Enhancing Security for MANETs against Black hole attacks

Anbarasan K, Lokesh Kumar S, Kanthimathi S*, Sivakami Raja
Vellore Institute of Technology, Chennai, Tamilnadu, India.
kanthimathi.s@vit.ac.in

***Abstract*— Mobile Ad Hoc Networks(MANETs) are highly scalable in nature because of the extensive availability of mobile devices and are used for many critical employments like emergency preparedness and response, military crisis operations etc. Because of MANETs unique features such as self-configuration and infrastructure-less property, they are vulnerable to many routing attacks. Black-hole attacks are considered to be extremely dangerous in cases of critical applications where loss of data can lead to loss of money, and in military situations, loss of lives. Plenty of research has gone to the development and maintenance of security in MANETs but still security in wireless network is questionable. The existing solutions responds slow in detecting the malicious node and by this time the host could lose data of significant value. The prime focus of this research is to detect Black-hole attacks in MANETS. Our proposed approach is faster since it doesnt use a timing constraint unlike the Cooperative Bait detection scheme in short CBDS, rather uses a Modified Bait Scheme to the network, which in turn reduces the time and computation overhead to find the black-hole nodes. Simulation results show that performance is readily increased compared to base approaches.**

Keywords: Mobile-AdHoc-Network(MANET), Cooperative Bait Detection scheme (CBDS), blackhole, Modified Bait Scheme.

I. INTRODUCTION

Due to extensive availability of mobile devices, a lot of research has gone into the development of MANETs and it is widely used. Mobile Ad Hoc Network (MANET) is also referred to as wireless Ad Hoc network or mesh mobile network. An ad hoc network consists of a network in which individual devices communicate with each other without using any WAP (Wireless Access Point) devices i.e, it communicates directly with each other. MANETs are self-configuring Ad Hoc networks i.e., its free to move independently in any direction and change its links to other mobile devices. In MANETs each node in the network can send and receive routing requests and therefore acts like a router or a host. Due to their infrastructure-less property and self-configuring nature, it poses serious drawbacks from security point of view, like routing attacks. We focus on black-hole a attack that falls under Denial-of-Service of routing attacks. Black-hole attack is an attack on routers where the malicious node sends a router reply stating that, the shortest distance to destination is through the malicious node.

II. MOBILE AD HOC NETWORKS (MANETS)

A wireless ad-hoc network is an combination of portable/semi-versatile hubs with no pre-built up foundation, shaping a very small network. Every node of the hub has a wireless interface and interact with each other over either using radio or infrared. PCs advanced collaborators that discuss specifically with each other are a few cases of nodes in an ad-hoc network. Hubs in the ad-hoc network are usually portable, however could also be stationary hubs [2]. Semi-adaptable hubs can be utilized to shift focuses in different regions. The farthest hubs are not inside the transmitter's scope of area. However, the hubs coming in the pivotal region can be utilized to forward packets between the distant hubs. The hub in the central region is going about as a switch and the three hubs have framed an ad-hoc network.

III. LITERATURE SURVEY

Thani Kanti Sudhakar Babu et al [1] discussed a secure neighbor selection approach with recurrent reward integration using machine learning in mobile ad hoc networks. This method has three phases they are state determination, multi attribute analysis and route selection in which state determination will protect nodes from being contaminated from the attacker, whereas the multi attribute analysis we can find which node is suitable for transmission with the available neighbor nodes, so that even if the properties of the neighbor node change it does not create a major impact in transmission, finally it will select which node is suitable. All these three methods pre classify the node states and based on their communication behavior it will estimate neighbor rewards. The limitation of this proposed method is, the scalability of the system is poor so that it will become challenge when we are implementing this method in a large scale.

S. Naveena et al [2], discuss employing trust-based analysis and countermeasures to identify and segregate secured nodes from unsecured or attacker nodes using a trust-based routing scheme. In the trust initialization stage, every node in the network is allocated a basic trust value of 0.5. In the subsequent stage, a confidence factor is determined and extended to a data routing table. From this table, the determined trust value level is compared to a threshold value. If the value reaches the threshold, the node is set to 0, indicating it as an untrustworthy node. Conversely, if it does not reach the threshold, the node is set to 1, signifying it as a trustworthy node. Consequently, the black hole attack is reduced, thereby reducing the packet drop ratio. However, it is noted that this approach leads to high energy consumption in MANET nodes.

