International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Routing and Security Based Ad-Hoc Networks Configuration for Identification of Attack Using Reinforcement Learning Approach

Dr. J. Avinash*[1], Dr. N. Sudhakar[2]

Submitted: 26/01/2024 **Revised**: 04/03/2024 **Accepted**: 12/03/2024

Abstract: In many fields of Research, wireless sensor networks have grown in popularity. Depending on the dangerous situation the networks fields, there are more chances to attack wireless sensor network. This research explains how to locate rogue nodes in the networks based on investigation and responses from each node in the networks. In generally a malicious node blocks the transmission of signal to other nodes. So, in order to increase network performance, avoid much traffic for the server to buffer, causing them to slow down and eventually stop. Hence to identify the fake node in wireless sensor network is main aim of this research through Network Simulator with the help of Reinforcement Learning based routing algorithms. Further, attack vectors allow hackers to exploit system's vulnerabilities including manual elements. It is suggested that a workable security framework for the WSN (Wireless Sensor Network) used to estimate traffic or packet loss and throughput ratio in order to detect fault identity. So enhancing the networks performance is based on request-response mechanism of the nodes, which engages with features at various levels of the protocol's system, monitors and analyzes typical patterns and alerts node to ensure their dangerous activities cannot transmit across the network. Some of monitoring basic functions through routing algorithm and NS2 include overseeing server CPUs, paying attention to network traffic, identifying patterns in error rates, alerting you about slow pages and combing through your access logs to find out how long requests usually take.

Keywords: *False Node, Wireless Sensor Computer Networks, Denial of Service Attack, Packet Drop, Routing algorithm, Reinforcement Learning.*

1. Introduction

An ad-hoc network is made up of a number of wireless mobile hosts that come together to form a temporary network without the help of any centralized administration or stand-alone equipment. Mobile Ad-hoc networks are multi-hop wireless networks that are self-organizing and self-configuring and in which the network's structure is constantly changing [1]. The nodes' mobility is primarily to blame for this. These networks' nodes share a single random-access wireless channel and cooperate amicably to engage in multi hop forwarding [2]. In addition to serving as hosts, network nodes also function as routers, sending and receiving data to and from other nodes.

In an internet connection with multiple hops, nodes work together to relay and route traffic. This cooperative tendency might be used by an enemy to launch attacks [3]. For instance, the attacker can first pose as a helpful node during the route discovery procedure. Once a route includes the enemy, it begins discarding packets [4]. The infected node merely stops transmitting every packet it receives from upstream routers in the most severe instance, fully severing the connection between its origin and the destination. By dividing the system's topology, a Denial-of- (DoS) attack of this severity can eventually cripple the system [5].

They dynamically modify their attacks, especially for intelligent malicious nodes. They assault the network in the interim with questionable plausibility. When an attacker is dynamic, our static detection model cannot perform well [6]. The initial model cannot be used with the new network once the topology has changed dynamically. Because traditional detection algorithms typically artificially adjust the algorithm in various network environments to establish a trust evaluation model appropriate for the current situation, or design a trust-based routing protocol to detect malicious nodes, they are unable to meet these needs [7]. Finally, problems and difficulties in locating rogue nodes in networks based on research and answers from each network node. Typically, a malicious node prevents signals from reaching neighbouring nodes. So, to improve network performance, try to limit the amount of traffic that the servers have to buffer before they start to slow down and eventually cease. Identifying the bogus node in the wireless sensor network is necessary.

The developed Network Simulator, which uses reinforcement learning-based routing algorithms, to address the problems. Additionally, attack vectors enable hackers to take advantage of manual weaknesses in systems. It is recommended that practical security

[1] *Associate Professor, Department of Computer Science & Engineering, N.B.K.R Institute of Science & Technology, Vidyanagar, Kota(M), Tirupati – 524413, India.*
ORCID ID: 0000-0003-4920-8040
** Corresponding Author Email: idreamavi@gmail.com*
[2] *Professor, Department of Computer Science & Engineering, Bapatla Engineering College, Bapatla – 522102, India.*
ORCID ID: 0009-0001-9449-3365
Email: suds.nagalla@gmail.com

architecture be utilised for WSNs (Wireless Sensor Networks) to calculate throughput ratios and traffic or packet loss estimates in order to identify faults. The request-response mechanism of the nodes, which interacts with characteristics at various levels of the protocol's system, monitors and analyses common patterns, and informs nodes to ensure their risky behaviours cannot propagate over the network, is therefore the basis for improving the networks' performance. Even if persistent packet loss might drastically reduce the network's throughput, such an "always-on" attack has disadvantages from the attacker's point of view.

2. Related Work

2.1. Problem Definition

It is quite difficult to identify targeted packet-dropping assaults in a wireless network that is constantly changing [8]. The challenge arises from the necessity that it is necessary to determine if the packet drop was purposeful or accidental in addition to locating the location (or hop) where it occurs [9]. Due to the open architecture of wireless technology, adverse channel characteristics including fading, noise, and disruption, connection faults, or insider attacker activity can all result in packet drops in a network [10]. Link faults are fairly important in an open wireless setting and might not be significantly lesser than the internal attacker's loss of packets rate. As a result, the insider hacker can blend in with the tough channel environment.

