IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111241

Efficient Trust-based Malicious Node Identification and Recovery Technique in Resource-Constrained Wireless Sensor Networks

Mohammad Sirajuddin[1], Dr. B. Sateesh Kumar[2]

Research Scholar, Department of Computer Science & Engineering, JNTU, Hyderabad, Telangana, India[1]

Professor, Department of Computer Science & Engineering JNTUH-College of Engineering, Jagitial, Telangana, India[2]

Abstract: Protecting Wireless Sensor Networks from various security attacks is challenging. The effect of destructive security attacks like black-hole and warm-hole are more on resource-constrained Wireless Sensor Networks; these attacks target the nodes and cause packet alteration, routing disruption, and node failure. Adding malicious nodes to an existing wireless sensor network is one of the common threats. Malicious nodes may reduce network reliability by saturating the network with traffic, sending data, or creating new paths.This paper proposes a methodology based on the AODV protocol to detect and recover malicious nodes using trust metrics like node behaviour, acknowledgements, and residual energy, nodes fail to score threshold value declared as malicious, and node recovery mechanism activated, idle node present near to the malicious node recover the affected node and make it eligible for further communication. Experimental results are conducted using NS2 and proved that the proposed methodology enhances the Throughput, Packet Delivery Ration and reduces End to End Delay by identifying and recovering the malicious nodes.

Keywords: Security, Malicious Nodes, AODV, Node Recovery, Wireless Sensor Network.

I. INTRODUCTION

Wireless Sensor Network (WSN) is a highly dispersed network made up of several little sensor nodes that are light and compact, each of which has a sensor to measure physical phenomena like pressure, heat, and light. A base station, a sink, and sensor nodes built up a WSN. The sensor nodes can perceive, interpret data, and interact with one another wirelessly. They are typically placed under challenging settings[1]. The network is seriously threatened by the existence of malicious nodes. Attackers can carry out a wide range of internal and external attacks by manipulating these nodes, including keeping track of the private information that is transmitted through them, flooding sensor networks with false data, demolishing the typical data gathering operation by altering with the information, conducting different Types of attacks, and more. Malicious multi - path nodes are more unsafe even though they and sent false or altered information to nodes parallel to the longitudinal multiple paths at the same time, making it easy for pollution data to expanded, consuming a large amount of important resources from intermediate forwarding nodes, and ultimately reducing the lifespan of the entire wireless sensor network. In multipath networks, it is critical to recognise, find, and isolate hostile nodes [1].

In wireless sensor networks, identifying malicious nodes has long been a hot subject. Many academics have put forth some successful detection methods for harmful nodes. Many sensor data are, nevertheless, sent through multipath in wireless sensor networks in order to ensure the accuracy of data transmission. Malicious node detection systems now in use concentrate mostly on discovering and identifying malicious nodes along a single route[2].

In addition to identifying unusual activity or network intrusions, trust assessment methods promote ongoing trust between the nodes, improving overall security and avoiding some intrusions. Distributed and centralised trust evaluation techniques are both used today[2]. We discuss numerous complex intrusions from the examination of known intrusions, including denial of service (DoS), Black hole, Gray-hole, tunnelling, and Sybil assault. DoS attacks target a network's node availability. In this attack, an unauthorised node transmits more packets into the network than trustworthy nodes. Several system elements detect an intrusion during the Sybil attack implementation. In this instance, an intrusion attempts to gain more influence within the network by posing as a benign node [2].

The main challenge in WSN is data security because it is easily accessed. Intruders attack networks by transmitting malicious data packets over them. A subset of sensor nodes is constructed and brought into the network outside in black hole attacks. As a result of this attack, the intruder introduces new routing pathways with the assistance of a malicious node as though they are part of the planned algorithm and therefore manipulates the routes. As packets must be transmitted

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022
DOI: 10.17148/IJARCCE.2022.111241

in the shortest route possible from source to destination in the network, the black hole attack enables even non-shortest pathways to be shown as the shortest, leading the sensor network to become unstable as packets are rejected [2].

