IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

Cooperative Black Hole Attack Detection: A Survey

Alphonsa George[1], Dhanya Narayan[2], Cincy Mary Sebastian[3]

M.Tech Scholar (Wireless Technology), ECE Department, College of Engineering, Kidangoor, India [1, 3]

Assistant Professor, ECE Department, College of Engineering, Kidangoor, India [2]

Abstract: Mobile ad hoc networks (MANETs) are composed of a set of stations or nodes that communicating through wireless channels, without any fixed backbone support in which different nodes are allowed to join and leave the network at any point of time. MANETs are generally more vulnerable to information and physical security threats than wired networks, so security is a vital requirement in MANETs to provide secured communication between mobile nodes. Most of the routing protocols rely on the cooperation among the nodes for secure transmission due to lack of centralized administration. There is no general algorithm for security of principle routing protocols like AODV against various attacks. One of the most common attacks against routing in MANETs is the Black Hole attack. A black hole is a malicious node that uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In this paper, we survey some attacks of MANET and compare the existing solutions to combat the single or cooperative black hole attack.

Keywords: MANET, Black Hole Attack, Wormhole Attack, Rushing Attack.

I. INTRODUCTION

Ad hoc networks are autonomous and self-configurable systems consisting of routers and hosts, which are able to support mobility and organize themselves arbitrarily. This means that the topology of the ad-hoc network changes dynamically and unpredictably. Also, the ad hoc network can be either constructed or destructed quickly and autonomously without any infrastructure. Without support from the fixed infrastructure, it is undoubtedly difficult for us to distinguish the insider and outsider of the wireless network. That is, it is not easy for us to tell apart the legal and the illegal participants in wireless systems. If the nodes of ad hoc networks are mobile and with wireless communication to maintain the connectivity, it is known as mobile ad hoc network (MANET) and require an extremely flexible technology for establishing communications in situations which demand a fully decentralized network without any fixed base stations, like battlefields, military applications, and other Emergency and disaster situations. Since, all participants are mobile, the network topology of a MANET is generally dynamic and may change frequently.

MANETs have special limitation and properties such as limited bandwidth and power, highly dynamic topology, high error rates etc. Moreover, compared to infrastructure based networks, in a MANET, all nodes are mobile and can be connected dynamically in an arbitrary manner. Nodes of MANET behave as router and take part in discovery and maintenance to establish a reliable route of each other. Therefore, routing protocols for wired networks cannot be directly used in wireless networks and numerous protocols have been developed for MANETs. These routing protocols are divided into three categories based on management of routing tables. These categories includes table driven, on demand and hybrid routing protocol.

II. ROUTING IN MANET

The routing protocols can be classified in to three categories- Proactive (Table-Driven) routing protocols, Reactive (On-Demand) routing protocols and Hybrid routing protocols.

A. Proactive Routing Protocols

In proactive or table-driven routing, each node has to maintain one or more tables to store routing information. Any changes in network topology need to be reflected by propagating updates throughout the whole network in order to maintain a consistent network view. Examples of such schemes are the conventional routing schemes: Destination sequenced distance vector (DSDV). They attempt to maintain consistent, up-to-date routing information of the whole network. It minimizes the delay in communication and allows nodes to quickly determine which nodes are present or reachable in the network.

B. Reactive Protocols

Reactive routing is also known as on-demand routing protocol since they do not maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a data packet to another node then this protocol searches for the route in an on-demand fashion and establishes the connection in order to transmit and receive the packet. The route discovery proceeds by flooding the route request packets throughout the network. Examples of reactive routing protocols are the Ad-hoc On-demand Distance Vector routing (AODV) and Dynamic Source Routing (DSR).

C. Hybrid Protocols

Hybrid routing protocols are the combination of proactive and reactive routing protocols to overcome the defects of both the protocols. Most of hybrid routing protocols are designed as a hierarchical or layered network framework. The Zone Routing Protocol is a hybrid routing protocol

DOI 10.17148/IJARCCE.2015.412148

that divides the network into zones. ZRP provides a hierarchical architecture where each node has to maintain extra topological information requiring extra memory.

