Vol. 05, No. 4 (2023) 693-700, doi: 10.24874/PES05.04.011

Proceedings on Engineering Sciences

www.pesjournal.net

A MODIFIED AODV PROTOCOL TO MITIGATE COMBINED IMPACT OF MULTIPLE ATTACKS IN MANET

Ms Monika Dangore[1]
Dr Hare Ram Sah

Received 21.04.2023.
Accepted 06.09.2023.
UDC – 004.056.5

Keywords:

MANET, AODV Protocol, Security Threats, Grayhole, Wormhole.

ABSTRACT

Since past two decades MANET researchers have focused on providing security solution to MANET to protect them from various network attacks. Most of the recent security approaches are restricted to address specific attacks only. This makes them obsolete when a different attack is introduced in the network. The objective of this research work is to offer a comprehensive solution to protect MANET from different security threats. We have proposed Multiple Attacks Protected Ad-hoc On-demand Distance Vector (MAP-AODV) Routing Protocol. It provides a consolidated approach to address different security threats in the network with the lowest computational overhead. The Node Behavior Score (NBS) module of the proposed protocol performs precise detection of the attack whereas Node Reliability Analysis (NRA) module achieves attack mitigation and reliable route formation. The efficiency of the proposed protocol is tested in the simultaneous presence of grayhole and wormhole nodes using NS2 simulation and compared against two existing protocols. The simulation results show better performance of the proposed protocol against different attack types.

1. INTRODUCTION

MANET is an infrastructure less network which means that the inter node communication is not governed by a central access point. The nodes are equipped with a wireless transmitter and receiver which allows communication with the nodes in the communication range and multi hop communication with the nodes which are outside the range. The nodes in MANET are mobile and act as both hosts and routers. MANET can function as a standalone network or can be connected to external networks (Abdel-Fattah et al., 2019). The original purpose of designing MANET was to support military and disaster management operations but in recent years MANETs have evolved from special-purpose to general-purpose application networks. MANET supports a wide variety of applications ranging from inter-vehicle communications to multimedia file sharing. Dynamically changing topology, limited bandwidth, limited battery power, absence of central access point are the main limitations of MANET which makes routing a challenging task (Karthigha et al., 2020). Routing is one of the most vital operations of mobile adhoc network. The routing protocol used by the system governs the Quality of Service (QoS) performance of the network. The routing protocols in MANET don't have inbuilt security provisions. Due to mobility, congestion, security attacks, etc, MANET's

[1] Corresponding author: Monika Dangore
Email: monikaresearch2020@gmail.com

Quality of Service is ruined at the routing layer. Since past two decades, MANET researchers have put their focus on providing security services to MANET. MANET is susceptible to various types attacks such as sybil attacks, grey hole attacks, black hole attacks, sleep deprivation attacks, wormhole attacks, sink hole attacks, etc. A range of security procedures have been developed at the routing layer for protecting MANETs from security attacks. However, no methodology is fully adequate and each one has limitations. In most of the cases it is observed that the security method is targeting one or two types of attacks. Such method becomes obsolete once a different type of attack enters the network. The key challenge is to develop an effective and a generalized solution that will guard the MANETs from different kinds of attacks that may occur concurrently. Here we propose the innovative Multiple Attacks Protected Ad-hoc On-demand Distance Vector (MAP-AODV) Protocol to offer an efficient approach for multiple attacks detection and mitigation in MANETs. We modified the existing AODV protocol (Saini & Sharma, 2020) with the proposed security procedures and tested the efficiency of the proposed protocol for simultaneous presence of grayhole and wormhole attacks. During the development of the proposed trust-based methodology, we successfully achieved lowest computational requirements, higher detection accuracy and security against multiple types of the attacks.

2. OVERVIEW OF GRAYHOLE AND WORMHOLE ATTACKS

We have tested our generalised trust-based solution against following two most frequently occurring attacks in MANET:

2.1 Grayhole Attack

A grayhole node (Kumar et al., 2017) normally takes part in the route discovery process. It may have a valid route to the destination. Many times it shows a normal behaviour during data transfer and directs data packets to intended destination. For a certain period of time it may show mischievous behaviour and drops packets. It may also target packets coming out from a specific node while for other nodes it delivers packet. Packet drop can also happen with genuine nodes due to network traffic. Hence grayhole attack is hard to discover.

