International Journal of Advances in Computer Networks and Its Security– IJCNS
Volume 4 : Issue 3 [ISSN 2250 – 3757]
Publication Date : 30 September, 2014

Technique for Detection of Cooperative Black Hole Attack in Mobile Ad-hoc Networks-Survey

Gayatri Wahane[1], Ashok M. Kanthe[2], Dina Simunic[3]
[1, 2] Sinhgad Institute of Technology, Lonavala, Pune, India
[2, 3] Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia

Abstract— ***Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. Security is a major challenge for these networks owing to their features of open medium, dynamically changing topologies. The black hole attack is a well known security threat in MANET. However, it spuriously replies for any route request without having any active route to the specified destination. Sometimes the black hole nodes cooperate with each other with the aim of dropping packets. These are known as cooperative black hole attack. In this paper, we have reviewed different techniques for detection against Cooperative Black hole attacks in Mobile Ad-Hoc networks and thoroughly compare these schemes to find out their various advantages and disadvantages.***

Keywords— AODV, Black hole attack, MANET, routing protocols, Security.

I. Introduction

A Mobile Ad hoc network (MANET) is a self –configuring network [1,2] that does not require any fixed infrastructure, which minimizes their cost as well as deployment time. As each node in this network is free to move that makes the network to change its' topology continuously. These infrastructure-less mobile nodes in ad hoc networks dynamically create routes among themselves to and form own wireless network on the fly. Because of the dynamic nature, these networks are more vulnerable to attacks so security is an important as well as serious issue in MANET. One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. A set of nodes in a MANET 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 most widely used routing protocols in MANETs is the Ad hoc on-demand distance vector (AODV) routing protocol. We use AODV protocol because it is widely used and vulnerable to these attacks. Security in Mobile Ad-hoc Network is the most important for the network. Therefore, efficient detection techniques must be deployed to facilitate the identification and isolation of attacks. In this paper we have surveyed various detection techniques in MANET against Cooperative black hole attack. According to how the information is acquired, the routing protocols can be classified into proactive, reactive and hybrid routing.

The proactive routing protocols are table-driven. In this routing protocol, mobile nodes periodically broadcast their routing information to the neighbour's nodes. Each node needs to maintain their routing table of not only adjacent nodes and reachable nodes but also the number of hops. Therefore, the disadvantage is the rise of overhead due to increase in network size, a significant big communication overhead within a larger network topology. However, the major advantage is of knowing the network status immediately if any malicious attacker joins. The most familiar types of the proactive routing protocol are: - Destination sequenced distance vector (DSDV) routing protocol and Optimized link state routing (OLSR) protocol.

The reactive routing protocols (e.g. AODV) create and maintain routes only if these are needed, on demand. They usually use distance-vector routing algorithms that keep only information about next hops to adjacent neighbours and costs for paths to all known destinations. In compare to the proactive routing, the reactive routing is simply starts when nodes desire to transmit data packets. The disadvantage of reactive routing protocol method is loss of some packet. The most familiar on-demand routing protocols are: - Ad hoc on-demand distance vector (AODV) and Dynamic source routing (DSR) protocol.

The hybrid routing protocol as the name suggests have the combine advantages of proactive routing and reactive routing to overcome the defects generated from both the protocol when used separately. Design of hybrid routing protocols are mostly as hierarchical or layered network framework. In this system initially, proactive routing is employed to collect unfamiliar routing information, and then at later stage reactive routing is used to maintain the routing information when network topology changes. The familiar hybrid routing protocols are: - Zone routing protocol (ZRP) and Temporally-ordered routing algorithm (TORA).

This paper is organized as follows. In Section II related work for detecting cooperative black hole attack has been discussed. Section III provides AODV and its work in which discuss overview of AODV protocol with the description of black hole attack characteristics. Section IV presents a comparison table among the solutions and finally, concludes the paper with plan for future work in Section V.

II. Related Work

In this section we will discuss research work has been done by various authors.

J. Sen, S. Koilakonda and A. Ukil [3] proposed a mechanism for defending against a cooperative black hole attack. The mechanism modifies the AODV protocol by introducing two concepts, (I) data routing information (DRI) table and (II) cross checking. In the DRI scheme, two bits of additional information are sent by the nodes which respond to the RREQ message of a source node during route discovery process. Each node maintains an additional data routing information (DRI) table. In the DRI table, the bit 1 stands for "true" and the bit 0 stands for "false". The first bit "From" stands for the information on routing data packet from the node (in the Node filed), while the second bit "Through" stands for information on routing data packet through the node. The process of cross checking the intermediate nodes is a one-time procedure which should be affordable for security. The cost of crosschecking the nodes can be minimized by allowing the nodes to share the DRI table of their trusted nodes with each other.

