International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/218507 Volume 10, Issue 1, January – February (2023)

RESEARCH ARTICLE

NDTRA-MAT: A Novel Technique for Evaluating the Data Transfer Rate, Reducing the False Alarm Rate, and avoiding Packet Droppings Rate against Malicious Activity in Wireless Sensor Networks

Minakshi Sahu
Department of Computer Science and Engineering, GIET University, Odisha, India.
minakshi.sahu@giet.edu

Nilambar Sethi
Department of Computer Science and Engineering, GIET University, Odisha, India.
nilambar@giet.edu

Susant Kumar Das
Department of Computer Science, Berhampur University, Berhampur, Odisha, India.
dr.s.k.das.1965@gmail.com

Umashankar Ghugar
Department of Computer Science and Engineering, GITAM School of Technology (Deemed to be University), Vishakhapatnam Campus, Andhra Pradesh, India.
ughugar@ieee.org

Received: 12 October 2022 / Revised: 06 December 2022 / Accepted: 31 December 2022 / Published: 26 February 2023

Abstract – Wireless Sensor Networks (WSN) are under attack from insider packet drops. Each node will employ a trust mechanism to assess the trustworthiness of its neighbor nodes to send packets to only the trustworthy neighbors to distinguish packets dropped by inside intruders from network faults. The false alert arises when a normal node's trust value decreases and is removed from the routing paths using trust-aware routing algorithms. Optimizing the packet delivery ratio is a critical design consideration for WSNs. WSNs have long benefited from a secure zone-based routing mechanism already in place. A new routing criterion was developed for packet transfer in multi-hop communication. The routing metric was designed to protect against message manipulation, dropping, and flooding assaults. The method used an alternative way to route a packet while avoiding dangerous zones safely and efficiently in the routing process. Despite energy conservation and greater attack resilience, congestion in the WSN has increased, and the packet delivery ratio has been reduced. Each node has computing power that serves as a transceiver for the network. A packet-dropping node is hacked and forwards any or all the packets it receives. All or some boxes are packages modified by a hacked node that is intended to deliver them. In multi-hop sensor networks, packet dropping and alteration are two popular methods that an adversary can use to interrupt communication. The proposed model NDTRA-MAT is used to avoid packet loss with reduced false alarms. It is compared with the existing models, and the performance is calculated in terms of Malicious Node Detection Accuracy Levels, Packet Loss Rate, and Packet Data rate.

Index Terms – Network Security, Packet Delivery Rate, Packet Loss, Routing, Malicious Node, False Alarms, Network Performance.

1. INTRODUCTION

Wireless networks are made up of nodes that communicate with each other over a wireless link. In most cases, Wi-Fi connections are made via the last hop. Examples of mobile networks include those for phones, data, and IP, all of which are on the go. Desktop computers have evolved over the previous five years into networked agents that primarily rely on connections from separate workstations. Some unique educational and business services provided include email, cloud services, and access to the World Wide Web. In addition, the use of mobile devices, tablets, and notebook computers is increasing each year [1]. Wireless communication services are widely available, necessitating a new study into mobile ad hoc networks in recent decades. A

RESEARCH ARTICLE

wireless sensor network is a continuous, self-configured network connected to the infrastructure using signals. It is po Due to their mobility and self-government, it is possible to deploy nodes for various objectives, such as monitoring the environment, aiding in adversity, and military communication kept loss is predicted in sensor networks at a minimum to an appropriate percentage. All the lost packets are not malicious. Dropping packets can be caused by a variety of factors. Sinkhole, blackhole, and gray hole attacks are the three most common methods of generating packets to be dropped from a WSN. Nodes that have been in sinkhole attacks claim to have an excellent connection with the base station, encouraging other nodes that sinkhole attacks have harmed to take that same route to get to their destinations [2]. A compromised node alters routing packets to give make it appear to have a connection to the ground station and attract traffic. On the other hand, the compromised node's neighbors use a forged path for data exchange. A compromised node broadcasts fake route information so that it appears that it has an excellent post to the base station and thereby misleads its neighbors [3-4]. To get the data to the base station, the sinkhole's neighbors use this node to send packets. As a result, the sinkhole node attracts the attention of its nearby nodes. The data packets can be dropped, selectively dropped, or tampered with. The sink node data transmission process causing packet loss is shown in Figure 1.

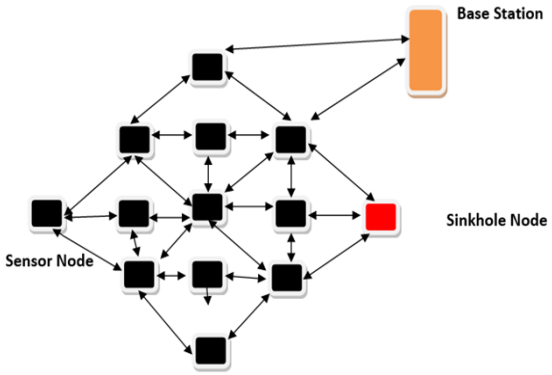

Figure 1 Sinkhole Attack in WSN

There is little to no security on WSNs, and the wireless medium is broadcast in nature. This makes WSNs vulnerable to a wide range of Dos and sinkhole assaults, making them a target for cybercriminals. In hostile situations, an adversary can launch various attacks if security measures are not in place [5-6]. These attacks can potentially interfere with the regular operation of WSNs and potentially derail their deployment. Some episodes are possible even if the adversary does not have access to the cryptographic keys used in the solution. Packet drops, fake routing requests, or flood assaults can deplete the network's energy with little effort from an attacker [7]. Because of this, malicious node detection models are essential to identify DoS and sinkhole assaults for reducing packet loss. Solutions that detect attacks should be lightweight if they are to be implemented on WSNs.