III.TYPES OF ATTACKS

Some of the unique characteristics that exist in the ad hoc networks are dynamic topology, distributed operation, and resource constraints, which inevitably increase the vulnerability of such network. Many characteristics are used to classify attacks in the ad hoc networks like the behaviour of the attacks (passive vs. active) and the source of the attacks (external vs. internal).

Passive Attacks

A passive attack does not alter the information transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates data from it. Here, attacker does not disrupt the operation of a routing protocol but it attempts to discover the important information from routed traffic. Detection of these type of attacks is difficult since the operation of network itself doesn't get affected. Examples of passive attacks in ad hoc network are eavesdropping attacks and traffic analysis attacks. In order to overcome this type of attacks powerful encryption algorithms are used to encrypt the data being transmitted.

Active attacks

Active attacks are severe attacks that prevent message flow between the nodes. Active attacks actively modify the data with the intention to block the operation of the targeted networks. Examples of active attacks consist of actions like message modifications, message replays, message fabrications and the denial of service attacks. Active attacks may be internal or external.

External Attacks

External attacks launched by adversaries who are not initially authorized to be involved in the network operations. These attacks usually aim to cause network congestion, denying access to specific network function or to interrupt the whole network operations. External attacks prevent the network from normal communication and generating additional overhead to the network.

Internal Attacks

Internal attacks are initiated by the authorized nodes in the networks, and might come from both misbehaving and compromised nodes. Internal nodes are identified as compromised nodes if the external attackers hijacked the authorized internal nodes and are then using them to launch attacks against the ad hoc networks. Security requirements such as authentication, confidentiality and integrity are severely vulnerable in these networks with the compromised internal nodes because communication keys used by these nodes might be steal and passed to the other colluding attackers. On the other hand, if nodes are authorized to access the system resources, but fail to use these resources in a way they should be, then they will be classified as misbehaving.

Wormhole Attacks

Wormhole attacks are another severe attack of MANET routing protocols. In wormhole attack, attacker node receive data packet at one point in the network and tunnels them to another attacker node. The tunnel exist between two malicious nodes is refer as a wormhole. Attackers usually use wormholes in the network to make their nodes appear more attractive so that more data is routed through their nodes. In a wormhole attack, an attacker records data packet at one location in the network, tunnels them to another location, and retransmits them into the network at that location. For tunnelled distances longer than the normal wire-less transmission range of a single hop, it is simple for the attacker to make the tunnelled packet arrive with better metric. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received. An attacker can create a wormhole even for packets not addressed to itself, since it can hear them in wireless transmission and tunnel them to the attacker at the opposite end of the wormhole.

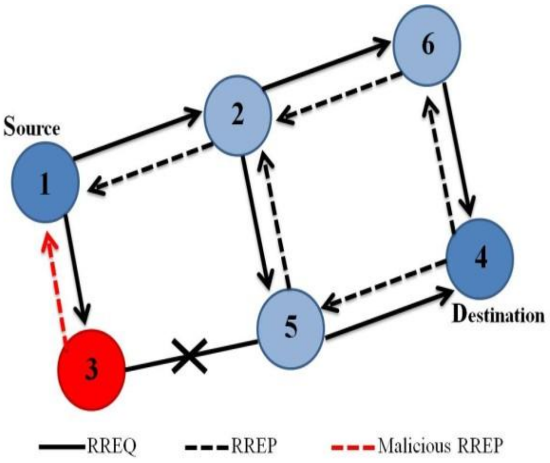

Fig.1. Blackhole Attack

Black hole Attacks

In this attack, malicious nodes trick all their neighbouring nodes to attract all the routing packets to them. As in the wormhole attacks, malicious nodes could found the black hole attacks by advertising themselves to the neighbouring nodes as having the most suitable route to the requested destinations. However, unlike in the wormhole attacks where multiple attackers conspired to attack one neighbouring node, in the black hole attacks, only one attacker is involved and it threatens all its neighbouring nodes.When the malicious node insert itself between communication route, it is able to drop the packet, it is retrieve information from the data packet and can be modify it.

Figure 1 shows black-hole attack. Here, node 4 is the destination. Node 3 will send fake RREP to source showing it has routing to node 4 with higher sequence number. Source transmits data packet to 3 before waiting other RREPs. Node 3 is a black-hole, so it simply drops data.

