Volume 3, Issue 5, May 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review Paper on Pooled Black Hole Attack in MANET

Sonia [1]
Research Scholar, S.K.I.E.T
Kurukshetra, Haryana, India

Abhishek Aggarwal [2]
Asst.Prof., S.K.I.E.T
Kurukshetra, Haryana, India

Abstract: Ad-hoc networks are emerging technology, due to their spontaneous nature, are frequently established insecure environments, which makes them vulnerable to attacks. These attacks are launched by participating malicious nodes against different network services. Ad hoc On-demand Distance Vector routing (AODV) is a broadly accepted network routing protocol for Mobile Ad hoc Network (MANET). Black hole attack is one of the severe security threats in ad-hoc networks which can be easily employed by exploiting vulnerability of on-demand routing protocols such as AODV. In this paper, a review on different existing techniques for detection of pooled or co-operated black hole attacks with their defects is presented.

Keywords: Mobile Ad Hoc Network, DoS, Single Black Hole Attack, Collaborative Black Hole Attack.

I. Introduction

A MANET is a collection of wireless hosts that can be rapidly deployed as a multi-hop packet radio network without the aid of any established infrastructure or centralized administrator. MANETs have some special characteristic features such as unreliable wireless media (links) used for communication between hosts, constantly changing network topologies and memberships, limited bandwidth, battery, lifetime, and computation power of nodes etc. MANETs are vulnerable to various types of attacks. These include passive eavesdropping, active interfering, impersonation, and denial-of service. One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. One of the most widely used routing protocols in MANETs is the *ad hoc on-demand distance vector* (AODV) routing protocol [1]. It is a source initiated on-demand routing protocol. However, AODV is vulnerable to the well known black hole attack. In [2], the authors have assumed that the black hole nodes in a MANET do not work as a group and have proposed a solution to identify a single blackhole.However,their proposed method cannot be applied to identify a cooperative black hole attack involving multiple malicious nodes. In this paper various schemes are discussed which are used to detect and prevent collaborative black hole node in MANET.

II. Security Issues

Security in Mobile Ad-Hoc Networks is an important concern for the network functioning. MANET often experience different security attacks because of its following features: Dynamically changing network topology, lack of central monitoring, cooperative algorithms and absence of a certification authority and etc [3, 4]. These features are explained below:

1) *Dynamically changing network topology*: Nodes are free and they can move arbitrarily. So the network topology changes unpredictably and frequently, which results in change in routes, frequent partitioning of network and loss of packets.
2) *Lack of centralized monitoring*: MANETs does not have any established infrastructure and centralized administration. MANET works without any preexisting infrastructure. This lack of centralized management leads MANET more vulnerable to attacks. Detecting attacks and monitoring the traffic in highly dynamic and for large scale Ad-Hoc network is very difficult due to no central management.
3) *Cooperative algorithms*: In MANET the routing algorithms need to have trust between their neighboring nodes.
4) *Bandwidth constraint*: Wireless links have lower capacity as compared to the infrastructures networks.
5) *Limited physical security*: Mobility of nodes results in higher security risks, which increases the possibility of spoofing, eavesdropping and masquerading and DoS attacks.
6) *Energy constrained operation***:** The only energy means for the mobile nodes in Ad-Hoc network is the battery power. And they also have a limited storage capacity and power.

A. Black Hole Attack

A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. A single black hole attack is easily happened in the mobile ad hoc networks [25]. An example is shown as Figure 1, node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. As what mentioned above, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem. The most critical influence is that the PDR diminished severely.

Figure 1 is an example of single black hole attack in the mobile ad hoc networks [25]. Node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. In the mobile ad hoc networks, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the netwoek operation is suffered from this problem.

