A GENERALIZED APPROACH FOR DETECTING AND MITIGATING MANET ATTACKS

Ms Monika Y. Dangore[1], Dr. Hare Ram Sah[2]

[1]*Ph.D. Scholar, Sage University, Indore, M.P, India*

[2]*Professor, Department of CSE & IT, Institute of Engineering and Technology, Sage University, Indore, M.P, India*

Abstract

Most of the existing security solutions to safeguard Mobile Adhoc Networks are based on specific attack detection and mitigation techniques that limits efficiency against the other attack types. To offer a generalized solution to protect MANET from different security threats, we have proposed the novel Multiple Attacks Protected Ad-hoc On-demand Distance Vector (MAP-AODV) routing protocol. The principal objective of the MAP-AODV protocol is to present a consolidated approach to detect and mitigate different security attacks in the network with the minimum computational overhead. The Node Behavior Score (NBS) module of the proposed protocol performs accurate detection of the attack whereas Node Reliability Analysis (NRA) module accomplishes the objective of attack mitigation and reliable route formation. The efficiency of the proposed solution is tested against blackhole, grayhole and wormhole attacks using NS2 simulation. The simulation results confirm steady and promising performance of the proposed solution against different attack types.

Keywords:MANET, AODV, Blackhole, Grayhole, Wormhole

1. INTRODUCTION

Mobile Adhoc Networks (MANETs) is a consistently growing field of research with the continuing evolution of networking devices and services. Day–to-day devices like smartphones, home appliances, vehicles, drones have wireless connection capabilities. Applications like file sharing, community networks, location-based services, and inter-vehicle communications, can be supported efficiently by local ad hoc networks. Such networks do not rely on any infrastructure, they may not be connected to the internet and can even be segregated during their operation. All these developments suggest that MANETs may finally find their way to the ‘‘masses” [1]. Mobile Ad hoc networks don’t have a centralized management system such as a server or intrusion detection system, which leads to many security threats. MANET nodes are allowed to move randomly and can leave and join the network anytime hence the network topology keeps changing arbitrarily and quickly. This unpredictable dynamic topology also gives chance to the intruder to carry out malicious activity in the network. In the wired network system, the device needs to pass the firewalls and gateways, whereas in the ad-hoc network, there is no such protection walls due to the usage of wireless link [2]. Ad hoc networks mostly have lower bandwidth capability than traditional wired networks. Attacking nodes can exploit this weakness, consuming ad hoc network bandwidth to disrupt regular network activities.

Routing is one of the most vital operations of mobile adhoc network where processes such as route discovery, shortest route formation, and data transmission between source and destination node are accomplished. The routing protocol used governs the

Quality of Service (QoS) performance of the network. There are numerous reasons why MANET's Quality of Service is degraded at the routing layer. It includes mobility, congestion, attackers, etc. As security is the main hurdle to the general implementation of MANET applications, a significant portion of the research work has focused on providing security services for MANETs. As mentioned above, MANET is susceptible to numerous forms of attacks because of its open medium, dispersed nature, and dynamic topology, such as grey hole attacks, Sybil attacks, black hole attacks, sleep deprivation attacks, wormhole attacks, packet dropping attacks, etc. Due to the presence of malicious nodes in the network, the burdens of frequent route breaks and route discovery results into high packet loss and computational overhead by genuine mobile nodes. Over the past two decades, a range of security measures have been developed at the routing layer for wireless communications. However, each methodology has limitations when dealing with malicious nodes in wireless networks.

The challenge is to develop not only an efficient solution, but also a generalized one, that will protect the MANETs from different kinds of attacks. We proposed the innovative Multiple Attacks Protected Ad-hoc On-demand Distance Vector (MAP-AODV) routing solution in this research work to describe an efficient approach for multiple attacks detection and mitigation in MANETs. The primary functionality of our proposed protocol mainly depends on the proposed trust-management model in which we computed the trust parameters of each mobile node from different layers. We modified the existing AODV protocol with the proposed security procedures against the different kinds of attacks in the network. We tested the efficiency of the proposed protocol for blackhole, grayhole and wormhole attacks. During the development of the proposed trust-based approach, we ensured the lowest computational requirements, higher detection accuracy and protection against the attacks.

2. OUTLINE OF THE ATTACKS UNDER FOCUS

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

2.1 BLACKHOLE ATTACK

Blackhole attack is carried out by an intruder node which exploits the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [4]. The malicious node pretends to be the intermediate node of the route to the destination. The attacker redirects all packets destined to a target node to itself then drops all the packets. This is the most frequently occurring routing attack in MANET and most of the research work addresses the issue of handing blackhole attacks.

2.2 GRAYHOLE ATTACK

The grayhole attack is more subtle than blackhole attack [4]. The attacker selectively forwards or drops the packets as per the attack requirement. Mostly it takes part in route discovery phase and shows its attacking behavior in the data transfer phase hence it is harder to detect.

2.3 WORMHOLE ATTACK

A wormhole attack works in pair to damage the network's performance [5]. A wormhole node forms a pair with another wormhole through a high-speed tunnel. Once the wormhole captures the route, it directs the data packets through the tunnel then it can modify, drop, or divert the data packets to carry out the malicious activity.

