**A Modified and secured Ad-hoc on-demand distance vector protocol (AODV) to defend blackhole attacks in Mobile Ad-hoc Network (MANET)**

# Hiren Thakor – [h3.hiren@gmail.com](mailto:h3.hiren@gmail.com)

Table of Contents

[Chapter-1 3](#_Toc79488237)

[Introduction: 3](#_Toc79488238)

[Problem statement: 4](#_Toc79488239)

[Significance: 4](#_Toc79488240)

[Resources: 4](#_Toc79488241)

[Chapter-2 Literature Review 5](#_Toc79488242)

[Chapter-3 7](#_Toc79488243)

[Methodology: 7](#_Toc79488244)

[Tool: 9](#_Toc79488245)

[Chapter - 4 10](#_Toc79488246)

[Implementation 10](#_Toc79488247)

[Part 1 Deployment of Network. 10](#_Toc79488248)

[Path Establishment 11](#_Toc79488249)

[Part 2: The blackhole attack simulation 15](#_Toc79488250)

[Part 3: Identification of Malicious nodes. 16](#_Toc79488251)

[Part 4 Alert the others. 19](#_Toc79488252)

[Comparison 20](#_Toc79488253)

[Problems and outcomes: 22](#_Toc79488254)

[Chapter - 5 23](#_Toc79488255)

[Conclusion: 23](#_Toc79488256)

[Implications 23](#_Toc79488257)

[Limitations and weaknesses 23](#_Toc79488258)

[Challenges 23](#_Toc79488259)

[Future Work 23](#_Toc79488260)

[Recommendation 23](#_Toc79488261)

[Summary 24](#_Toc79488262)

[Acronyms: 24](#_Toc79488263)

[References: 25](#_Toc79488264)

# Chapter-1

## Introduction:

MANETs (Mobile Ad-hoc Networks) comprise several nodes whose movable type is and interact with other nodes through data packets moving in the multi-hops in the absence of a central regulator[10]. These networks contain a huge number of movable hosts which utilized wireless connections for contact with one another. The mobility of the nodes is of an arbitrary kind in any route because this network does have any infrastructure. Therefore, there is no central control as well. Because of these qualities, all the nodes in this system behave like a router in which data packets are transmitted via the host. The MANET provides several finest elucidations just like in wired or wireless structure where some problems related to the spoiled and congested remains present often.

A picture containing text

Description automatically generated

Figure diagram of MANET

From the literature review, we plan to improvise traditional AODV protocols so that mitigating blackhole nodes from the system will drastically enhance. The Ad-hoc on-demand vector protocol is a widely used routing protocol in Mobile Ad-hoc network systems such as low bandwidth sensors, IoT devices, non-centralized network devices[1]. Still, the AODV protocol suffers from various security flows like Greyhole attacks, blackhole attacks, flooding attacks, and selfish attacks. The black hole attack is the most common attack that occurs in the MANET system[11]. Also, it is difficult to identify and mitigate the threat; that is why we will study AODVs from the security perspective in this project and propose a new methodology that efficiently identifies and mitigates the black hole nodes from the system.

Application, background pattern

Description automatically generated

Figure blackhole attacks

## Problem statement:

The study suggests that the traditional AODV Protocol does not perform very efficiently in throughput, Delay and Packet-loss while having malicious blackhole nodes.

In this project, we will find a new algorithm that improves the security of AODV in terms of mitigating blackhole attacks.

Firstly, the biggest challenge for this project is developing a new algorithm that identifies the malicious node. Therefore, identifying the malicious node in the system will be the primary goal of our project. After that, the next step is to remove the malicious node for the MANETs.

Finally, we will implement the proposed algorithm in the simulation-based environment; to implement all of these scenarios, we will use network simulator 2. We will create a MANET system that consists of server nodes, and some of that is malicious. After that, we plan to compare the simulation results between traditional AODV and our proposed AODV. The results are illustrating with throughput packet loss and delay [2].

