International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Enhancing Mobile Ad Hoc Network Security: A Study on Termite Colony Optimization for Wormhole Detection

Gurgeet Kaur Sandhu[1], Dr. Parveen Kakkar[2]
Research Scholar[1], Assistant Professor[2]
Department of Computer Science and Engineering, DAVIET Jalandhar, Punjab

Abstract: An ordinary, self-orbiting communication network with the ability to manage mobile nodes is called a mobile ad-hoc network (MANET). The vulnerability of the MANET to various threats and attacks is addressed by numerous proposed protocols. The malicious node takes advantage of these weaknesses to launch attacks, such as wormhole attacks, particularly when nodes are mobile and the network's topology is unstable. The termite method for detecting wormhole attacks in MANETs is presented in this research.

Keywords: MANET, Denial of service, Wormhole attack, Termite approach

I.INTRODUCTION

A group of wireless mobile nodes that connect with one another without the aid of network infrastructure make up a mobile ad hoc network (MANET) [1]. Because of their special qualities, MANETs are more susceptible to a wide range of assaults than other kinds of wireless networks [2]. Researchers address the defense against wormhole attacks in this study. A wormhole in a wormhole assault is made up of two malicious nodes that collaborate, also known as wormhole nodes, and a tunnel that connects them. These nodes are often located far apart. A specialized communication channel, like a tunnel, might be used for long-range wireless devices [3]. At one point in the network, a single wormhole node gathers routing traffic and tunnels it to a peer wormhole node at a different location. As a result, routing is compromised & the structure of the network is tainted. Wormhole attacks may be prevented by any

cryptographic method, since wormhole nodes do not require modification or creation of new packets.

Packets are encapsulated by a wormhole node (W_1) and sent along the path connecting them to a peer wormhole node (W_2). After that, a process known as decapsulation allows (W_2) to retrieve the original packets that were taken from the encapsulated packets. The original packets on the path between W_1 and W_2 are not altered by intermediary nodes because they are encapsulated. Therefore, despite the fact that they are typically several hops apart, it appears as though W 2 received the packets straight from W 1 with the same hop count [4]. As a result, wormhole-containing roads are probably shorter than other regular paths. Senders thus favor the path with wormhole nodes over other regular routes when selecting which to use for packet transmission.

The Termite technique can be applied in Mobile Ad-Hoc Networks (MANET) to identify wormhole attacks. The way termites in the wild identify and battle off threats as a group is the model for the termite system. When it comes to MANET security, Termite sets up virtual "termites" throughout the network to keep an eye on all node-to-node communication. These virtual termites look for unusual

activity suggestive of a wormhole attack by timing and sequencing communication exchanges. The system can identify the existence of a wormhole assault and notify the network nodes to take precautionary action by utilizing swarm intelligence and cooperation among virtual termites. By employing distributed monitoring and group decision-making to proactively detect and mitigate the threat of wormhole assaults, this strategy improves MANET security by imitating the effective defense mechanisms seen in nature.

The organization of the paper is as follows. Section II explains the literature review. Section III proposes an proposed work which implement the prevention of wormhole attacks. Section IV presents the results . Section V concludes the paper and presents our future works.

II.LITERATURE REVIEW

Pandey et al.,[5] The research framework is used to identify BHA in the MANET. In suggested work, presented the method for appropriate routing. The ANN and SVM are used in the existing contract. The MSE is one of the variables examined here. With the help of the ANN & SVM, the approach is consistent among the route that is fought as a black hole as well as the enhanced path. The advancement in energy usage along with the secure route is mentioned as 54.72 percent, as well as the throughput is increased by 84.42 kbps, PDR acquired is 75.93 percent, as well as the E to E delay is enhanced by 32.09 ms. All of the findings are given for a system with 100 nodes. The suggested routing framework is both reliable and effective. It is also useful for detecting black holes.

Elmahdi et al.,[6] suggested an improved AOMDV approach to split the message into multiple paths and use a homogeneous encryption method to make data transmission flexible & secure in the existence of malicious nodes in the MANET. Simulation outcomes demonstrated that the suggested method gives greater packet forwarding rate and higher throughput, which is a good feature for emergency MANET applications. Also, since there are many active routes in each group in the network, it guarantees targeted delivery of the suggested packet and has a very high probability of success.

