www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-1, Issue-2, June- 2013
Research Paper

Int. J. Sci. Res. in
Network Security
and Communication
ISSN: 2321-3256

An Implementation of the Gray Hole Prevention Technique for MANETs Based on Sequence Number

Vaibhav Jain

Department of Computer Engineering, Institute of Engineering and Technology, DAVV Indore- India

Received: 17 March 2013 Revised: 22 May 2013 Accepted: 11 June 2013 Published: 30 June 2013

***Abstract*- Protecting the network layer from malicious attacks is an important and challenging security issue in mobile ad hoc networks (MANETs). MANETs are used most commonly all around the world because it has the ability to communicate with each other without any fixed network. It has the tendency to take decisions on its own which is the autonomous state. A security solution is very much needed for networks to protect both route and data forwarding operations in the network layer. A Gray Hole is a node that selectively drops and forwards data packets after it advertises itself as having the shortest path to the destination node in response to a route request message from a source code. Gray holes are difficult to detect. In this work, we have proposed a method that can be used to find the secured routes and prevent the black holes nodes (malicious nodes) in the MANET by checking whether there is a large difference between the sequence number of the source node or intermediate node. For this, we have created 3 scenarios for implementation i.e. Normal AODV, AODV with attack, and AODV with gray hole prevention. Our results confirm that our proposed prevention technique based on sequence number was effective and successful in identifying Gray Hole nodes in a network and could remove these malicious nodes from the network.**

Keywords- *Gray Hole Prevention, MANET security, Ad hoc Network Security*

I. INTRODUCTION

The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the public networks. Security is an essential requirement in MANETs. However, MANETs are vulnerable to various types of attacks including passive eavesdropping, active interfering, impersonation, and denial-of-service attacks. Among these types of vulnerabilities, security of routing protocols is a big challenging task. A set of nodes may be compromised in such a way that it may not be possible to detect their malicious behaviour easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and flood other nodes with routing traffic.

One of the widely known attacks is the Gray Hole attack. It is the variation of Black hole attack in which traffic is redirected to such a node that actually does not exist in the network and that node drops the entire packets. But in Gray Hole attack, nodes will drop the packets selectively. Gray Hole attack is launched by a single malicious node or cooperatively by a set of malicious nodes. Among the various routing protocols available for MANETs, AODV is most vulnerable to such attacks. AODV is susceptible to Gray Hole attacks due to its inherent characteristics and the lack of security mechanisms in the protocol. Following are the reasons why AODV is vulnerable to Gray Hole attacks:

- *Lack of authentication:* AODV does not provide strong mechanisms for authenticating nodes in the network. This means that any node can claim to be a legitimate part of the network and participate in the routing process. A malicious node can impersonate a valid node and attract traffic towards itself, selectively dropping or modifying packets.
- *Route discovery process:* AODV relies on the route discovery process, where nodes broadcast route request (RREQ) packets to find a route to the destination. During this process, intermediate nodes can respond with route reply (RREP) packets if they have a valid route to the destination. However, a malicious node can intercept and modify these RREQ or RREP packets to redirect traffic toward itself or disrupt the communication.
- *Lack of route verification:* AODV does not have a mechanism to verify the integrity or authenticity of the received routing information. When a node receives a route, it assumes that the information is valid and uses it for forwarding packets. A malicious node can exploit this lack of verification to provide false routing information, leading to traffic being redirected or dropped.
- *Cooperative behaviour assumption:* AODV assumes that nodes in the network will cooperate and follow the protocol's guidelines. However, in a gray hole attack, a malicious node behaves selectively, dropping or modifying packets only for certain communication flows while allowing others to pass through normally. This

*Corresponding Author: *Vaibhav Jain, vabyjain@gmail.com*

behaviour violates the cooperative assumption of AODV and can disrupt the network's overall performance.

-

To mitigate the gray hole attack vulnerabilities in AODV, additional security mechanisms can be employed, such as node authentication, secure route discovery, and route verification techniques. These enhancements can help ensure the integrity and trustworthiness of the routing process in ad hoc networks.

II. RELATED WORK

The problem of security and cooperation enforcement has received considerable attention by researchers in the ad hoc network community. Marti et al. [1] proposed to trace malicious nodes by using a watchdog and pathrater approach. It uses a pathrater algorithm where each node uses the watchdog's monitored results to rate its one-hop neighbours. Further the nodes exchange their ratings, so that the pathrater can rate the paths and choose a path with the highest rating for routing. The shortcoming of this approach is that the idea of exchanging ratings genuinely opens door for blackmail attack. Another approach proposed in [2] exploits two ideas to protect the mobile ad hoc networks. It used local collaboration and information cross-validation to prevent from gray hole attacks. In this approach, once a malicious node is convicted by its neighbours, the network reacts by depriving its right to access the network by revoking its token.