II. LITERATURE SURVEY

The paper [3] provides a method for identifying malicious nodes based on the optimisation of environmental parameters and a temporal reputation model (TRM-EPO). First, using both the indicated indirect reputation and the direct reputation, the total reputation is calculated. The ecological factors matrix is calculated on the operating status of the nodes and takes into account their power usage, data volume, amount of adjacent nodes, and node separability. The results of the experiments reveal that the proposed approach improves the security and trustworthiness of sensor nodes in a complex environment. Additionally, when compared to competing algorithms, the TRM-EPO improves recognition by far more than 1% while decreasing false positives by more than 1%.

The paper [4] offers a novel localised approach for detecting malicious nodes in WSNs, in which existing validated nodes detect harmful nodes using neighbourhood information and message signatures. The results of the testbed experiments and simulations reveal that the suggested algorithm is a practical and efficient method for detecting malicious nodes.

This article [5] offers a WSN HFDLMN technique based on homomorphic fingerprinting for malicious node identification and localisation. Homomorphic fingerprint and coding technology used on the original data is separated into n packets and delivered to the base station via n pathways in the HFDLMN scheme. The base station checks the authenticity of the packets to see if there are malicious nodes in each path; if there are, the location algorithm of the malicious node is applied to find the particular malicious nodes in the path. The findings show that the method is effective.

[6] proposes the BSCSR Protocol to address failed nodes in WSN. The suggested solution uses a trust-based mechanism to differentiate antinodes from safe nodes, protecting the network against fake information insertion while simultaneously offering an efficient route free of carousal and stretch assaults. The efficacy of BSCSRP is evaluated by comparing it against the performance of current approaches like AF-TNS, BTEM, RSA, and ERF.

A Secure Data Aggregation Protocol (SDAP) is described in the research publication [7], which detects malicious nodes by displaying a logical group as a tree topology. In order to provide a greater approximation and precision against security issues, a high level of confidence is required. Aggregation is produced in the tree topology by aggregating non-leaf nodes. As a consequence, data aggregation efficiency is reached while the data is securely aggregated.

The paper [8] offers a theory-based correlation method for spotting hostile nodes that prevents fault data injection attacks. The first step is to utilise temporal correlation to find anomalies in similar kinds of sensor data. Second, by exploiting geographical correlation, malicious nodes are found. Third, utilising event correlation, the malicious identified nodes are validated. In terms of recall and false-positive and false-negative rates, the experimental findings and comparisons with current approaches reveal that the proposed method surpasses the standard fuzzy reputation system and normalised strategies.

Proposed Model

The proposed model was developed using the AODV protocol and with the addition of a trust, model to detect malicious nodes. This paper proposes a methodology based on the AODV protocol to detect and recover malicious nodes using trust metrics like node behaviour, acknowledgements, and residual energy, nodes fail to score threshold value declared as malicious, and node recovery mechanism activated, idle node present near to the malicious node recover the affected node and make it eligible for further communication.

Calculation of Trust Score

In the proposed methodology, a wireless network scenario in which nodes are initially initialised with a trust score of zero in order to determine the trust value of nodes. In our architecture, transmission is accomplished via the AODV routing protocol. We used the two restrictions below to get each node's trust score. First, the first category comprises Nodes that honestly acknowledge their neighbours after receiving packets. Second, nodes determined to be in group 2 are those that lost more packets. Using the following equation, which indicates the rate of authentic acknowledgement, the first trust score is now calculated.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111241

$$S1 = \left[\frac{\left(k_1 * \left(\frac{N_a}{N_P}\right) + k_2 * Temporal\ Score + k_3 * Spatial\ Score\right)}{(k_1 + k_2 + k_3)}\right]$$

Here k_1, k_2, and k_3 are the weights given for different factors, N_a is the number of acknowledgements received, and N_p is the number of packets received. The following equation generates a second trust score based on lost packets

$$S_2 = \left[\frac{D_p}{TD_P}\right]$$

Here, D_P stands for the number of lost packets, TD_P for the overall number of dropped packets in the network, and s2 for the second trust score for a node.
The following equation calculates the final trust score

Final Trust score $$S_f = \frac{S_1 + S_2}{2}$$

Using Trust Metrics to Identify Malicious Nodes
Packet delivery ratio (PDR), node behaviour, and residual energy are used to identify malicious nodes.