2.2. Disadvantages

- The majority of the linked research assumes that packet loss can only come from malicious dropping.
- A rogue node could still obtain sufficient funds via the credit-system-based mechanism if it sent the majority of the packets it got from upstream peers.
- By sending the majority of the packets towards the next hop, the rogue node can retain a respectable reputation under the reputation-based strategy.
- Although the Bloom-filter system can offer an envelope forwarding proof, its accuracy is uncertain and it can be flawed.
- Regarding the ACK-based approach and all other techniques in the second group, simply counting the number of lost packets does not provide a reliable basis for determining the actual reason for packet loss.

2.3. Contribution of the Research

To generate a reliable technique for identifying packets drop caused specifically by insider attackers. As further evidence to support the identification of choice, this system also offers decision data that are accurate and openly verifiable [11]. Packet losses (bitmaps describing lost/received social statuses of packets for consecutive packet transmissions) auto correlation function (ACF) generated from relative locations of lost packets is employed to provide precise detection capabilities [12]. One can determine whether a packet loss is caused by malicious dropping in addition to typical network problems by looking for correlations in dropped packets [13].

The key difficulties with our system are in ensuring that the package-loss bitmap images given by specific nodes along the route are accurate and accurately represent the state of each packet transfer [14]. This level of sincerity is necessary for a precise estimation of the relationship between missing packets, and it can be attained by some auditing. We further contend that as traditional mobile phones have limited resources, users might assign monitoring and identifying chores to public servers to save their own. The foundation brings up the subject of an open audit.

3. Design and Implementation

3.1. Structure of NS2

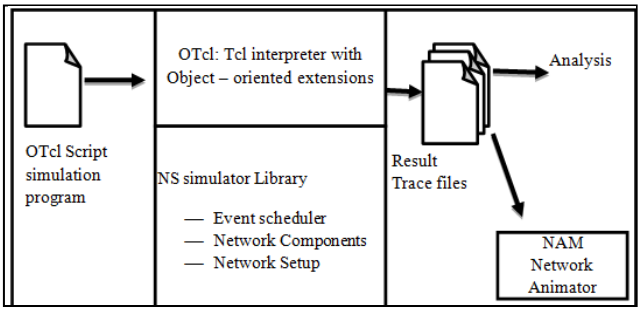

Fig. 1. Simplified User's View of NS2

3.2. Input data

An assortment of data obtained from a random system is used to create simulation models. By matching a statistical distribution to the information and then evaluating its significance, it is required to ensure that the data is scientifically legitimate. Additionally, as with any modelling procedure, the correctness of the input data must be examined, and any anomalies must be eliminated [15–16].

3.3. Data output

After a simulation is finished, the results must be analyzed. Only a plausible estimation of actual events will be produced by the simulation's final result data. There are several ways to improve the accuracy of the output information, such as running simulations again while analyzing the results, breaking events up into batches as well as processing each one separately, and comparing the outcomes of simulations run in close proximity to one another.

The fundamental concept is to carry out HTTP, FTP, and TCP protocols in part. Selecting routes through a network in order to convey network traffic is an aspect of routing [17]. Routing is done for a variety of the networks, such the internet, communication networks (like the telephone network), and systems for transportation. The main topic of this article pertains to routing for digital information networks that use the packet switching technologies.

Routing varies from bridging in a more specific sense since it presumes that network domains are organized and that addresses are similar, denoting closeness within the network. Although bridging is still frequently used in limited situations, has overtaken all other forms of addressing in big networks, including the Internet [18].

3.4. Semantics of sending messages vary between routing schemes

Broadcasts send communications to nodes in the node groups and typically to nodes closest to sources. Unicast sends email to a specific node; broadcasts send messages to the entire network; multicast sends messages to a set of nodes who have indicated interest in receiving the message.

3.5. Reinforcement learning based routing

A system can use the framework of reinforcement learning (RL), a subclass of machine learning, to efficiently choose future actions by learning from prior interactions with its environment. In order to create automated systems that get better over time, RL has been used to a variety of application fields, including gaming, robotics and control, networking, and telecommunications. It is well acknowledged that RL is effective in resolving optimisation issues pertaining to distributed systems in general and network routing in particular.

The base of reinforcement learning is discovering optimal action value function $\boldsymbol{Q^*(s,a)}$ by maximizing expected returns starting from state $\boldsymbol{s}$, actions $\boldsymbol{a}$ and following policies $\boldsymbol{\pi}$ resulting in subsequent action-state configurations [19]:

$$\boldsymbol{Q^*(s,a) = max\pi E[R_t|s_t = s, a_t = a, \pi]} \qquad (1)$$

The Bellman equation, which is the basis for the aforementioned ideal action value function, is followed by many reinforcement learning methods that repeatedly estimate the action value function. Given the current state s and the action a taken from this state, determine the updated value of the action value function according to

$$\boldsymbol{Q_{i+1}(s,a) = E\left[r + \gamma \max_{a'} Q^*(s',a')|s,a\right]} \qquad (2)$$

This function takes into account the expectation of the current reward r and the maximum future reward multiplied by the discount factor.