## Significance:

The MANETs network is complex and widely used in IoT and sensor devices, and the AODV is the leading protocol for routing in these kinds of networks. As technology grows day by day, cyber-attacks are more complexed and accurate in MANETs. Thus, our proposed protocol can be used against complex blackhole attacks. Also, we can significantly improve the performance of the routing in MANETs. The modified version of AODV can defend against other such attacks as grey hole attacks and selfish attacks.[3]

## Resources:

To solve the problem mentioned above, we will use Ubuntu Linux, journal articles, literature, Network Simulator2.

# Chapter-2 Literature Review

Elbasher Elmahdi, (2018) proposed a novel mechanism to ensure that a reliable and secure data transmission can be performed [4]. The AOMDV protocol was extended here such that a message is split into multiple paths. Furthermore, a homomorphic encryption method was applied in this algorithm. As a result, a higher packet delivery ratio and throughput were achieved as per the simulation results calculated for the proposed method. Thus, for the emerging applications of MANETs, this approach was considered to be highly beneficial. Further, due to several active paths in every network, a higher success rate and guarantee of delivering the packet to the target were provided. To apply this mechanism within emergency applications, end-to-end delay can be reduced in the future by extending this research (p. 463-467).

Avni Tripathi, (2016) proposed a new confirmation packet-based mechanism for detecting and blacklisting the blackhole nodes from the communications being held in the network [5]. For blacklisting the blackhole node, a black packet was broadcasted by the source node by this proposed method when the confirmation packet did not reach before the threshold time. The hop count value was used as the base for the threshold time value. Due to the absence of the exact definition of the high destination sequence number used by the blackhole node, the limitations of using path rejection for communication based on high destination sequence numbers were not held by the proposed mechanism. The QualNet network simulator was used to implement this proposed work. Around 31% of the average packet delivery ratio was achieved for AODV previously, which was improved to approximately 60% by implementing the proposed approach. Considering the security requirements, challenges, and scope of improvement, the researchers have explored several opportunities to derive novel solutions in the future (p. 437-441).

Sagar R Deshmukh, (2016) presented a study that discussed the black hole attack and then proposed a solution to eliminating it from the networks. Heavy processing or extra memory is not needed within the system proposed in this paper [6]. The black hole attack was prevented before the actual data transmission phase or before the malicious node participated in the network due to negligible overhead. Thus, the confirmation of the legitimacy of the route was done. During the presence of other reactive routing protocols as well, the proposed mechanism was considered highly compatible. Future work can be extended for this research by implementing the proposed method for other reactive routing protocols(p. 1960-1964).

Guoquan Li, (2018) proposed a research work based on detecting the impact caused by blackhole attacks on the network in the presence of AODV protocol [7]. The performance parameters like packet loss, end-to-end delay, and throughput were considered when measuring the impact. Total numbers of nodes, the number of black hole nodes, and mobile nodes' speed were modified to analyze the network performance. The properties of blackhole attacks were provided through the experimental results, reflecting the behaviors of blackhole attack and their effect on the network(p. 1-6).

Guido Oddi, (2012) stated that the interaction was carried out through wireless links in the wireless networks. In this kind of network, the movable nodes were configured independently. The routing protocol scheming was identified as the primary concern in the mobile ad-hoc network. Several constraints occurred in this kind of network because of the dynamical alteration in the network topology. This happened because of the movement of the nodes since the nodes could travel arbitrarily in any route [8].  Therefore, the direction of the nodes in the system affected the functioning of the network. However, the finest connectedness had been presented through the MANETs in the tragic situation during the nonexistence of network framework. Therefore, it assisted in dangerous circumstances. A proactive routing protocol was projected in this study, according to the evolved ground positioning system. This projected technique was reasonable and provided the flexibility to connection breakdowns. This technique was appropriate for the Mobile Ad-hoc Networks in which GPS information was utilized to attaining advantages(p. 1259-1264).