Packet delivery ration
The packet delivery ratio (PDR), which measures the proportion of packets sent from a source node to a destination node within a network that is actually delivered, is known as the network. Delivering the maximum amount of data packets is required.

$$\text{Packet Delivery Ratio} = \frac{Number\ of\ Packets\ Recived}{Number\ of\ Packets\ Sent}$$

DoS attacks are easily identified by monitoring node packet delivery ratios. The packet delivery ratio goes from 0 to 1. The PDR is one of all packets that are successfully transmitted out of the total number of packets sent. The PDR is 0 if the node does not successfully transmit any amount of packets.

Node behaviour:
Every node in a Wireless Sensor Network (WSN) communication transmits data packets to surrounding nodes, consuming battery power, bandwidth, and memory space. In an ideal arrangement, all nodes send packets to other nodes based on their needs. The following equation determines node behaviour, where weights are utilised for trust score and mobility.

$$NB = W_1 * TS + W_2 * M$$

Here TS trust score, M, is the mobility

Residual Energy:
The sensor node's remaining energy may be estimated by adding the energy depleted while the node was in each condition. The residual energy is the energy that remains after a series of transmission processes. Because it is the residual energy, it is utilised to locate new neighbours and execute routing.

$$RE = E_i - S_f * E + D * E$$

He Ei is the initial energy, D distance, TS is the trust score

The Normalisation of Trust parameters

$$N_T = \frac{PDR + NB + RE}{3}$$

Calculate the threshold value for the network scenario using the following equation

$$\text{Threshold (T)} = \sum_{i=0}^{n} \frac{sf}{n}$$

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111241

III. RESULTS AND DISCUSSIONS

Simulation Setup:

Network Simulator 2 was used to simulate the wireless sensor network. The protocol is AODV, and there are 20 nodes. The network's major quantitative factors are the packet delivery ratio, throughput, and end-to-end delivery ratio. Node 10 is the sender node, and Node 20 is the receiver. The proposed methodology identifies malicious nodes based on Acknowledgments, Node behaviours, and Residual energy.

Table 1. Simulation Parameters

	Parameter	Quantity
1	Protocol	AODV
2	Simulator	NS-2
	Simulation Area	500x500m
3	Number of Nodes	20
4	Packets	TCP Packets
5	Transmission Range	200m
6	Simulation Time	100 sec
7	Packet Size	1000 to 1200 kb
8	Packets Transmission Speed	30-70 bps
9	Packet Transmission Frequency	2.5 to 5 GHz
10	Sink Node	Yes

The node which not satisfy the basic threshold of trust value is declared as a Malicious node, and the nearby idle node is raised as a resolver node which identifies the ability of the failure node and transfers the required root catch, and makes it eligible for further communication, in present network scenario Node 13 is recognised as a failed node and a nearby node, Node 2 is raised as a resolver node, Node 2 works a supplier node and recovers failure node, and allow it to participate in AODV routing process.

