International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 03 | March - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Termite-Based Approach for Wormhole Attack Detection in Mobile Ad-Hoc Networks (MANETs)

Gurvir Singh[1], Tajinder Kaur[2]

[1]Department of computer science engineering, Punjab Institute of Technology, GTB Garh (Moga), Punjab, INDIA
[2]Purana patti, Bagha purana (Moga) Punjab, INDIA

Abstract: Mobile ad-hoc networks (MANETs) are regular, self-orbiting communication networks that may control mobile nodes. Many protocols have been developed to alleviate the MANET's susceptibility to different risks & attacks. When nodes are mobile or the network architecture is unstable, the hostile node exploits these flaws to initiate assaults, including wormhole assaults. This study presents the termite approach for wormhole detection in MANETs.

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

I.INTRODUCTION

A mobile ad hoc network (MANET) is a collection of wireless mobile nodes that communicate with each other without the use of network infrastructure [1]. Compared to other types of wireless networks, MANETs are more vulnerable to a variety of attacks due to their unique characteristics [2]. In this article, researchers discuss how to defend against attacks via wormholes. Two cooperative malicious nodes, referred to as wormhole nodes, plus a tunnel connecting them comprise a wormhole in a wormhole attack. These nodes are frequently spread out widely. Distant wireless devices may require a dedicated communication route, such as a tunnel [3]. One wormhole node collects routing traffic at one point in the network & tunnels it to another peer wormhole node at a different location. As a result, the network's framework is distorted and routing is impaired. Any cryptographic technique can stop wormhole attacks since wormhole nodes don't need to be modified or new packets made.

A wormhole node (W1) encapsulates packets and sends them along the path that leads to a peer wormhole node (W2). The original packets that were extracted from the encapsulated packets can then be recovered by (W2) using a procedure called decapsulation. Because they are enclosed, the original packets on the path connecting W1 and W2 are not changed by intermediate nodes. As a result, it looks as though W2 received the packets directly from W1 with the same hop count, even though they are usually separated by a number of hops [4]. Wormhole-containing roadways are therefore most

likely shorter than other types of roads. Thus, while choosing which path to employ for packet transmission, senders choose the one with wormhole nodes over other conventional routes.

Mobile Ad-Hoc Networks (MANET) may detect wormhole attacks by using the Termite approach. The termite network is modeled after how termites in the natural recognize and fight off dangers collectively. Termite deploys virtual "termites" around the network to monitor all communication between nodes in order to provide MANET security. By timing and sequencing communication exchanges, these virtual termites search for anomalous activity that could indicate a wormhole attack. Mobile Ad-Hoc Networks (MANET) may detect wormhole attacks by using the Termite approach. The termite network is modeled after how termites in the natural recognize & fight off dangers collectively. Termite deploys virtual "termites" around the network to monitor all communication between nodes in order to provide MANET security. By timing & sequencing data transfers, these virtual termites search for unusual activity that could indicate a wormhole attack.

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] BHA in the MANET is found using the research framework. The approach for suitable routing was described in the proposed work. The current contract makes use of the ANN and SVM. Among the factors analyzed here is the MSE. The method matches between the upgraded path and the route that is treated as a black hole thanks to the assistance of ANN and SVM. Along with the secure route, the energy consumption has improved by 54.72 percent, the throughput has risen by 84.42 kbps, the PDR has improved by 75.93 percent, and the E to E delay has improved by 32.09 ms. All of the results are shown for a 100-node structure. The recommended routing architecture is dependable and efficient. It can also be used to find black holes.

Elmahdi et al.,[6] proposed a better AOMDV technique that uses a homogeneous encryption mechanism and divides the message into numerous pathways to make data transmission safe and adaptable even in the presence of hostile nodes in the MANET. The results of the simulation showed that the recommended approach provides faster throughput and a higher transmission rate, which is a useful feature for emergency MANET systems. Additionally, it ensures targeted delivery of the recommended packet and has a very high chance of success because each group in the system has a large number of active routes.