# Chapter-3

Our research is conducted by reading several published papers. After reading the articles, we concluded that the original protocol is not effective for the blackhole attack. Thus, our hypothesis is to mitigate the blackhole attack in the MANETs. We will test our hypothesis using standard AODV routing protocol and simulation tools such as the NS2 simulator. **The simulation provides us the data about the throughput, delay, and packet loss. We will use this data to compare and contrast with the previous results of the original AODV protocol to test our hypothesis.**

## Methodology:

The first proposed methodology is based on the behavior of malicious nodes in the network**. We will start with the deployment of Ad-hoc mobile networks with a limited number of nodes**. We will use a very stable node in the MANETs to find a malicious node; we can call this node" IDS node." The IDS node needs to be created in the network, which is the node inside the network. The IDS node is the node that is maximum stability and cannot change its location frequently. The IDS node starts creating each node's profile; the IDS node will sense its adjacent node, and information of its adjacent node is stored. The stored information contains the packet type, whether it sends control packet or data packet, the data rate of sending packets (CBR or VBR), threshold values**.**

**Moreover, the initiating node will check route requests, and if it finds the least packet forwarding node, it will check the time of route request packet; otherwise, it will establish a path from source to destination. If the route request packet comes in the least amount of time, then the ids node will declare the route request initiate node as a malicious node or establish a path from source to the destination again. After establishing a path, it will trace a path from where the data packets will be initiated. If that node is the same as the packet header, then the communication will be continued; otherwise, it will get back to the creation profiling of each node.** When the network throughput is reduced to threshold values, then the IDS node compares the previous profile of each node with the current profile. The node with a mismatched profile will be detected as malicious nodes from the network.

Diagram

Description automatically generated

The reactive routing protocols are which establish a path from source to destination when required. The AODV protocol is the most common and best-performing protocol for path establishment in a mobile ad hoc network. In the AODV protocol, the path is established based on the route request and route reply packets. The source node flood route requests packets in the network, and nodes adjacent to the destination will reply with the route reply packets. The source has multiple destination options, and the best path is selected based on hop count and sequence number. The path with the least hop count and the maximum sequence number is chosen as the best path.

The malicious nodes enter the network, which triggers various types of attacks. In the black hole attack, when the malicious nodes receive the route request packets in the network, it will send route reply packets to the destination. The malicious node also presents its maximum sequence number. The source gets forced to select the path from the malicious node to the destination. When the source sends data, the malicious nodes drop all the packets in the network.

The second proposed methodology is to send a fake route request. The source will find the shortest path to send its data packet to the destination, and to find the shortest path, the source will send a request to all its adjacent nodes, but in this case, the request is fake, and the destination node does not exist in the network. Therefore, a malicious node or black hole node will respond, and we will isolate this node by creating an alert in the system.

## Tool:

NS2 simulator: The Network Simulator (Version 2), or NS2, is a simple event-driven simulation program that has proven beneficial in researching the dynamic nature of communication networks. NS2 can be used to simulate wired and wireless network functions and protocols (e.g., routing algorithms, TCP, UDP). In general, NS2 allows users to specify network protocols and simulate their behavior.[9]

# Chapter - 4

The proposed methodology is about mitigating blackhole attacks in the AODV protocol with the MANETS network in this project. So we had used a process that relies on fake route requests to the network. The proposed methodology is implemented in network simulator version 2. The network simulator version 2 is the simulator that provides both types of simulation, which are text-based and animation. In the NS2, the back end of the simulator is C++, and the front end is TCL. When the script is executed, it provides the trace file and animation file. In table 1, the various simulation parameters are described.

## Implementation

In this part, we created a simulation that represents a blackhole attack and our proposed methodology to mitigate this blackhole attack. The implementation part consists of five parts which are:

1. Deployment of Network
2. The black hole attack simulation.
3. Identification of malicious node.
4. Alerting all the nodes about the malicious nodes in the network.
5. Comparing the quality of services(QoS) of the network with blackhole attack and without blackhole attack.