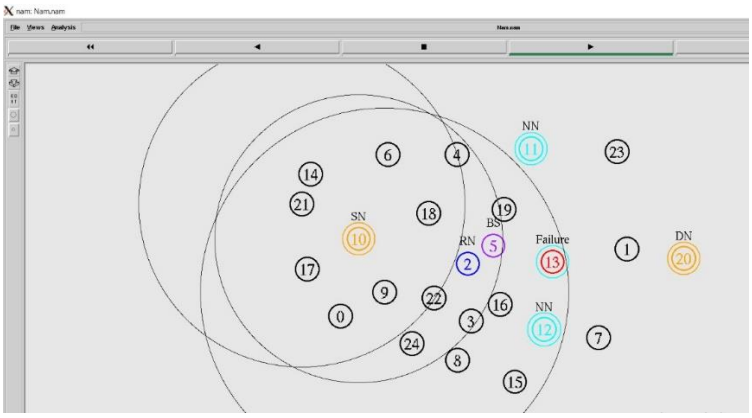

Fig 1. Malicious node detection in WSN

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111241

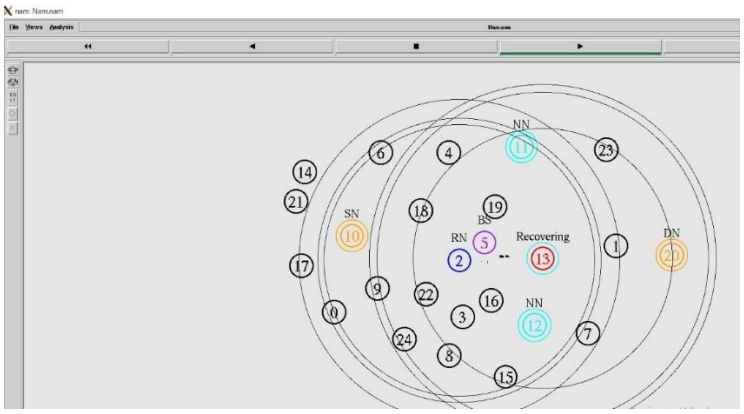

Fig 2. Recovering the Malicious Node in WSN

Packet Delivery Ration

The packet delivery ratio (PDR) is defined as the proportion of total received packets to total packets sent in the network from the source node to the destination node [9]. It is intended that the greatest amount of data packets reach the destination. The network's performance improves as the value of PDR climbs. PDR is computed by comparing the network with and without malicious nodes. A malicious node's presence reduces PDR significantly compared to the ratio without a malicious node, indicating that fewer packets reach the sink node.

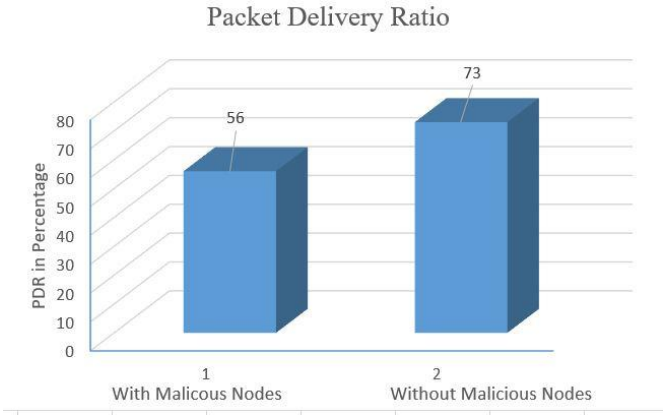

Fig 3. Analysis of Packet Delivery Ratio

Throughput

Throughput in a wireless sensor network is defined as the number of successfully transferred packets from source to destination per second. The value of throughput should be high for a well-designed network; if it is attacked, the value of throughput will be significantly reduced. Throughput is computed by comparing the network with and without malicious nodes. It is discovered that the presence of a malicious node reduces throughput significantly when compared to the proposed method, where malicious nodes are identified and recovered.

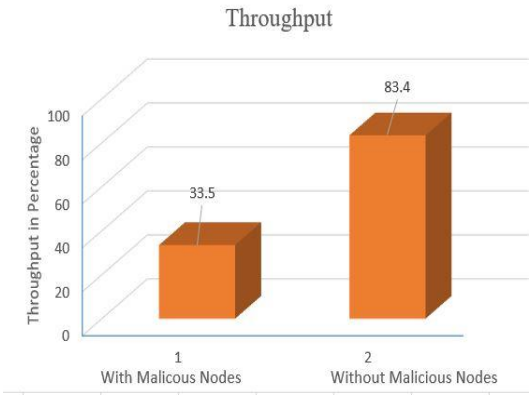

Fig 4. Throughput Analysis

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111241

End To End Delay

The time used to build the network, map out the route, encrypt at the sender, decrypt at the receiver, and other steps makes the difference between transmission and reception. The suggested method, which is superior to the previous AODV routing protocol, reduces the data transmission time to a certain level, as shown in Fig. 5.

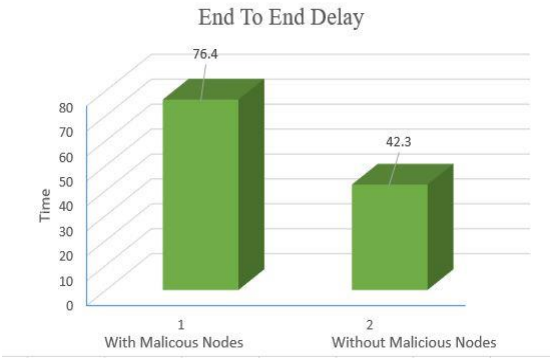

Fig 5. End To Delay Analysis

Retransmission Ratio

The figure above, Fig.6, shows how the new scheme's retransmission ratio analysis cross-validates the classical AODV Routing protocol and demonstrates that the proposed methodology is superior to the traditional technique**.**