$$\boldsymbol{Q^*(s,a) = E_{s'\sim\xi}\left[r + \gamma \max_{a'} Q^*(s',a')|s,a\right]} \qquad (3)$$

In real-world applications, the best action value function is estimated using the approximation $\boldsymbol{Q(s,a;\theta)}$. Convolutional neural networks (CNN) [20] or fully connected networks are examples of deep neural networks that are employed in DRL as function approximators. It's common to refer to the neural network employed in the technique as a Q network. The loss functions $\boldsymbol{L_i(\theta_i)}$, which can be calculated using equation (3), are minimised in order to train the Q network using a series of sequences and actions. Here, the aim of "iteration i" is $\boldsymbol{y_i = E\left[r + \gamma \max_{a'} Q^*(s',a')|s,a;\theta_{i-1}\right]}$, and ρ(s,a) are probability distributions across states and actions.

By differentiating loss functions w.r.t weights $\boldsymbol{\theta_i}$, gradient Eqn.(4) can be obtained. Networks are trained with stochastic gradient descents based on gradients and on training; actions can be obtained from networks following greedy strategies (ε).

$$\boldsymbol{L_i(\theta_i) = E_{s,a\sim\rho(.)}(y_i - Q(s,a;\theta_i)^2} \qquad (4)$$

$$\boldsymbol{\nabla_{\theta_i} L_i(\theta_i) = E[r + \gamma \max_{a'} Q\ \ (s',a';\theta_{i-1}) - Q(s,a;\theta_i))dQ]} \qquad (5)$$

$$\boldsymbol{dQ = \nabla_{\theta_i} Q(s,a\theta_i)} \qquad (6)$$

3.6. Choosing a route

Applying a routing measure to numerous routes in order to choose the best one is known as path selection. When it comes to computer social media, the metric is calculated by an algorithm for routing and can include data on the bandwidth, network postponement, trip count, path expense, load, MTU, dependability, and expenses for communication (for a list of recommended metrics, check this study, for example) [21].

Multi-protocol networks must employ an external heuristic to choose between routes discovered using several routing protocols since a measure of routing is unique to a certain routing protocol, Routers from Cisco [22]. In certain circumstances, a regional network administrator can configure specific to the host routes to a specific machine, giving them greater authority over network traffic, enabling testing, and improving overall safety. When it is necessary to troubleshoot connections to networks or routing tables, this can be useful.

There seems to be an increase with interest in approaches and methods for tracking the connectivity posture of networking as the World Wide Web and IP networks have become essential business tools. Inadvertent performance deterioration, flapping, and/or downtime are brought on by incorrect router or routing problems. Using Route analytics techniques and equipment, routing in a network may be monitored.

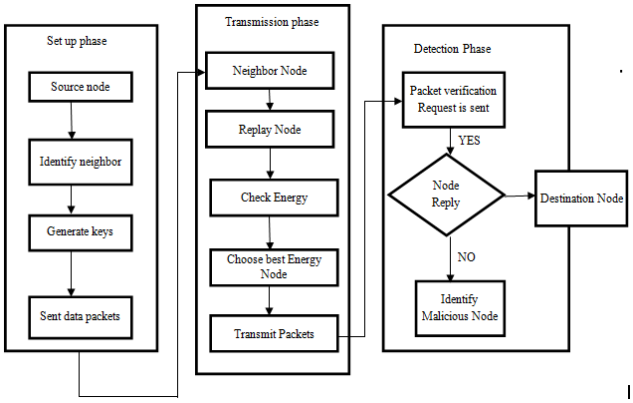

Fig. 2. System Architecture

3.7. Pseudo Code

Source "S" chooses a symmetric-key encryption system (encryptkey, decryptkey) и K keys that are symmetric key1,.., keyK in step 1, where encrypt key or decrypt key constitute the keyed methods of encryption and decryption operations, respectively.

Step 2: Assign Energy ("E") to each network node (N1, N2,....Nn).

Step 3: For j = 1,...,K, S safely transmits the decode key and an asymmetrical keyj to the node nj on PSD.

In step 4, S encodes key j using network n's public key before sending the encrypted text to the node.

In step 5, nj uses the private key it holds to unlock the text of the cipher in order to acquire keyj.

Source Node "S" moves into the packet transfer phase in step 6. PSD receives packets from S.

Step 7: PSD is designed so that it measures the amount of energy used to transmit packets for the neighborhood list.

Step 8: To transport data, a list of nearby nodes is established using the PSDE (Energy Effective Path for Sources and Destination) protocol.

Step 9: S determines ri = H1(Pi) and creates HLA signatures before sending a message to Pi, where i is an array number that distinguishes Pi.

The general population auditor Ad gets an ADR communication from S, which initiates step 10 of the audit process.

n1,..., nK, S's HLA public key data, pk = (v, g, u) contains the ADR notifications, the associated sequence numbers in most of M packets previously transmitted by S, and sequence data of some of these M messages received by D in step 11.

Step 12: The government auditor after getting and going over each node's response to its challenge on PSD, Ad moves into the detecting phase.

Step 13: Ad determines whether malicious activity is present by identifying any understatement of the loss of packets at each node, creating a packet-loss image for each hop, computing the function of self-correlation for the message loss for every hop, and creating a package-loss map for each hop.