Ramaswamy et al. [3] presented an algorithm which claims to prevent the cooperative black hole attacks in ad-hoc networks. In this approach, each node maintains an additional data routing information table to identify trustworthy node in the network. However, it fails to prevent from gray hole attacks. Agrawal et al. [4] proposed a technique for detecting chain of cooperating malicious nodes in ad hoc networks. In this proposed approach, initially, a backbone network of strong nodes is established over the ad hoc network. Each strong node is assumed to be a trustful node. However, the approach would not work if an intruder attacks strong nodes because it violates the assumption that strong nodes are always trusted nodes.

Nadeem et al. [5] use a combination of anomaly-based and knowledge-based intrusion detection to secure MANETs from a wide variety of attacks. Deng et al. [6] have suggested a mechanism of defense against a black hole attack on AODV routing protocol. The proposed scheme completely eliminates the black hole attached by a single attacker, it fails miserably in identifying a cooperative black hole attack involving multiple malicious nodes. Researchers have also investigated means of discouraging selfish routing behaviour in ad hoc networks, generally through payment schemes [7]. These approaches either require the use of tamper-proof hardware which may not be appropriate in some truly ad hoc network scenarios. In Padilla et al. [8] approach, a mechanism to identify nodes that attempt to create black hole attacks in MANETs. It detects an attack by topology graph, looking at the number of neighbours a node claims to have and the actual number of neighbours according to the graph.

Banerjee [9] proposed a mechanism for the detection/removal of cooperative black and gray hole attack. In this approach, instead of sending the total data traffic at a time, it divide the total traffic into some small-sized blocks. Overall the approach is not efficient as it takes time in converting of total traffic into small-sized blocks. Sen et al. [10] proposed a mechanism to detect and defend the network against such an attack which may be lauched cooperatively by a set of malicious nodes. Himral [11] suggested a solution for identifying the malicious node in AODV protocol by using destination sequence number field. Their approach compares the first destination sequence number with the source nod sequence number, if there exist much more differences between them, surely that node is the malicious node and removes the entry of the malicious node from the routing table.

III. SECURITY CHALLENGES WITH MANET'S LIMITATIONS

The following is the list of limitations that could deter the security of such networks.

- *Limited Memory and Storage Space* – A mobile node is a tiny device with a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm.

- *Power Limitation* - Energy is the biggest constraint to mobile node capabilities. When implementing a cryptographic function or protocol within a mobile node, the energy impact of the added security code must be considered. The extra power consumed by mobile nodes due to security is related to the processing required for security functions.

- *Unreliable transferring of Packets* – Normally the packet-based routing of the mobile network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. More importantly, if the protocol lacks the appropriate error handling it is possible to lose critical security packets.

- *Packet Conflicting* – Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless mobile network. If packets meet in the middle of the transfer, conflicts will occur and the transfer itself will fail. This could lead to various security threats in such situations. A malicious node can capture an entire network and act as a network leader by broadcasting the biggest sequence number. It can become a black hole to the entire sub-network.

IV. GRAY HOLE ATTACKS IN MANETS

In Mobile Ad hoc Networks (MANETs), a gray hole attack is a type of security threat where a malicious node selectively drops or modifies network traffic, causing disruption or unauthorized manipulation of communication within the network. This attack can have serious consequences in MANETs, where nodes dynamically form a network without relying on a centralized infrastructure.

In a gray hole attack, the malicious node behaves in a deceptive manner by selectively participating in the routing process. It may drop or modify packets for specific flows or destinations while allowing others to pass through normally. This targeted manipulation of network traffic can lead to various harmful effects, including:

Packet loss: The malicious node selectively drops packets, causing loss of data or disruption in the communication flow. This can impact the reliability and performance of the network.

Routing disruption: By dropping or modifying control packets, the malicious node can disrupt the routing process. It can manipulate route request (RREQ) or route reply (RREP) packets to mislead other nodes about the available routes, leading to routing failures or inefficient routing paths.

Traffic redirection: The attacker may redirect traffic towards itself, acting as a malicious intermediate node. This can allow the attacker to eavesdrop on sensitive data or launch further attacks on the network.

Denial of Service (DoS): By selectively dropping or modifying packets, the attacker can launch a DoS attack on specific nodes or entire network segments. This can degrade the overall network performance or render certain nodes or services unavailable.

Gray hole attacks exploit the cooperative nature of MANETs, where nodes rely on each other for relaying packets and establishing routes. The attacker takes advantage of the lack of centralized control and the absence of strong security mechanisms in the network.

V. PROPOSED SEQUENCE NUMBER BASED PREVENTION TECHNIQUE

Our proposed technique makes use of sequence numbers in routing information between neighbours to detect Black Holes and Gray Holes.