WSN packet drop attacks are a significant concern in this research. Packets may be dropped for other reasons, including collisions and congestion, in add ancient intent. For example, false alarms can be avoided by finding solutions that take these aspects into account [8]. Ad hoc network packet drop detection now relies on monitoring individual nodes. Constant monitoring is impossible because those nodes in WSNs adhere to the sleep-wake schedules. Moreover, WSNs cannot afford to monitor individual nodes. Overhearing, collision, and other issues with protocol overheads and idle listening were addressed in the developed WSN communication protocols. A collision occurs when more than one node tries to send a packet simultaneously. The cost of receiving and retransmitting data from several WSNs simultaneously increases at the destination network and the source node [9]. To avoid collisions, nodes often listen for input on the channel. It is still possible to overhear packets if nodes stay awake and listen to them several times. Wireless medium broadcasting packets cause all one-hop neighbors to hear transmissions, which exacerbates overhearing in overhearing scenarios [10].

As a rule, sinkhole attacks make malicious nodes appear particularly desirable to other nodes concerning the fake routing algorithm used. An intruder can use a sinkhole attack to harm WSNs by providing routing data that redirect all network traffic to itself. The network load balance and other assaults benefit from these effects [11]. Clustering is the process of dividing nodes into smaller groupings known as clusters. Each group has a head whose job is to keep everything running well. Communication between cluster heads and their members is their responsibility. Cluster head selection can be accomplished in a variety of ways.In some cases, the network designer chooses the cluster leader; in other cases, the cluster members choose the head node. Depending on the algorithm, the cluster head may fluctuate or remain constant over the network. There are two ways sensors can be clustered: the cluster head or a member that the leader must accept before becoming a member. Only the cluster head can receive and transmit data amongst the members and monitor the nodes for packet loss [12-13].

The objective of the proposed model is as follows:

- The packet loss rate of the network will impact the system’s performance.
- This research presents a Node Data Transfer Rate Assessment with Malicious Activity Trigger (NDTRA-MAT) model to avoid packet loss in the network with reduced false alarms.

RESEARCH ARTICLE

- The proposed model is compared with the existing Low Energy Consumed Long Life Network with Reliable Routing Protocol (LECLLN-RRP) model.
- The proposed model exhibits better results than the traditional models in terms of Malicious Node Detection Accuracy Levels, Packet Loss Rate, and Packet Data rate.

The organization of the paper has been presented as follows: section 1 deals with the introduction part, section 2 deals with the related work, section 3 deals with the system model, section 4 and section 5 deal with the proposed model and its algorithm part, section 6 deals with result analysis and finally section 6 deals with the conclusion and future work.

2. RELATED WORK

WSN data transmissions are made using radio; several safety issues and dangers exist. Sensor nodes are constrained by their available power sources. As a result, it is often impossible to safeguard them with advanced safety rules and approaches. WSN safety methods and mechanisms are designed to minimize the resources needed to protect the network. In contrast to sensor nodes, attackers can deploy equipment with better resources and capabilities, such as better signal emission antennas, consistent power supplies, and powerful processors and memory capacities. Attacks against WSNs are on the rise partly due to this. Attacks against WSNs aim to put the network at risk, abuse the data being moved within it, spy on it, or interfere with it in some other way. The layer of the protocol stack that is being attacked might be used to classify an attack. The DOS assault is one of the most frequent WSN attacks because it affects all protocol stack layers. The primary goal of this assault is to disrupt network operations. The attacker or attackers restrict legitimate network nodes from accessing network resources through a variety of attack techniques and causes packet loss. The term distributed attack refers to a situation in which the network is under attack from numerous sources simultaneously. Unlike attacks on a single node, this attack can significantly impact network performance.

The attacker may be an unaffiliated node outside the WSN or a valid node that the attacker has hacked. Both possibilities exist. The network's low performance is the result of malicious nodes. Sensor nodes are vulnerable to several assaults when this malicious node enters the network. By overloading with data and information, a sinkhole attack causes sensor nodes to respond in a time-consuming manner to route packets. This research recommends that sensor devices be mutually authenticated and malicious nodes must be isolated. The loss of packages can be caused by congestion, link layer collisions, buffer overflows, and other issues. Due to low traffic rates in WSNs, congestion and buffer overflows are unlikely to occur. It is impossible to discard a packet due to collisions if the MAC protocol is reliable. Assuming a solid MAC protocol and modest traffic rates, intentional non-forwarding or packet dropping by an attacker or compromised nodes is the most likely cause of WSN packet losses. The packet delivery and malicious action detection process using the activity trigger model is shown in Figure 2[14-15].