3. LITERATURE REVIEW

Sandeep et al. [6] in 2017 proposed a technique to detect Blackhole and Grayhole attack using Opinion Request Methodology. It asks opinion about the replying node from its neighbours to observe the past behavior of the node to identify it as genuine or attacker node. Shashi et al. [7] in 2017 examined the performance of existing solutions to blackhole attack in the presence of two types of grayhole nodes- sequence number based and smart grayhole nodes. D.Sasirekha et al. [8] in 2017, addressed the issue of wormhole and sinkhole attack collectively by using node collusion methodology through A3AODV protocol. When a node sends alarge number of RREQ packets in a certain time interval, or if it shows sequence number abnormality, it is detected as sinkhole node. If a node shows abnormality in Round Trip Time, it is detected as wormhole node. Neha Sharma et al. [9] in 2016 proposed a technique to address blackhole and grayhole attacks. The technique makes use of Trap RREQ Packets and Packet Drop Ratio. Niranjan Panda et al. [10] in 2018 proposed a Zone Splitting Method to detect External and Internal Blackhole and Grayhole attack. Here the whole network is divided in zones with each zone having a coordinating node (Static Intelligent Node-SIN which has better resources) and normal nodes. This method can detect internal and external malicious nodes.

Aly M. El-Semary et al. [11] in 2019 proposed a solution to detect Cooperative Blackhole Attack based on exchange of secrete values. The authors then introduced a modified protocol called Blackhole Protected AODV Protocol (BP-AODV) that detects cooperative blackhole attack by introducing chaotic map in its design.The malicious nodes are detected when difference is observed in the secrete parameters exchanged between source and destination. Parvinder Kaur et al. [12] in 2017 proposed a method to detect Wormhole Attack on the basis of Threshold Delay Value between one hop away neighboring nodes. J. P. Singh et al. [13] in 2017 proposed a method to identify Gray Hole Attack in MANET by considering the threshold value calculation for Hop Count. S. Sankara Narayanan et al. [14] in 2018 proposed a Modified Secure AODV Protocol [MSAODV] to prevent wormhole attack in MANET on the basis of Forward Ratio (PFR) and Round-Trip Time (RTT).

Muhannad et al.[15] in 2021 proposed a hybrid method to detect in-band and out-of-band wormhole attack. The nodes having neighbor ratio higher than neighbor ratio threshold (NRT) are detected as out-of-band wormhole nodes. When the Round-Trip Time value between two nodes is greater than threshold, in-band wormhole link is detected between the nodes. Aditya Bhawsar et al. [16] in 2020 proposed a trust-based method to detect wormhole attack on the basis of packet drop percentage of false packets. For additional security of the data packets, elliptic curve cryptography is applied. This method employs multipath approach to find the best route for data transfer. Mukul Shukla et al. [17] in 2021 developed a protocol to mitigate Wormhole and Blackhole Attack Using Elliptic Curve Cryptography. Vijigripsy et al. [18] in 2022 developed SRMAD-AODV protocol to detect and defend the black and gray-hole attacks on the basis of behavioral data. Dhanagopal et al [19] in 2022 developed a modified AODV protocol named MTBD to mitigate the black hole attack in MANET using a multipath approach.

As observed in the literature survey, most of the mitigation methods are able to deal with a particular type of attack. The methods mainly focus on the nature of the attack. Hence, they may fail if any other type of attack is introduced in the network.

4. MOTIVATION

A review of various recently proposed methodologies [6-19] is done in this research work which protect the MANETs from attacks such as the black hole, grey hole, wormhole, etc. The contemporary solutions have focused on developing trust-based detection and mitigation methodologies with limited scope. Most of the existing solutions focused on detecting the black hole attacks in the network but such solutions may fail to work with the other kinds of MANET attacks effectively. Hence a scalable trust-based solution is lacking to protect MANET from several simultaneous attacks. Also, an integrated security solution ensuring accurate attacker node detection and reliable route formation is also missing. Some solutions simply detected attacks in the network but failed to construct reliable routes, restricting QoS performance. Other systems detect and alleviate attacks only during trust-based route construction, resulting in unreliable methods and unnecessary routing overhead. In essence, multiple attack detection and reliable route formation cannot be addressed using the existing methodologies in [6-19]. These lacunas in the existing solutions motivated us to develop a generalized solution to address a variety of attacks, which we named as Multiple Attacks Protected Ad-hoc On-demand Distance Vector (MAP-AODV) Protocol.

5. THE PROPOSED MAP-AODV PROTOCOL

The MAP-AODV protocol involves three phases-Network Setup, Threat Detection, and Data Transmission Phase as described below:

5.1 THE NETWORK SETUP PHASE

It involves the deployment of MANET network with various numbers of mobile nodes, constructing source-destination traffic pairings, introducing 10% attacker nodes (blackhole / grayhole / wormhole) into the network.

5.2 THREAT DETECTION PHASE

After the network is set up, we run the threat detection algorithm periodically through the Node Behavior Score (NBS) technique. Each mobile node is evaluated using the dynamic trust-based NBS process. The decision of NBS is then utilized to classify each node as genuine or attacker node.

