Journal of Advanced Zoology

ISSN: 0253-7214

*Volume **44** Issue **I-3 Year 2023** Page **627:634***

AN IMPROVEMENT OF NETWORK SECURITY IN MOBILE AD HOC NETWORKS USING NOVEL THREAT DETECTION AND MITIGATION TECHNIQUES

[1]Mrs.M.Kundalakesi, [2]Dr.M.Renuka Devi

[1]Research Scholar, Assistant professor, [2]HOD & Associate Professor

[1,2] Department of Computer Applications

[1, 2]Sri Krishna Arts and Science College, Coimbatore

[1]kundalakesim@skasc.ac.in, [2]renukadevim@skasc.ac.in

Article History

Received: 08July2023

Revised: 29 Aug 2023

Accepted: 02 Oct 2023

ABSTRACT

MANETs are important as intermediary routers, yet they are an infrastructure-free communication network that falls under autonomous devices. There are two types of MANET routing protocols: proactive and reactive. Proactive routing protocols are known as OLSR, whereas reactive routing methods are known as AODV [1] and DSR [2]. Compared to proactive OLSR [3,], reactive AODV and DSR are more efficient and scalable due to their reduced routing expense.

AODV and DSR were designed with the assumption that all nodes should trust each other and that there should be no malicious spying between nodes in the network. As a result, the existence of any node poses security difficulties. Also, bandwidth is vital in network communication because wireless links are considerably better than wired links. Noise, interference from other signals, and fading could all damage wireless link communications.

Keywords: AODV, DSR, OLSR, MANET, Protocols

I. INTRODUCTION

A central infrastructure governs wireless communication networks. If absent, it's an Ad hoc Network. Mobile nodes communicate via a Mobile Ad hoc Network (MANET), part of a Wireless Ad hoc Network.

In MANET, nodes work alone. No main node to help. They help each other to send data. If the sender and receiver are far, nodes connect them. Rewrite with simple words and short sentences.

As a result of dynamic changes, node mobility reaches 00 topologies. MANET routing protocols will be designed to adapt to dynamic topology changes [1].

Energy is a crucial component for connectivity in MANET. This means that each node has a fixed small amount of energy. The work should be carried out using effective mechanisms and protocols to avoid wasting energy because MANET nodes are only connected via wireless links. As a result, bandwidth is critical in network connectivity because wireless links are far superior to wired links. Noise, interference from other signals, and fading could all affect wireless link signals [2].

MANET can be attacked easily. A spying threat is possible because the nodes in MANET use wireless links. An unwanted user can see or change the data. MANET has no main network to help nodes talk to each other. The nodes work alone to send data to the end node. So, the bad attacker can break the link or drop the data.

DoS attacks hurt MANETs. A bad node uses another node's energy by asking for data. There are two types of

attacks. Bad nodes change or stop data or kill the battery in one type. In another type, bad nodes hear connections but do nothing. Rewrite with simple words and short sentences.

II. RELATED WORK

New trap ways use node names. A trap ask goes to near nodes with SSN and source name. The source node sees answers for a DSN more than its SSN. This means the answer is from a bad hole because no node should have more DSN than the source node's SSN.

When a black hole is found in a network, the source tells nearby nodes. The smart black hole node can check and ignore requests from the same source. It also sends false alarms to isolate some nodes from the network.

The CBDS method has three parts: bait, reverse trace and reactive defence. In the bait phase, the source node sends a bit request to a random neighbour. In the reverse trace phase, a list of suspicious nodes is made from the RREP of RREQ bait. Nearby nodes check for attacker nodes
A new system uses a fake ID to bait black hole nodes. The source node sends a bait request with an offline ID. The black hole node responds to the bait. The system modifies RREQ and RREP titles to find the black hole node. When found, a warning is sent to nearby nodes. The source node monitors for drops before restarting baiting. This increases control packet size and overhead.

The model in [12] floods the network with fake requests. Any response is suspicious. Nearby nodes find black hole nodes. The model has a location system for military use. The limitation is network congestion from fake requests.

The system in [13] uses guard nodes to find black hole nodes. Guard nodes check other nodes' behaviour. They record behaviours in tables. Each node has a trust value based on behaviour. It decreases if the node only sends RREP without RREQ

If a node's trust value is low, it gets blocked. Guard nodes send an alarm if they detect a black hole. This needs many guard nodes and has a high overhead. In [14], the model depends on the validation component in RREP. The attacker node cannot send RREP if it does not have minimum authentication [12]. The source node checks the validity bit in RREP before processing it.