Sbai et al.,[7] presented the computation outcomes of single and multiple black hole attacks in the AODV and OLSR approaches of the NS3.27 simulator. In this computation, we considered the model of network density, node speed, mobility, explained by the amount of nodes connected to the network, and even chose the IEEE 802.11ac protocol for the physical layer. Simulations covering more general and more realistic scenarios.PDR, routing overhead, throughput, and average end-to-end latency were chosen as performance metrics to formulate the effect of an attack on the network.

Nabendu Chaki et al., [8] covered the analysis of MANET's efficiency under wormhole attack. Among the QoS considerations are throughput, latency, packet delivery ratio, node energy, or density. This article evaluated different routing protocols and considers the possibility of wormhole attacks on such protocols. It provides information on a variety of wormhole attack detection and prevention techniques. The effect of node density and starting energy on throughput is examined using the NS2 network simulator and the reference point group mobility model (RPGM). The authors also thoroughly simulate the impact of the wormhole using the MANET AODV and DSR routing technologies. The study

focuses on how wormhole assaults affect a network's QoS. The study described here lays the framework for upcoming initiatives to build a system to identify nodes that are supporting this attack.

Saad Al-Ahmadi et al.,[9] suggested an energy-saving detecting technique, which was put into practice and verified in MATLAB to make sure it worked. The suggested technique used little energy while achieving a 77.6% detection rate.

Su et al.,[10] suggested the Wormhole Avoidance Routing Protocol (WARP), a secure routing protocol built on top of the AODV routing system. Hardware is not needed for it. In order to prevent malicious nodes, it provides more path selection options and takes into account link-disjoint multi-paths during path discovery; yet, in the end, it only employs one path to transfer data. Through WARP, the neighbors of wormhole nodes can learn that their neighbors have aberrant path attractions, based on the feature that wormhole nodes can easily grasp the route from source node to destination node. The wormhole nodes would then eventually be quarantined by the entire network after being gradually isolated by their regular surrounding nodes. However, because they are positioned in the network's most important connectivity hubs, some nodes can be mistakenly identified as wormhole nodes.

Shi et al.,[11] suggested a time-based defense against MANET wormhole assaults. Authors made the unreal assumption that the source node and the destination node are reliable , even if additional hardware or a synchronization scheme is not needed. The assumption does not exactly match the real situation, since MANET demand that every node in the network have the same security level. One of the primary enhancements in our suggested approach is that authors view the source and destination nodes as regular nodes without making any additional assumptions.

III.PROPOSED WORK

- **PROBLEM FORMULATION**

The authors were unable to concentrate on employing ad hoc networks in a sizable topological area, which offered wireless networks more flexibility and improved detection performance. We will also be able to overcome the energy consumption caused by the mobile node's limited energy source[18]. The need for more effective and precise detection algorithms to thwart complex assaults in dynamic and resource-constrained network environments is the research gap in hybrid wormhole attack detection in Mobile Ad-Hoc Networks (MANETs). Although previous studies have concentrated on identifying different kinds of attacks in MANETs, such as wormhole attacks, a hybrid strategy that blends several detection methods is comparatively unexplored.

The authors have relied on neighborhood ratio, round trip times and packet delivery ratio to detect the wormhole attack in the network. The drawback with first method can be related to random deployment scenarios, for instance, some portion of the network may have dense deployment as compared to other portions. This may lead to higher neighborhood ratios for the legitimate nodes as well which might increase the number of nodes in the checking list for the suspected wormholes. This will lead to more energy consumption in the network. As far as round trip times method is concerned, in the highly congested scenarios, the nodes usually experience delays in the packet transmission which may be bad for RTT kind of approaches.

Furthermore, the packet delivery ratio method can detect the malicious nodes but it will lead to loss of much more data before a node gets detected. Therefore, an alternate method is required which can work in highly congested as well as dense scenarios and also avoid loss of data while detecting the malicious nodes.