3.8. Design and Analysis of Network model

Each hop across a PSD (Path to Sources and Destination) of the wifi channel is depicted as an erratic procedure that swings among positive and negative states. In the good nation, packets are successfully transferred, whereas in the bad the nation, packets are lost. It is believed that quasistatic networks, in which the path PSD is relatively stable across time, will produce wide-sense static (WSS) random connection error statistics for wireless channels. Since route interruption is the main cause of loss of packets in highly portable networks due to their rapidly changing structure, identifying malicious packets being dropped may not be a problem. In this instance, preventing rogue nodes from being detected is more important than preserving steady connectivity among nodes.

3.9. Independent auditor

In the system, there is a third-party auditor Ad. Ad is autonomous in a way that it is not connected to any PSD node and is unaware of any of the secrets (such as the encryption keys) that different PSD nodes may hold. An auditor is in charge of immediately identifying malicious nodes. In particular, it is expected that D informs S when D believes that the path is being attacked. Following notification of potential attacks, S sends Ad an attack-detection response (ADR) [23]. Ad wants to get specific data from the nodes along route PSD to help with its inquiry. Each of these nodes must respond to Ad's question in order to avoid being viewed as acting inappropriately. Truthful responses will be provided by normal nodes, but malevolent nodes illustrates in the Fig. 3.

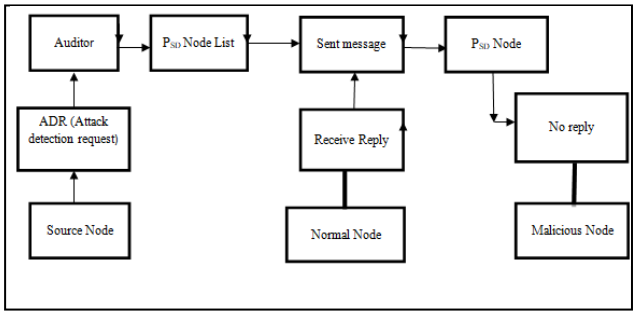

Fig. 3. Data Transmission Procedure

3.10. Setup Phase

S chooses an asymmetric-key crypto system (encryptkey, decryptkey) or K generates symmetric keys key1,..., keyK in this phase. Encryptkey and decryptkey are keyed both

encryption and decryption functions, etc. For j = 1,...,K, S securely delivers decryptkey and the symmetric keyj to every node nj on PSD. The public-key cryptosystem may serve as the foundation for key distribution: S encodes key j using node nj's public key before sending nj the cipher text. To obtain keyj, nj uses its encryption key to decrypt the encrypted text. Additionally, S broadcasts hash function H1 to all PSD nodes identified in the Fig. 4.

3.11. Packet Drop Detection

Finding connections between the missed packets along each pipeline step is the basis for the suggested strategy. Simulating hop-level packet loss as an unpredictable procedure that cycles between (0) (loss) and one (no loss) is the basic idea. Consider a communication stream M, for instance, which is transferred one after the other across a wireless channel. Distinctive drop patterns

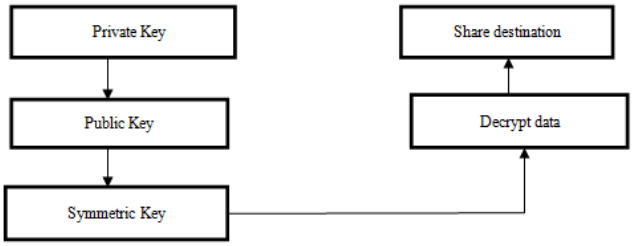

Fig. 4. Transmission and Reception Algorithm

and distinct packet drop events, such as malicious drops or link faults, will be seen as signs of random packet loss represented in the Fig. 5. When there was a connection problem, the information contained in the package drop may be low, but when an attacker's node sends packets of data, it will be high.

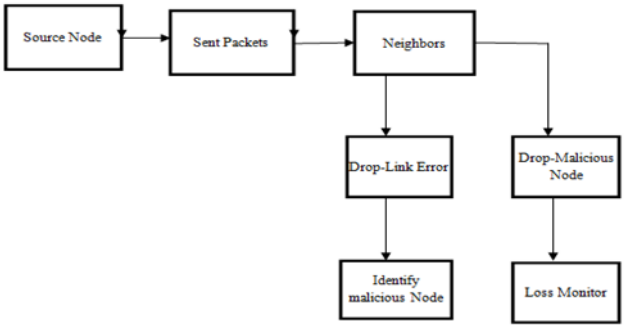

Fig. 5. Identification of Malicious Node

3.12. Energy based routing

Energy-based routing is implemented using the BFS (Breadth First Search) technique. The BFS checks each node within its immediate area after starting at a root node. Then, for each of the investigated neighbouring nodes, it inspects each on the unvisited neighbour nodes in consequently, and so forth. This makes it simpler to develop a path that concentrates on the destination and is realistic. The amount of energy required to transport packets can be decreased as a result.

4. Analysis of Routing Protocol

As a result, if there are numerous wormhole linkages existing, the capacity to resist the wormhole's attack will be diminished. We give a maximum limit on the amount of packet lost as a result of adversarial behaviour, that is, behaviour that lowers the success rate of packet transmission below a certain level.