III. TYPES OF ATTACKS IN MANET

Security is one of the most significant challenges in ad-hoc wireless networks [9,10]. The first step in improving good security solutions is always to learn all of the possible features of an attack. The security of the MANET connection is required to ensure the transmission of all required details. Internal, external, active, and passive attacks are the most common types of MANET attacks. These classifications are critical because an attacker can cause damage to the network at any time, whether it is internal, external, or active or passive.

External Attack: External attacks come from outsiders. They send fake info to break the network.

Internal Attack: An internal attack is when a new node in a network does something bad. It pretends to be a good node but gains illegal access

Passive Attack: In passive attacks, attackers listen and track info exchanged between two nodes. This way they can find details about the network for hijacking or injecting an attack. They don't change the message. Passive attacks are harder to detect than active attacks.

Active Attack: In an active attack, the attacker changes or adds data to harm the network. The attacker can change, add or remove data to carry out the attack. This can cause problems for the network.

Wormhole Attack: In a wormhole attack, the attacker captures packets at one point in the network and sends them to another point. This can disrupt routing. The wormhole is the tunnel between the two points

Denial of Service attack: This attack sends many unwanted packets to a server to slow it down. This makes resources unavailable to users. The attacker uses radio jamming and drains the battery

Impersonation: If verification is not done right, a bad node pretends to be real. It can see network data and send fake routing packets. It may also get secret information.

Routing Attacks: Because routing is the most critical service in a MANET, a hostile node attacked it [14]. This routing assault consists of two bites. The first assault targets the routing protocol, while the second targets the packet transport or delivery technique. The first is designed to prevent the routing information from spreading to the node. The second is designed to disrupt packet delivery against the previously established approach. Rewrite with less frequent vocabulary, replacing long sentences with short and bare minimum words

Black hole Attack: The attacker sends false information about having the best route. This makes nearby nodes send packets to it. The attacker is a rogue node that tricks good nodes into using it to route data.

A bad node stops all packets but still gets them. It does not send them on. The attacker listens for requests using a flood-based method

Replay Attack: The replay attacker keeps sending real data to put in old network traffic. These attacks often go after the route's uniqueness. They are used to getting around weak security.

Jamming: During jamming, the attacker checks the wireless channel to find the frequency of the sender's signal. The signal is then sent to that frequency. This blocks the right receiver

Man-in-the-middle attack: A network attacker gets between the sender and receiver and sees all details sent between them. Sometimes the attacker pretends to be the sender or receiver.
Received message. A network attacker gets between the sender and receiver and sees all details sent between them. Sometimes the attacker pretends to be the sender or receiver.

IV. PROPOSED METHOD

The MOMM technique helps improve service quality in mobile ad hoc networks by detecting and stopping many attacks. The Traffic-Register Task makes a record of traffic. The traffic Route sequence is made of node names to show the path in the traffic pattern.

We take a picture of the network at different times. We find out if there are any holes in the network. The picture below shows what we do.