5.3 DATA TRANSMISSION PHASE

The last phase of the proposed protocol performs the route formation between the intended source-destination pair in the network. It involves selection of efficient and reliable node as an intermediate node using the Node Reliability Analysis (NRA) technique.

6. PROPOSED ALGORITHMS

The proposed MAP-AODV protocol is composed of the two algorithmic modules as given below.

6.1 NBS-BASED ATTACK DETECTION

Each mobile node is periodically evaluated using the Node Behavior Score (NBS) Model as follows:

1. Compute the Forwarding Ratio (FR) of the node
2. Compute the Channel Availability (CA) of the node
3. Compute the NBS value of the node using FR and CA parameters of the node
4. If the NBS value of the node is greater than the predefined threshold value, classify the node as Genuine node otherwise Attacker node
5. Update the NBS value of the node in its routing table entries

6.2 ATTACK MITIGATION USING NRA

The novel Node Reliability Analysis (NRA) approach is used for reliable route formation along with attack mitigation as follows:

1. Broadcast the Route Requests (RREQs) to initiate the route formation between the intended source and destination pair
2. Observe the status of the node replying with RREP as per step (4) of algorithm-1 shown above (genuine / attacker)
3. Discard the attacker node from being evaluated using NRA. This ensures the attack mitigation mechanism of the MAP-AODV protocol.
4. The legitimate respondent node is evaluated using the NRA approach as follows:

i. Calculate the Mobility Rate (MR) of the node. The objective is to select a node with the least amount of mobility to obtain stable routes in the network and avoid data loss.

ii. Calculate the Distance to Destination (DD) parameter of the node by computing the geographical distance of the node towards the destination node. Here the objective is to select the node with the shortest distance to destination to reduce overhead, network latency, and total transmission delay.

iii. Finally, the joint trust factor-NRA value of the node is computed by combining its NBS score, DD and MR parameters.

5. Among all the NRA values of legitimate responded nodes, the node with a higher NRA value is selected as the next forwarding relay.

6. The process is repeated until the intended destination D is discovered.
7. The reverse route is formed, and data transmission starts between the source and the destination.

7. PERFORMANCE ANALYSIS AND SIMULATION RESULTS

NS2 Simulation tool is used here to analyze the efficiency of the proposed MAP-AODV protocol. The experiments are performed using the NS2.35 version, Ubuntu 16.04 as a guest operating system using a virtual machine tool, 8 GB RAM, and an I5 processor. The networks are designed with varying node densities starting from small network size of 30 to large network size of 150 nodes. Other simulation parameters are listed in Table 1. We have introduced 10 % gray hole, black hole and worm hole threats in the network individually and analyzed their performances using each security measure. Each network has a total of five source-destination pairs. The performances are measured using the parameters like average throughput, PDR, average end-to-end delay, communication overhead, and data loss rate.

The standard AODV protocol does not have security provisions hence the results of the parameters for standard AODV in presence of threats would be very low. Hence we have compared the performance of MAP-AODV protocol under attack with standard AODV protocol with no-attack scenario to check how close the results of the proposed protocol are, to the attack-free scenario.

Table 1. MANETs Simulation Parameters

Parameter	Significance
Number of nodes	30, 60, 90, 120, 150
CBR traffic pairs	5
Number of attackers	10 %
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
Attack type	“Black hole” or “Gray Hole” or “Worm hole”

7.1 ANALYSIS OF BLACKHOLE ATTACK

Here we present the comparative analysis of different security parameters to protect against 10% of black hole nodes. Figures 1-5 represent the simulation results for the performance metrics such as average throughput, packet delivery ratio, data loss rate, average delay, and communication overhead, respectively