Dac - Nhuong Le [3] discussed how the Dual Cooperative Bait Detection Scheme is differ from the traditional Cooperative Bait Detection Scheme. In the conventional cooperative bait detection scheme (CBDS) the selected adjacent node will send the RREP message if it identifies any malicious node and it

will initiate the back tracking of malicious node. However, if that selected adjacent node itself a malicious node then CBDS will fail. So, in order to overcome this, they have come up with the method of Dual Cooperative Bait Detection Scheme, this method will not depend on the single neighboring node but on two so that even if both node is malicious, they will report each other by sending the RRPE message and so the we can identify the nodes which is malicious even if the initially selected adjacent node is malicious.

Rashmi Ramesh et al [4] discussed that the AODV protocol, routing, algorithm that helps in detecting and preventing from blackhole attacks. AODV is a lightweight process to identify the blackhole attacks and hence it helps to reduce delay in reaching the destination. The methodology is not feasible to hold the blackhole nodes, a threshold time is sent with RREQ and RREP is received then it is not blackhole nodes. The mobility speed is varying when compared in performance by SMCBA scheme and already existing blackhole detection scheme. Fake reply messages are accounted in blackhole list. False and shortest path can be achieved by SMBCA process. The logistic chaotic map which has details about all neighbouring nodes.

Fatima El Haoussi et al [5] used a technique to eliminate risk and surround blackhole by messages and timer. In the verifying if the fake messages are not identified then it comes under blackhole list. Then it cannot be contacted to the neighbouring nodes. To avoid overloading by the false demands, the timer gets modified when sending messages. The PDR which is implied for the performance through the sum of packet obtained by sum of packet sent with hundred units. The data received and sent are calculated to find the Throughput (TH) and the time of packet sent and received are calculated then the PacketLoss(D) is found. MANET has a major drawbacks in central control and infrastructure. The prevention of blackhole attacks are by modifying AODV protocol uses bait and timer methods. The BTT testing is found by takin the ratio of packet delivery and packet loss through NS3 simulator which is useful in solving the problems.

Nitika Kapoor et al [6] outlined a technique for detecting and averting black hole attacks in Multi-Agent Networks (MANETs) using a recognizing and avoidance system (DPS). This method has three categories of nodes they are normal node, malicious nodes and DPS nodes in which DPS nodes plays a vital role. The Normal nodes will transmit the date packets to the other adjacent nodes, whereas the malicious black hole node will not transmit the request to the other nodes instead it will absorb the request so that the total request transmission count is very less when compared to other normal nodes, finally the DPS node will evaluates other nodes based on the total transmission count and when it encounters a node that has less transmission rate, it will label that node as black hole node.

IV MODIFIED BAIT SCHEME

The problem with MANETs is that it is susceptible to black hole attacks. Black hole nodes are the attacker nodes that pretend as if they have route to destination and drop all the packets received from the source. Hence there's data loss happening in the network. In the proposed algorithm that is modified bait scheme, we set the destination to be an invalid node and broadcast the bait request to all nodes in the system and only the blackhole nodes respond to this request saying they have route to destinations. Once we have identified them, we blacklist them and create an alternate path between source and destination which doesn't include any of the blackhole nodes. Thus, data gets delivered from source to destination safely without getting lost.

A. Sequence Diagram

A succession chart or sequence model in unified modeling language (UML) is a sort of interaction graph that demonstates every component as protest, how they work with each other and in what arrange. Arrangement Diagram has parallel vertical lines speaking to life savers of each question. It demonstrates every one of the messages being traded among those articles. Arrangement graph speaks to the activation time of each protest. Figure 1 shows the sequence diagram of the Modified Bait Scheme.

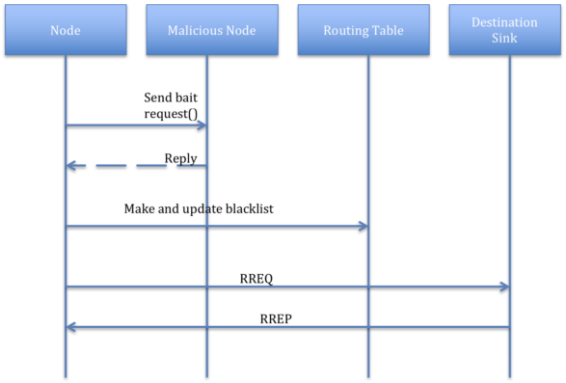


Fig 1: Sequence diagram

B. Flow chart

The flow chart given in Fig 2 consists of the following:

- Initiate Network :- A MANET network is created using Network Simulator ns2 version 2.34. The network comprises of mobile and randomly distributed nodes.
- Introducing Attack :- We introduce a blackhole attack by configuring few of the nodes as malicious in the network.
- Create a Blacklist :- Assign an array of some specified length to which we add the index of the blackhole nodes

  present in the network.
- Send bait RREQ: - The origin node sends a bait request RREQ to the adjacent node with a destination node index which is not present in the network.
- Receive a reply RREP :- If a reply is received, the index of the node which sends a reply to this previously send RREQ, the index of that node is added to the blacklist to ensure that no packets are sent to this malicious node.
- No reply received :- If no reply is received, this means there are no blackhole nodes in the network and hence,

the packet delivery takes place normally.