Sbai et al.,[7] displayed the results of calculations for both single and multiple black hole attacks using the NS3.27 simulator's AODV and OLSR techniques. The model of network density, node speed, and mobility—which are explained by the number of nodes linked to the network—were taken into account in this computation. The IEEE 802.11ac protocol was even selected for the physical layer. Simulations that address more realistic & general circumstances. To determine the impact of an attack on the network, metrics for performance such as PDR, routing overhead, throughput, and average end-to-end latency were selected.

Nabendu Chaki et al., [8] discussed the evaluation of MANET's effectiveness in the face of wormhole attacks. Throughput, latency, packet delivery ratio, node energy, and density are some of the factors that affect quality of service. This article examined different methods of routing and examined the potential for wormhole attacks against each. It offers details on various methods for identifying and avoiding wormhole attacks. The reference point group mobility model (RPGM) or Report Word the NS2 network simulator are used to investigate the impact of node density and initial energy on throughput. Using the MANET AODV and DSR routing methods, the authors also extensively model the wormhole's impact. The study concentrates on how wormhole attacks impact the quality of service (QoS) of a network. The research presented here establishes the foundation for future efforts to develop a system to detect nodes facilitating this attack.

Saad AL-Ahmadi et al.,[9] proposed an energy-saving detection method that was implemented and tested in MATLAB to ensure its effectiveness. The recommended method achieved a 77.6% detection rate with little energy use.

Su et al.,[10]proposed a safe routing protocol based on the AODV routing system called the Wormhole Avoidance Routing Protocol (WARP). It doesn't require hardware. Although it considers link-disjoint multi-paths during path discovery and offers additional path selection choices to prevent malicious nodes, it ultimately uses just one path to transport data. Given the fact that wormhole nodes can readily understand the path from source node to destination node, WARP enables the neighbors of wormhole nodes to discover if their neighbors have anomalous path inclinations. After being increasingly isolated by their normal surrounding nodes, the wormhole nodes would finally be placed under quarantine by the whole system. Yet, some nodes may be wrongly labeled as wormhole nodes due to their placement in the most significant connection hubs of the system.

Shi et al.,[11] proposed a time-based defense against attacks using MANET wormholes. Even if further hardware or a synchronization scheme is not required, the authors made the unrealistic assumption that the source and destination nodes are

dependable. Since MANET requires that all nodes in the network have the same level of security, the assumption does not precisely reflect what is actually happening. The fact that writers treat the source or destination nodes as ordinary nodes without making any extra assumptions is one of the main improvements in our proposed method.

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.

- **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.