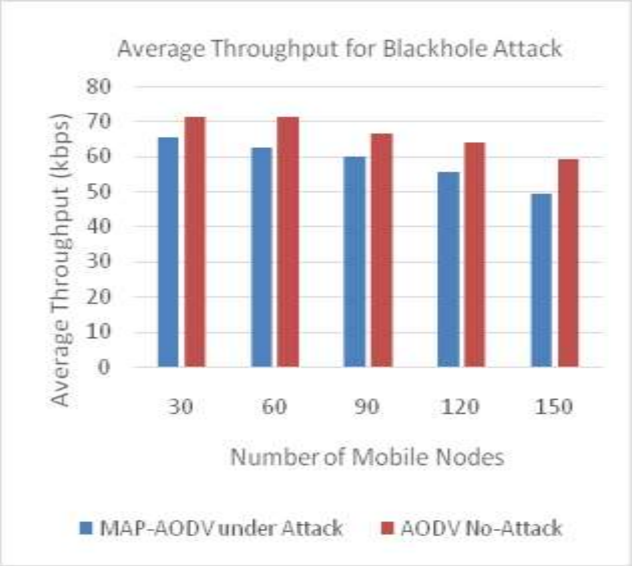

Fig 1. Average throughput analysis for blackhole

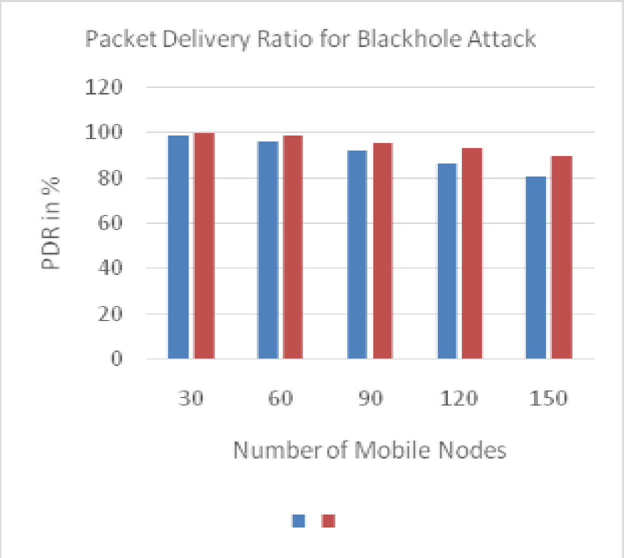

Fig 2. PDR analysis for black hole threats

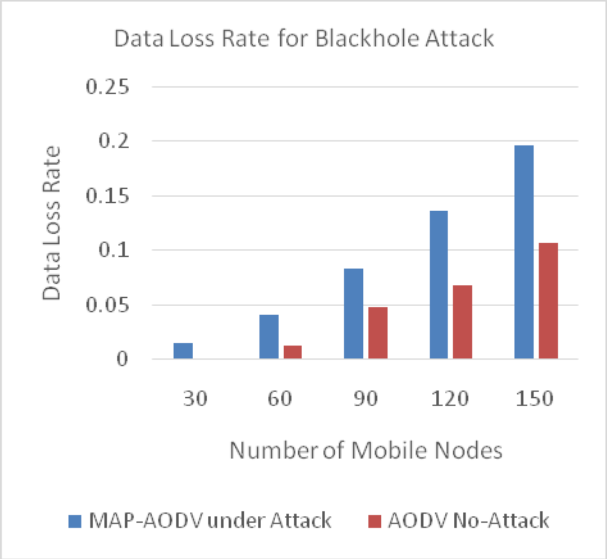

Fig 3. DLR analysis for black hole threats

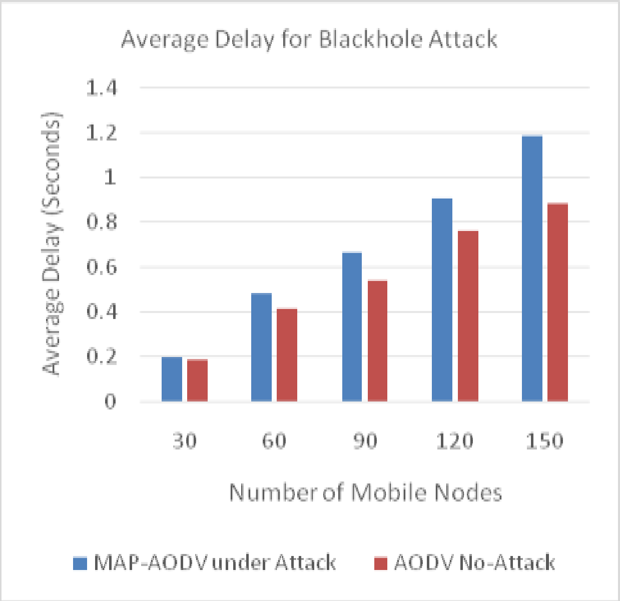

Fig 4. Average delay analysis for blackhole

It is observed through the results that the performance of network parameters is decreasing with increase in the number of mobile nodes in the network. The average throughput (figure 1) and PDR (figure 2) decreases with increase in the number of the mobile nodes. Whereas the other parameters like DLR (figure 3), average delay (figure 4), and communication overhead (figure 5) are increased with increase in the number of the mobile nodes. It shows that MANETs with higher density results in frequent route formation operations and hence it leads to a performance drop. Another reason for such a trend of results is that with the increasing mobile nodes density, the number of attacker nodes also increase. It leads to increasing operations for attack detection and mitigation which results in a higher delay and overhead with lower throughput and PDR performances.

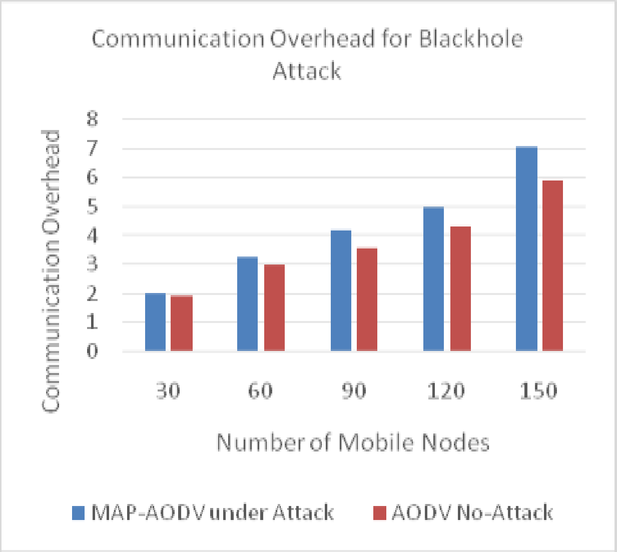

Fig 5. Communication overhead analysis

Similar to the average throughput results, the PDR outcomes in figure 2 shows a promising PDR rate achieved using MAP-AODV. The efficient detection of security threats in the MANET and reliable route discovery approach in MAP-AODV results in strong protection against the attacks. Hence, it significantly improves the successful packet transmission rate and reduces the overall data loss rate (figure 3). The DLR outcomes are the exact mirror image of the PDR outcomes. It shows that the MAP-AODV protocol is able to reduce the data loss caused by the attacker nodes in the network.