The number of sequences in the forwarding table of the nodes getting the route reply. Learning System. If the packet's size exceeds that of the route reply, it is either destroyed or allowed to go through. An attacker node should not have a sequence number more significant than this. This threshold value changes dynamically. Time constraints are lessened while routing overhead increases, according to simulation results. The approach proposed by Sohraby et al. [16] is divided into two phases: recognition and response, depending on the area and the rehabilitation protocol. Packets are analyzed to discover the first information collection from the neighbor node. John et al. [17] established the dynamic confidence intrusion detection technology to help identify and safeguard selfish nodes to improve network security. The use of an AODV accomplished path generation for this example. The greedy networks were found using direct and indirect levels of trust. In addition, the trust levels of the neighbors were analyzed through direct dialogue exchanges and recommendations from the neighbors themselves. The frequent topology increased data transfer time. Shafiei et al. [18] developed the Secure Routing Mechanism (SRP) to protect On-Demand routing that uses broadcasting as its route query mechanism by the DSR protocol. A security connection (SC) is required between a source address and a destination node. Between the two nodes, a shared key will define the SC. Kumar et al. [19] detected gray hole and blackhole attacks using code and response sequence packets. Sender and receiver details are contained in the code sequence packet, and the reply sequence includes the recipient's details. When a node must send a data packet to another node, a route demand is broadcast throughout the communication range. If the receiver sequences ID is significantly higher than the sender sequences ID, the algorithm believes that the node is malicious.

The trust-distrust protocol (TDP) developed by Sanchez-Casado et al. [20] has improved data routing among WSN nodes. The data on the track was broken down into four parts utilizing the protocol created. The first stage of network topology management was completed with the introduction of the k-means algorithm. In the second stage, the Signal Strength Appraisal (SSA) is used to determine the quality of the node. SSA values dictate that grading be included in the third phase of the evaluation process and the final stage of data routing in WSNs determines the secure path. Using the proposed method, high security is provided while consuming minimal energy. This solution fails because it relies on an agent-based mechanism to improve routing performance in

RESEARCH ARTICLE

WSNs. Researchers from Balakrishnan et al. [21] proposed the idea of creating an algorithm for WSN routing that is both energy mindful and trustworthy. The trust rating was used to identify questionable users in WSNs. The decision trees use spatial and temporal restrictions to determine the best route. The technique improves performance based just on security & packet delivery ratio. Fuzzy limits should have been considered when dealing with gaps in knowledge. Using an energy-efficient network protocol, Liu et al. [22] created a trust-aware routing framework that provides trust-based routing. The method's network lifetime is extended by using an energy-efficient route. This approach was unable to deal with selective forwarding and DOS attacks. Sinkhole attacks target IoT networks and are simple to conduct and hard to protect against. According to Heydari et al. [23], a detection strategy for pit attacks has been presented. When an attack mode is avoided by combining reverse, equal and minimal hop routing of distant sinks, the defense uses a routing strategy that allows for a safe path to the actual sinks. Network energy consumption characteristics are utilized in the detection path, and the detection path is primarily located in an area where residual energy is available. Because of this, the suggested system has little effect on the network's lifespan.

Trust-based identity hierarchical energy balancing routing protocol was created by Sundararajan et al. [24] to address the storage and security challenges of WSNs. The protocol helps to extend the life of wireless networks by ensuring that the energy levels of sensor nodes are maintained. Without considering delays and jitter, this protocol improves packet delivery. A time-series security mechanism based on trust-based autoregressive and non-orthogonal matrices for WSN data transmission security has been developed by Madria et al. [25]. The proposed technique proved effective in determining attacks. However, it was not implemented in heterogeneous and large-scale networks. Node-level trust is evaluated utilizing the resources of an internal node, dubbed Self-Attestation, and a Self-Scrutiny method proposed by Liu et al. [26]. The methodology was deemed successful as a mediate method independent of network topology or other data. Its peers provide computation for the model to evaluate trust and enable secure communication. Using this strategy, nodes' energy could be improved, but contact could only be processed if each node trusted itself enough.

A hidden Markov machine (HMM) developed by Sathish et al. [27] detects malicious WSN nodes to prevent data loss attacks on the network. End-to-end delays and packet delivery rates are the foundations of this approach, which uses the empirical measurement method developed by HMM. Instead, Mohamed et al. [28] used node reputation and various verification methods to solve black-hole assaults. The value of a node's reputation is influenced by the circumstances in which it is observed. With this strategy, nodes can better detect and destroy cooperative attackers while increasing their collaboration. Most research found that trust acquisition and dissemination used a significant amount of energy, which is detrimental to network longevity.

With Network attacks, the attacker considers the costs and rewards of the attack before carrying it out. When Sybil attacks occur, Qin et al. [29] developed a game-theoretic strategy to defend against them. The suggested method uses its characteristics to define a global trust limit to keep nodes in the network and identify their trust level, making an attack more expensive. The author also explained the roles of attackers and defense in their practical applications.