## Part 1 Deployment of Network.

In this project, we use the same simulation parameters for testing our hypothesis. The following table shows the parameter of the simulation.

|  |  |
| --- | --- |
| **Parameters** | **Value** |
| Number of nodes | 15 |
| Area | 800 \* 800 meters |
| Queue type | Priority Queue |
| Size of Queue | 50 |
| Mobility Mode | Random mobility |
| Link Layer | LL |
| Antenna type | Omi-Directional |

Table 1 Simulation Parameters

The wireless ad hoc network is deployed with 15 mobile nodes. The reactive routing protocol is used in the network for the path establishment of which AODV routing protocol. The source and destination nodes are defined in the network for the data transmission, which is 0 and7. The source node flood *route requests packets* in the network from destination path to destination. The two parameters will be counted for the path establishment, which are *hop count* and *sequence number*.

## Path Establishment

As shown in the below figures, the source node flood the route request packets in the network to establish a path to the destination. **The nodes which are adjacent to the destination will reply to the source with route reply packets.** The nodes which have a direct link to the destination will respond with the route reply packets. The source selects the best path based on the hop count and sequence number. The nodes which have a direct link to the destination will reply with the route reply packets. The source selects the best path based on the hop count and sequence number.

A screenshot of a computer

Description automatically generated

Figure 3 Path establishment

A screenshot of a computer

Description automatically generated with medium confidence

Figure 4

A screen shot of a computer

Description automatically generated with medium confidence

Figure 5

A screenshot of a computer

Description automatically generated

Figure 6

A picture containing text, screenshot, computer

Description automatically generatedFigure 7

A screenshot of a computer

Description automatically generated

Figure 8

A screenshot of a computer

Description automatically generated

Figure 9

By checking the simulation, the shortest path will choose for the communication. In the above simulation, the path will be *0-14-9-7* for communication.

## Part 2: The blackhole attack simulation

We created a black hole. TCL script that represents the simulation of the black hole attacks. We assigned two nodes as our black hole nodes in the network by adding the following parameters to the simulation.

*$ns at 2.4 "$node\_(5) label FAKE-RREP."*

*$ns at 2.6 "$node\_(5) label BLACK-HOLE-NODE."*

*$ns at 2.4 "$node\_(11) label FAKE-RREP."*

*$ns at 2.6 "$node\_(11) label BLACK-HOLE-NODE."*

So the node numbers 5 and 11 will be our malicious node and act as a black hole attack.

The figure below shows that the malicious nodes enter the network, triggering a black hole attack. The malicious node replies with the minimum hop count and maximum sequence number, and the source starts transmitting data through a malicious node. The screenshots below show us that all the shortest route for the destination is 0 – 5, but node 5 is our malicious blackhole node.

Graphical user interface, application

Description automatically generated

Figure 10

A screenshot of a computer

Description automatically generated

Figure 11

## Part 3: Identification of Malicious nodes.

We first initiate fake route requests in the network by requesting an unknown node that is randomly chosen.

# Provide the initial location of mobile nodes  
$ns at 0.0 "$ns trace-annotate \"Network Deployed\""  
$ns at 0.0 "$ns trace-annotate \"NODE0 became a SOURCE\""  
$ns at 0.0 "$ns trace-annotate \"NODE7 becme a DESTINATION\""  
$ns at 0.5 "$ns trace-annotate \"NODE0 flood FAKE-RREQ packets with FAKE-DESTINATION-ADDRESS\""  
$ns at 2.0 "$ns trace-annotate \"NODE11 and NODE5 flood FAKE-RREP with threr ID\""  
$ns at 2.5 "$ns trace-annotate \"NODE0 generate ALARM-MESSAGE and flood to all nodes\""  
$ns at 2.7 "$ns trace-annotate \"NODE11 and NODE5 ISOLATED from network\""  
$ns at 3.0 "$ns trace-annotate \"NODE0 flood RREQ packets\""  
$ns at 4.1 "$ns trace-annotate \"NODE5 flood RREP packets\""  
$ns at 4.7 "$ns trace-annotate \"Show all paths\""  
$ns at 5.0 "$ns trace-annotate \"DATA-TRANSMISSION\""

In the above coding, we set the nodes. So for node0, the source node that requests the fake route request and the malicious nodes will respond to this with a fake route reply. From that, we can identify these nodes as malicious.

