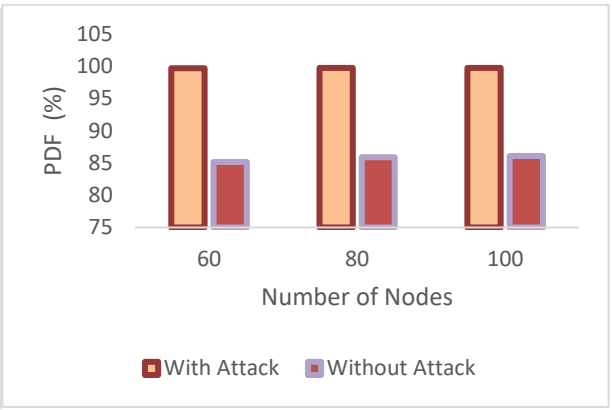

Figure 4: Comparison of PDF

The table 4 provides the estimated throughput and PDF value for the with and without attack environment.

Table 4: Comparison of throughput for denial of service based wormhole attack

No. of Nodes	Throughput (KBPS)		PDF (Percentage)	
	Without Attack	With Attack	Without Attack	With Attack
60	84	62.30	99.70	59.40
80	84.75	62.65	99.76	*59.85*
100	85.10	62.75	99.78	60.10

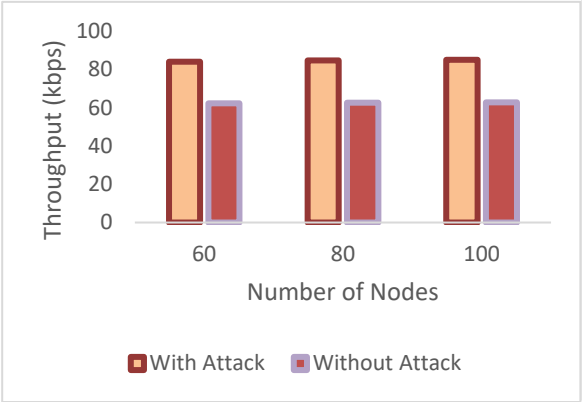

Figure 5: Comparison of Throughput

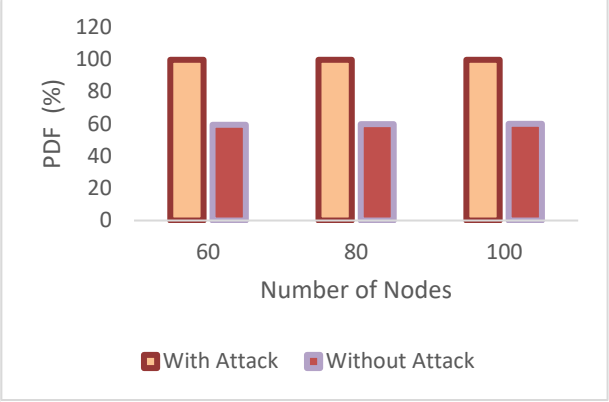

Figure 6: Comparison of PDF

The figure 3 and figure 4 provides the computed throughput and PDF value for the proposed PNE under with attack and without attack environment.

5. Conclusion

The WSN model comprises of the challenges and issues associated with the improved security in the network. To improve the security in the WSN the PNE model for the computation of the features based on the distance computation in time information, secure neighboorhood estimation, connectivity information and location information. The presented mode uses the estimation of the neighbourhood distance between the variables for the estimation and computation of the features. The performance of the proposed PNE model is comparatively examined with the existing P worm and RTT based approach. The analysis of the results expressed that the proposed PNE model achieves the effective performance for the throughput and PDF value of 0.99 which is a significantly higher value than the 0.91 and 0.98. The analysis expressed that the proposed model ~6 – 7% than the existing models.

References

[1] Cao, C., Tang, Y., Huang, D., Gan, W., & Zhang, C. (2021). IIBE: an improved identity-based encryption algorithm for WSN security. Security and Communication Networks, 2021.

[2] Singh, S., & Saini, H. S. (2021). Learning-based security technique for selective forwarding attack in clustered WSN. Wireless Personal Communications, 118(1), 789-814.

[3] Qichen, W. (2022, April). Research progress on wireless sensor network (WSN) security technology. In Journal of Physics: Conference Series (Vol. 2256, No. 1, p. 012043). IOP Publishing.

[4] Ávila, K., Sanmartin, P., Jabba, D., & Gómez, J. (2021). An analytical survey of attack scenario parameters on the techniques of attack mitigation in WSN. Wireless Personal Communications, 1-32.

[5] Ramasamy, K., Anisi, M. H., & Jindal, A. (2021). E2DA: Energy efficient data aggregation and end-to-end security in 3D reconfigurable WSN. IEEE Transactions on Green Communications and Networking, 6(2), 787-798.

[6] Majumdar, P., Mitra, S., & Bhattacharya, D. (2021). IoT for promoting agriculture 4.0: a review from the perspective of weather monitoring, yield prediction, security of WSN protocols, and hardware cost analysis. Journal of Biosystems Engineering, 1-22.

[7] Hema Kumar, M., Mohanraj, V., Suresh, Y., Senthilkumar, J., & Nagalalli, G. (2021). Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN. Journal of Ambient Intelligence and Humanized Computing, 12(5), 5287-5295.

[8] Sumalatha, M. S., & Nandalal, V. (2021). An intelligent cross layer security based fuzzy trust calculation mechanism (CLS-FTCM) for securing wireless sensor network (WSN). Journal of Ambient Intelligence and Humanized Computing, 12(5), 4559-4573.

[9] Aljadani, N., & Gazdar, T. (2022). A Novel Security Architecture for WSN-Based Applications in Smart Grid. Smart Cities, 5(2), 633-649.

[10] Soni, G., & Chandravanshi, K. (2021, August). Security scheme to identify malicious maneuver of flooding attack for WSN in 6G. In 2021 8th International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 124-129). IEEE.

[11] Kwon, D. K., Yu, S. J., Lee, J. Y., Son, S. H., & Park, Y. H. (2021). WSN-SLAP: Secure and lightweight mutual authentication protocol for wireless sensor networks. Sensors, 21(3), 936.

[12] Jayatunga, E. H., Ranaweera, P. S., & Balapuwaduge, I. A. M. (2021). Blockchain advances and security practices in WSN, CRN, SDN, opportunistic mobile networks, delay tolerant networks. In Revolutionary Applications of Blockchain-Enabled Privacy and Access Control (pp. 1-34). IGI Global.

[13] Butt, T. M., Riaz, R., Chakraborty, C., Rizvi, S. S., & Paul, A. (2021). Cogent and energy efficient authentication protocol for wsn in iot. Comput. Mater. Contin, 68, 1877-1898.

[14] Rhim, H., Tamine, K., Abassi, R., Sauveron, D., & Guemara, S. (2021, March). Enhancing security using digital signature in an efficient Network Coding-enabled WSN. In 2021 18th International Multi-Conference on Systems, Signals & Devices (SSD) (pp. 70-78). IEEE.

[15] Gulganwa, P., & Jain, S. (2022). EES-WCA: energy efficient and secure weighted clustering for WSN using machine learning approach. International Journal of Information Technology, 14(1), 135-144.

[16] Bakshi, G., & Sahu, H. WSN Security: Intrusion Detection Approaches Using Machine Learning. In Computational Intelligence for Wireless Sensor Networks (pp. 151-174). Chapman and Hall/CRC.