Black Hole Attack in Mobile Ad Hoc Networks – Issues and Solutions

Hardik Bhanabhai Patel
Research Scholar, Department of Computer Engineering, MECE
Parul Institute of Engineering and Technology, Limda

Prof. Jwalant Baria
Department of Computer Science and Engineering
Parul Institute of Engineering and Technology, Limda

Abstract

A Mobile Ad-Hoc Network is a collection of mobile nodes that are dynamically and arbitrarily located. Due to the mobility of these nodes, the interconnections between them continuously changes. Due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are vulnerable to attacks of the malicious nodes such as Cybil attack, jellyfish attack, black hole attack etc. A black hole attack has become a severe threat to the wireless ad hoc networks, which affects network's performance. Different techniques have been proposed to detect and evict the malicious nodes from the wireless ad hoc network. In this paper, these techniques are studied and there advantages and disadvantages are discussed.

1. Introduction

A Mobile Ad Hoc Network (MANET) is a group of mobile nodes that cooperate and forward packets for each other. Such networks extend the limited wireless transmission range of each node by multi-hop packet forwarding, and thus they are ideally suited for scenarios in which pre-deployed infrastructure support is not available. To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake.

As wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. Due to the autonomous behavior of these nodes, such networks are vulnerable to different types of attack such as passive eavesdropping, active interference and denial-of-service. One of these attacks is the Black Hole attack. In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything. In this way, all packets in the network routing through that node are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV.
Black Hole attack may occur due to a malicious node which is deliberately

misbehaving, as well as a damaged node interface.

2. Black Hole Attack

Black hole attack is a kind of Denial of Service (DoS) attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. A black hole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets.

During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires.

Black hole attack can be done by single malicious node or a group of malicious node, which is known as cooperative black hole attack. Also as we know packet dropping may be done due to various reason like node's malicious behavior, unavailability of resources, temporary network congestion etc. Sometimes node drops packet only for particular time duration or node drops packets which come from particular source or are meant to be delivered to particular destination. This way they misbehave temporarily. Such nodes or this kind of packet dropping attack is known as Gray hole attack.

Figure 1.a shows the single black hole attack and figure 1.b shows the cooperative black hole attack.

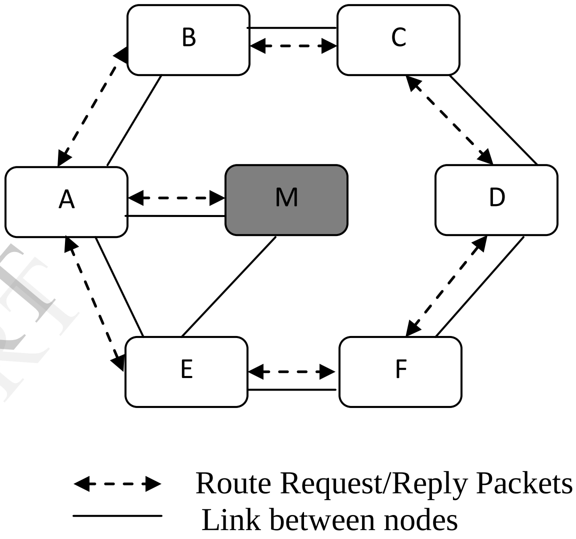

Figure 1.a Single Black hole attack

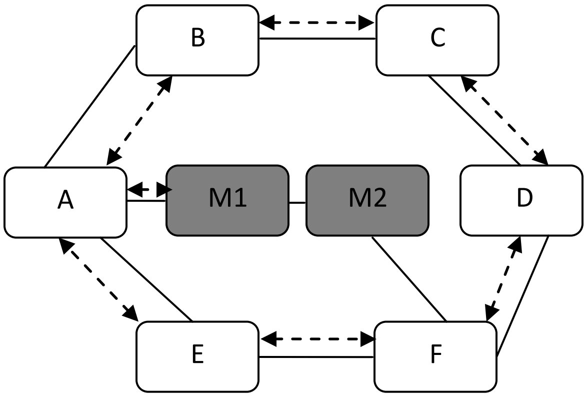

Figure 1.b Cooperative Black hole attack

As the packet dropping attacks affect network's performance and become high threat to the security of network, detection and prevention of such attack is necessary.

3. Related Works

Over years, many different techniques have been proposed for the detection and eviction of the black hole attack in the network. All these techniques can be categorized based on the mechanism they use [3]. These categories are as follows.