Let q be the total amount of unsuccessful packet transmissions and q+ represent the overall amount of successful packet transmissions. The transmission n's success rate should ideally be a bit greater than the initial threshold, q q+ 0. This indicates that a small percentage of the transmitted packets are lost due to packet loss.

$$q^{-} - \rho . q^{+} \leq \emptyset \tag{1}$$

Assume there were N nodes and that k of them is hostile, with kN. The group of links that hostile nodes control is designated by the symbol E. E can grow as large as kN.

Think about a bad link e, who was ae times rehabilitated and je times convicted. Then, the weight of the network, we, is, no more than n, a where m is the maximum length of a network's nonfaulty path. A link is effectively driven out of a network if it reaches a weight of n since it is far more costly that any potential nonfaulty path. The algorithm gives us with the following formula:

$$w_e = 2^{\mathrm{je}-\mathrm{ae}} \tag{2}$$

The number of convictions is at least $q-/\mu$, so

$$\frac{q^{-}}{\mu} - \sum_{e \epsilon \bar{E}} j_e < 0 \tag{3}$$

Also, the number of rehabilitation operations is, at most, $q+ \mu/\rho$, so

$$\sum_{\mathrm{e}\epsilon\bar{\mathrm{E}}} \mathrm{a_e} - \frac{\mathrm{q}^{+}}{\mu/\rho} < 0 \tag{4}$$

Where μ is the number of lost packets that exposes a link as faulty. Thus

$$\frac{q^{-}}{\mu} - \frac{q^{+}}{\mu/\rho} \leq \sum_{e\ \bar{E}} (j_e - a_e) \tag{5}$$

From Eq. (2) we have $j_e - a_e = \log w_e$. Therefore,

$$\sum_{\mathrm{e}\epsilon\bar{\mathrm{E}}} (\mathrm{j_e} - a_e) = \sum_{e \epsilon \bar{E}} \log w_e \tag{6}$$

By combining Eqs. (5) and (6), we obtain

$$q^{-} - \rho . q^{+} \leq \mu \sum_{e \epsilon \bar{E}} \log w_e \leq \mu . \kappa N . \log n \tag{7}$$

And sinceμ = $b$log n, where b is the number of lost packets per window, Eq. (5) becomes

$$q^{-} - \rho . q^{+} \leq \mathrm{b} . \hbar \mathrm{N} . \log^{2} \mathrm{n} \qquad (8)$$

Therefore, the amount of disruption a dynamic adversary can cause to the network is bounded.

5. Results and Discussions

The average of each data point over all nodes with destinations and 30 distinct random environments is shown in the figures in this section. To produce paired statistics, AODV and Off Demand Secured Routing are mimicked in a comparable set of random situations. The biggest value of p for any collection, according to a paired t-test examination of all of our data, is 0.0093. Therefore, with a confidence level of above 97%, the reported performance variances between AODV and On Time Secure Forwarding are statistically significant.

We utilised using NS2 network simulator to put our protocol into practise. For symmetric encryptions, we assumed the protocol employs AES with 128-bit keys, hash-based message authorization code (HMAC), using SHA1 being the message verification code, and RSA with 1024-bit keys enabling digital signature operations and represented by the (Fig. 6-13).