To overcome these drawbacks, following objectives have been laid out:

1. To study various techniques for wormhole attack detection in MANETs.

2. To detect wormhole attack using termite colony algorithm for a scenario of 50 nodes.

3. To evaluate the performance of the proposed method based on throughput, energy consumption, packet delivery ratio and end to end delay.

4. To compare the proposed method with existing schemes based on above parameters.

3.2 Research Methodology:

In order to detect the wormhole attack in these networks, this work proposes the use of termite colony to detect the wormhole attack. This works as:

- When the source node has some data to forward to destination node, it will check up its routing table for a valid route. When the route is not available, the source node creates a route request packet with ID of the destination. This request packet is forwarded to the neighboring nodes.
- All the neighboring nodes upon receiving the packet again checks their routing tables for address of the destination; the request packet is broadcasted again to the next hop neighbors in case the route to destination is not available. This process is repeated until the route to destination is found.
- At the destination node, the routes are created. The destination node replies back to source node over all the paths.
- At the source node, now the routes to destination are available. The source node normally selects the route having lowest hop count as it is considered to be the shortest one. In the presence of wormhole nodes, the route request is tunneled to the destination; the routes passing through such tunnel tend to have least hop count. The source node has very high probability of selecting such route.
- Therefore, in order to detect such routes the termite colony optimization will be used. As per this algorithm, the pheromone value for each hill computed and this value depends upon the fitness value of the hill. Applying this concept in this research work, the fitness value will be computed for every route created from source to destination node. This fitness value will depend upon received signal strength between two nodes. According to the fitness function, the pheromone value for each route will be computed.
- In the normal network having only legitimate nodes, the range of the nodes is 250 meters. Above this range, the nodes cannot communicate with each other. So, the pheromone computed according to the normal communication range of the nodes serve as the threshold value. In network with wormhole nodes, the pheromone value of the link created between two wormhole nodes will be very high as pheromone value is inversely proportional to the fitness function which in turn is directly proportional to received signal strength.

And in wormhole link due to longer length of tunnel, the RSSI will be less.

- When the pheromone value of every link will be compared with threshold value, the pheromone for the tunneled link will be very high and the wormhole pair will be detected.
- After detection, the source node will choose another route from the available list of the routes to forward data to destination node. This is how, out-of-band wormhole will be detected.
- For in-band wormhole attack, the malicious nodes route the data over the longer path. In such scenario, the average hop count for each of the path to destination will be considered as threshold value. The path with malicious nodes will have higher hop count and therefore will be avoided for the data transmission.

IV.RESULTS

This section presents the findings and discussions of the approaches for wormhole attack detection and prevention in MANETs that were covered. This section also discusses the outcomes and contrasts the current strategy with the suggested termite methodology for utilizing several QoS metrics like as energy consumption, packet delivery ratio, throughput, latency, and End to End delay for mobile adhoc networks. Random node deployment in a 100x100 area can have a big effect on the connectivity and performance of a Mobile Ad hoc Network (MANET). The network structure and connection in a MANET become unpredictable when nodes are randomly deployed. Problems include an unequal node distribution, possible coverage gaps, and a higher chance of interference might result from this randomness.

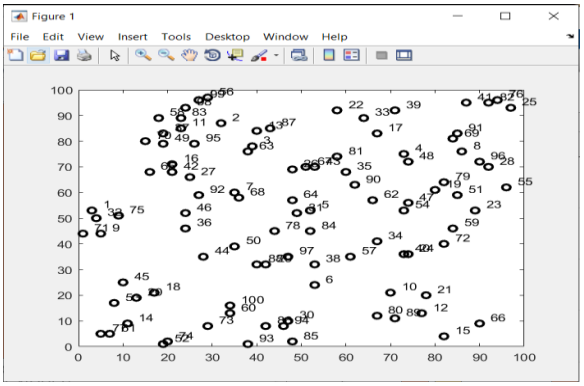

Figure 1: Random Deployment of Nodes

- **Packet Delivery Ratio:** It is defined as the ratio of Number of packets received to the number of packets sent in the network.