J. Eriksson, S. V. Krishnamurthy, M. Faloutsos [4] proposed an algorithm to detect a wormhole attack by using True-link concept. True-link is a timing based countermeasure to the wormhole attack. Using True-link, a node can verify the existence of a direct link to an apparent neighbor. Verification of a link operates in two phases. In the rendezvous phase, the nodes exchange nonce. This is done with tight timing constraints, within which it is impossible for attackers to forward the exchange between distant nodes. In the authentication phase, i and j transmit a signed message, mutually authenticating themselves as the originator of their respective nonce. True-link is meant to be used together with a secure routing protocol. True-link is virtually independent of the routing protocol used. This work shows that True-link provides competent protection against potentially devastating wormhole attacks.

S. Banerjee [5] proposed a mechanism capable of detecting and removing the malicious nodes launching these two types of attacks. Their approach consists of an algorithm which works as follows. Instead of sending the total data traffic at a time we divide the total traffic into some small sized blocks. So that malicious nodes can be detected and removed in between the transmission of two such blocks by ensuring an end-to-end checking. Source node sends a prelude message to the destination node before start of the sending any block to alert it about the incoming data block. Flow of the traffic is monitored by the neighbors of the each node in the route.

L. Tamilselvan and V. Sankar Narayana [6] proposed a solution with the enhancement of the AODV protocol which avoids multiple black holes in the group. A technique is used to identify multiple black holes that are cooperating with each other and discover the safe route. It was assumed in the solution that nodes are already authenticated and therefore can participate in the communication. It uses fidelity table where every node that is participating is given a fidelity level that will provide to that node. Any node having 0 value is considered as malicious node and is eliminated.

H. Weerasinghe [7] proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by the Ramaswamy to improve the accuracy. This algorithm uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. This protocol is slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (RREP).

C. Wu Yu, Tung-Kung, W. ReiHeng, Cheng and S. Chao Chang [8] proposed a distributed and cooperative procedure to detect black hole node. In this each node detect local anomalies. It collects information to construct an estimation table which is maintained by each node containing information regarding nodes within power range. This scheme is initiated by the initial detection node which first broadcast and then it notifies all one-hop neighbors of the possible suspicious node. They cooperatively decide that the node is suspicious node.

III. AODV and its security problems

1. Ad Hoc On Demand Distance Vector Routing Protocol

AODV is a reactive [9,10] routing protocol that does not require maintenance of routes to destination nodes. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is demand from mobile node. In ad hoc network first route discovery takes place, which means if a mobile node that wishes to communicate with other node first broadcast a RREQ (Route Request) message to find a fresh route to a desired destination node. Every neighbour node that receives RREQ broadcast first saves the path the RREQ was transmitted along its routing table. It then checks its routing table to see if it has a fresh enough route to the destination node provided in RREQ message. Destination sequence number attached to it indicates the freshness. If a node finds a fresh enough route it uncast a RREP (route reply) message back along the saved path to the source node or it rebroadcast the RREQ message otherwise. The same process continues until an RREP message from the destination node or an intermediate node that has a fresh route to the destination node received by the source node.

2. Cooperative Black Hole Attack

A black hole attack is a kind of Denial of service (DoS) attack in mobile ad hoc networks. In this attack [11], a malicious node sends a fake RREP packet to the source node that has initiated a route discovery, in order to show itself as a destination node or an intermediate node to the actual destination node. In such a case the source node would send all of its data packets to the malicious node. The malicious node then absorbs all the packets and drops them fully or sometimes partially. As a result source and destination node will not be able to communicate with each other shown in Fig.

1.

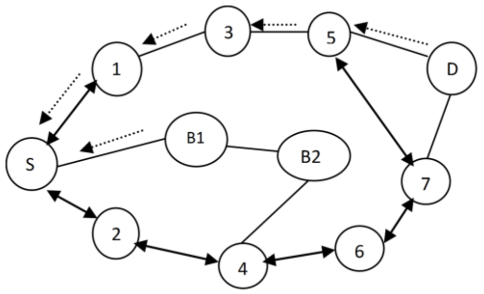

Figure 1. Detection of cooperative black hole attack

Consider the case where S is the source node, D is the destination node and B1 is the malicious node, here node S starts with the route discovery process then the node B1 advertises itself as having a valid shortest route to the destination, here the route is false with the purpose of intercepting packets. Moreover a malicious node does not need to check its routing table when sending a false message; its response is more likely to reach the source node first. This makes the source node think that the route discovery process is complete, ignore all other reply messages and begin to send data packets. As a result, all the packets through the malicious node are simply absorbed discarded and then lost. The malicious node could be said to form a black hole in the network. Sometimes these malicious nodes cooperate with each other with the same aim of dropping packets, these are known as cooperative black hole nodes and the attack is known as cooperative black hole attack.