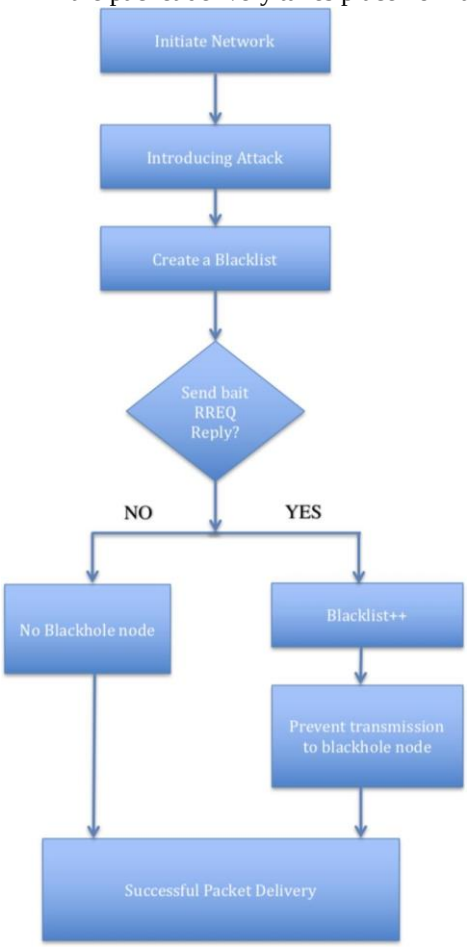


Fig 2: Flow diagram

- Prevent transmission to blackhole nodes: - Each time an origin node wants to a forward a packet to a destination, it avoids sending that packet to a blackhole node by referring the blacklist.
- Successful Packet delivery: - After the identification and prevention of blackhole nodes, the packet is delivered successfully.

V. PROCESSING STEPS

To prevent the black-hole attack in the network we use a Modified Bait Scheme. The steps involved in the processing are:

- A MANET network is created using Network Simulator ns2 version 2.34. The created network comprises of mobile and randomly distributed nodes and every node in the system behaves as a host as well as router.
- We introduce a black-hole attack by configuring few of the nodes as malicious in the system. These harmful nodes drop the routing packets but does not forward packets to its neighbours.
- Assign an array of some specified length to which we add the index of the black-hole nodes present in the network.
- The source node sends a bait request RREQ to the surrounding node with a destination node index which is not present in the network. The network becomes in bait mode when the RREQ' is used for routing and while waiting for a reply for this RREQ'
- When the bait routing request is recieved by a blackhole node, then it replies with a fake route reply. Once we get the false reply then we can identify the black hole node.
- If there is no RREP is received, this means there are no harmful nodes in the system and hence, the packet delivery takes place normally.
- After the recognition and avoidance of black-hole nodes, the packet is delivered successfully.

A. Modified Bait Scheme

- Make a blacklist array
- Send Bait request
- Check for nodes that give RREQ.
- Note the index values of these nodes and add them to the blacklist.
- Send the blacklist to the routing table.
- Prevent transmission of the data from or to these nodes.

VI. SIMULATION

Simulation is process of imitation of a certain activity of a functionality, process or a system. These imitations or simulations are enacted under similar conditions as the original activity takes place. A model is created so that it simulates a certain function or activity, this model addresses key characteristics, activities or processes, even the structure of the enacted model. This helps the simulation to address the task on the model, which addresses the system itself.

