

COMPARISON BETWEEN VARIOUS BLACK HOLE DETECTION TECHNIQUES IN MANET

Akanksha Saini, Harish Kumar
UIET, Panjab University Chandigarh-160014
sainiakanksha@gmail.com

Abstract: An ad hoc network is a collection of mobile nodes that dynamically form a temporary network and are infrastructure less. A black hole is a malicious node that incorrectly replies the route requests that it has a fresh route to destination and then it drops all the receiving packets. The damage will be serious if malicious nodes work together as a group. This type of attack is called cooperative black hole attack. This paper compares the method proposed by various authors according to their assumptions and the corresponding simulation result in ns2 demonstrates that our protocol not only prevents black hole but also improves performance.

Keywords – Ad hoc network, black hole attack, MANET, AODV

1. INTRODUCTION

Ad hoc network [1] is a wireless network without having any fixed infrastructure. Each mobile node in an ad hoc network moves arbitrarily and acts as both a router and a host. A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. The interconnections between nodes are capable of changing on a continual and arbitrary basis. Nodes within each other's radio range communicate directly via wireless links, while those that are far apart use other nodes as relays. Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks

Black hole attack is one of many possible attacks in MANET. Black hole attack can occur when the malicious node on the path directly attacks the data traffic and intentionally drops, delay or alter the data traffic passing through it. This attack can be easily lessen by setting the promiscuous mode of each node and to see if the next node on the path forward the data traffic as expected. Another type of black hole attack is to attack routing control traffic.

In other type, a malicious node sends a forged Route Reply (RREP) packet to a source node which initiates the route discovery to pretend as destination node. When a source node received multiple RREP it compares the destination sequence number contained in RREP packets and judge the greatest one as the most recent routing information selecting the route contained in that RREP packet. When sequence numbers are equal it selects the route with the smallest hop count. If the attacker spoofed the identity to be the destination node and sends RREP

with destination sequence number higher than the real destination node to the source node, the data traffic will flow toward the attacker.

2. SECURITY ISSUES

MANETs are much more vulnerable to attack than wired network. This is because of the following reasons:

2.1 Open Medium

Eavesdropping is easier than in wired network as there is no centralized medium.

2.2 Dynamically Changing Network Topology – Mobile Nodes comes and goes from the network. They dynamically change their topology. This allows any malicious node to join the network without being detected.

2.3 Cooperative Algorithms - The routing algorithm of MANETs requires mutual trust between the neighbor nodes which violates the principles of Network Security.

2.4 Lack of Centralized Monitoring – There is absence of any centralized infrastructure that prohibits any monitoring agent in the system.

2.5 Lack of Clear Line of Defense - The only use of I line of defense - attack prevention may not secure. Experience of security research in wired world has taught us that we need to deploy layered security mechanisms because security is a process that is as secure as its weakest link. In addition to prevention, we need II line of defense - detection and response.

Realizing security in ad hoc environments is exceedingly difficult since many different types of ad hoc networks exist. Any variation is possible ranging from predominantly static sensor networks to highly mobile vehicular network scenarios. So, it is necessary to design specialized security solutions adapted to the underlying ad hoc network. Not only the network architecture has to face security threats,

also the services and protocols used within the network have to withstand many different attacks.

3. SECURITY ATTACKS

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following two types:

External attacks: In this attack the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

Internal attacks: It is an attack in which the opponent wants to gain the normal access to the network and participates the network activities by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

Examples of security attacks:

3.1 Denial of Service (DoS): It aims to grab the availability of certain node or even the services of the entire ad hoc networks. In the traditional wired network, the DoS attacks are carried out by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and make the services provided by the target become unavailable.

3.2 Impersonation: Impersonation attack is a severe threat to the security of mobile ad hoc network. If there is not such a proper authentication mechanism among the nodes, the opponent can capture some nodes in the network and make them look like benign nodes. In this way, the compromised nodes can join the network as the normal nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

3.3 Eavesdropping: Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

3.4 Sinkhole attack: The attacking node tries to offer a very attractive link e.g. to a gateway. Therefore, a lot of traffic bypasses this node. Besides simple traffic analysis other attacks like selective forwarding or denial of service can be combined with the sinkhole attack.