IV. COMPARISON OF VARIOUS SOLUTIONS TO BLACK HOLE ATTACK

The comparison of various black hole attack detection technique that have been proposed by several authors has been mentioned in Table I.

TABLE I COMPARISON OF VARIOUS SOLUTION TO BLACK HOLE ATTACK

Technique proposed by	**Techniques / Solutions**	**Type of black hole attack**	**Drawbacks**
J. Sen et al. [3]	Data Routing Information(DRI) table of Next hop node	Co-operative black holes	Maintenance of DRI tables apart from normal routing information .
J. Eriksson et al. [4]	True-link	Wormhole	Identify only wormhole
S. Banerjee [5]	Divide the total traffic into some small sized blocks	Co-operative black holes	More overhead
L. Tamilselvan and V. Sankar Narayana [6]	Fidelity table based on the acknowledgements received by the source node.	Co-operative black holes	Time delay
H. Weerasinghe [7]	Enhancment in DRI table and crosschecking	Co-operative black holes	more communication overhead of route request.
C. Wu Yu et al. [8]	Each node detect local anomalies and used estimation table	Single black holes	Time delay
S. Kurosawa et al. [9]	A new detection method based on dynamically updated training data	Single Black hole	Network delay
G..D. Wahane et al.[13]	A new technique based on crosschecking and true-link concept	Multiple Black Hole	-

V. CONCLUSION

Black Hole Attack is a main security threat that degrades the performance of the AODV routing protocol. Its' detection is the main matter of concern. Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have conducted diverse techniques to propose different types of detection and prevention mechanisms for black hole problem. This paper has discussed various works related to black hole attack detection methods in AODV-based MANETs and pointed out their drawbacks. We compared these methods from some aspects and observe that the mechanisms detects black hole node, but no one is good since most of the solutions are having drawbacks such as more time delay, much network routing overhead because of newly introduced packets. As a future work, we intend to find an effective solution to the cooperative black hole attack in AODV protocol.

REFERENCES

[1] R. Prasad, S. Dixit, R. Van Nee, "Globalization of Mobile and Wireless Communication", March 2011, Springer, p. 335.

[2] L. Gavrilovska, R. Prasad, "Ad Hoc Networking Towards Seamless Communications", Springer 2006, p.284.

[3] J. Sen, S. Koilakonda and A. Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks". Second international conference on intelligent system, modeling and simulation, Kolkata, 2011, 25-27 .

[4] J. Eriksson, S. V. Krishnamurthy, M. Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", 2011. The Communications and Networks Consortium sponsored by the U. S. Army Research Laboratory under the Collaborative Technology Alliance Program.

[5] S. Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks". The World Congress on Engineering and Computer Science 2008.

[6] L. Tamilselvan and V Sankar Narayana, "Prevention of Black Hole Attack in MANET". Journal of Networks, 2008, Volume 3, Number 5, pp 13-20.

[7] H. Weerasinghe, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking, 2007,Volume 2, pp 362-367.

[8] C. Wu Yu, Tung-Kuang, W. ReiHeng, Cheng and S. Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks". PAKDD International Workshop, Nanjing, China,2007, pp 538-549

[9] C. Perkins, E. B. Royer and S. Das, "Ad hoc On Demand Distance Vector (AODV) Routing, Internet Draft", RFC 3561, IETF Network Working Group, July 2003.

[10] C. Perkins, E. B. Royer and S. Das, "Ad hoc On-Demand Distance Vector Routing", Proceeding of the 2nd IEEE Workshops on Mobile Computing System and Applications (WMCSA), pp. 90-100, 25-26 Feb.,1999.

[11] A. M. Kanthe, D. Simunic, M. Djurek, "Denial of Service (DoS) Attacks in Green Mobile Ad-hoc Networks", MIPRO 2012, IEEE Conference, Proceedings of the 35th International Convention, ISBN:978-1-4673-2511-6, May21-25, 2012, Opatija, Croatia.

[12] A. M. Kanthe, D. Simunic, "Denial of Service (DoS) Attacks in Green Mobile Ad-hoc Networks", MIPRO 2012, IEEE Conference.

[13] G. D. Wahane, A. M. Kanthe, D. Simunic, "Technique for detection of Cooperative black hole attack using true-link in Mobile Ad-hoc Networks " , unpublished.