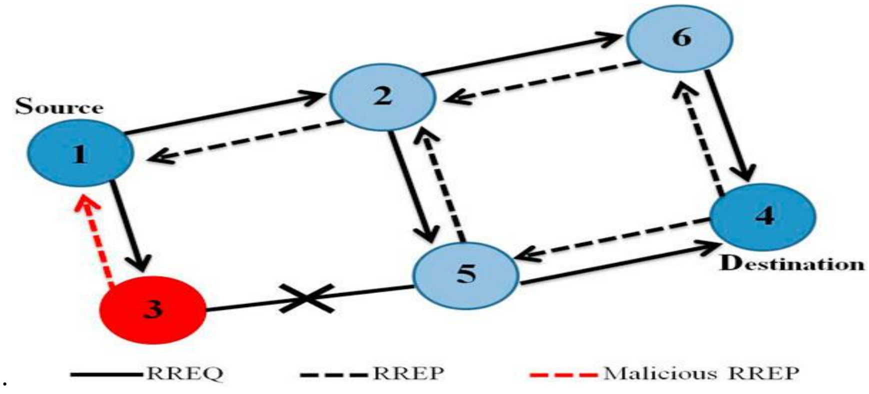

Figure 1 The single black hole problem

B. Pooled Black Hole Attack

There are various mechanisms have been proposed for solving single black hole attack .In recent years. However, many detection schemes are failed in discussing the cooperative black hole problems. Some malicious nodes collaborate together in order to beguile the normal into their fabricated routing information, moreover, hide from the existing detection scheme. As a result, several cooperative detection schemes are proposed preventing the pooled black hole attacks [5].

In the following, different detection schemes for the cooperative black hole attack are presented in a chronological order.

1) *DRI Table and Cross Checking Scheme [6, 7]:* Sanjay Ramaswamy et al. exploit data routing information (DRI) table and cross checking method to identify the cooperative black hole nodes, and utilize modified AODV routing protocol to achieve this methodology. Every node needs to maintain an extra DRI table, 1 represents for true and 0 for false. The entry is composed of two bits, “From” and “Through” which stands for information on routing data packet from the node and through the node respectively. The procedure of proposed solution is simply described as below. The source node (SN) sends RREQ to each node, and sends packets to the node which replies the RREP packet. The intermediate node (IN) transmits next hop node (NHN) and DRI table to the SN, then the SN cross checks its own table and the received DRI table to determine the IN’s honesty. After that, SN sends the further request to IN’s NHN for asking its routing information, including the current NHN, the NHN’s DRI table and its own DRI table. Finally, the SN compares the above information by cross checking to judge the malicious nodes in the routing path. Authors propose a detection method to overcome the multiple black hole problems and the collaborative attacks, and submit the simulation result in [7]. The experiment result shows that this solution performs an almost 50% better than other solutions. However, it wastes 5 to 8% communication overhead, and slightly increases the packet loss percentage because of the secure route discovery delay.

2) *Distributed Cooperative Mechanism (DCM) [8]:* Chang Wu Yu et al. propose a distributed and cooperative mechanism viz. DCM to solve the collaborative black hole attacks. Because the nodes works cooperatively, they can analyze, detect, mitigate multiple black hole attacks. The DCM is composed of four sub-modules which shown as Figure 2. In the local data collection phase, an estimation table is constructed and maintained by each node in the network. Each node evaluates the information of overhearing packets to determine whether there is any malicious node. If there is one suspicious node, the detect node initiates the local detection phase to recognize whether there is possible black hole. The initial detection node sends a check packet to ask the cooperative node. If the inspection value is positive, the questionable node is regarded as a normal node. Otherwise the initial detection node starts the cooperative detection procedure, and deals with broadcasting and notifying all one-hop neighbors to participate in the decision making. Because the notify mode utilizes broadcasting method, the network traffic is increased. A constrained broadcasting algorithm is used to restrict the notification range within a fixed hop count. A threshold viz. thr represents the maximum hop count range of cooperative detection message. Finally, the global reaction phase is executed to set up a notification system, and sends warning messages to the whole network. There are reaction modes in global reaction phase. Though the first reaction mode notifies all nodes in the network, but might waste lots of communication overhead. Each node only concerns its own black hole list and arranges its transmission route in other mode, however it might be exploited by malicious nodes and needs more operation time. In the simulation

results, the notification delivery ratio is from 64.12 (thr as 1) to 92.93% (thr as 3) when using different threshold values. Compare with the popular AODV routing protocol in MANET, the simulation result shows that DCM has a higher data delivery ratio and detection rate even if there are various black hole nodes. Even though the control overhead can be reduced due to the distributed design method, DCM wastes few overhead inevitavle.