We have conducted two test cases as follows:

Simulation Test Case ID	Test case 1
Description	To test the default aodv routing protocol in presence of blackhole nodes.
Input	Link aodv.cc file to point to default aodv.
Expected Output	No transmission takes place.
Actual Output	No transmission took place.
Remarks	Passed

Fig 3: Test Case 1

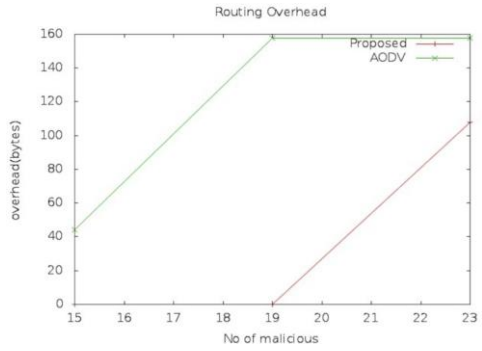
Simulation Test Case ID	Test Case 2
Description	To test the aodv routing with the modified bait algorithm.
Input	Link aodv.cc file to point to blackhole_aodv which has modified bait algorithm.
Expected Output	Nodes should find an alternate path to the destination and packets must be sent from source to the destination.
Actual Output	Nodes found out an alternate path from source to destination and most of the packets from source were received at destination.
Remarks	Passed

Fig 4: Test Case 2

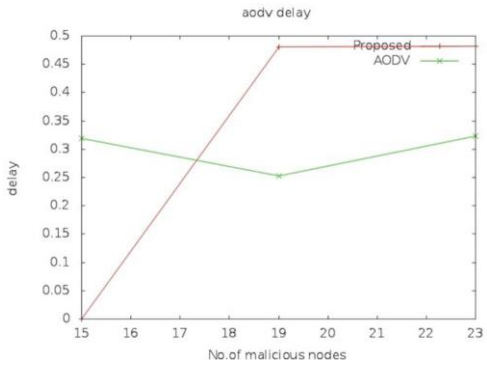
A. Results:

The results we got for the simulations were:

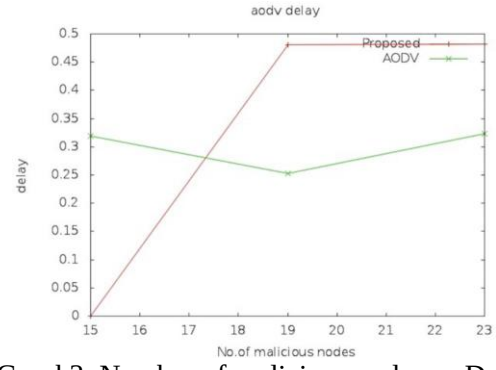
1) Routing Overhead: The routing overhead for the default aodv is very high compared to modified bait scheme, this happens due to the existence of harmful nodes in default aodv (Graph 1). It finds it very difficult to establish any path between source and destination, thus increasing routing overhead. And in modified bait scheme since we have blacklisted all the blackhole nodes, establishing a route between source and destination becomes simpler.



Graph 1: Number of malicious nodes vs Routing Overhead



Graph 2: Number of malicious nodes vs Throughput



Graph3: Number of malicious nodes vs Delay

2) Throughput: In throughput graph (Graph 2), as we can see that throughput for the default AODV is almost constant as there is no transmission taking place between Source and destination. In case of modified bait scheme which is proposed approach, throughput increases with raise in number of harmful nodes thus depicting the effectiveness of proposed approach.

3) Delay: In delay graph (Graph 3), As we can see that delay for the default AODV routing protocol is almost constant as there is no transmission taking place between source and destination. In case of modified bait aodv (proposed) scheme, the delay increases as the number of malicious nodes increases. This happens because, when the number of malicious nodes increases it takes time to establish path between source and destination nodes.

C. Future Enhancement

• This implementation can be further improvised by considering other parameters of the network for identifyinand blacklisting malicious nodes.

• This approach solely concentrates on sending bait request and identifying malicious nodes and thereby blacklisting them.

• This method can be implemented for networks which are more stable for more efficient routing.

• This can be implemented for AMMNETs to avoid network partitioning malicious node.

VII. CONCLUSIONS

The graphs above demonstrates that the Modified bait scheme will be effective to identify and keep the blackhole attacks on MANET under AODV protocol. Our algorithm will give ample security for the MANET and also will keep the network free from blackhole attacks. The algorithm also makes sure that the system is lightweight and get a good throughput value and lesser delay in packets. Essentially making the network active and wroking even in the sight of blackhole nodes. From the above results, we conclude that the proposed plan will proficiently distinguish and avert blackhole assault in MANETS.

A. Assumption

We consider a adhoc wireless network with the set of nodes and assuming that there is a possibility of one or more attacker nodes. Thereby we implement our proposed algorithm in order to prevent and avoid the attacker node from the network.