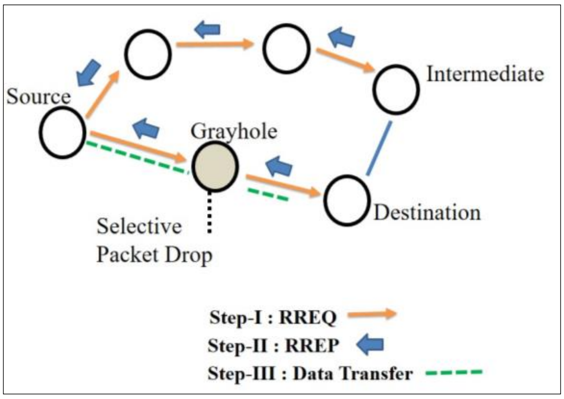

Figure 1. Grayhole Attack

As seen in the figure 1, grayhole node takes part in the route discovery process and forwards RREQ packet. But when data packets are transferred through it, it shows malicious behaviour by selectively dropping some data packets while forwarding other packets to destination.

2.2 Wormhole Attack

Wormhole attack (Khan et al., 2021) is collectively carried out by minimum two or more nodes in the network. The attacking nodes maintain a high speed communication channel between them. This channel or tunnel is normally maintained at two ends in the network. Whenever one wormhole node receives data packets, it sends them through the high speed tunnel to the other wormhole and then it broadcasts the packet from there. As the packets travel through the fast tunnel, they reach to the destination faster than any other route. As the hop count through this path appears to be shorter, this wormhole tunnel route is formed between source and destination for data transmission. Once the data transmission begins through this route, the wormhole node misbehaves with the data. It may selectively or completely drop the data packets or analyse the network traffic. Shorter round trip time an important factor to identify wormhole attack due to the utilization of high speed tunnel.

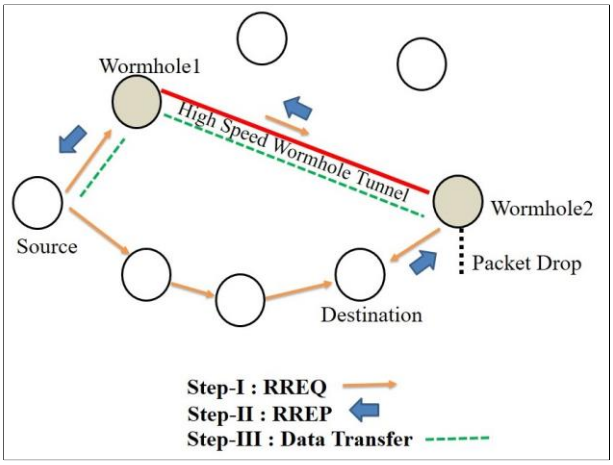

Figure 2. Wormhole Attack

As seen in the figure 2, once wormhole1 receives RREQ packet from source, it immediately transmits it to wormhole2 through high speed tunnel and it reaches to the destination faster than any other route. Destination sends RREP which travels through same fast channel and reaches to the source node. Although the two wormhole nodes are actually far from each other, they appear to be one hop neighbours. This wormhole route is formed between source and destination. Once data transmission begins from this channel, the wormhole nodes misbehave with the data.

3. RELATED WORKS

Geetanjali and Gupta (2017) used Particle Swarm Optimization (PSO) Algorithm to detect Cooperative Grayhole Attack in MANET. The parameter used by PSO algorithm is Shortest path and Closeness Centrality. The gray hole node is detected under AODV protocol by Partical Swarm Optimization algorithm. Gurung and Chauhan (2017) examined how the existing three modified AODV protocols which were designed to mitigate blackhole attack were able to two types of grayhole nodes- sequence number based and smart grayhole nodes. Sasirekha & Radha (2017) proposed A3AODV protocol to address the issue of Wormhole and sinkhole attack collectively by using node collusion methodology. When a node sends a large number of RREQ packets in a certain time interval, or if it shows sequence number abnormality, it is detected as sinkhole node. Wormhole is detected on the basis of abnormality in Round Trip Time. Dhende et al. (2017) proposed a technique to detect Blackhole and Grayhole attack using Opinion Request Methodology. On the basis of the type of opinion received from neighbours about a suspicious node, it classifies the attacking node as blackhole or grayhole node. Panda and Pattanayak (2018) proposed a Zone Splitting Method to identify External and Internal Blackhole and Grayhole attack. As'adi, et al. (2018) presented a method to detect wormhole attack using Number of Neighbours parameter. Wormhole node density needs to be high for this method to work accurately. Kaur et al. (2017) presented a method to detect Wormhole Attack on the basis of Threshold Delay Value between one hop away neighbouring nodes. This method does not use any of extra information like special hardware, position or clock synchronization information. But the method may fail to detect wormholes when they are actually in communication range of the genuine nodes.