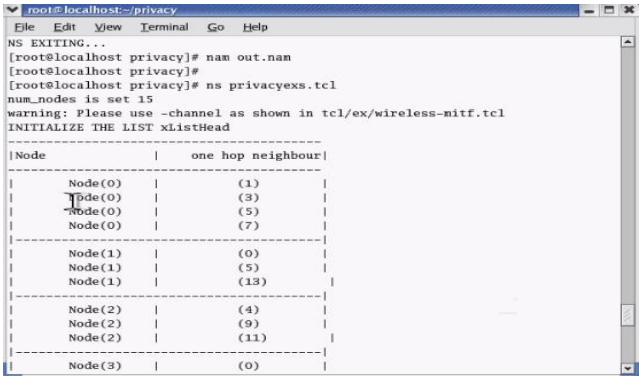

Fig. 6. Initialize the node list

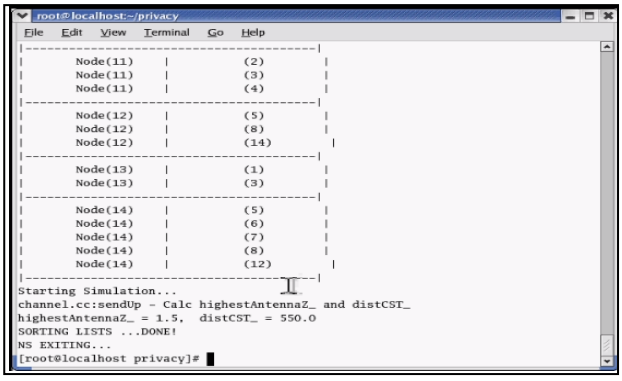

Fig. 7. Sorting List

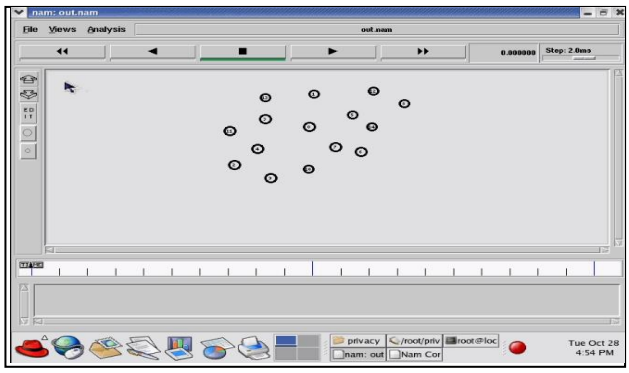

Fig. 8. Node Visualization

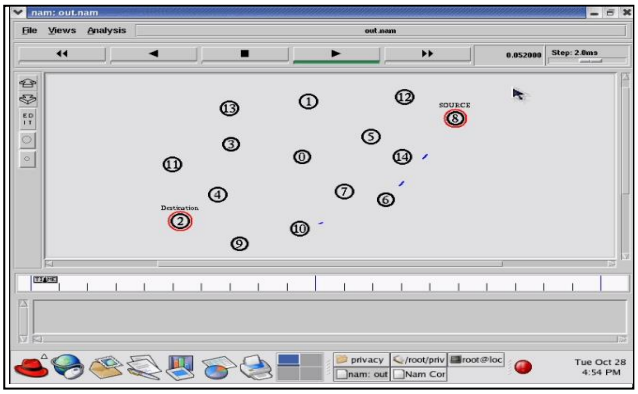

Fig. 9. Source node to destination node packets to send

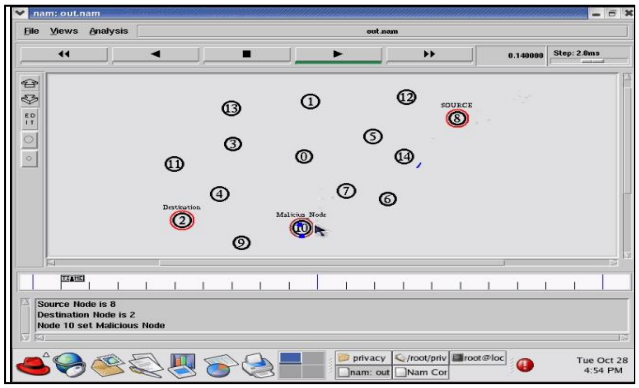

Fig. 10. Source node 8 destination node 2 node and malicious node identify (dos attack)

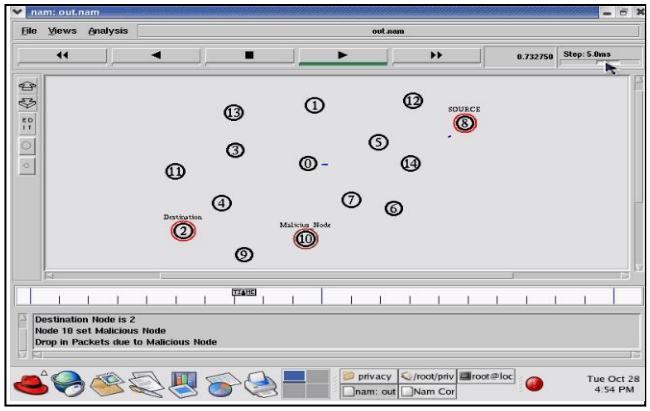

Fig. 11. Destination node is 2 node 10 malicious node drops in packets dues to malicious node (dos attack)

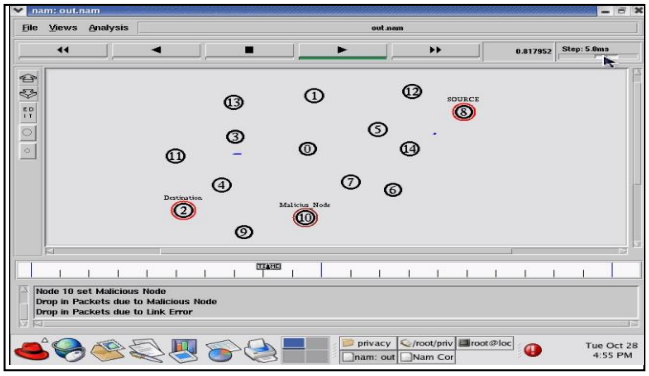

Fig. 12. Node 10 malicious node drop in packets dues to drop in packets

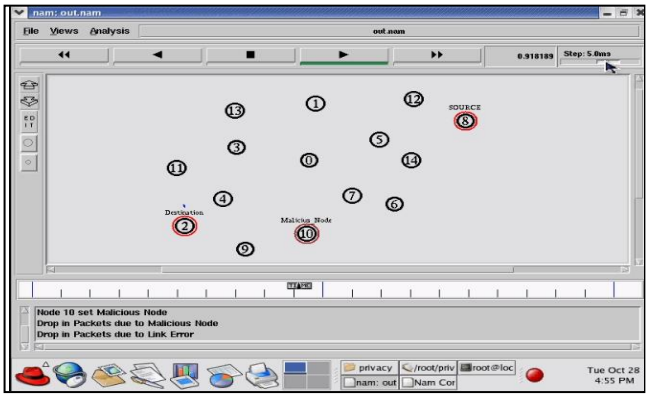

Fig. 13. Drop link error and malicious node

We used the NS2network simulator to run simulations. Fig.14 illustrates that the average packet drop ratio is decreased when it compares it with the existing methods. The network's nodes were set up to employ 802.11 radio with a 3 Mbps bandwidth and a 260 m nominal range. Within a 1000 square 1000m2 space, 50 nodes were distributed at random.