- Traffic-Register Task
- Traffic Changeover Task
- time abnormal snapshot Task

- sinkhole attack detection
- routing attack detection
- DoS attack detection

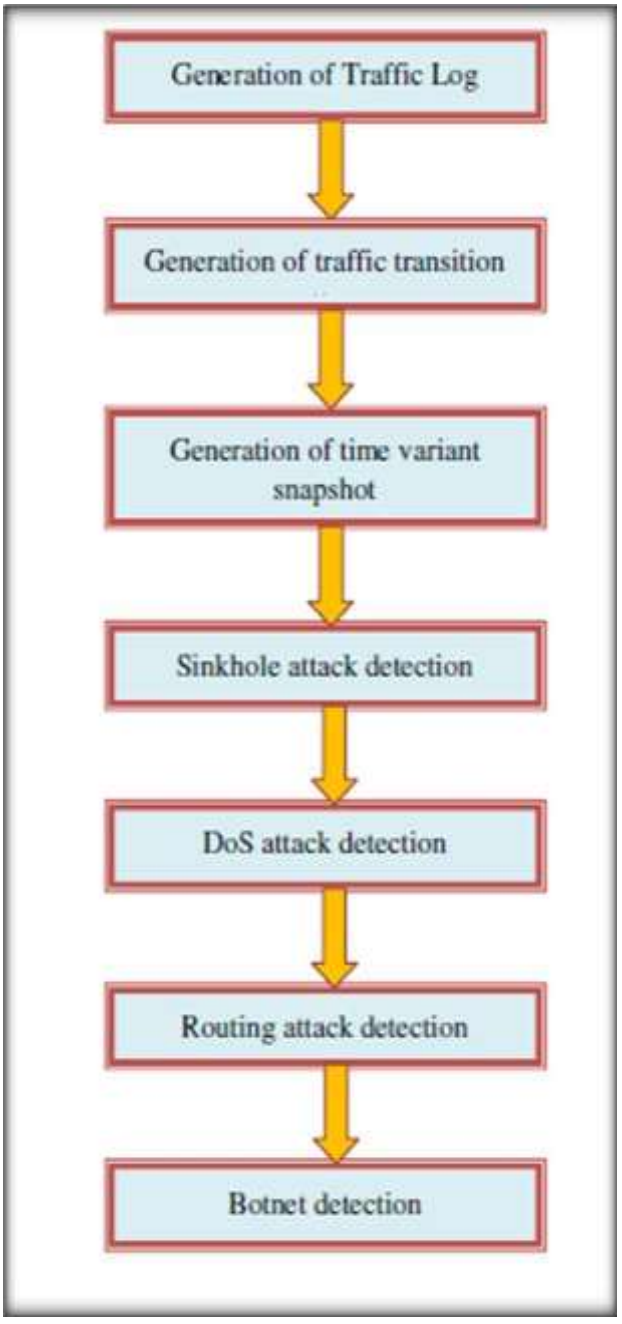


Figure 1. Process flow of Proposed Method

Traffic-Register Task

The method says the node gives the packet to the end through some neighbours and puts its address in the packet's field. The system gets the field and finds the nodes in the path logs to the database. The register keeps packet data like Source Address (SA), time got, and Destination Address.

Traffic Changeover Task

The job uses the node's log. The node sees traffic patterns and adds a new pattern to the database each time. The log file has data on packets got before. The method makes the log each time by cutting it from the log trail. The time-based pattern will be made using the log trail.

Time Abnormal Snapshot Task

We see how the network looks at different times. We make a picture and write down the paths and neighbours of each node[10]. Then we check if there are any holes in the network. We compare the traffic with the old one. We find out which nodes are not working well.

Sinkhole Attack prediction

The route table Rt is used to find the possible routes for these nodes. The length of the route in the pattern is determined based on the identified routes and the route from the transition path. There is a sinkhole in the trail if the journey is longer. A control message will be issued to all nodes to avoid a sinkhole caused by packet transmission.

DoS Prediction

The DoS attack detection is carried out using the created traffic pattern. The node generates the traffic pattern and computes the traffic status at the current time window whenever a packet is received.

Routing Attack prediction

The time-variant snapshot approach is used to detect routing attacks. This method returns a list of all possible network routes to the node. This approach calculates the distance and traffic rate for each route.

V. PERFORMANCE METRICS

The proposed method's performance is examined using a simulator. The following parameters, such as Packet Deliver, End to End Deliver, and Throughput Ratio, are utilized to estimate the performance of the proposed technique.

Packet Delivery Ratio

The PDR is calculated by dividing the total number of data packets received at destinations by the total number of data packets supplied from sources. Packet Delivery Ratio= $\frac{\sum \text{Total packets received by all destination node)}}{\Sigma(\text{ Total packets send by all source node})}$ -□(1)

End-to-end delay

Average E2E delay is when a packet goes through the network from a start to an end[7]. The average end-to-end delay can be found by getting the mean of E2E delay of all messages that got there. So, end–to-E2E delay partly depends on the packet delivery ratio.

* 1000 [ms] □2 $D = \frac{1}{n}\sum_{i=1}^{n} (\text{Tri - Tsi})$

Where,
D = Average E2E Delay i = packet identifier
Tri = Reception time Tsi = Send time
n = Number of packets successfully delivered
Throughput Ratio
TIL is how long the time is. It is how many packets go in a time. It uses packets per TIL. It can be like equation (v).