Singh et al. (2017) proposed a method to detect Gray Hole Attack in MANET by considering the threshold value calculation for Hop Count. If any abnormality is observed in the threshold value of hop count for a particular node, that node is considered as Gray Hole node. Sankara Narayanan and Murugaboopathi (2018) proposed a Modified Secure AODV Protocol (MSAODV) to prevent wormhole attack in MANET on the basis of Packet Forward Ratio (PFR) and Round Trip Time (RTT) for each consecutive nodes from source to destination. This method detects active and passive wormhole attacks without the use of any special hardware like GPS or special antenna. Tahboush and Agoyi (2021) presented a hybrid method to detect in-band and out-of-band wormhole attack. Out-of-band wormhole nodes are detected as the nodes having neighbour ratio higher than neighbour ratio threshold (NRT). When the Round Trip Time value between two nodes is greater than threshold, in-band wormhole link is detected between the nodes. Bhawsar et al. (2020) proposed a trust-based method to detect wormhole attack. If the packet drop percentage for the false packets sent by source is greater than a threshold value, the node is detected as wormhole node. Elliptic curve cryptography is used for additional security of the data packets. This method employs multipath approach to find the best route for data transfer. Shukla et al. (2021) developed a protocol to mitigate Wormhole and Blackhole Attack Using Elliptic Curve Cryptography. Jebaseelan and Raju (2022) developed SRMAD-AODV protocol to detect and defend the black and gray-hole attacks by examining the behavioural data.

As observed in the literature survey, most of the methods to address security attacks in MANET focused on a particular type of attack or combination of two types of attacks. The pattern of the attack is considered for designing the security solution. These security methods are limited to their attack types and may fail if any other type of attack is introduced in the network.

4. ANALYSIS OF RESEARCH GAPS

Various methodologies mentioned above to protect the MANETs from grey hole, wormhole attacks are reviewed in this research work. These methodologies have limited scope with a focus on a specific type of attack or a combination of two types of attacks. The methods dealing with a particular type of attack may fail to work with the other kinds of MANET attacks effectively. It is observed that a scalable trust-based solution is missing to protect MANET from several simultaneous attacks. Also an integrated security solution comforting accurate attacker detection and reliable route formation is lacking. Some solutions could only detect attacks in the network but failed to construct reliable routes which restrict QoS performance. To sum up, the combined goal of multiple attack detection and reliable route formation cannot be achieved using the existing methodologies. These designing gaps in the present solutions motivated us to design a generalised protocol solution to address a variety of attacks, which we call “Multiple Attacks Protected Ad-hoc On-demand Distance Vector (MAP-AODV) Protocol”.

5. THE ARCHITECTURE OF THE PROPOSED MAP-AODV PROTOCOL

The architecture of the proposed MAP-AODV protocol is shown below in the following diagram (figure 3).

Initially the MANET is deployed with varying numbers of mobile nodes. Source-destination traffic pairs are constructed and 10% attacker nodes (grayhole / wormhole) are introduced into the network. The threat detection algorithm is executed periodically through the

Node Behavior Score (NBS) technique. Each mobile node is evaluated using the dynamic trust-based NBS process. Each node is evaluated as genuine or attacker node on the basis of its NBS value. The route construction process between the source and destination involves selection of efficient and reliable node as an intermediate node using the Node Reliability Analysis (NRA) technique.