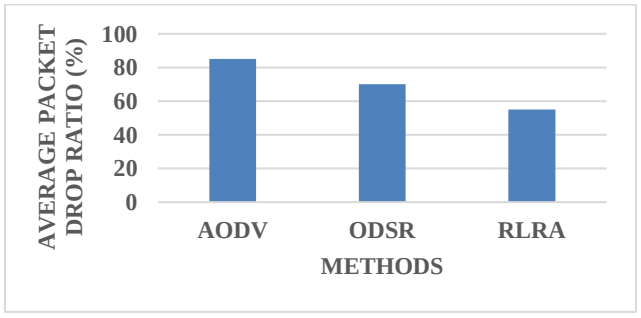

Fig. 14. Packet drop ratio in WSN

The nodal speed was changed from 0 to 12 m/s. Depending on the attack configuration under consideration; up to 10 hostile nodes were added into the simulation as well to these 50 nodes. The ad hoc network was modelled using traffic capacities of ten consistent bit rates (CBR) flows to simulate data transfers. The total load given to the network was 0.6 Mbps, with each flow sending 256-byte bits at a rate of about 4.9 packets per second.

We used a modified random waypoint migration model to overcome the problems with the traditional random waypoint model's applicability and improve the network life time and represented in Fig.15. Speed selections have a consistent distribution from 10% to 88 "maximum" speeds chosen in order to produce more steady mobility and guarantee that the average speed does not drastically drop over the course of the simulation Fig. 16 illustrates the packet delay ratio and Fig. 17 indicates the packet throughput comparison with the existing methods.

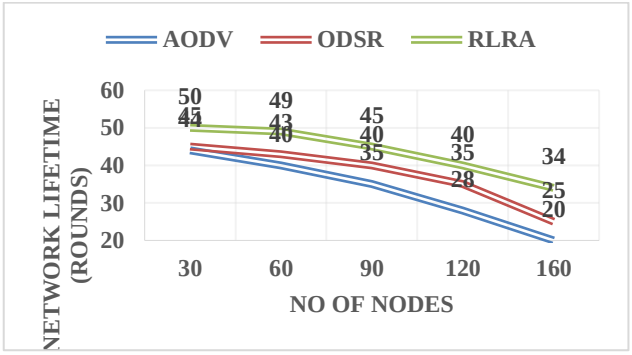

Fig. 15. Network lifetime in WSN

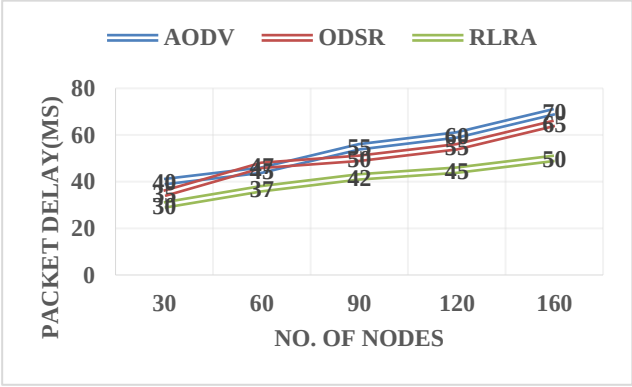

Fig. 16. Packet delay in WSN

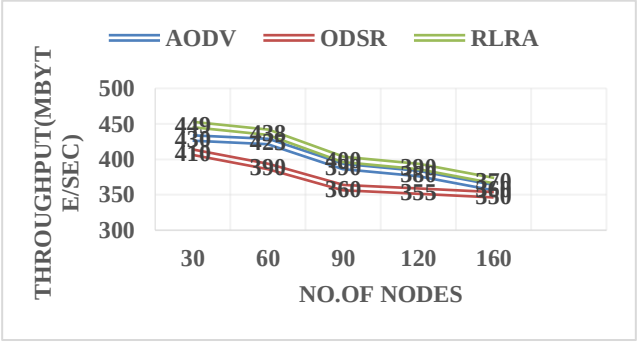

Fig. 17. Packet throughput in WSN

6. Conclusion

Utilizing the relationship between packets that went missing greatly enhances the accuracy in identifying malicious packets fall compared to conventional detection techniques, which merely use a calculation of the amount of lost packets. When quantities of transmitted malicious data are comparable to errors in links, such improvement

becomes especially evident. It is essential to gather accurate packet-loss information at each node in order to calculate the relationship between lost packets accurately. A public auditing system based on HLA was created to guarantee accurate packet-loss reports for each person nodes. At the base node, this anti-collusion design necessitates a large amount of processing power. In order to alter the detection accuracy for less computational complexity, a pack block-based strategy has also been suggested. This approach lowers the computational cost of creating the baseline.