Average Throughput $= \frac{(recvdSize}{(stopTime-startTime)}))*(8/1000)$ (3) Where, recvd Size = Store received packet's size stop Time = Simulation stop time start Time = Simulation start time

VI. RESULT AND DISCUSSION

PDR shows how good the network is. In this case, nodes change from 25 to 150. Figure 2 shows how more nodes make PDR change. AODV with the attack has PDR go down by 5% when nodes go from 25 to 150. MOMM, with the attack, has PDR go down by 1.5% only.

Figure 2. Comparison of Packet Delivery Ratio

Figure 3 indicates throughput of all schemes decreases marginally when the number of nodes increases. The proposed approach achieved a throughput of 1700kbps, an improvement over he700kbps in an attacked situation.

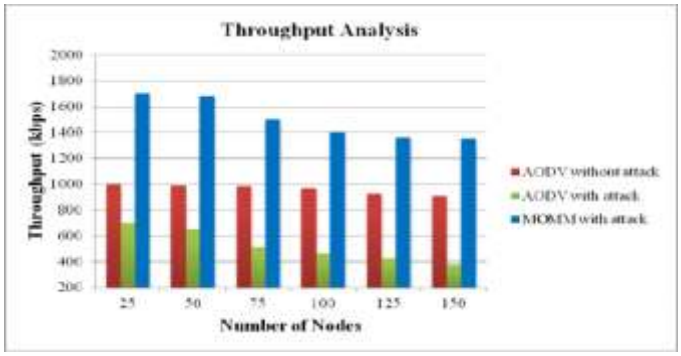


Figure 3 Comparison of Throughput Ratio

Figure 4 shows AODV with the attack has a high delay. MOMM with the attack has less delay by 0.8 seconds than AODV under attack.

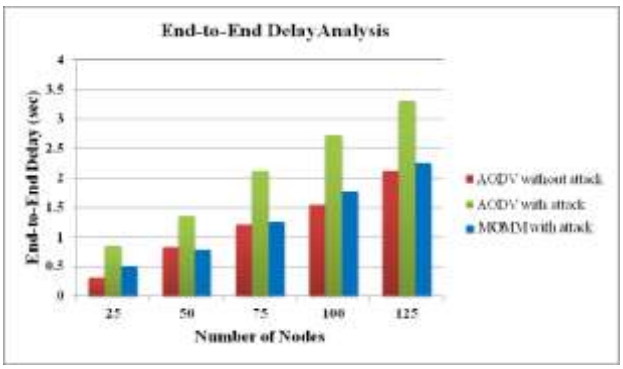
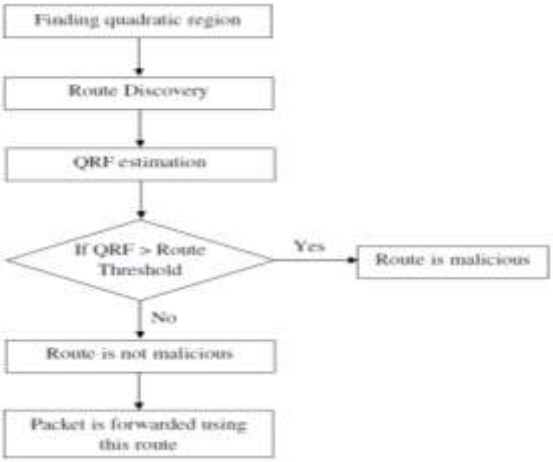


Figure 4 Comparison of End to End Delay

VII. QUADRILATERAL ROUTE FACTOR ESTIMATION (QRFE)

To detect assaults, the QRF approach employs four phases: discovering the quadratic region, route discovery, QRF estimate, and routing attack detection. Quadrilateral Route Factor estimate algorithms keep track of route details and network information at each time frame based on distinct quarters of the geographical network region. This approach divides the entire network into four quadrants and stores a time-based snapshot and route data for each quadrant.



VIII. TRUSTWORTHY ROUTE BY USING ROUTE INFERENCE THEORY (RIT)

MOMM and QRFE attack detection systems handled these attacks without taking traffic flow into account. .

Some systems stop attacks but ignore traffic. This paper uses route inference theory to stop attacks and consider traffic. It uses route, flow and sink inference to protect MANET. It has a new way to find and stop attacks[9]. It studies three ways to find attacks on AODV routing. It has a multi-optional way to stop attacks. It uses traffic patterns from the traffic log of the node. The system works well with packet delivery ratio, throughput, collision rate and end-to-end delay. The test results show that the system finds attacks well with a packet delivery ratio of 96.5%, throughput of 1700kbps and end-to-end delay of 0.34 seconds.