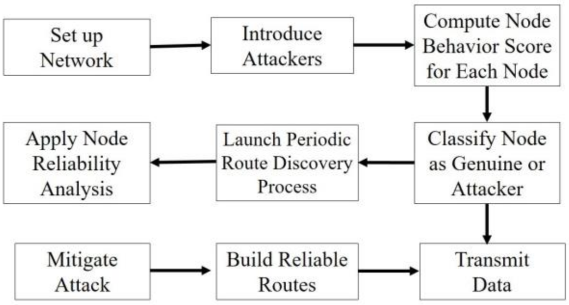
Set up Network
Introduce Attackers
Compute Node Behavior Score for Each Node
Classify Node as Genuine or Attacker
Launch Periodic Route Discovery Process
Apply Node Reliability Analysis
Transmit Data
Build Reliable Routes
Mitigate Attack

Figure 3. The Architecture of MAP-AODV Protocol

The main two mechanisms of the protocol- Attack detection using NBS and Attack mitigation using NRA method are described below in detail.

6. NBS-BASED ATTACK DETECTION MECHANISM

Each mobile node is periodically assessed using the Node Behaviour Score (NBS) process as part of Attack Detection Mechanism. First the Forwarding Ratio (FR) of the node is calculated to validate its packet dropping behaviour. NSB defines the direct trust of a node m^i which is computed by node m^j at current time interval t if those nodes are one hop neighbor. Thus, node m^j uses its direct observation towards node m^iduring each periodic trust evaluation round.

$$FR(m^i, m^j(t)) = 1 - \left(\frac{P\left(m^{i,j}(t)\right) - R\left(m^{i,j}(t)\right)}{P\left(m^{i,j}(t)\right) + R\left(m^{i,j}(t)\right)}\right) \qquad (1)$$

Where, $FR(m^i, m^j)$ represents the Forwarding Ratio of node m^i by node m^j, $P(m^{i,j}(t))$ is number of successful packets forwarded by m^i to m^j at time t and $R(m^{i,j}(t))$ is number of successful packets received by m^j at time t.

The Channel Availability (CA) of the node is calculated to validate its congestive behaviour.

The HELLO packet is transmitted by m^j to analyze bandwidth of m^i to receive this packet. Once ACK is received for HELLO packet from m^i at m^j, it defines the availability of m^i as:

$$CA(m^i, m^j(t)) = \frac{ack(m^{i,j}(t))}{ack(m^{i,j}(t)) + nonack(m^{i,j}(t))} \qquad (2)$$

Where, $ack(m^{i,j}(t))$ represents the number of acknowledged HELLO packets and $nonack(m^{i,j}(t))$ represents number of non-acknowledged HELLO packets.

The outcomes of $FR(m^i, m^j(t))$ and $CA(m^i, m^j(t))$ trust parameters are in the range of 0-1. The mobile node's authentic behaviour is represented by a trust value close to value one.

$$nbs\ (m^i(t)) = \left(a1 \times FR(m^i, m^j\ )\right) + \left(a2 \times CA(m^i, m^j)\right) \qquad (3)$$

Eq. (3) utilizes the calculated FR and CA values resulting into an integrated NBS value ranging from 0 to 1. Here $a1$ and $a2$ represents weight whose values are set to 0.5 such that $0.5 + 0.5 = 1$. The calculated NBS value is compared with the pre-defined trust threshold value T for the detection of threats in the network. If the T is lower than the NBS value for the particular mobile node, then it is classified as legitimate node and vice versa. After conducting the experimental analysis of different threshold values T, we discovered that 0.4 thresholds delivered the optimum results for the MAP-AODV protocol.

The NSB value of each mobile node is then regularly updated in its routing table entries. This NSB value is also used during route creation to create stable and trustworthy routes.

7. NRA BASED ATTACK MITIGATION MECHANISM

The Node Reliability Analysis (NRA) method is used for reliable route construction along with attack mitigation. The route discovery process is initiated between the intended source and destination traffic pairs by broadcasting the RREQ packets. The current status of the node replying with RREP is collected from its NSB score as either Genuine or Malicious. The malicious node is rejected from being evaluated using NRA process. This guarantees the attack mitigation mechanism of the MAP-AODV protocol. The genuine respondent node is further evaluated using the NRA process as given below.

The Mobility Rate (MR) of the node is computed to choose a node with the minimum amount of mobility. Obtaining stable routes in the network is very important to avoid data loss.

The $MR(m^i)$ at time t is computed as:

$$MR\ (m^i(t)) = 1 - \left(\frac{getMobility\left(m^i(t)\right)}{max}\right) \qquad (4)$$

Where, $getMobility\left(m^i(t)\right)$ function returns currently moving speed of the node m^i using the geographical positioning system. The max represents the maximum mobility speed of the mobile nodes assigned at time of network deployment in meters/second. Node with higher $MR\ (m^i(t))$ is good candidate for forwarding relay selection.