Higher data loss in the network considerably impacts the other two parameters such as average delay (figure 4) and communication overhead (figure 5). As the proposed MAP-AODV protocol can reduce the impact of attacks on the network communications efficiently, it lessens the data loss and improves the throughput with PDR performances. The reduction in data loss results in a reduction in re-transmissions. The lost data packets are frequently re-transmitted until they are successfully received at the intended destinations. Therefore, the higher data loss is directly proportional to the higher re-transmissions in the network. The higher re-transmissions lead to higher communication delay and overhead in the networks to perform the frequent routing operations. From Figures 4 and 5, we discovered that the proposed model shows a significant reduction in the average communication delay and overhead performances.

7.2 ANALYSIS OF GRAYHOLE ATTACKS

Here in this section, we present the simulation results for similar MANETs in presence of 10% of gray hole nodes. The results shown in figure 6-10 for average throughput, PDR, DLR, average delay, and communication overhead evaluates the performance of the MAP-AODV protocol in presence of gray hole nodes in the network. From these results, two points are found common with the black hole outcomes-the impact of increasing node density on the performances and promising results given by the proposed MAP-AODV protocol.

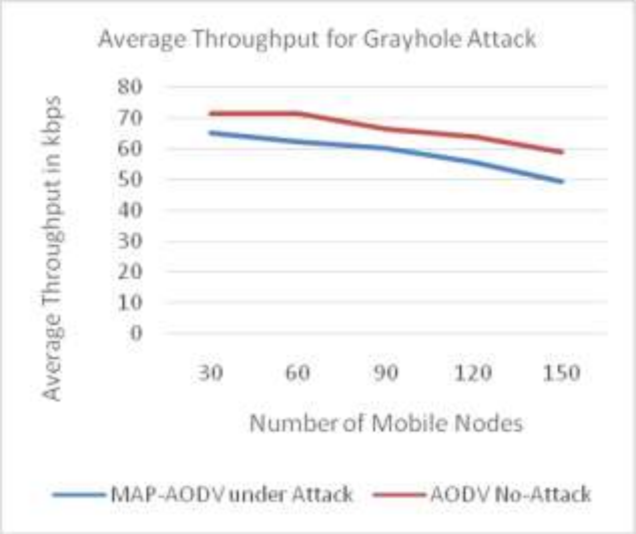

Fig 6. Average throughput analysis for grayhole

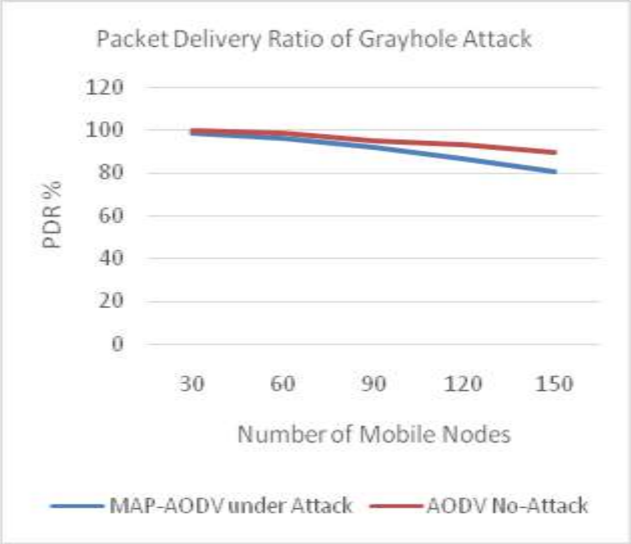

Fig 7. PDR analysis for grayhole threats

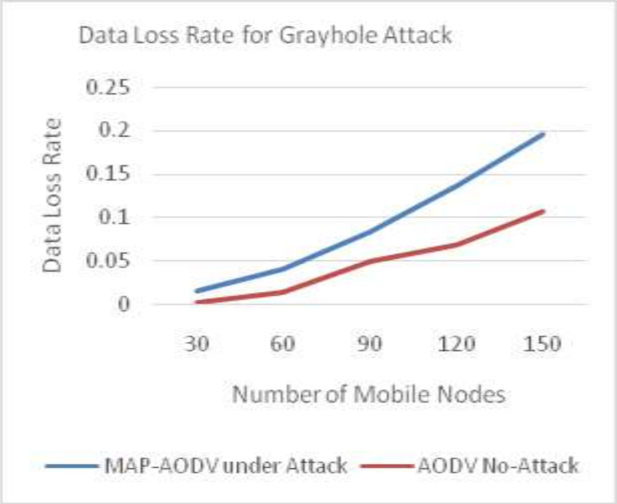

Fig 8. DLR analysis for grayhole threats

From the graphs it is observed that the MAP-AODV protocol shows a promising throughput closer to the no-attack scenario. The attack detection mechanism of the MAP-AODV utilized the direct trust factors to assess the attacking behavior of each mobile node in the network regardless of the type of threat. It helps to identify the threats accurately in the network. Along with the accurate threat detection approach of MAP-AODV, the NRA-based attack mitigation while establishing reliable routes leads to more stable data transmissions in the network. It results in higher PDR (figure 7) and lowers DLR (figure 8).