As illustrated in the figure, whenever we need to identify the malicious node, the source node requests a fake route request and broadcasts this route request into the network. Considering the network, if any adjacent node has the path of this request, it will reply; otherwise, no one will respond to this request. If the malicious node replies to this request stating that it has the shortest path, we will determine that this node is malicious, and by alerting every other node, we can isolate them.

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

––A picture containing text, screenshot, computer, computer

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

## Part 4 Alert the others.

In this phase, we will generate the alert as a broadcast message excluding the malicious node. We will tell other adjacent nodes that nodes 5 and node 11 are malicious in the alert message. After the alert, we will restore the communication.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Comparison

We conducted this experiment and compare our solution with a conventional protocol with blackhole nodes. As we can see, the results are represented as the blue line in the graph.

The time duration is displayed on the x-axis, and the number of the packet is displayed on the y-axis.

Graphical user interface, chart

Description automatically generated

The above graph shows the delay comparison for the old and new simulations of the blackhole attack. The upper line shows that the delay is more significant while having a black hole attack.

Chart, line chart

Description automatically generated

The above graph shows that a drastic drop in the throughput and the sudden line indicate that the throughput is less, which belongs to the old simulation. In comparison, throughput is high on new simulations.

Chart, box and whisker chart

Description automatically generated

The above graph shows that the packet loss is high on the old simulation, which contains the black hole nodes, while you can see that the packet loss is so low in the isolated simulation.

## Problems and outcomes:

We tried several ways to implement our first hypothesis to create an IDS node, but due to complexity in the project and the coding, we did not succeed, and the results are not as projected. So, we use our second methodology, fake route deployment, and succeed in performing the isolation of the malicious node.

# Chapter - 5

## Conclusion:

To develop the methodology, we studied several research papers related to AODV protocol and MANETs. Moreover, we had also learned about the NS2 simulator using the NS2 simulator Guidebook. Further, we had tried various simulation scenarios to fulfill our hypothesis to mitigate the blackhole attack in the MANETs.previously, our agenda was to develop an IDS node in the network. We had tried various methods to implement them. Still, due to a shortage of time, we could not pursue the modification of AODV. Finally, In the end, we come up with one suitable solution that is a fake route request.

To sum up, to meet our hypothesis, we finally managed to isolate the malicious node by alerting the adjacent node in MANETs using the fake route request methodology in the NS2 simulator.

## Implications

### Limitations and weaknesses

the problem arises If the network is vast and a source node sends a fake route request for the fake node and that fake node is present in the network. But we can solve this problem by verifying it with the adjacent node.

### Challenges

While implementing this approach, we have faced isolating the malicious node and alerting the neighboring node about this malicious node. Also, we want to present a routing table for each simulation, but we could not find a reliable method to get the result due to time constraints. The results are significant regarding the network's quality of service(QoS), but we can further improve it by optimizing our code.

### Future Work

Following are the various future possibilities of this work:-

1. The proposed approach will be further improved to isolate cooperative blackhole attacks in mobile ad hoc networks.
2. The proposed approach can extend to various other types of attacks like distributed denial of service attacks.
3. In the future, we can also try to implement this methodology in physical devices.

## Recommendation

Further, we can improve this approach by introducing more security functions like node profiling, and other QoS (Quality of Service) controls.

## Summary

MANETs comprise several movable nodes and interact with other nodes through data packets moving in the multi-hops without a central regulator. These networks contain a huge number of movable hosts which utilized wireless connections for contact with one another. The mobility of the nodes is of the arbitrary kind in any route because this network does have any infrastructure. The black hole attack is the type of attack which affects network performance to a great extent. In the black hole attack, the source transmits information through a malicious node which drops all the data. Therefore, we proposed a fake route request methodology that only depends on nodes in the network to isolate the malicious nodes. The proposed approach is implemented in NS2, and it is analyzed that performance of the proposed approach is excellent in terms of specific parameters like throughput, delay, and packet loss.