The Distance to Destination (DD) factor of the node is computed by computing the geographical distance of the node towards the target node. Selecting the node with the shortest distance to destination reduces overhead and total transmission delay.

The $DD(m^i)$ value of the mobile node m^i is computed as:

$$DD(m^i(t)) = 1 - \left(\frac{dist\ (m^i,\ D)}{\mathrm{d_{max}}}\right) \qquad (5)$$

Where, $\mathrm{d_{max}}$ any positive maximum distance value. The maximum permissible distance in this task is 900 metres. RSSI is used to measure the distance parameter between node and destination node at the network layer. Finally, the joint trust factor $nra(m^i(t))$ for each mobile node m^i is computed at time t using the dynamic weight management technique combining the values of NBS, MR and DD as follows:

$$nra(m^i(t)) = (nbs\ (m^i) \times w^1) + (DD\ (m^i) \times w^2) + (MR\ (m^i) \times w^3) \qquad (6)$$

Where, $w^1,\ w^2, and\ w^3$ represents the dynamic weight parameters whose summation is equal to 1. We have assigned equal weights to each trust factor such as 0.33 for nbs, 0.33 for DD, and 0.34 for MR such that $0.33 + 0.33 + 0.34 = 1$. In this manner, we choose the next forwarder node from among all accessible nodes based on this value. The node with the highest value is chosen as the relay node contender. This process is repeated until the intended destination is discovered. The reverse route is formed and data transmission begins between the source and the destination.

8. SIMULATION SET-UP

To evaluate the efficiency of the proposed MAP-AODV protocol, we have compared its performance with two recently suggested protocols- MSAODV (Sankara et al., 2018) and MDMA (Marathe & Shinde, 2021). Like MAP-AODV, these protocols are modified and secured variations of the standard AODV protocol (Soomro et al., 2022). The MSAODV protocol is designed to address the wormhole threats. The MDMA protocol is designed with a trust-based mechanism to handle multiple types of threats but with limited trust parameters. The experiments were carried out with the NS2.35 version, Ubuntu 16.04 as a guest operating system through a virtual machine tool, 8 GB RAM, and an I5 CPU. The node densities were ranging from 30 nodes to 150 nodes.

Table 1 describes the remaining simulation settings. We have inserted 10 % of the total nodes in the network as attacker nodes. Grayhole and wormhole nodes are added as attackers. For example, the network of 60 nodes consists of six attackers- three grayholes and three wormholes. There are five source-destination traffic pairs in each network. The protocols are compared on the basis of average throughput, PDR, average end-to-end latency, communication overhead, and data loss rate.

Table 1. MANET Simulation Parameters

Parameter	Significance
Number of nodes	30, 60, 90, 120, 150
Protocols	MSAODV, MDMA, MAP-AODV
CBR traffic pairs	5
Number of attackers	10 % (Grayhole and Wormhole)
Network size	1000m x 1000m
Simulation duration	200 seconds
Mac protocol	802.11
Antenna model	Omni antenna
Propagation model	Two ray ground
Queue	Prequeue
Packet size	512 bytes
Processor	Intel processor, 3Gz
Link bandwidth	1 Mbps
Mobility speed	20 m/s

9. RESULTS ANALYSIS

Throughput: This metric calculates the rate of message delivery over a communication channel. The figure 4 shows the throughput generated by networks with node densities ranging from 30 to 150 in presence of 10% attacker nodes.

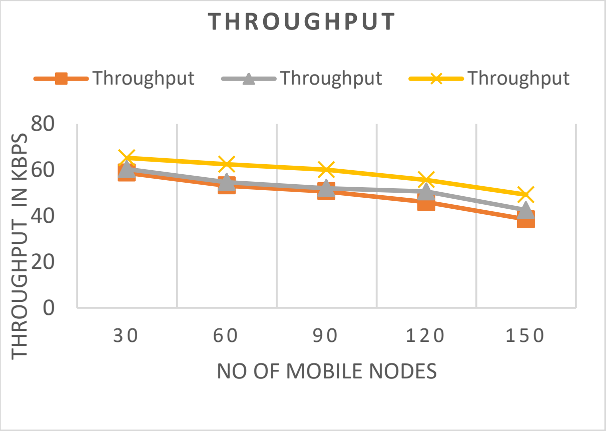

Figure 4. Average Throughput Analysis

As observed in the graph, the average throughput decreases as the node density increases. Higher node density leads to frequent routing operations which ultimately results in to performance loss. It is observed that the proposed MAP-AODV protocol achieved a greater average throughput as compared to other two protocols in presence of 10% attacker nodes. The unique NBS mechanism for attack detection and NRA mechanism for reliable route formation are the main reasons for this performance improvement.