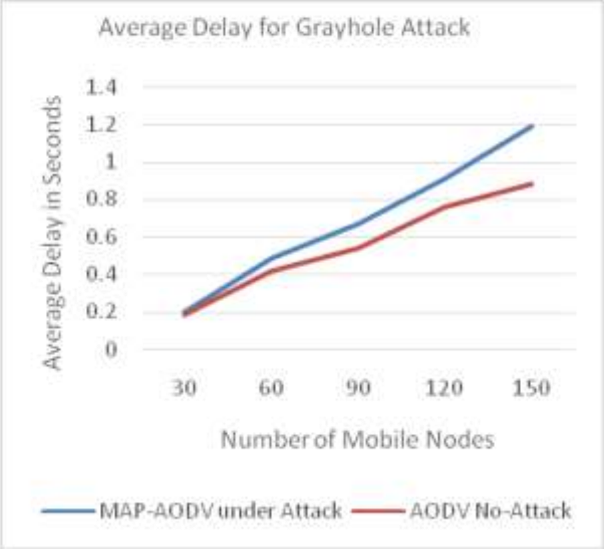

Fig 9. Average delay analysis for gray hole threats

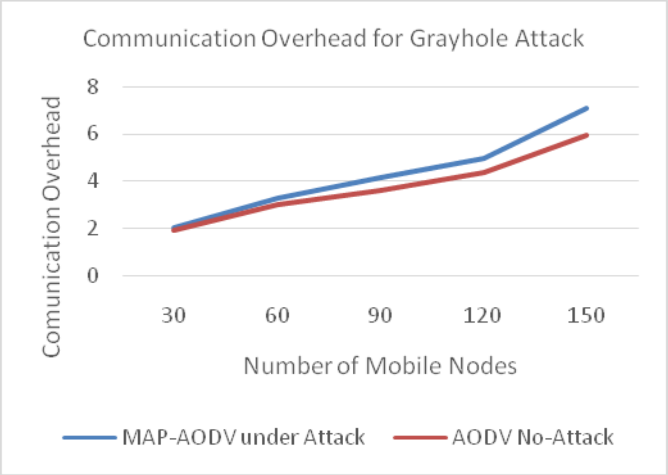

Fig 10. Communication overhead analysis

Finally, figure 9 and figure 10 demonstrate the computational complexity-related parameters called average delay and communication overhead, respectively. Lesser computational overhead represents lesser space complexity requirement. And lesser average delay represents the lesser time complexity requirement. The outcomes of PDR and DLR directly affect the average delay and communication overhead performances. Therefore, the MAP-AODV protocol shows lower communication delay and overhead requirements to protect against the gray hole threats.

7.3 ANALYSIS OF WORM HOLE THREATS

Here we show the simulation outcomes for similar MANETs in presence of 10 % worm hole threats. The results shown in figure 11-16 for average throughput, PDR, DLR, average delay, and communication overhead evaluate the performances of each security protocol in presence of worm hole threats in the network. In these outcomes also, we have observed the impact of increasing density on the performances and promising results using the proposed MAP-AODV protocol.