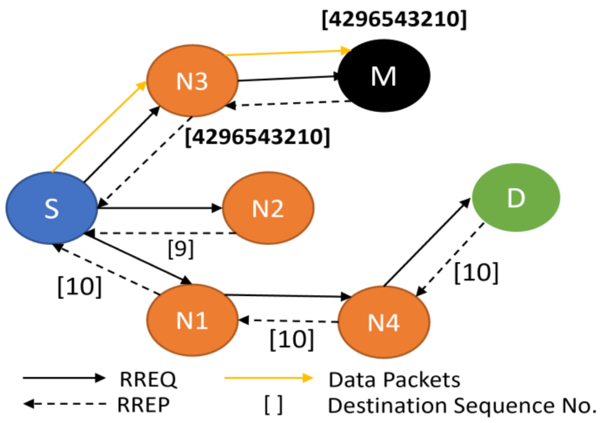

Fig. 1: AODV Protocol Packet Exchange Example

As shown in Fig. 1, destination sequence number is a 32-bit integer associated with every route and used to decide the freshness of a particular route. The larger the sequence number, the fresher is the route. Node N3 will now send it to a node. Since nodes N1 and N2 do not have a route to node D, they would again broadcast the RREQ control message. RREQ control message broadcasted by node N3 is also expected to be received by node M (assumed to be a malicious node). Thus, node M would generate false RREP control message and send it to node N3 with a very high destination sequence number, that subsequently would be sent to Node S. As per AODV, node S would start sending data packets to node N3. But, in our proposed approach, AODV before sending data packets, node S will check the difference between sequence numbers. If it is too large, obviously the node will be identified as malicious one, and it will be isolated from the network.

5.1 Algorithm for Prevention Technique

Here, we present an algorithm used for the prevention of Gray Hole attacks in MANETs. The logic is implemented through ReceiveReply method of AODV. So, whenever ReceiveReply method will be called, given below method would be called and later normal AODV ReceiveReply method would be called upon.

ReceiveReply Method, Parameters: DSN – Destination Sequence No., NID – Node ID, MNID – Malicious Node ID {keyword: RR – Table – Routing Table, SSN – Source Sequence No.}

Step 1 : Initialization Process
Start the route discovery phase with the source node S.

Step 2: Storing Process
Store all routes replies DSN and NID in RR - Table

Step 3: Identify and Remove Malicious Node
Retreive the first entry from RR - Table

```
If DSN is much greater than SSN then discard entry from RR
– Table as
            Select Dest_Seq_No from table
            If(Dest_Seq_No >>> Src_Seq_No){
            Mali_node = Node_id
            Discard entry from table
}

Step 4:   Node Selection Process
            Sort the contents of RR – Table entries according to
            the DSN
            Select the NID having highest DSN among RR –
            Table entries

Step 5:   Continue default process
         Call ReceiveReply method of default AODV Protocol
```

VI. IMPLEMENTATION AND RESULTS

For the experimental setup, we used a network simulator NS (version 2.35) in order to simulate a MANET. In our work, the simulation is configured with varying number of nodes starting from 5 nodes to 50 nodes scenario. Simulation is performed with random movement of nodes. Identical mobility and traffic scenarios are used across protocols to gather fair results. Table 1 shows simulation parameters used in one of the experimental scenarios.

Table 1: Simulation Parameters Used for MANET

Channel Used	Wireless	Link Layer	LL
Propagation	Two Ray Ground	Antenna	Omni Antenna
Network interface	Wireless Phy	Interface Queue Length	150
Platform	Ubuntu 14.04	No. of Nodes	5-50
NS Version	Ns-allinone-2.35	Simulation area size	750 * 750
MAC	802_11	Traffic Pattern	CBR Sessions
Interface Queue	Drop tail / Pri queue	CBR Packet Size	512 Bytes

The simulation work carried out in three scenarios. Initially, all nodes in each scenario are normal and no malicious node is present in the scenario.

Scenario 1: It describes the normal situation of MANETs with normal AODV routing protocols.
Scenario 2: It described the impact of Gray Hole attack on the performance of ad hoc networks.
Scenario 3: It implements the proposed technique to prevent Gray Hole attacks in MANETs.

The metrics used for evaluating the proposed mechanism are:

a) *Throughput* can be defined as the amount of data transferred successfully on a communication network or network link over a period of time. Throughput is calculated in bytes/sec or bits/seconds.
b) *Data Packet Delivery Ratio* can be defined as the percentage of data packets that are successfully delivered to the destination. Packet drop affects the network performance by consuming time and more bandwidth to resend a packet.
c) *Packet Loss Rate* can be defined as the total number of packets that are not received by the destination node. It is the summation of the number of data packets send by the source node to the number of data packets received by the destination node.
d) *Misdetection* Rate can be defined as the probability of not identifying the malicious node. The misdetection rate increases as the nodes move faster.

Table 2 shows the complete analysis of throughput, PDR, PLR obtained with 3 scenarios simulated.