B. Limitations

In our approach, we have only considered a single parameter for detecting the black-hole nodes i.e, the reply to the bait request. Whenever a malicious node gives a reply to bait request, the details of that node is added to the blacklist. There can be several other parameters that can be taken into account such that it doesn't compromise with the time taken to detect malicious node.

REFERENCES

[1] Thanikanti Sudhakar Babu and Hassan Haes Alhelou, “A Recurrent Reward Based Learning Technique for Secure Neighbour Selection in Mobile AD-HOC Networks”, January 28, 2021.

[2] S. Naveena, C. Senthilkumar and T. Manikandan, “Analysis and Countermeasures of Black-Hole Attack in MANET by Employing Trust-Based”, 2020 6th International Conference on Advanced Computing & Communication Systems (ICACCS).

[3] Dac-Nhuong Le, “Efficient Dual-Cooperative Bait Detection Scheme for Collaborative Attackers on Mobile Ad-Hoc Networks”. December 15, 2020

[4] Rashmi Ramesh, G.Seshikala , “Link Aware Multipath Routing to Defend Against Black Hole Attacks for MANETs”, 2023 3rd International Conference on Intelligent Technologies (CONIT)

[5] Fatima El Haoussi, Nabil El Akchioui, Nabil El Fezazi, Youssef El Fezazi, Said Idrissi, “Detecting black hole attacks in MANET using baiting and timer technique with AODV protocol”, 2023 9th International Conference on Optimization and Applications (ICOA)

[6] Nitika Kapoor, Imran Ali Shah, “To Detect and Prevent Black Hole Attack in Mobile Ad Hoc Network”, 2021 2nd Global Conference for Advancement in Technology (GCAT)

[7] H. Xia, F. Xiao, S.-S. Zhang, X.-G. Cheng, and Z.-K. Pan, ‘‘A reputationbased model for trust evaluation in social cyber-physical systems,’’ IEEE Trans. Netw. Sci. Eng., vol. 7, no. 2, pp. 792–804, Apr. 2020.

[8] S. K. Prasad, J. Rachna, O. I. Khalaf, and D.-N. Le, ‘‘Map matching algorithm: Real time location tracking for smart security application,’’ Telecommun. Radio Eng., vol. 79, no. 13, pp. 1189–1203, 2020

[9] Saudi, NurAmirahMohd, et al. "Mobile Ad-Hoc Network (MANET) Routing Protocols: A Performance Assessment. "Proceedings of the Third International Conference on Computing, Mathematics, and Statistics” (iCMS2017). Springer, Singapore, 2019

[10] X. Hu, H. Zhang, D. Ma, and R. Wang, ‘‘A tnGAN-based leak detection method for pipeline network considering incomplete sensor data,’’ IEEE Trans. Instrum. Meas., early access, Dec. 18, 2020, doi: 10.1109/ TIM.2020.3045843

[11] M. Shukla, B. K. Joshi, and U. Singh, ‘‘Mitigate wormhole attack and blackhole attack using elliptic curve cryptography in MANET,’’ Wireless Pers. Commun., vol. 121, no. 1, pp. 503–526, Nov. 2021, doi: 10.1007/s11277-021-08647-1.

[12] R. Wang, Q. Sun, D. Ma, D. Qin, Y. Gui, and P. Wang, ‘‘Line inductance stability operation domain assessment for weak grids with multiple constant power loads,’’ IEEE Trans. Energy Convers., early access, Sep. 2, 2020, doi: 10.1109/TEC.2020.3021070

[13] Malnar, M., & Jevtic, N. (2022). An improvement of AODV protocol for the overhead reduction in scalable dynamic wireless ad hoc networks. Wireless Networks, 28(3), 1039-1051.

[14] Gurung, S.; Chauhan, S. A survey of black-hole attack mitigation techniques in MANET: Merits, drawbacks, and suitability. Wirel. Netw. 2020, 26, 1981–2011.

[15] L. Yang, A. Moubayed, and A. Shami, ‘‘MTH-IDS: A multitiered hybrid intrusion detection system for Internet of Vehicles,’’ IEEE Internet Things J., vol. 9, no. 1, pp. 616–632, Jan. 2022

[16] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, ‘‘Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles,’’ IEEE Access, vol. 8, pp. 199618–199628, 2020.

[17] M. D. Chawhan, K. D. Kulat, S. B. Pokle and A. U. Khan, “An Advanced Trust-Based Routing Protocol for Mobile AdHoc Network under Blackhole Attack,” Biosci. Biotechnol. Res. Commun., vol. 13, no. 14, pp. 120–124, 2020