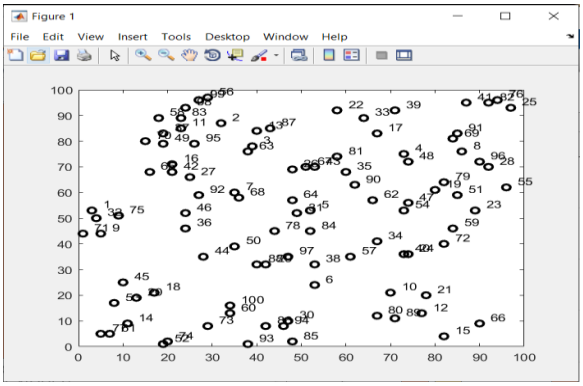

Figure 1: Random Deployment of Nodes

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

$$PDR = \frac{TotalPacketsRecieved}{TotalPacketsSent * 100}$$

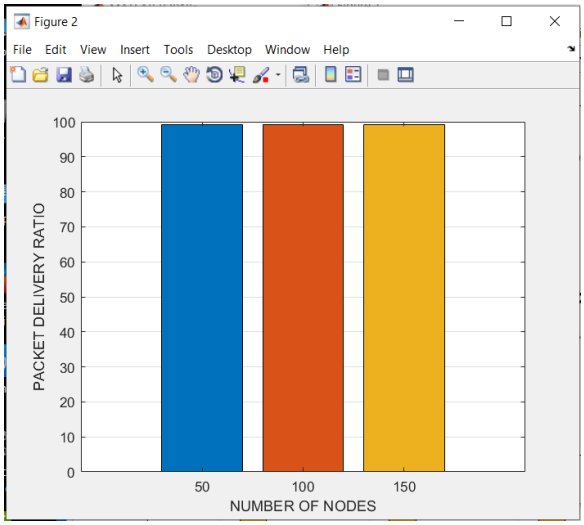

Figure 2: Packet Delivery Ratio

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

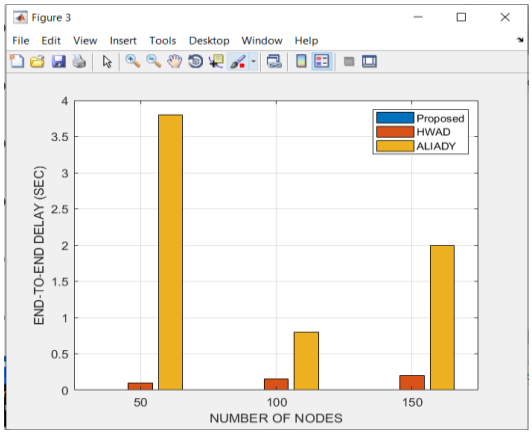

Figure 3: End To End Delay (Sec)

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.

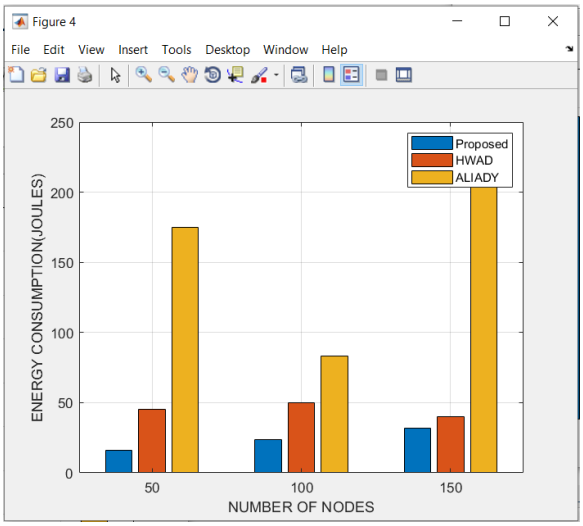

Figure 4:Energy Consumption(JOULES)

- **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

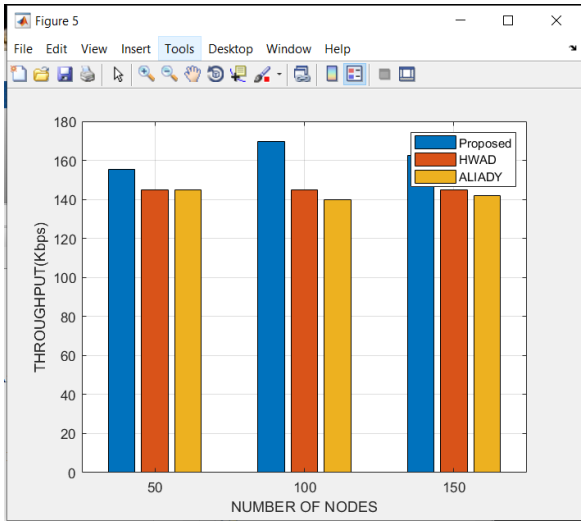

Figure 5: Throughput (Kbps)

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, employing the Termite Colony Method to detect wormhole attacks in Mobile Ad-Hoc Networks (MANET) is a workable method for improving network security. By mimicking termites' collective intelligence and cooperative nature, the system is able to effectively monitor network activities, identify unusual trends suggestive of wormhole attacks, and react quickly to potential threats. The distributed design of the Termite Colony Equation enhances MANET's defenses against hostile activity by enabling real-time detection & reaction abilities. All things considered, the metaheuristic Termite strategy provides a robust and proactive defense mechanism to shield MANET from the destructive consequences 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; AbdulmohssenAlRashedy, "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).