$$PDR = \frac{Total\ Packets\ Recieved}{Total\ Packets\ Sent * 100}$$

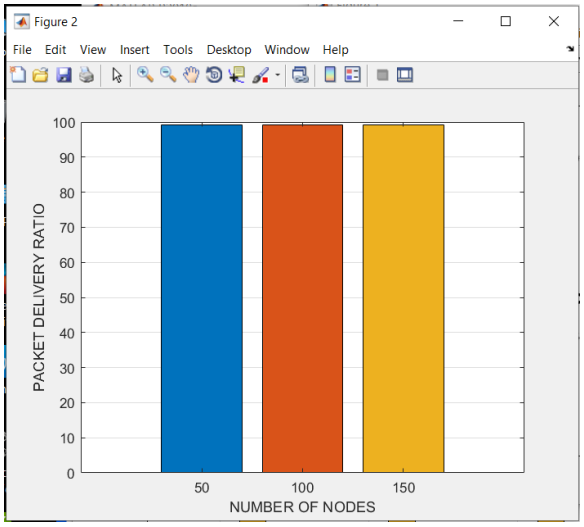

Figure 2:Packet Delivery Ratio

As seen in Figure 2, Speed increases cause the link to fail and cause packets to not arrive at their destination exactly. Although our PDR in the network is lower than the current approach, the fitness function makes it greater.

- **Delay:** It is the time taken by the packets to travel from source to destination node in the path.

- **End-to-End Delay** = $\sum_{i=1}^{n} \frac{Delayi - Delay\ i-1}{n-1}$

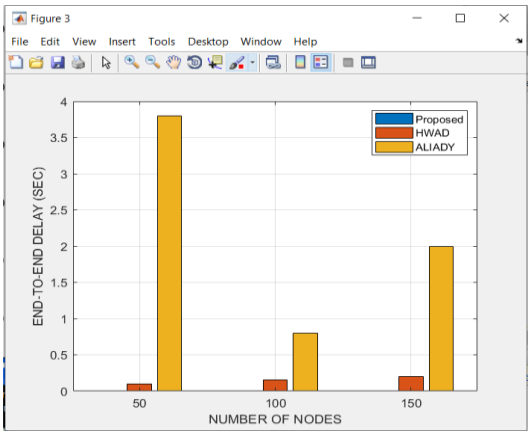

Figure 3:End To End Delay(Sec)

As we increased the speed in Fig. 3, the latency decreased even though there was a connection break that resulted in a delayed arrival of the data at the destination. Nevertheless, the delay should be shorter than using the current method. It is evident that the suggested strategy reaches its objective quickly.

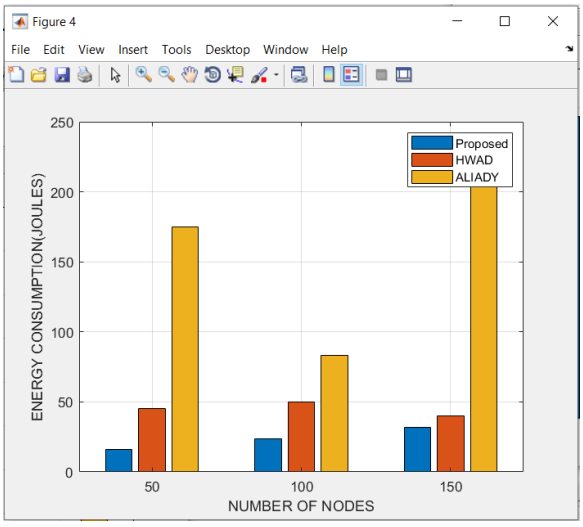

Figure 4:Energy Consumption(JOULES)

- **Throughput:** The throughput is generally defined as the amount of success data transmission in the network. The unit is Kbps. In this context, the following formula is used to calculate the throughput:

Throughput = Total Number of packets successfully transferred
Total Number of packets transferred