- Passive feedback based schemes: It encloses all the solutions whose principle consists in overhearing the neighbor's transmission to check the authorization.
- Acknowledgment-based schemes: In this category, a node requests an acknowledgement from its succeeding neighbors.
- Reputation-based schemes: It represents the solutions that judge a node is malicious or well-behaved according to an assessment of its trustworthiness level which is computed based on several observation of its behavior.
- Incentive based schemes: It includes the solutions which uses payment systems to stimulate network nodes for relaying packets.

Some of the popular techniques have been discussed here.

Watchdog and Pathrater [1] technique uses the concept of observation scheme to detect the misbehaving nodes and report observed misbehavior back to the source of the traffic. However, the scheme cannot punish the malicious nodes; instead they are relieved of their packet forwarding burden. This way, malicious behavior is beneficiary for nodes so they don't have to spend their resources.

Another technique is based on the mechanism proposed by Deng, Li and Agrawal [2] which protect against a black hole attack on AODV routing protocol. In this scheme, when RouteReply packet is received from one of the intermediate node in the path, another RouteRequest is sent from the source node to the neighbor node of the intermediate node in the path. This checks weather a path really exists between intermediate nodes and destination node. This scheme eliminates the black hole attack by a single attacker, but it fails identifying a cooperative black hole attack involving multiple malicious nodes. This also fails in case of the gray hole attack.

To overcome this limitation, Jaydip Sen, Harish Reddy and other teammates proposed a solution for the detection of the gray hole attack [4]. This solution is based on four different modules, which are neighborhood data collection module, local anomaly detection module, cooperative anomaly detection module and global alarm raising module. This scheme not only detects the cooperative black hole attack but also detect the gray hole attack. However, it cannot stimulate nodes to forward other nodes packets. So rational packet dropping becomes a headache.

As we know, packet dropping may happen due to different reasons as low resources, network congestion, malicious behavior of the node etc. So packet droppers can be divided into two categories; rational and irrational packet dropper. Rational packet dropper only occasionally drops packets due to low resources or network congestion, but irrational packet droppers drop the packets no matter what. And it is hard to stimulate the nodes to relay other's packets. So a new scheme was proposed known as the cooperation stimulation mechanism [7] [8].

Cooperation stimulation mechanisms us credits or micropayments to motivate the rationale packet droppers to relay packets. The nodes in the network earn credits for relaying other's packet and spend them to send their own packets. So it is more beneficial for nodes to relay other's packets rather than dropping them. However, this mechanism cannot detect the irrational packet droppers because it assumes that the nodes will relay packets faithfully using credits.

So to stimulate the nodes and to identify the packet droppers a new scheme named TRIPO [9] was introduced by Mohamed Elisalih Mahmoud and Xuemin Shen. TRIPO uses credits to stimulate the rational packet droppers to relay packets and uses a reputation system to identify and evict the irrational packet droppers. As in TRIPO, nodes are stimulated to relay packets and not forced because it costs node's energy to relay packets, no cooperation does not become a problem. Also it uses a trusted third party to charge and pay the nodes accordingly to the receipts generated. The trusted third party measures node's packet dropping frequency based on the receipts rather than medium overhearing technique, so false accusation is not possible. TRIPO also ensures fairness, as it can compensate the nodes that relay more packets by rewarding them with credits. Since packets pay for relaying their own packets, it discourages launching a resource exhaustion attack by sending spurious packets to exhaust the resources of the intermediate nodes.

Here, in figure 2, the basic architecture of the TRIPO has been given. As we can see, there are basically four phases which are divided among the network nodes and the trusted third party. The four phases are:

- Communication Phase: This phase contains functions as data generation and relay, acknowledgement generation and relay, receipt composition and submission.
- Processing Phase: This phase is all about the processing of the submitted receipts by the trusted third party.
- Credit Account Update Phase: This phase updates the credits of network nodes after processing the receipts.
- State Update Phase: This phase checks the behavior of the nodes and updates them as honest, suspicious or evicted nodes.