Packet Delivery Ratio: It is the ratio of number of packets received at the destination to the number of packets sent from the source (Al-Shareeda & Manickam, 2022). The pdr results are similar to throughput results as seen in the figure 5.

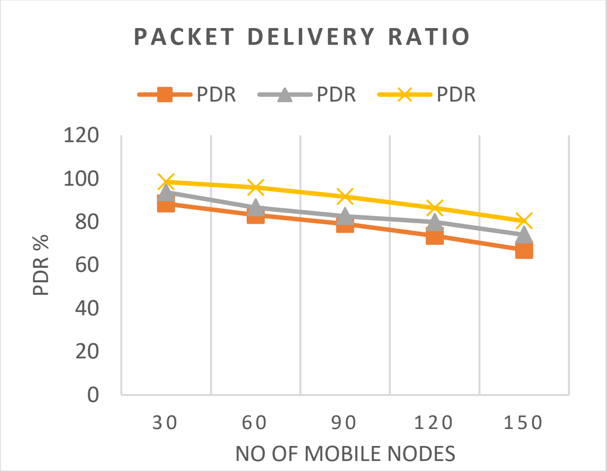

Figure 5. PDR Analysis

As the network density increases, packet delivery ratio decreases. The route finding technique of the proposed protocol significantly improves the packet delivery ratio as compared to other two protocols.

Data Loss Rate: This metric calculates the ratio of the number of packets not received to the total number of packets sent. The results given by Data Loss Rate are exact mirror images of the pdr results (figure 6).

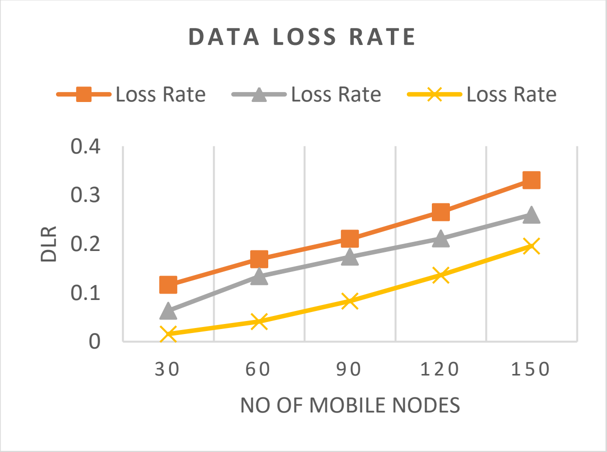

Figure 6. DLR analysis

With increase in the number of nodes, the data loss rate also increases. As the packet delivery ratio improves, the data loss caused by grayhole and wormhole nodes is reduced as compared to other two protocols.

Average Delay: This metric calculates the time on average, between a packet is sent from all sources and the time it arrives at all destinations (figure 7).

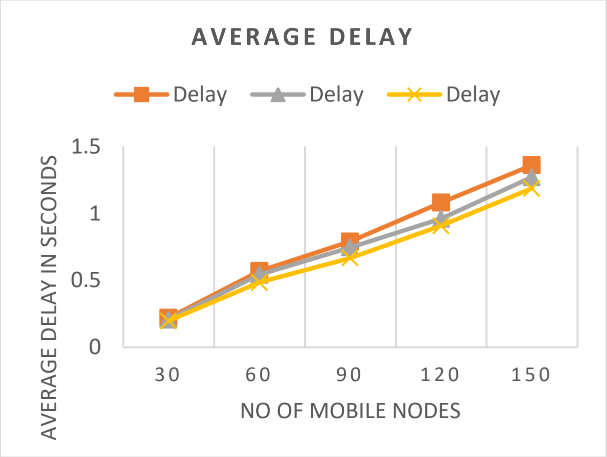

Figure 7. Average Delay Analysis

Communication Overhead: This metric is calculated by dividing the number of routing packets by the number of data packets in the network (Usha et al., 2017).