Cooperative blackhole attacks

This attack is similar to Black-Hole attack, but more than one malicious node tries to interrupt the network simultaneously. Sometimes these nodes cooperate with each other with the same target of dropping packets. This

DOI 10.17148/IJARCCE.2015.412148

kind of attack is known as cooperative black hole attack. It is one of the most severe DATA traffic attack and can totally disrupt the operation of an Ad Hoc network.

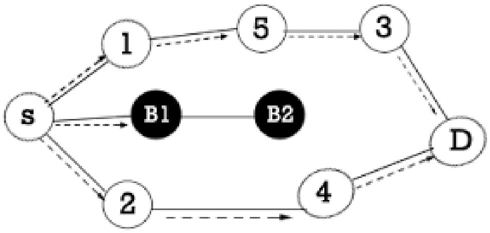

Fig.2. Cooperative Blackhole Attack

Figure 2 shows cooperative blackhole attack in which B1 and B2 are cooperative blackholes.

Rushing Attacks

In AODV or related protocol, each node before transmitting its data, first establishes a valid route to destination. Sender node broadcasts a RREQ (route request) message in neighbourhood and valid routes replies with RREP (route reply) with proper route information. Some of the protocols use duplicate suppression mechanism to limit the route request and reply chatter in the network. Rushing attack exploits this duplicate suppression mechanism. Rushing attacker suddenly forwards with a malicious RREP on behalf of some other node skipping any proper processing. Due to duplicate suppression, actual valid RREP message from valid node will be discarded and consequently the attacking node becomes part of the route. In rushing attack, attacker node does send packets to correct node after its own filtering is done, so from outside the network behaves normally as if nothing happened. But it might increase the delay in packet delivering to destination node.

IV. DETECTION TECHNIQUES

Various methods has been proposed to detect and prevent cooperative blackhole attacks. Review of some of these methods is presented below:

A. Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks [1,2]

Ramaswamy et a proposed a methodology for identifying multiple black hole nodes cooperating as a group with slightly modified AODV protocol by introducing Data Routing Information (DRI) Table and Cross Checking. The solution to identify multiple black hole nodes acting in cooperation involves two bits of additional information from the nodes responding to the RREQ of source node S. In the DRI [2] table, 1 stands for 'true' and 0 for 'false'. The first bit "From" stands for information on routing data packet from the node (in the Node field) while the second bit "Through" stands for information through the node (in the Node field). Whenever an intermediate node (IN) responds to a RREQ it sends the id of its next hop neighbour (NHN) and DRI entry for NHN to the source. Suppose IN is not reliable for the source then source sends a further route request (FREQ) to NHN. Then NHN responds with FREP including DRI entry for IN, the next hop node of current NHN, and the DRI entry for the current NHN's next hop. If NHN is a trusted node then source checks whether IN is a black hole or not using the DRI entry for IN replied by NHN and that for NHN replied by IN. If IN is not malicious, they should be consistent. Also if NHN is not reliable then the same cross checking will be continued with the next hop node of NHN. This cross checking loop will be continued until a trusted node is found. The solution fails to accommodate the Grayhole Attack where the nodes keep alternating between malicious and normal behaviour. Extra FRRQ and FREP from neighbour add overhead in processing.

B. Prevention of Co-operative Black Hole Attack in MANET [3]

Latha Tamilselvan & Dr. V. Sankaranarayan proposed a solution for prevention of black hole attack. The tactic used in this solution is as follows: The source node after broadcasting RREQ messages to all neighbours will wait for RREP messages from its neighbouring nodes before starting the sending of data packets. The source node first ensures the safe route for sending data packets to its destination.

The source node collects the RouteREQuest messages from its neighbouring nodes by using timer and maintains those routes in a table of all the receiving RREP messages. Once the time set in the timer gets over, source node selects the most consistent route including more repeated common nodes from the table. If such consistent nodes are not in the table, then source node opts for the route where the replying node is able to provide the information of next hop in the route. This solution suffers from a drawback of processing delay and causes additional delay for waiting for reply from neighbouring node, also if the next hop node is Black hole then this solution will not work.