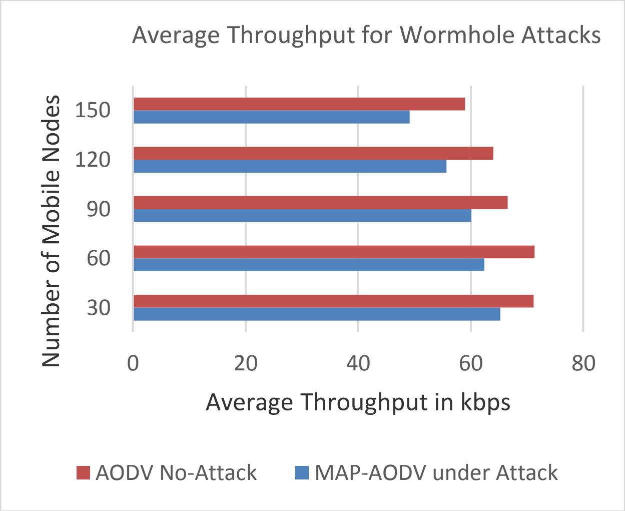

Fig 11. Average throughput analysis

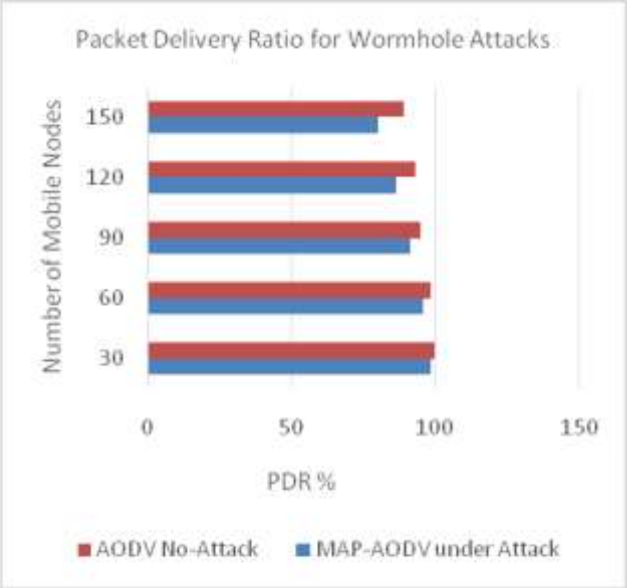

Fig 12. PDR analysis for worm hole threats

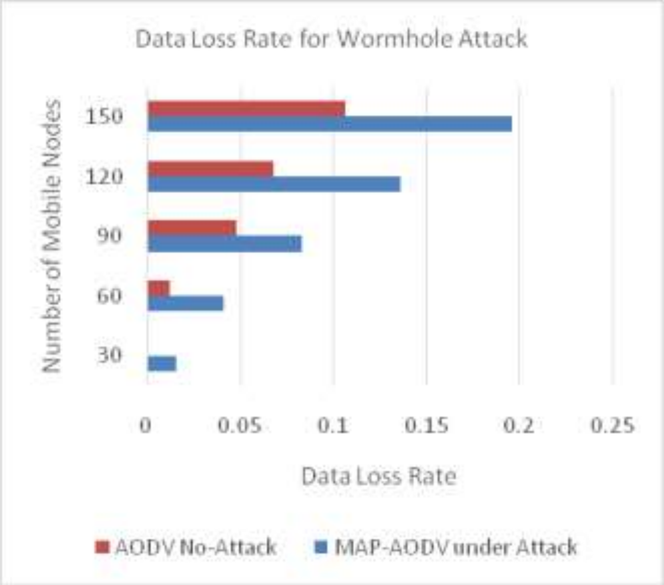

Fig 13. DLR analysis for worm hole threats

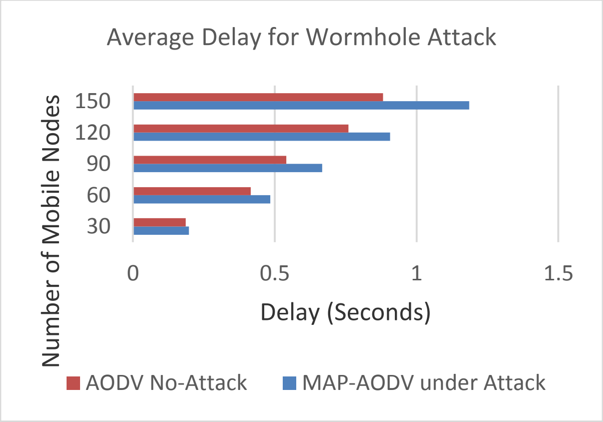

Fig 14. Average delay analysis for worm hole

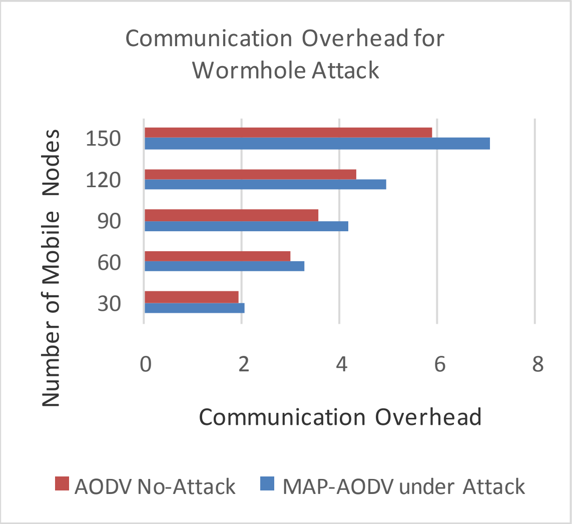

Fig 15. Communication overhead analysis

The outcomes in presence of 10 % worm hole attackers shows similar results obtained in case of blackhole and grayhole. This observation confirms that the proposed MAP-AODV protocol shows steady performance in presence of multiple types of threats. It is not bound to any specific attack type and its functionality is not altered by the nature of the attack. The attack detection and mitigation mechanism of MAP-AODV protocol takes the performance of network parameters close to the attack-free scenario.

8. CONCLUSION AND FUTURE WORKS

Addressing the different types of security attacks in MANETs is a challenging research problem. We have proposed the Multiple Attacks Protected Ad-hoc On-demand Distance Vector Protocol in this paper to detect and mitigate various attacks in the MANET using a lightweight trust-based approach. The solution is particularly tested against blackhole, grayhole and wormhole attacks individually. It was observed that the MAP-AODV protocol delivers a steady performance against all these attacks and does not get altered by the nature of the attack as it is not bound to any specific type of attack. It is a generalized approach to mitigate a variety of attacks in MANET. The proposed NBS algorithm of the MAP-AODV protocol performs accurate detection of the attacks in the network. The NRA algorithm achieves the goal of attack mitigation and reliable route formation using both direct and indirect trust parameters. On examining the performance of MAP-AODV protocol under individual presence of different types of attacks, we realized that the obtained results are close to the standard AODV protocol under no-attack scenario. In future the performance of this protocol can be compared against the existing attack mitigation technologies.