To avoid detection, random poisoned attacks can alter the behavior of nodes to evade detection by the system. Random poisoning assaults have been proposed by Kumar et al. [30] as a high-level conspiracy attack against cooperative intrusion detection networks. The author assumed that hostile nodes send negative feedback at random. Thus, the reimagined must be able to handle this. Even if they send misleading information, their trustworthiness is maintained considerably. More subtle difficulties arise from this. It also shows that to counter more advanced attacks, it is required to use a combination of approaches.

3. ATTACK MODEL

Any data packets sent to or from a particular area are routed through the malicious node, which rejects any packets it receives. This is called a sinkhole attack. Surrounding nodes recognize the malicious node as the most efficient data conduit. It does this by utilizing a powerful transmitter to reduce the hops required to reach the destination. More data is sent through a malicious node as it remains active in a network for longer. An artificially good path can be used to carry out a sinkhole attack. An intruder with better computing and communication capability than the other nodes can establish a high-quality single-hop link with the base station. After that, it sends a high-quality routing signal to the devices around it. All traffic is diverted to the base station, where the intruder is located, and the sinkhole attack begins. To deplete the resources of legitimate nodes, an attacker may use flooding to make many connection requests. WSNs are vulnerable to a sinkhole attack at nearly every protocol stack level. When a malicious node pretends to have the quickest path to the base station, it attracts traffic from its neighbors. Several critical security measures could be in jeopardy because of the attack. The sinkhole can target data transmission, performing several assaults against it, such as selectively discarding data packets and manipulating data aggregation techniques [31].The wormhole attacks are another option for digging a sinkhole. A malicious node first steals a routing packet from one of its neighbors and then uses a secret tunnel to deliver the package to another colluding node. The message is eventually returned to the base station by the

RESEARCH ARTICLE

colluding node. Despite its more considerable distance from the source than other routes, a tunnel can disrupt network functionality by preventing the head from identifying different legitimate routes more than two hops away from the destination. This research presents a Node Data Transfer Rate Assessment with a Malicious Activity Trigger model to avoid packet loss in the network with reduced false alarms explained clearly in the algorithm.

4. PROPOSED MODEL

The contribution of the proposed model is as follows:

- The packet loss rate of the network will impact the system's performance.
- This research presents a Node Data Transfer Rate Assessment with Malicious Activity Trigger (NDTRA-MAT) model to avoid packet loss in the network with reduced false alarms.
- The proposed model is compared with the existing Low Energy Consumed Long Life Network with Reliable Routing Protocol (LECLLN-RRP) model.
- The proposed model exhibits better results than the traditional models in terms of Malicious Node Detection Accuracy Levels, Packet Loss Rate, and Packet Data rate.

The technique of Node Authentication is used to ensure safe communication between the controlling server and data collectors. The Kernel, Data Collectors, or Port Consolidator all operate securely when dealing with Node Authentication. Node authentication verifies the node behavior in the data transmission process.

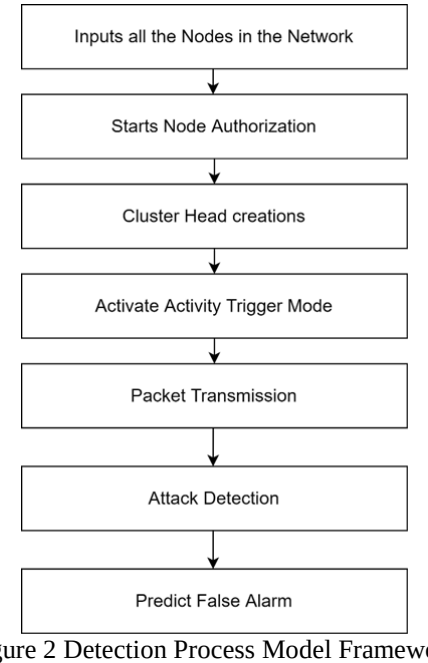

Figure 2 Detection Process Model Framework

5. ALGORITHM FOR NDTRA-MAT

Input: No. of Nodes-{N_1, $N_{2,\ldots\ldots\ldots}$, N_L}

Output: Packet Delivery Rate, Packet Loss Rate

{

Step-1: In the initial level, perform the node authorization process to monitor every node's identity. The node authorization process is performed a$NodeReg(N_L) = \sum_{i=1}^{M} getNodeID(N_i) + \bigcup_{i=1} Nodeaddr(N_i) + K$ (1)

Here K is the Time instance where the node is registered and the Node address is considered for node authorization process in the network.

Step-2: The cluster head is selected from the authorized nodes to monitor the remaining nodes and communicates with other cluster heads. The cluster head will be selected based on the node individual performance and data transmission rate. The cluster head selection is performed as

$$CH\big(Node(i)\big) = \sum_{i=1}^{M} getNodeReg\big(N(i)\big) + maxPDR\big(NodeID(i)\big) + \frac{\delta}{\gamma} \in N \quad (2)$$

Here δ is the consumed energy and γ is the total allocated energy for the node. The cluster head selected that has the best performance than the remaining nodes.