References

[1] Liu, X., Abdelhakim, M., Krishnamurthy, P. and Tipper, D., 2018, May. Identifying malicious nodes in multihop IoT networks using diversity and unsupervised learning. In *2018 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

[2] Lai, Y., Tong, L., Liu, J., Wang, Y., Tang, T., Zhao, Z. and Qin, H., 2022. Identifying malicious nodes in wireless sensor networks based on correlation detection. *computers & security*, *113*, p.102540.

[3] J. N. Arauz. 802.11 Markov channel modeling. Ph.D. Dissertation, School of Information Science, University of Pittsburgh, 2004.

[4] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), pages 598–610, Oct. 2007.

[5] G. Ateniese, S. Kamara, and J. Katz. Proofs of storage from homomorphic identification protocols. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), 2009.

[6] Liu, L., Yang, J. and Meng, W., 2019. Detecting malicious nodes via gradient descent and support vector machine in Internet of Things. *Computers & Electrical Engineering*, *77*, pp.339-353.

[7] Khalid, N.A., Bai, Q. and Al-Anbuky, A., 2019. Adaptive trust-based routing protocol for large scale WSNs. *IEEE Access*, *7*, pp.143539-143549.

[8] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens. ODSBR: an on-demand secure byzantine resilient routing protocol for wireless ad hoc networks. ACM TISSEC, 10(4), 2008.

[9] K. Balakrishnan, J. Deng, and P. K. Varshney. TWOACK: preventing selfishness in mobile ad hoc networks. In Proceedings of the IEEE WCNC Conference, 2005.

[10] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. Journal of Cryptology, 17(4):297–319, Sept. 2004.

[11] S. Buchegger and J. Y. L. Boudec. Performance analysis of the confidant protocol (cooperation of nodes: fairness in dynamic ad-hoc networks). In Proceedings of the ACM MobiHoc Conference, 2002.

[12] L. Buttyan and J. P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. ACM/Kluwer Mobile Networks and Applications, 8(5):579–592, Oct. 2003.

[13] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring. Modelling incentives for collaboration in mobile ad hoc networks. In Proceedings of WiOpt, 2003.

[14] J. Avinash and N. Sudhakar, "Location and Quality of Service Guaranteed Optimized Routing In Wireless Sensor Network Environment," Journal of Advanced Research in Dynamical and Control Systems, Vol. 10, no. 11, pp. 295-306, Nov. 2018.

[15] Basi Reddy A., Liyaz P., Surendra Reddy B., Manoj Kumar K., Sathish K. (2019) Advanced Spatial Reutilization for Finding Ideal Path in Wireless Sensor Networks. In: Singh M., Gupta P., Tyagi V., Flusser J., Ören T., Kashyap R.(eds) Advances in Computing and Data Sciences. ICACDS 2019. Communications in Computer and Information Science, vol 1046. Springer, Singapore.

[16] J. Avinash and N. Sudhakar, "Interference Reduction Aware Optimal Route Path Establishment In Wireless Sensor Network Environment," International Journal of Engineering and Advanced Technology, Vol. 8, no. 5, pp. 642-648, June. 2019.

[17] Ch Muni Koteswara Rao, T N Siva Kumar J. Avinash, "Detection of Network Intrusion by using Supervised Machine Learning Technique with Feature Selection," International Conference on Advances in Science, Engineering and Technology, Vol. 6, no. 12, pp. 1-4 Dec. 2019, ISSN 2394-2320.

[18] J. Avinash and N. Sudhakar, "Route Breakage Concerned Non Interfering Multi Path Routing Protocol for Wireless Sensor Network Environment," International Journal of Advanced Science & Technology, Vol. 28, no. 13, pp. 38-48, Nov. 2019.

[19] Lolai, A., Wang, X., Hawbani, A., Dharejo, F.A., Qureshi, T., Farooq, M.U., Mujahid, M. and Babar, A.H., 2022. Reinforcement learning based on routing with infrastructure nodes for data dissemination in vehicular networks (RRIN). *Wireless Networks*, *28*(5), pp.2169-2184.

[20] R. Anderson and M. Kuhn, Tamper resistance û a

cautionary note, in: tiProceedings of the Second Usenix Workshop on Electronic Commerce, Oakland, CA (November 1996).

[21] J. Avinash, K. Geetanjali, and Ch. Bhaskar Rao, "Active direction finding for files integrity and interruption segregated services in wireless sensor networks," International Journal of Innovative Technology and Research, Vol. 5, Issue No. 2, pp. 5637-5641, Feb-Mar. 2017, ISSN 2320-5547.

[22] Srivastava, S. and Singh, J.P., 2021, October. Efficiency of Multi-Protocol LABEL Switching over Traditional Switching. In *2021 5th International Conference on Information Systems and Computer Networks (ISCON)* (pp. 1-4). IEEE.

[23] Çakmakçı, S.D., Hutschenreuter, H., Maeder, C. and Kemmerich, T., 2021, June. A framework for intelligent DDoS attack detection and response using SIEM and ontology. In *2021 IEEE International Conference on Communications Workshops (ICC Workshops)* (pp. 1-6). IEEE.