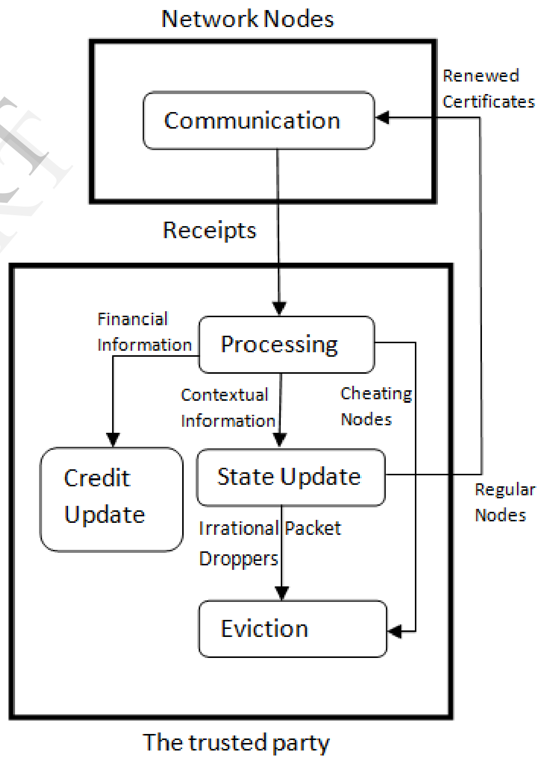

Figure 2. Architecture of TRIPO

The mechanism of the TRIPO is not just useful against the irrational packet droppers but it also ensures fairness and stimulates the nodes to relay other's packet. In addition, it also punishes the malicious nodes and becomes useful to maintain network's sustainability and stability.

4. Comparison between different algorithms

As we have seen earlier, these solutions can be categorized based on the basic idea for the mechanism. A comparison is shown in Table 1 between these categories.

Categories	Main Idea	Limitations
Passive Feedback based schemes	Medium overhearing	Most of the drawbacks of watchdog
Ack – based schemes	Acknowledge ment and authorization	Huge Overhead of Ack packets
Reputation based schemes	Trustworthiness level calculations	Overhead in sharing reputation
Incentive based schemes	Payment system to stimulate nodes	Node's location can affect the node's credits

Table 1. Comparison between different categories

So far we have reviewed different proposed schemes based on different ideas. All these solutions have their advantages and limitations. Some of them lack capability to motivate nodes to relay others packets or some of them lack the punishment system. We can summarize them according to the availability of stimulation of the nodes and punishment. Table 2 represents the summary of these solutions. Other important features can also be included to this summary like network or computation overhead, or scalability, latency, defense against collusive attack etc.

Name of the solution	Availability of stimulation	Availability of punishment
Watchdog and Pathrater	No	No
Detection of black hole on AODV by Deng	No	Yes
Detection of gray hole by Jaydip Sen	No	Yes
Cooperation Simulation	Yes	No
TRIPO	Yes	Yes

Table 2. Summary of different mechanisms

5. Conclusion

In this paper we have studied about the black hole attack and some mechanisms to resolve this attack. All these mechanisms have their pros and cons. Out of all these mechanisms, TRIPO seem to be better than other techniques as it not only detects and punishes the attacker node but also stimulate network nodes to relay other nodes' packets.

Although, TRIPO is better than others, it also has some limitations such as it cannot protect the route discovery process. Also some improvement needs to be done so that he overhead generated by submitting the receipts to the trusted party can be reduced. So in our future work, we would like to work on the routing protocol and modify it to safely route the traffic through the nodes that have low probability of dropping packet. This can be checked by the node's past history. We believe that it should help against different cheating strategies and improve the route stability and network performance.

References

1. S.marti, K. lai, T. Guili and M. Baker, ”Mitigating routing misbehavior in mobile ad hoc networks”, In proceedings of MOBICOM 2000, pp. 255-265, 2000.

2. H. Deng, W. Li, and Dharma P. Agrawal, “Routing Security in Ad Hoc Networks,” IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol. 40, No. 10, October 2002, pp. 70-75.

3. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, “Prevention of Cooperative Black hole Attack in Wireless Ad Hoc Networks”

4. Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamurlidhar (Embedded System Research Group, TCS), “Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks”, IEEE 2007

5. W. Yu, Y. Sun and K. R. Liu, “ Defense against Routing Disruptions in Mobile Ad Hoc Networks”, 24th IEEE INFOCOM, USA, March 2005.

6. Soufiene Djahel, Farid Nait-abdesselam and Zonghua Zhang, “Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges”, IEEE Communications Survey & Tutorials. Vol.13, No.4, Fourth Quarter, 2011.

7. G. Marias, P. Georgiadis, D. Flitzanis and K. Mandals, “Cooperation enforcement schemes for MANETs: A Survey”, J.Wrel. Commun. Mobile Comput., vol.6, No.3, pp. 319-332, May 2006.

8. M. Mahmoud and X. Shen, ”Stimulating Cooperation in Multi-Hop Wireless using cheating detection system”, in proc. IEEE INFOCOM, San Diego, CA, Mar.2010, pp 776-784.

9. Mohmed Elsalih Mahmoud and Xuemin (Sherman) Shen, Fellow, IEEE, “An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Dropping Attack in Multi-hop Wireless Networks”, IEEE Transactions on Vehicular Technology, Vol. 60, No. 8, October 2011.

10. “Packet Drop Attack” - http://en.wikipedia.org/wiki/Packet_drop_attack

11. “Black hole Attack in MANET” – http://scholers.google.co.in