Step-3: The malicious node activities are monitored by initialing the Activity Trigger Model that monitors all nodes activities and if any malicious action occurs like, packets loss, huge traffic, load in the network. The activity trigger model is initiated as

$$ATM(CH\big(Node(i)\big) = PDR^{i} + \sum_{i=1} maxPDR\big(Node(i)\big) + maxener(Node(i)) \left\{ \frac{if\ PDR<Th\ \&\&availener<30\&\&load>60\ T\leftarrow 1}{else\ T\leftarrow 0} \right\} \quad (3)$$

Step-4: The node packet receiving rate and packer delivery rate is monitored at each authorized node and the packet delivery rate is analyzed for identifying the malicious nodes. The node packet delivery rate is calculated as

$$PDR\big(Node(i)\big) = \sum_{i=1}^{M} \frac{maxPDR\big(Node(i)\big) - PL(Node(i))}{count(PG)} \quad (4)$$

Here PDR is the packet delivery rate, PL is the packets lost and PG is the total packets generated.

Step-5: The attacks in the network are analyzed and monitored. The sink hole attack and DoS attacks are analyzed and identified that are monitored by the cluster head at each node is performed as

RESEARCH ARTICLE

$$AttackL(CH(i)) = \sum_{i=1}^{M} \frac{PDR(Node(i))}{Count(PG)} + \frac{\beta(Node(i))}{\mu} + \frac{\max(\tau)}{G} \begin{cases} \text{if PDR} < 80 \;\&\&\; \beta > 60 \;\&\&\tau > 60 \text{ Att} \leftarrow 1 \\ \text{else Att} \leftarrow 0 \end{cases} \quad (5)$$

Step-6: The false alarms by the activity trigger module can be reduced by the accurate detection of malicious nodes. The false alarms are reduced as

$$FAR = \sum_{i=1} \min(PDR(Node(i)) + minener(Node(i)) \quad (6)$$

}

6. RESULTS AND ANALYSIS

The proposed model is implemented in TCL and AWK scripts and executed in NS2 simulator. The packet loss rate of the network will impact the performance of the system. This research presents a Node Data Transfer Rate Assessment with Malicious Activity Trigger (NDTRA-MAT) model to avoid packet loss in the network with reduced false alarms. The following simulation parameter and value are used during the numerical analysis. The simulation parameters are listed in Table 1.

Table 1 Simulation Parameters

Sl. No	Simulation Parameter	Values
01	Frame work	M-Sim
02	Network Size	1000 x 1000
03	Mac type	802.11
04	Transmission Range	100m
05	Routing Protocol	AODV

The proposed model is compared with the existing Low Energy Consumed Long Life Network with Reliable Routing Protocol (LECLLN-RRP) model. The proposed model exhibits better results than the traditional models.

The technique of Node Authentication is used to ensure safe communication between the controlling server and data collectors. The Kernel, Data Collectors, or Port Consolidator all operate in a secure manner when dealing with Node Authentication. Node authentication verifies the node behavior in the data transmission process. The node validation time levels of the proposed and existing models are shown in Figure 3.

There are nodes in a WSN that collect data on environmental characteristics and send it through radio waves to a network gateway. The node authorization helps in easy and accurate recognition of normal and malicious nodes. The node authorization accuracy levels of the existing and proposed models are shown in Figure 4.