3) *Hash based Scheme [9]:* Weichao Wang et al. design a hash based defending method to generate node behavioral proofs which involve the data traffic information within the routing path. The developing mechanism is based on auditing technique for preventing collaborative packet drop attacks, such as collaborative black hole and grey hole problems. The proposed solution is originated from an audit-based detection method videlicet REAct [12]. The vulnerability of REAct system is that cooperative adversaries can specialize in attacker identification phase by sharing Bloom filters of packets between them. The major difference between these two schemes is discussed as follows. A hash based node behavioral proofs is proposed to defend the collaborative attacks. The audited node n_i is needed and settled by the source node S, and then S sends the sequence numbers of selected packets to auditing node. After source node sends out these packets, an additional random number t_0 is attached to the tail of every packet. The intermediate node n1 combines the received packet and its own random number r_1 to calculate its value t_1, and this operation is continued within every intermediate node until n_i receives the packet. Nevertheless, this paper doesn't give the results, so that it's hard to figure out the enhancement.

4) *Hashed-based MAC and Hash-based PRF Scheme [10]:* Zhao Min and Zhou Jiliu propose two hash-based authentication mechanisms, the message authentication code (MAC) and the pseudo random function (PRF). These two proposals are submitted to provide fast message verification and group identification, find the collaborative suspicious hole nodes and discover the secure routing path to prevent cooperative black hole attacks. The public key infrastructure (PKI) is difficult to utilize in MANET due to the inherently design disadvantages, which is no centralized infrastructure. To deserve to be mentioned, authors overcome this bottleneck and design an authentication mechanism. The key point of this solution is that each node acquires a secret key K_i, and K_i = Gk (r_i). The sharing key K_i is undisclosed to all other nodes, hence, it is formulated by choosing a random number r_i and repeatedly applying PRF on r_i by k times. When source node receives a packet, it checks K_i-d to find whether the key used for the MAC is disclosed or not, and checks the MAC when Ki is disclosed. After checking the above two conditions, this packet is regarded as available packet and the route is confirmed as a secure route. The simulation result shows that both solutions have better data delivery ratio than AODV routing protocol. But, the detection time increases as the pause time raises, and the control overhead of both solutions is higher than the ordinary AODV.

5) *Bait DSR (BDSR) based on Hybrid Routing Scheme [11]:* Po-Chun Tsou et al. design a novel solution named Bait DSR (BDSR) scheme to prevent the collaborative black hole attacks. The proposed mechanism is composed of proactive and reactive method to form a hybrid routing protocol, and the major essence is the DSR on-demand routing. This solution is briefly introduced as below. In the beginning of routing stage, the source node sends bait RREQ packet before starting route discovery. The target address of bait RREQ is random and non-existent. To avoid the bait RREQ inducing the traffic jam problem, BDSR use the same method with DSR. That is all bait RREQ packets only survive for a period time. The malicious nodes are easily expelled from the initial phase, because the bait RREQ is able to attract the forged RREP from black hole node. In authors' mechanism, the generator of RREP is recorded in the RREP's additional field. Therefore the source node can recognize the location of attacker from the reply location of RREP. In the beginning of routing stage, the source node sends bait RREQ packet before starting route discovery. The target address of bait RREQ is random and non-existent. To avoid the bait RREQ inducing the traffic jam problem, BDSR use the same method with DSR. That is all bait RREQ packets only survive for a period time. The malicious nodes are easily expelled from the initial phase, because the bait RREQ is able to attract the forged RREP from black hole node. In authors' mechanism, the generator of RREP is recorded in the RREP's additional field. Therefore the source node can recognize the location of attacker from the reply location of RREP. Compare with the primitive DSR scheme and watch dog method, the simulation results show that BDSR provides an excellent packet delivery rate. The packet delivery ratio of BDSR is 90% which is more superior to DSR and WD approach. Moreover, the communication overhead is also lower than watch dog scheme but slightly higher than original DSR routing protocol.