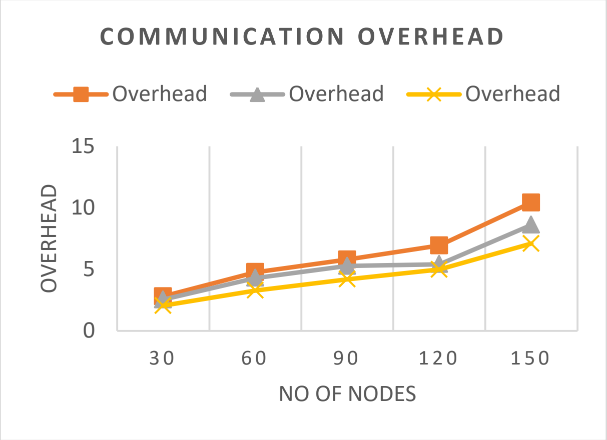

Figure 8. Communication Overhead Analysis

Higher data loss (Sivapriya & Mohandas, 2022) is directly proportional to the higher data re-transmission in the network. Higher re-transmissions lead to higher communication delay and communication overhead in the network for performing repeated routing operations. As seen in the above graphs of average delay and communication overhead (figure 8), the proposed protocol shows a significant reduction in the average communication delay and routing overhead as compared to underlying protocols. MDMA protocols shows better outcomes as compared to MSAODV protocol because MDMA is a trust-based mechanism designed to handle any type of attack.

10. CONCLUSION AND FUTURE WORK

One of the most challenging research problems in MANET is addressing different types of security attacks that exist simultaneously in the network. In this paper, we have proposed "MAP-AODV-Multiple Attacks Protected Ad-hoc On-demand Distance Vector Protocol" to address various attacks in the MANET using a lightweight trust-based approach. The NBS algorithm of the MAP-AODV protocol performs correct detection of the attacks whereas the NRA algorithm achieves attack mitigation and reliable route formation using both direct and indirect trust parameters. The solution is tested in the simultaneous presence of grayhole and wormhole attacks. When the results are compared against two existing protocols, it was observed that the MAP-AODV protocol delivers a better performance than the two existing protocols. The MAP-AODV protocol delivers a steady performance. It does not get affected by the nature of the attack as it is not bound to any specific attack type. In future the performance of this protocol can be compared against other packet dropping attacks.

References:

Abdel-Fattah, F., Farhan, K. A., Al-Tarawneh, F. H., & AlTamimi, F. (2019, April 1). *Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs*. IEEE Xplore. https://doi.org/10.1109/JEEIT.2019.8717449

Al-Shareeda, M. A., & Manickam, S. (2022). Man-In-The-Middle Attacks in Mobile Ad Hoc Networks (MANETs): Analysis and Evaluation. *Symmetry*, *14*(8), 1543. https://doi.org/10.3390/sym14081543

As'adi, H., Keshavarz-Haddad, A., & Jamshidi, A. (2018, August). A New Statistical Method for Wormhole Attack Detection in MANETs. In *2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)* (pp. 1-6). IEEE.https://doi.org/10.1109/iscisc.2018.8546943

Bhawsar, A., Pandey, Y., & Singh, U. (2020, July). Detection and prevention of wormhole attack using the trust-based routing system. In *2020 International conference on electronics and sustainable communication systems (ICESC)* (pp. 809-814). IEEE.https://doi.org/10.1109/icesc48915.2020.9156009

Dhende, S., Musale, S., Shirbahadurkar, S., & Najan, A. (2017, March). SAODV: Black hole and gray hole attack detection protocol in MANETs. In *2017 International conference on wireless communications, signal processing and networking (WiSPNET)* (pp. 2391-2394). IEEE.https://doi.org/10.1109/WiSPNET.2017.8300188

Geetanjali, & Gupta, J. (2017). Improved approach of co-operative gray hole attack prevention monitored by meta heuristic on MANET. *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, 356–361. https://doi.org/10.1109/ISPCC.2017.8269703

Gurung, S., & Chauhan, S. (2017). Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET. *Wireless Networks*, *25*(3), 975–988. https://doi.org/10.1007/s11276-017-1639-2