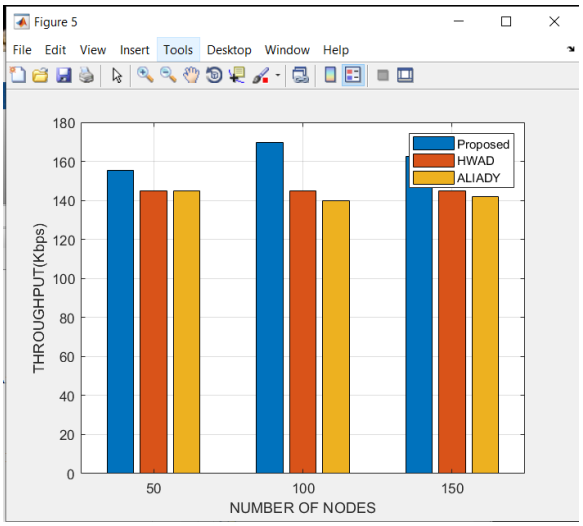

Figure 5:Throughput(Kbps)

Figure 5 illustrates how the link breaks and packets are not correctly delivered to their destination as speed increases. Our throughput drops as the speed rises, but it is still superior to the earlier approach.

Since nodes in a MANET move independently of one another and the link breaks when they do, the aforementioned testing showed that the proposed approach lowers time when compared to the current architecture. Packets take longer to get from the source to the destination when a link fails. Using the suggested scheme, we prioritize three characteristics while choosing a route: the node's energy, throughput, and delay. We also select nodes inside

the system that move slowly. Additionally, selecting slowly moving nodes reduces the likelihood of a link break while facilitating information transfer to the destination, making this approach better than the one currently in use.

V.CONCLUSION

In conclusion, a viable strategy for boosting network security is to use the Termite Colony Algorithm to identify wormhole attacks in Mobile Ad-Hoc Networks (MANET). The system can successfully monitor network behavior, detect suspicious patterns indicative of wormhole assaults, and promptly respond to possible threats by imitating the collective intelligence and collaborative nature of termites. The Termite Colony Algorithm's distributed architecture allows for real-time detection and reaction capabilities, strengthening MANET's defenses against hostile activity. All things considered, the Termite technique, which applies a metaheuristic approach, offers a strong and proactive defense mechanism to protect MANET against the damaging effects of wormhole attacks.

REFERENCES

[1]Isaac, J. T., Zeadally, S., & Cámara, J. S. (2010). Implementation and performance evaluation of a payment protocol for vehicular ad hoc networks. Journal of Electronic Commerce Research, 10(2), 209–233.

[2] Zhou, X., Ge, Y., Chen, X., Jing, Y., & Sun, W. (2012). A distributed cache based reliable service execution and recovery approach in MANETs. Journal of Convergence, 3(1), 5–12.

[3] Nagrath, P., & Gupta, B. (2011). Wormhole attacks in wireless ad hoc networks and their counter measurements: a survey. In 3rd international conference on electronics computer technology (pp. 245–250).

[4] Loukola, M. V., & Skyttä, J. O. (2001). Enhanced augmented IP routing protocol (EAIRP) in IPv6 environment. Journal of Electronic Commerce Research, 1(4), 359–370.

[5] Pandey, S., & Singh, V. (2020). Blackhole Attack Detection Using Machine Learning Approach on MANET. 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC).

[6] Elmahdi, E., Yoo, S.-M., & Sharshembiev, K. (2018). Securing data forwarding against blackhole attacks in mobile ad hoc networks. 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC).

[7] Sbai, O., & Elboukhari, M. (2018). Simulation of MANET's Single and Multiple Blackhole Attack with NS-3. 2018 IEEE 5th International Congress on Information Science and Technology (CiSt).

[8] Nabendu Chaki and Reshmi Maulik, " A Study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications, Volume 3, pp. 271-279,2011.

[9] Saad Al-Ahmadi; Wateen Aliady; Abdulmohssen AlRashedy, "An Efficient Wormhole Attack Detection Method in Wireless Sensor Networks", 26th International Conference on Circuits, Systems, Communications and Computers (CSCC),2022.

10.Su, M.-Y. (2009). WARP: a wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks. Journal of Computers & Security, 29(2), 208–224.

11.Shi, F., Jin, D., Liu, W., & Song, J.-S. (2011). Time-based detection and location of wormhole attacks in wireless ad hoc networks. In International joint conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11 (pp. 1721–1726).