III. CONCLUSION AND FUTURE WORK

A Black Hole attack is one of the serious security problems in MANETs. It is an attack where a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have conducted diverse techniques to propose different types of prevention mechanisms for black hole problem. In this paper a survey on different existing techniques for detection of pooled black hole attacks in MANETs with there defects is presented. The detection techniques which make use of proactive routing protocol have better packet delivery ratio and correct detection probability, but have higher overheads. The detection techniques which make use of reactive routing protocols have low overheads, but have high packet loss problem. Therefore, we suggest having a hybrid detection technique which combines the advantages of both reactive and proactive routing for future research direction. Although these may not be avoided in totality, there is a need for trade-offs to achieve a secure optimal performances. The detection of Black Holes in ad hoc networks is still considered to be a challenging task. Future work is intended to an efficient pooled or collaborative Black Hole attack detection and elimination algorithm with minimum delay and overheads that can be adapted for ad hoc networks susceptible to Black Hole attacks.

References

1. Perkins, E. Belding-Royer, and S. Das, "Ad-hoc on-demand distance vector (AODV) routing", Internet Draft, RFC 3561, July 2003.
2. H. Deng, H. Li, and D. Agrawal, "Routing security in wireless ad hoc networks", *IEEE Communications Magazine*, Vol. 40, No. 10, Oct 2002.
3. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, Issue 3, Nov 2007, pp 338–346.
4. Yuh-Ren Tsai, Shiuh-Jeng Wang, *"*Routing Security and Authentication Mechanism for Mobile Ad Hoc Networks*"* Chung-Shan Institute of Science and Technology, Taiwan, R.O.C., under Grant BC-93 B14P and the National Science Council, Taiwan, R.O.C., IEEE 2004.
5. Oliveira R, Bhargava B, Azarmi M, Ferreira EWT, Wang W, Lindermann M (2009) Developing Attack Defense Ideas for Ad Hoc Wireless Networks. Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, 27 September 2009 35
6. Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K (2003) Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003.36
7. Weerasinghe H, Fu H (2007) Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc network smulation Implementation and Evaluation. Paper presented at the Future Generation Communication and Networking, Jeju-Island, Korea, 6-8 December 2007 37
8. Yu CW, Wu T-K, Cheng RH, Chang SC (2007) A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network. Paper presented at the PAKDD workshops, Nanjing, China, 22-25 May 2007 38
9. Wang W, Bhargava B, Linderman M (2009) Defending against Collaborative Packet Drop Attacks on MANETs. Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, 27 September 2009 39
10. Min Z, Jiliu Z (2009) Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks. Paper presented at the International Symposium on Information Engineering and Electronic Commerce, Ternopil, Ukraine, 16-17 May 2009 40
11. Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L (2011) Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs. Paper presented at the 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 13-16 Feb. 2011 43
12. Kozma W, Lazos L (2009) REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits. Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16- 18 March 2009 30
13. B urbank JL, Chimento PF, Haberman BK, Kasch WT (2009) Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology. IEEE Communication Magazine 44(11):39–45. doi: 10.1109/COM-M.2006.248156
14. Dow CR, Lin PJ, Chen SC, Lin JH, Hwang SF (2005) A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-hoc Networks. Paper presented at the IEEE 19th International Conference on Advanced Information Networking and Applications, Tamkang University, Taiwan, 28-30 March 2005
15. Yan g H, Lou H, Ye F, Lu S, Zhang L (2004) Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications 11(1):38–47. doi: 10 .1109/MWC.2004.1269716
16. Deng H, Li W, Agarwal DP (2002) Routing Security in Wireless Ad-hoc Networks. IEEE communications Magazine 40(10):70–75. doi: 10.1109/MCOM.2002.1039859