Jebaseelan, V., & Raju, K. K. (2022). Protecting MANETs from Black and Gray Hole Attacks Through a Detailed Detection System. *International Journal of Intelligent Engineering & Systems*, *15*(6), 237–246. https://doi.org/10.22266/ijies2022.1231.23

Karthigha, M., Latha, L., & Sripriyan, K. (2020). A comprehensive survey of routing attacks in wireless mobile ad hoc networks. *2020 International Conference on Inventive Computation Technologies (ICICT),* 396–402. https://doi.org/10.1109/icict48043.2020.9112588

Kaur, P., Kaur, D., & Mahajan, R. (2017). Wormhole Attack Detection Technique in Mobile Ad Hoc Networks. *Wireless Personal Communications*, *97*(2), 2939–2950. https://doi.org/10.1007/s11277-017-4643-z

Khan, A. U., Chawhan, M. D., Mushrif, M. M., & Neole, B. (2021). Performance analysis of adhoc on-demand distance vector protocol under the influence of black-hole, gray-hole and worm-hole attacks in mobile adhoc network. *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 238–243. https://doi.org/10.1109/ICICCS51141.2021.9432072

Kumar, S., Goyal, M., Goyal, D., & Poonia, R. C. (2017). Routing protocols and security issues in MANET. *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS)*, 818–824. https://doi.org/10.1109/ICTUS.2017.8286119

Marathe, N., & Shinde, S. K. (2021). Multidimensional Multi-Attribute Approach to Counter the Routing Attacks on MANET. *Wireless Personal Communications*, *119*(3), 1993–2016. https://doi.org/10.1007/s11277-021-08315-4

Panda, N., & Pattanayak, B. K. (2018). Defense against co-operative black-hole attack and gray-hole attack in MANET. *International Journal of Engineering & Technology*, *7*(3.4), 84-89. https://doi.org/10.14419/ijet.v7i3.4.16752

Saini, T. K., & Sharma, S. C. (2020). Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept. *Ad Hoc Networks*, *103*, 102148. https://doi.org/10.1016/j.adhoc.2020.102148

Sankara Narayanan, S., & Murugaboopathi, G. (2018). Modified secure AODV protocol to prevent wormhole attack in MANET. *Concurrency and Computation: Practice and Experience*, *32*(4). https://doi.org/10.1002/cpe.5017

Sasirekha, D., & Radha, N. (2017, October). Secure and attack aware routing in mobile ad hoc networks against wormhole and sinkhole attacks. In *2017 2nd international conference on communication and electronics systems (ICCES)* (pp. 505-510). IEEE. https://doi.org/10.1109/cesys.2017.8321128

Shukla, M., Joshi, B. K., & Singh, U. (2021). Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET. *Wireless Personal Communications*, *121*(1), 503–526. https://doi.org/10.1007/s11277-021-08647-1

Singh, J. P., Goyal, D., Shiwani, S., & Gaur, V. (2017). Hindrance and riddance of Gray Hole attack in MANETs multipath approach. *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*, 1–5. https://doi.org/10.1109/CIACT.2017.7977391

Sivapriya, N., & Mohandas, R. (2022). Analysis on Essential Challenges and Attacks on MANET Security Appraisal. *Journal of Algebraic Statistics*, *13*(3), 2578-2589. https://publishoa.com ISSN: 1309-3452

Soomro, A. M., Fudzee, M. F. B. M., Hussain, M., Saim, H. M., Zaman, G., Atta-ur-Rahman, H. A., & Nabil, M. (2022). Comparative review of routing protocols in manet for future research in disaster management. *Journal of Communications*, *17*(9), 734–744. https://doi.org/10.12720/jcm.17.9.734-744

Tahboush, M., & Agoyi, M. (2021). A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET). *IEEE Access*, *9*, 11872–11883. https://doi.org/10.1109/access.2021.3051491

Usha, G., Babu, M. R., & Kumar, S. S. (2017). Dynamic anomaly detection using cross layer security in MANET. *Computers & Electrical Engineering*, *59*, 231-241. https://doi.org/10.1016/j.compeleceng.2016.12.002

Monika Dangore
Sage University,
Indore, M.P.
India
monikaresearch2020@gmail.com

Dr Hare Ram Sah
Sage University,
Indore, M.P.
India
ramaayu@gmail.com