C. A Novel Technique for a Secure Route by Detection of Multiple Blackhole Nodes in MANET [4]

Meenakshi Sharma proposed a paper to prevent the cooperative black hole attack in MANET which aims at decreasing end to end delay while increasing the Packet Delivery Ratio (PDR). When black hole attack is encountered in the network, throughput of the network is reduced while the delay increases. They focused on finding a secure route for communication by detecting and isolating all the malicious nodes in mobile Adhoc network.

By using fake RREQ packet and modified RREP packet, the black hole nodes are detected at the initial stage before the actual route discovery process of AODV. It leads to less routing overhead and high packet delivery ratio. But this method is not much suitable for large networks.

D. Technique for Detection of Cooperative Black Hole Attack using True-link in Mobile Ad-hoc Networks[5]

Gayatri Wahane proposed a method for detecting as well as defending against a cooperative black hole attack using DRI table and True-link concept. True-link refers a timing

DOI 10.17148/IJARCCE.2015.412148

based countermeasure to the cooperative black hole attack. They also suggest the modification of Ad-hoc on Demand Distance Vector (AODV) routing protocol. The DRI table method is actually introduced from detection techniques of Ramaswamy [1] and J sen [2].True-link crosschecking method is designed to isolate and mitigate the effect of black hole attacks in MANET.

True-link- crosschecking enhances AODV protocol to improve the network performance by improving routing update condition. The enhancement only involves a minimum modification in DRI based cross checking with True-link rendezvous phase by changing the existing AODV protocol scheme. This solution reduces routing overhead and delay. It achieves maximum throughput when number of nodes and pause time more.

V. CONCLUSION

In this paper a survey on different existing techniques for detection of cooperative black hole attacks in Moble Adhoc Networks (MANET) with their defects is presented. Based on the performance comparisons, it can be concluded that there is need for perfect detection and elimination mechanisms. The detection of Black Holes in ad hoc networks is still considered to be a challenging task. Future work is intended to an efficient Black Hole attack detection and elimination algorithm with minimum delay and overheads that can be adapted for ad hoc networks susceptible to Black Hole as well as Cooperative Black Hole attacks.

REFERENCES

[1] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K, " Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", Paper presented at the International Conference onWireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003.

[2] 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, modelling and simulation, Kolkata, 2011, 25-27.

[3] Tamilselvan L, Sankaranarayanan V, "Prevention of Blackhole Attackin MANET", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August2007.

[4] Meenakshi Sharmal, Davinderjeet Singh , "A Novel Technique for a Secure Route by Detection of Multiple Blackhole Nodes in MANET", International Journal of Advanced Research inComputer Science and Software Engineering, Volume 3, Issue 12, December 2013

[5] Gayatri Wahane, Ashok M. Kanthe, Dina Simunic, "Technique for Detection of Cooperative BlackHole Attack using True-link in Mobile Ad-hoc Networks", MIPRO 2014, 26-30 May 2014, Opatija.

[6] J. Eriksson, S. V. Krishnamurthy, M. Faloutsos, "True link, 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.

[7] 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.

[8] H. Deng, H. Li, and D. Agrawal,"Routing security in wireless ad hoc net-works", IEEE Communications Magazine, Vol. 40, No. 10, Oct 2002.

BIOGRAPHIES

Alphonsa George is pursuing M.Tech in Wireless Technology from College of Engineering Kidangoor. She received her B. Tech in Electronics and Communication Engineering from Mahatma Gandhi University College of Engineering, Thodupuzha, Kerala. Her primary research interest includes communication and computer networking.

Dhanya Narayan is working as Assistant Professor in Department of Electronics &Communication Engineering, College of Engineering, Kidangoor. She is currently pursuing Ph.D in Signal Processing from Division of Electronics, School of Engineering, Cochin University of Science & Technology, Kerala, India. She received her M.Tech in Wireless Technology from Department of Electronics, CUSAT and B.Tech in Electronics & Communication Engineering from Government Engineering College Palakkad. Her areas of research interest are communication and signal processing.

Cincy Mary Sebastian is pursuing M.Tech in Wireless Technology from College of Engineering Kidangoor. She received her B. Tech in Electronics and Communication Engineering from Amal Jyothi College of Engineering Kanjirappally, Kerala. Her primary research interest includes antenna designing and computer networking.

DOI 10.17148/IJARCCE.2015.412148