Table 2: Performance Analysis of Evaluation Metrics

No. of Nodes	Normal AODV			AODV with Gray Hole Attack			AODV with Prevention		
	T	PDR	PLR	T	PDR	PLR	T	PDR	PLR
5	19.68	97.86	47	3.35	1.09	399	19.16	95.2	94
10	45.88	99.16	47	9.62	20.87	800	45.02	97.45	143
20	89.36	99.03	97	10.01	11.11	1494	90.34	99.51	149
40	140.9	99.62	65	11.34	10.05	4485	140.1	99.25	124
50	220.5	99.43	169	75.18	33.62	4849	219	99.36	208

As shown in Table 2, the throughput of AODV is heavily affected by the malicious nodes where the throughput of proposed AODV is immune to it. The data confirms that the proposed implementation is secure against the Gray Hole attack. The data also confirms that PDR of AODV is affected by the malicious nodes whereas the PDR of the proposed AODV is immune to it. It also confirms that the number of packets dropped increases as the number of nodes increases and fewer no. of packets are dropped in the proposed AODV as compared to AODV with Gray Hole attack.

VII. CONCLUSIONS

In our work, we have implemented a mechanism for the detection and prevention of malicious Gray Hole nodes in MANETs. An efficient and simple approach for defending the AODV protocol against Gray Hole attack is implemented. The proposed method can be used to find the secured routes and prevent the Gray Holes nodes in the MANETs by identifying the node with their sequence number. Based on our experiments, we have found that modified AODV performance is better than AODV with Gray Hole attack as confirmed through Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), Throughput and misdetection rate numbers. We have used 3 scenarios for implementation i.e. Normal AODV, AODV with the attack, and AODV with Gray Hole prevention. The result of the experiment confirmed that throughput and PDR decrease during a Gray Hole attack but these parameters improve when we use our prevention technique. Finally, the results confirm that our proposed approach is effective in the detection and prevention of Gray Hole attacks in MANETs. The proposed algorithm based on sequence number could identify and remove malicious nodes from the network.

REFERENCES

[1]. Marti, Sergio, et al. “Mitigating routing misbehavior in mobile ad hoc networks.” Proceedings of the 6th annual international conference on Mobile computing and networking. 2000.

[2]. Yang, Hao, Xiaoqiao Meng, and Songwu Lu. “Self-organized network-layer security in mobile ad hoc networks.” Proceedings of the 1st ACM workshop on Wireless security. 2002.

[3]. Ramaswamy, Sanjay, et al. “Prevention of cooperative black hole attack in wireless ad hoc networks.” International conference on wireless networks. Vol. 2003. 2003.

[4]. Agrawal, Piyush, Ratan K. Ghosh, and Sajal K. Das. “Cooperative black and gray hole attacks in mobile ad hoc networks.” Proceedings of the 2nd international conference on Ubiquitous information management and communication. 2008.

[5]. Nadeem, Adnan, and Michael Howarth. “Protection of MANETs from a range of attacks using an intrusion detection and prevention system.” Telecommunication Systems Vol. 52, 2047-2058, 2013.

[6]. Deng, Hongmei, Wei Li, and Dharma P. Agrawal. “Routing security in wireless ad hoc networks.” IEEE Communications magazine Vol. 40.10, 70-75, 2002.

[7]. Jakobsson, Markus, Jean-Pierre Hubaux, and Levente Buttyán. “A micro-payment scheme encouraging collaboration in multi-hop cellular networks.” Financial Cryptography: 7th International Conference, FC 2003, Guadeloupe, French West Indies, January 27-30, 2003. Revised Papers 7. Springer Berlin Heidelberg, 2003.

[8]. Padilla, E., et al. “Detecting black hole attack in tactical MANETs using topology graph.” Proceeding of 32nd IEEE conference on local computer networks. 2007.

[9]. Banerjee, Sukla. “Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks.” proceedings of the world congress on engineering and computer science. Vol. 2008. 2008.

[10]. Sen, Jaydip, et al. “A mechanism for detection of gray hole attack in mobile Ad Hoc networks.” 2007 6th International Conference on Information, Communications & Signal Processing. IEEE, 2007.

[11]. Himral, Lalit, Vishal Vig, and Nagesh Chand. “Preventing aodv routing protocol from black hole attack.” International Journal of Engineering Science and Technology (IJEST), Vol 3.5, 3927-3932, 2011.

[12]. Paquereau, Laurent, and Bjarne E. Helvik. “Simulation of wireless multi-* networks in ns-2.” 3rd International ICST Conference on Performance Evaluation Methodologies and Tools. 2010.

[13]. Neha Singh, Rajeshwar Lal Dua, Vinita Mathur. “Network simulator ns2-2.35”. International Journal of Advanced Research in Computer Science and Software Engineering. 2012.