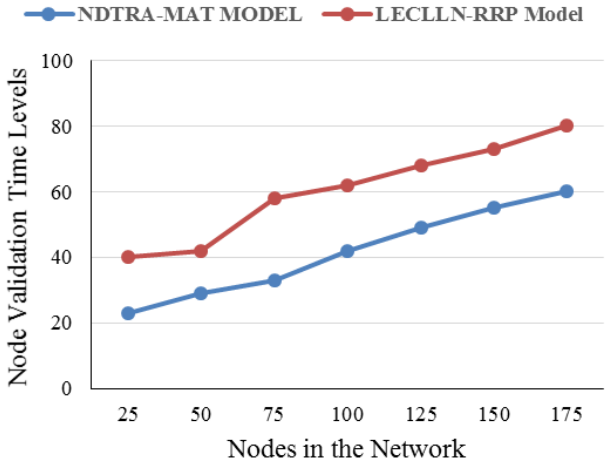

Figure 3 Node Validation Time Levels

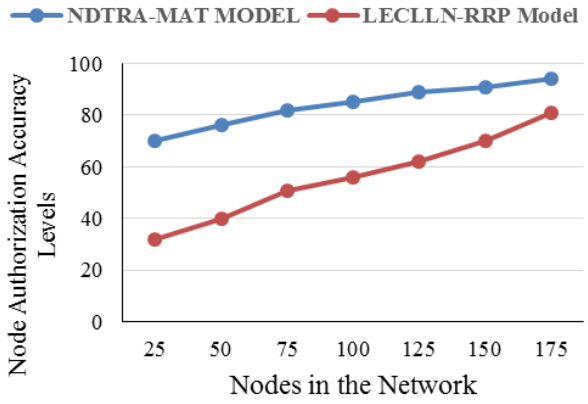

Figure 4 Node Authorization Accuracy Levels

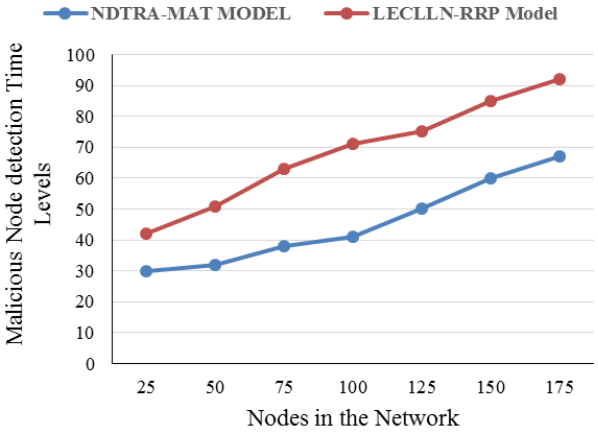

Figure 5 Malicious Node Detection Time Levels

RESEARCH ARTICLE

Malicious node detection research enhances the network performance by accurate detection. The network responsiveness can be negatively impacted by an attacker node's impact on the network's throughput. Malicious node detection is required to improve the data transmission rate. The malicious node detection time levels are shown in Figure 5.

A network can be determined by observing the behavior of evaluated nodes using multidimensional attributes and combining this information, so that the original function of a network can be established. A network can indeed be identified by observing the behavior of evaluated nodes using multidimensional attributes and combining this information so that the normal operation of a network can be established. Authentication is not required for a malicious node to enter the network.

This is done by putting stale packets into the network. The packet can be deliberately delayed by any malicious node, if they can do so. The malicious node detection accuracy levels of the existing and proposed models are shown in Figure 6.

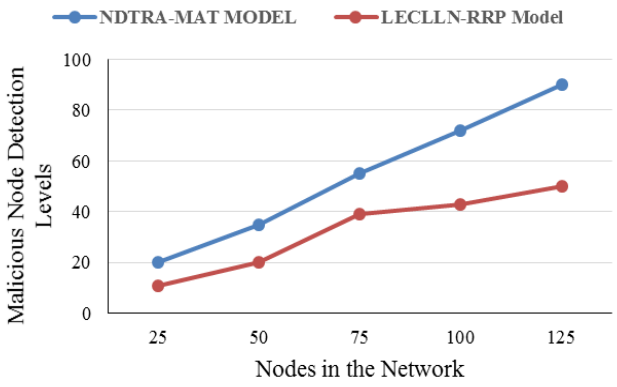

Figure 6 Malicious Node Detection Accuracy Levels

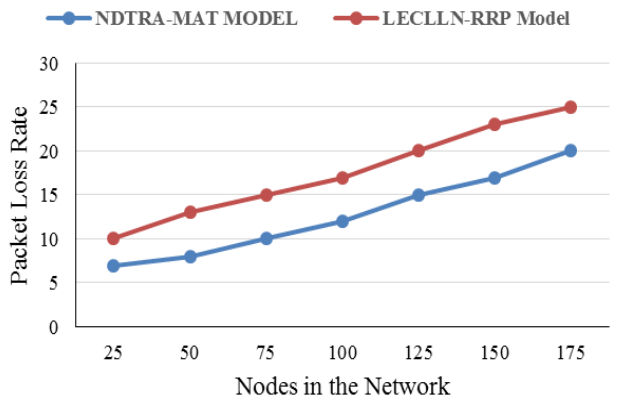

Figure7 Packet Loss Rate

The packet loss ratio is a measure of how many packets were sent out compared to how many were lost. The scheduler tries to minimize the number of packets lost due to deadline expiry if it is not possible to execute each one before the deadline has expired. The packet loss rate of the proposed model is significantly less when compared to the existing models. The Figure 7 represents the packet delivery rate of the proposed and existing models.

When calculating the "Packet Delivery Ratio," consider how many actual packets were sent from one network node to another, and divide that number by how many packets were delivered. The goal is to send as many data packets to the destination as possible. The proposed model packet delivery rate is high than the existing models. Figure 8 represents the packet delivery levels.

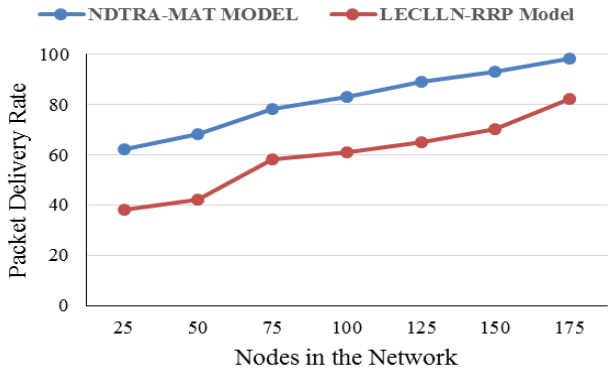

Figure 8 Packet Delivery Rate

7. CONCLUSION

WSNs have gained relevance in a wide range of commercial and military applications due to their appealing properties, such as their ease of use and low implementation costs. These networks have been the target of several security breaches because they lack centralized administration. In the packet drop attack, the malicious packets are dropped by a compromised node. However, none of the approaches used to identify packet drop attacks in WSNs can be used in the future to stop or isolate the attacks from occurring. For data forwarding, reputation systems have emerged as a means of determining which nodes are trustworthy. However, the lack of information classification in reputation systems influences the false positive rate. The broadcasting aspect of wireless media is intrinsically implicated in WSNs, which are usually unguarded. WSNs are vulnerable to a wide range of security concerns. Due to the transmission medium and distributed nature of WSNs, several attack types, including as hijack attacks, tampering attacks, hello-flood attacks, blackhole attacks, selective forwarding attacks, sinkhole attacks, and Denial of Service attacks, are involved. These attacks have the potential to impair WSN operations and perhaps defeat their deployment. This research presents a Node Data Transfer