# Acronyms:

1. AODV: Ad Hoc On-Demand Distance Vector Routing
2. MANET: Mobile Ad-hoc network
3. IDS Node: Intrusion Detection System's Node
4. AODV: Ad Hoc On-Demand Vector Routing Protocol
5. MANETs: Mobile Ad Hoc Networks
6. CBR: Constant bitrate
7. VBR: Variable bitrate
8. UDP: User Datagram Protocol
9. TCP: Transmission Control Protocol
10. NS2: Network Simulator

# References:

1. S.Umang, BVR Reddy, MN Hoda, "Enhanced intrusion Detection System for Malicious Node Detection in ADHoc Routing Protocols using Minimal energy Consumption", IET Communications volume 4, issue 17, pp-2084-2094. 2010.
2. B Wu, J Chen, J Wu, M Cardi, "A survey of attacks and countermeasures in mobile Adhoc networks", Wireless network security, volume 15, issue 7, pp-103-135, 2007.
3. A. Shastri, R. Dadhich, and R.C. Poonia, "Performance analysis of on-demand Routing protocols for vehicular ad-hoc Networks", International Journal of Wireless & Mobile Networks (IJWMN) Vol 3, issue 6, pp-103-111, 2011.
4. Elmahdi, E., yoo, S.-M., & Kumar, S. (2018). Securing Data Forwarding against Blackhole Attacks in Mobile Ad Hoc Networks. *IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, 463–467. https://twin.sci-hub.do/6705/6fe203b5a09bb11e0d2a323d45411823/elmahdi2018.pdf#view=FitH
5. Tripathi, A., & Mohapatra, A. K. (2016). Mitigation of Blackhole attack in MANET. *2016 8th International Conference on Computational Intelligence and Communication Networks*, 437–441. https://twin.sci-hub.do/6574/e4300e3ffd7513cda7a87da0905eaa07/tripathi2016.pdf#view=FitH
6. Deshmukh, S. R., Chatur, P. N., & Bhople, N. B. (2016). AODV-Based Secure Routing Against Blackhole Attack in MANET. *IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20–21, 2016, India*, 1960–1964. https://twin.sci-hub.do/6234/23c56e2ce01114ac3de3bcfe1f0e7271/deshmukh2016.pdf#view=FitH
7. Li, G., Yan, Z., & Fu, Y. (2018). A Study and Simulation Research of Blackhole Attack on Mobile AdHoc Network. *IEEE CNS 2018 - 1st International Workshop on System Security and Vulnerability (SSV)*, 1–6. https://twin.sci-hub.do/7060/72815c8f72515a59c9f6652e54386b8e/li2018.pdf#view=FitH
8. Oddi, G., Macone, D., Pietrabissa, A., & Liberati, F. (2012). A Proactive Link-Failure Resilient Routing Protocol for MANETs based on Reinforcement Learning. *2012 20th Mediterranean Conference on Control & Automation (MED) Barcelona, Spain, July 3–6, 2012*, 1259–1264. <https://moscow.sci-hub.do/2157/1e21c2c777dd4c28b8e80227a407a924/oddi2012.pdf#view=FitH>
9. Issariyakul, T. (2012). *Introduction to Network Simulator 2 (NS2)*. SpringerLink. <https://link.springer.com/chapter/10.1007/978-1-4614-1406-3_2?error=cookies_not_supported&code=3f9294fb-56f4-47d7-b849-47029ccc3237>
10. S. Hazra, and S.K. Setua. “Black Hole Attack Defending Trusted On-Demand Routing in Ad-Hoc Network.” In Advanced Computing, Networking and Informatics-Volume 2, issue 9, pp.59-66, Springer International Publishing, 2014.
11. MS Alkatheiri J Liu, A R Sangi, “AODV Routing Protocol under several Routing Attacks in MANETs” In Communication Technology (ICCT), 2011 IEEE 13th International Conferenceon, volume 6, issue 19, pp.614-618, IEEE, 2011.