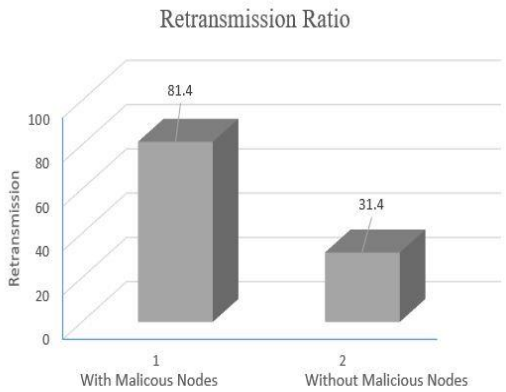

Fig 6. Analysis of Retransmission Ratio

IV. CONCLUSION

The vulnerable attacks carried out on several nodes by attackers have made wireless sensor networks an unsafe environment. This research offered a malicious node identification and recovery technique based on trust measures such as packet delivery ratio, node behaviour, and residual energy. If a node fails to achieve trust metrics, it is classified as malicious. If a malicious node detects a WSN environment, rather than taking another path, an idle node in the wireless network near the afflicted node will operate as a recovery node. The recovery node examines the efficiency level of the afflicted node and offers enough route cache to restore the node's status as a regular node and make it eligible for further communications. The experimental findings were obtained using NS2 and showed that the suggested technique improves throughput, packet delivery ratio, and end-to-end delay by recognising and recovering malicious nodes.

REFERENCES

[1]. Deebak B.D., Fadi Al-Turjman, A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks,
Ad Hoc Networks, Volume 97, 2020,102022, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2019.102022.

[2]. Selvi, M., Thangaramya, K., Ganapathy, S. *et al.* An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks. *Wireless Pers Commun* **105**, 1475–1490 (2019). https://doi.org/10.1007/s11277-019-06155-xJ.

[3]. Teng, Z., Pang, B., Sun, M. *et al.* A Malicious Node Identification Strategy with Environmental Parameters Optimization in Wireless Sensor Network. *Wireless Pers Commun* **117**, 1143–1162 (2021). https://doi.org/10.1007/s11277-020-07915-w

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111241

[4]. V. K. Akram and Y. M. Erten, "Localised Identification of Malicious Nodes in Wireless Sensor Networks," 2020 28th Signal Processing and Communications Applications Conference (SIU), 2020, pp. 1-4, doi: 10.1109/SIU49456.2020.9302076.

[5]. Abd El-Latif, Ahmed A. Zhang, Zhiming Yang, Yu Yang, Wei Wu, Fuying Li, Ping Xiong, Xiaoyong 20212021/09/24 Detection and Location of Malicious Nodes Based on Homomorphic Fingerprinting in Wireless Sensor Networks 9082570 - 2021 URL https://doi.org/10.1155/2021/9082570 Security and Communication Networks Hindawi.

[6]. Isaac Sajan R, Jasper J A secure routing scheme to mitigate attack in wireless adhoc sensor network, Computers & Security, Volume 103, 2021, 102197, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102197.

[7]. Gomathi, S. AU - Gopala Krishnan, C. 2020 DA - 2020/08/01 TI - Malicious Node Detection in Wireless Sensor Networks Using an Efficient Secure Data Aggregation ProtocolWireless Personal Communications SP - 1775 EP - 1790 VL - 113 IS - 4 1572-834X UR - https://doi.org/10.1007/s11277-020- 07291

[8]. Yingxu Lai, Liyao Tong, Jing Liu, Yipeng Wang, Tong Tang, Zijian Zhao, Hua Qin, Identifying malicious nodes in wireless sensor networks based on correlation detection, Computers & Security, Volume 113, 2022, 102540, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102540.

[9]. M. Sirajuddin and B. S. Kumar, "Efficient and Secured Route Management Scheme Against Security Attacks in Wireless Sensor Networks," 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), 2021, pp. 1045-1051, doi: 10.1109/ICESC51422.2021.9532779.