RESEARCH ARTICLE

Rate Assessment with Malicious Activity Trigger (NDTRA-MAT) model to avoid packet loss in the network with reduced false alarms that was used to detect sinkholes and DoS attacks in every location of the network using the triggering module. An additional monitoring strategy is employed, which uses a distributed approach. In future, optimization methods need to be considered for cost reduction and performance enhancement.

REFERENCES

[1] Vasanthi, G., and N. Prabakaran. "An Implementation of Low Energy Consumed Long Life Network (LECLLN) with Reliable Routing Protocol (RRP)." 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N). IEEE, 2021.

[2] Raymond, David R., and Scott F. Midkiff. "Denial-of-service in wireless sensor networks: Attacks and defenses." IEEE Pervasive Computing 7.1 (2008): 74-81.

[3] C. John and C. Wahi, "Security analysis of routing protocols for wireless sensor networks," International Journal of Applied Engineering Research, vol. 11, no. 6, pp. 4235-4242, 2016.

[4] S. Madria and J. Yin, "SeRWA: a secure routing protocol against wormhole attacks in sensor networks," Ad Hoc Networks, vol. 7, no. 6, pp. 1051-1063, 2009.

[5] R. E. Mohamed, A. I. Saleh, M. Abdelrazzak, and A. S. Samra, "Survey on wireless sensor network applications and energy efficient routing protocols," Wireless Personal Communications, vol. 101, no. 2, pp. 1019–1055, 2018.

[6] Salehi, S. Ahmad, et al. "Detection of sinkhole attack in wireless sensor networks." 2013 IEEE international conference on space science and communication (IconSpace). IEEE, 2013.

[7] Goyal, Priyanka, Sahil Batra, and Ajit Singh. "A literature review of security attack in mobile ad-hoc networks." International Journal of Computer Applications 9.12 (2010): 11-15

[8] D. Kumar, S. Chand, and B. Kumar, "Cryptanalysis and improvement of an authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 2, pp. 641–660, 2019.

[9] Ben-Othman, Jalel, and Bashir Yahya. "Energy efficient and QoS based routing protocol for wireless sensor networks." Journal of Parallel and Distributed Computing 70.8 (2010): 849-857.

[10] Ye, Wei, John Heidemann, and Deborah Estrin. "An energy-efficient MAC protocol for wireless sensor networks." Proceedings. Twenty-first annual joint conference of the IEEE computer and communications societies. Vol. 3. IEEE, 2002.

[11] Salehi, S. Ahmad, et al. "Detection of sinkhole attack in wireless sensor networks." 2013 IEEE international conference on space science and communication (IconSpace). IEEE, 2013.

[12] Chhabra, Gurpreet Singh, and Shahista Navaz. "Enhancing Network Lifetime in Wireless Sensor Networks using Cluster-Tree based Data Gathering." International Journal of Engineering Innovations and Research 3.4 (2014): 548.

[13] Younis, Ossama, Marwan Krunz, and Srinivasan Ramasubramanian. "Node clustering in wireless sensor networks: Recent developments and deployment challenges." IEEE network 20.3 (2006): 20-25.

[14] M. Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," Computer Communications, vol. 34, no. 1, pp. 107-117, 2011.

[15] Ghugar, U., and J. Pradhan. "ML-IDS: MAC layer trust-based intrusion detection system for wireless sensor networks." Computational Intelligence in Data Mining. Springer, Singapore, 2020. 427-434.

[16] Sohraby, Kazem, Daniel Minoli, and Taieb Znati. Wireless sensor networks: technology, protocols, and applications. John wiley & sons, 2007.

[17] John, Jacob, and Paul Rodrigues. "A survey of energy-aware cluster head selection techniques in wireless sensor network." Evolutionary Intelligence (2019): 1-13.

[18] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," Journal of Computer and System Sciences, vol. 80, no. 3, pp. 644-653, 2014.

[19] Tyagi, Sudhanshu, and Neeraj Kumar. "A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks." Journal of Network and Computer Applications 36.2 (2013): 623-645.

[20] Sánchez-Casado, Leovigildo, et al. "Identification of contamination zones for sinkhole detection in MANETs." Journal of Network and Computer Applications 54 (2015): 62-77.

[21] K. Balakrishnan, J. Deng, and V. K. Varshney, "TWOACK: preventing selfishness in mobile ad hoc networks," in Proceedings of 2005 IEEE Wireless Communications and Networking Conference, New Orleans, LA, 2005, pp. 2137-2142.

[22] 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.