IX. CONCLUSION

The network traffic pattern and time-variant snapshot are utilized in this approach to detect and mitigate various threats. The model's efficiency is evaluated using various performance indicators for AODV with the attack, AODV without attack, and MVMM with the attack. Compared to AODV with the attack, MVMM improves

packet delivery ratio to 96.5% and throughput by 1000kbps. Furthermore, it reduces control overhead by 17000 packets, collision rate by 6.64%, and end-to-end delay by 0.51 seconds. The simulation findings suggest that the MVMM model performs better under attack than the AODV model.

REFERENCES

[1] S. Mirza and S. Z. Bakshi, "Introduction to MANET," International Research Journal of Engineering and Technology, vol. 5, no. 1, pp. 17–20, 2018.
[2] V. Goyal and G. Arora, "Review paper on security issues in mobile ad-hoc networks," International Research Journal of Advanced Engineering and Science, vol. 2, no. 1, pp. 203–207, 2017.
[3] M. M. Alani, "MANET security: A survey," in Proceedings of the 2014 IEEE International Conference on Control System, Computing and Engineering (ICCSCE), pp. 559–564, Penang, Malaysia, November 2014.
[4] A. Joshi, "A review paper on black hole attack in MANET," International Journal of Advance Research in Computer Science and Management Studies, vol. 4, no. 5, pp. 16–21, 2016.
[5] A. K. S. Ali and U. V. Kulkarni, "Comparing and analyzing reactive routing protocols (aodv, dsr and tora) in QoS of manet," in Proceedings of the 7th IEEE International Advanced Computing Conference, IACC 2017, pp. 345–348, Hyderabad, India, January 2017.
[6] L. Prashar and R. K. Kapur, "Performance analysis of routing protocols under different types of attacks in MANETs," in Proceedings of the 5th International Conference on Reliability, Infocom Technologies and Optimization, ICRITO 2016, pp. 405– 408, Noida, India, September 2016.
[7] H. Moudni, M. Er-Rouidi, H. Mouncif, and B. El Hadadi, "Performance analysis of AODV routing protocol in MANET under the influence of routing attacks," in Proceedings of the 2nd International Conference on Electrical and Information Technologies, ICEIT 2016, pp. 536–542, Tangiers, Morocco, May 2016.
[8] N. Kalia and H. Sharma, "Detection of Multiple Black hole nodes attack in MANET by modifying AODV protocol," International Journal on Computer Science and Engineering, vol. 8, no. 5, pp. 160–174, 2016.
[9] P. L. Chelani and S. T. Bagde, "Detecting collaborative attacks by malicious nodes in MANET: An improved bait detection scheme," in Proceedings of the 2016 International Conference on Communication and Electronics Systems, ICCES 2016, Coimbatore, India, October 2016.
[10] M. Sathya and M. Priyadharshini, "Detection and removal of black hole attack in mobile ad-hoc networks using cooperative bait detection method scheme," International Journal of Scientifc& Engineering Research, vol. 7, no. 3, pp. 81–85, 2016.
[11] P.-C. Tsou, J.-M. Chang, Y.-H. Lin, H.-C. Chao, and J.-L. Chen, "Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs," in Proceedings of the 13th International Conference on Advanced Communication Technology: Smart Service Innovation through Mobile Interactivity, ICACT 2011, pp. 755–760, Seoul, Republic of Korea, February 2011.
[12] B. Singh, D. Srikanth, and C. R. S. Kumar, "Mitigating effects of black hole attack in mobile Ad-Hoc NETworks: Military perspective," in Proceedings of the 2nd IEEE International Conference on Engineering and Technology, ICETECH 2016, pp. 810– 814, Coimbatore, India, March 2016.
[13] A. R. Rajeswari, K. Kulothungan, and A. Kannan, "GNBAODV: guard node based –aodv to mitigate black hole attack in MANET," International Journal of Scientific Research in Science, Engineering and Technology, vol. 2, no. 6, pp. 671–677, 2016.
[14] S. R. Deshmukh, P. N. Chatur, and N. B. Bhople, "AODVBased secure routing against blackhole attack in MANET," in Proceedings of the 1st IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2016, pp. 1960–1964, Bangalore, India, May 2016.