REFERENCES

[1] Yiannis Thomas, Nikos Fotiou, Stavros Toumpis, George C. Polyzos, "Improving mobile ad hoc networks using hybrid IP-Information Centric Networking", Computer Communications, Volume 156, 15 April 2020, Pages 25-34, https://doi.org/10.1016/j.comcom.2020.03.029

[2] Gupta, Chitvan, Singh, Laxman and Tiwari, Rajdev. "Wormhole attack detection techniques in ad-hoc network: A systematic review" Open Computer Science, vol. 12, no. 1, 2022, pp. 260-288. https://doi.org/10.1515/comp-2022-0245

[3] Trilok Kumar Saini , Subhash C. Sharma , "Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept" , https://doi.org/10.1016/j.adhoc.2020.102148 1570-8705/© 2020 Elsevier B.V

[4] Farhan Abdel-Fattah, Khalid A. Farhan , Feras H. Al-Tarawneh , FadelAlTamimi , "Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs", 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)

[5] A. U. Khan, M. D. Chawhan, M. M. Mushrif and B. Neole, "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), 2021, pp. 238-243, doi: 10.1109/ICICCS51141.2021.9432072.

[6] S. Dhende, S. Musale, S. Shirbahadurkar and A. Najan, "SAODV: Black hole and gray hole attack detection protocol in MANETs," 2017 International IEEE Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2017, pp. 2391-2394, doi: 10.1109/WiSPNET.2017.8300188

[7] Gurung, S., Chauhan, S. Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET. Wireless Netw 25, 975–988 (2019). https://doi.org/10.1007/s11276-017-1639-2

[8] D. Sasirekha , Dr. N. Radha , "Secure And Attack Aware Routing In Mobile AdHoc Networks Against Wormhole And Sinkhole Attacks", Proceedings of the 2nd International Conference on Communication and Electronics Systems (ICCES 2017) IEEE Xplore Compliant - Part Number:CFP17AWO-ART, ISBN:978-1-5090-5013-0

[9] N. Sharma and A. S. Bisen, "Detection as well as removal of black hole and gray hole attack in MANET," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016, pp. 3736-3739, doi: 10.1109/ICEEOT.2016.7755409.

[10] Niranjan Panda, Binod Kumar Pattanayak, "Defense Against Co-Operative Black-hole Attack and Gray-hole Attack in MANET",June 2018, International Journal of Engineering & Technology 7(3.4):84-89, DOI: 10.14419/ijet.v7i3.4.16752

[11] Aly M. El-Semary, HossamDiab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs based on Chaotic Map", DOI 10.1109/ACCESS.2019.2928804, IEEE Access

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

[13] J. P. Singh, D. Goyal, S. Shiwani and V. Gaur, "Hindrance and riddance of Gray Hole attack in MANETs multipath approach," 2017 3rd IEEE International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, 2017, pp. 1-5, doi: 10.1109/CIACT.2017.7977391.

[14] S. Sankara Narayanan, G. Murugaboopathi," Modified secure AODV protocol to prevent wormhole attack in MANET", Concurrency ComputatPractExper. 2018;e5017,https://doi.org/10.1002/cpe.5017, ©2018 John

Wiley & Sons, Ltd.

[15] MuhannadTahboush, Mary Agoyia, "Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET)", IEEE Access, Digital Object Identifier 10.1109/ACCESS.2021.3051491, Volume 9, 2021

[16] Aditya Bhawsar, Yogadhar Pandey, UpendraSingh,"Detection and Prevention of Wormhole Attack using the Trust-based Routing System", Proceedings of the International Conference on Electronics and Sustainable Communication Systems (ICESC 2020), IEEE Xplore Part Number: CFP20V66-ART; ISBN: 978-1-7281-4108-4

[17] Shukla M, Joshi BK, Singh U. Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET. WirelPersCommun. 2021;121(1):503-526. doi: 10.1007/s11277-021-08647-1. Epub 2021 Jun 28. PMID: 34219973; PMCID: PMC8237045.

[18] VijigripsyJebaseelan, KanchanaKavartty Raju, "Protecting MANETs from Black and Gray Hole Attacks Through a Detailed Detection System", International Journal of Intelligent Engineering and Systems, Vol.15, No.6, 2022 DOI: 10.22266/ijies2022.1231.23

[19] Dhanagopal Ramachandran, Sasikumar S, Vallabhuni Rajeev Ratna, Vijayprasath S, Suresh Kumar R, Vasanth Raj P T, IlhanGarip, Umamahesawari K, "A Low-Latency and High-Throughput Multipath Technique to Overcome Black Hole Attack in Mobile Ad Hoc Network (MTBD)", Security and Communication Networks, vol. 2022, Article ID 8067447, 13 pages, 2022. https://doi.org/10.1155/2022/8067447

[20] G. Usha, M. Rajesh Babu, S. Saravana Kumar, "Dynamic anomaly detection using cross layer security in MANET", Computers & Electrical Engineering, Volume 59, 2017, Pages 231-241, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2016.12.002.