[23] V. Heydari and S. M. Yoo, "Lightweight acknowledgement-based method to detect misbehavior in MANETs," KSII Transactions on Internet And Information Systems, vol. 9, no. 12, pp. 5150-5169, 2015.

[24] R. K. Sundararajan and U. Arumugam, "Intrusion detection algorithm for mitigating sinkhole attack on LEACH protocol in wireless sensor network," Journal of Sensors, vol. 2015, Article ID. 203814, 2015.

[25] Madria, Sanjay, and Jian Yin. "SeRWA: A secure routing protocol against wormhole attacks in sensor networks." Ad Hoc Networks 7.6 (2009): 1051-1063.

[26] Q. Liu, J. Yin, V. C. Leung, and Z. Cai, "FADE: forwarding assessment based detection of collaborative grey hole attacks in WMNs," IEEE Transactions on Wireless Communications, vol. 12, no. 10, pp. 5124-5137, 2013.

[27] M. Sathish, K. Arumugam, S. N. Pari, and V. S. Harikrishnan, "Detection of single and collaborative black hole attack in MANET," in Proceedings of International Conference on Wireless Communications, Signal Processing and Networking, Chennai, India, 2016, pp. 2040-2044.

[28] Siddiqua, Ayesha, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. "Preventing black hole attacks in MANETs using secure knowledge algorithm." 2015 International Conference on Signal Processing and Communication Engineering Systems. IEEE, 2015.

[29] D. Qin, S. Yang, S. Jia, Y. Zhang, J. Ma, and Q. Ding, "Research on trust sensing based secure routing mechanism for wireless sensor network," IEEE Access, vol. 5, pp. 9599–9609, 2017.

[30] V. Kumar and R. Kumar, "An adaptive approach for detection of blackhole attack in mobile Ad hoc network," Procedia Computer Science, vol. 48, pp. 472-479, 2015.

[31] N. K. Sreelaja and G. A. Vijayalakshmi Pai, "Swarm intelligence-based approach for sinkhole attack detection in wireless sensor networks," Applied Soft Computing, vol. 19, pp. 68-79, 2014.

Authors

Minakshi Sahu working as Asst. Professor at Kalam Institute of Technology, Berhampur. She completed her M. Tech in Computer Science from Berhampur University in 2009. She is persuing her Ph.D at GIET University, Gunupur from 2019. She is having 12 years of teaching experience. She has published 5 National & International Journals. Her research interest is Machine learning, Network Security in WSN. She is a life member of IEEE.

RESEARCH ARTICLE

Nilambar Sethi working as Associate professor at GIET university Gunupur. He completed his M.Tech in Computer science from Utkal University in 2004. He also completed his Ph.D from Berhampur University in 2013. He is having 18 years of teaching experience. He has published more than 20 international and national journals. His research interests are machine learning, Natural language processing, Network Security in WSN. He was session chair for some conference. He is a Reviewer for some journals. He is life member of CSI, IE, ISTE.

Dr. Susanta Kumar Das joined the Dept. of Computer Science in 1993. He has teaching experience of 23 years in the department. He has attended no. of national & international conferences. To his credit, he has served as H.O.D for 2 years in the department. At present he is the coordinator of M.Tech(S.F) course & as coordinator of spoken tutorial project conducted by IIT Bombay & funded by MHRD, Govt of India. Fourteen no. of scholars are awarded Ph.D under his guidance. One D.Sc degree is awarded in Computer Science under his guidance. He has been felicitated award of honour by Dept. of Mathematics, Maharshi Dayanand University Rohtak, Haryana in the international conference on History & Development of Mathematical Science & Symposium on Nonlinear Analysis. His research are in Software Engineering & Network Security.

Umashankar Ghugar earned his full-time doctoral degree from Berhampur University, Odisha in 2021, and his M.Tech degree in Computer Science from Fakir Mohan University, Balasore in 2012. and his B.E degree in IT from Utkal University in 2006. He has 10 years of teaching experience in different organizations and is currently working as an Assistant Professor in the School of Technology, Department of CSE at GITAM University, Visakhapatnam. He has published 14 articles include journal, book chapter and conference in international publishers. His research interests are in Computer Networks, Network Security in WSN. He is a Reviewer of IEEE Access, IEEE Transaction on Education, IEEE Transactions on Neural Networks and Learning Systems, Security and Privacy (Wiley), International Journal of Communication Systems (Wiley), International Journal of Distributed Sensor Networks (Hindawi), International Journal of Knowledge Discovery in Bioinformatics (IGI Global), and International Journal of Information Security and Privacy (IGI Global) and also a member of IEEE, IACSIT, CSTA, and IRED.

How to cite this article:

Minakshi Sahu, Nilambar Sethi, Susant Kumar Das, Umashankar Ghugar, "NDTRA-MAT: A Novel Technique for Evaluating the Data Transfer Rate, Reducing the False Alarm Rate, and avoiding Packet Droppings Rate against Malicious Activity in Wireless Sensor Networks", International Journal of Computer Networks and Applications (IJCNA), 10(1), PP: 1-9, 2023, DOI: 10.22247/ijcna/2023/218507.