3.5 Wormhole attack: The attacker connects two distant parts of the ad hoc network using an extra communication channel (e.g. a fast LAN connection) as a tunnel. As a result two distant nodes assume they are neighbors and send data using the tunnel. The attacker has the possibility of conducting a traffic

analysis or selective forwarding attack.

3.6 Sybil attack: The sybil attack especially aims at distributed system environments. The attacker plays multiple roles. It tries to act as several different identities/nodes rather than one. This allows him to forge the result of a voting used for threshold security methods for more information. The cloud appears to be many different nodes to the outside.

3.7 Traffic Analysis: It is a passive attack used to gain information on which nodes communicate with each other and how much data is processed.

4. LITERATURE SURVEY

A number of protocols were proposed to solve the black hole problem. It requires a source node to initiate a checking procedure to determine the reliability of any intermediate node claiming that it has a fresh enough route to the destination.

Payal N. Raj, Prashant B. Swadas [6] proposed DPRAODV (detection, prevention and reactive AODV) to prevent security of black hole by informing other nodes in the network. It uses normal AODV in which a node receives the Route reply (RREP) packet which first checks the value of sequence number in its routing table. The RREP is accepted if its sequence is higher than that in the routing table. It also check whether the sequence number is higher than the threshold value, if it is higher than threshold value than it is considered as the malicious node. The value of the threshold value is dynamically updated in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The node that is detected as the anomaly is black listed and ALARM packet is sent so that the RREP packet from that malicious node is discarded. The routing table for that node is not updated nor is the packet forwarded to others. Their solution increases the average end to end delay and normalized routing overhead.

Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard [7] proposed a method for identifying multiple black hole nodes. They are first to propose solution for cooperative black hole attack. They slightly modified AODV protocol by introducing data routing information table (DRI) and cross checking. Every entry of the node is maintained by the table. They rely on the reliable nodes to transfer the packets. The Route request (RREQ) is sent by source to every node and it send packet to the node from where it get the RREP. The intermediate node should send NHN and the DRI entry to the table. The source node (SN) check own DRI whether intermediate node (IN) node is reliable or not. The SN send the further request to next hop node (NHN) for IN. If SN uses IN to send

the packet then it is considered as reliable node otherwise not. Cross checking is done on the intermediate nodes. It is one time procedure. The cost of cross checking is more. It can be minimized by letting nodes sharing their trusted nodes list with each other.

Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park [8] proposed two different approaches to solve the black hole attack. The first solution the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the redundancy of the network. The idea of this solution is to find more than one route for the destination. The SN unicast the ping packet using different routes. The IN or destination node or malicious node will ping requests. The SN checks the acknowledgment and processes them to check which one is safe or having malicious node. In the meantime the SN buffered its packet until it found the safe route. When the route is identified the buffered packets will be transmitted to it. The drawback of the solution is the time delay. The second solution is to store the last sent packet sequence number and the last received packet sequence number in the table. It is updated when any packet is arrived or transmitted. When node receives reply from another node it checks the last sent and received sequence number. If there is any mismatch then an ALARM indicates the existence of a black hole node. This method is faster and more reliable and has no overhead.

Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park [8] proposed two different approaches to solve the black hole attack. The first solution the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the redundancy of the network. The idea of this solution is to find more than one route for the destination. The SN unicast the ping packet using different routes. The IN or destination node or malicious node will ping requests. The SN checks the acknowledgment and processes them to check which one is safe or having malicious node. In the meantime the SN buffered its packet until it found the safe route. When the route is identified the buffered packets will be transmitted to it. The drawback of the solution is the time delay. The second solution is to store the last sent packet sequence number and the last received packet sequence number in the table. It is updated when any packet is arrived or transmitted. When node receives reply from another node it checks the last sent and received sequence number. If there is any mismatch then an ALARM indicates the existence of a black hole node. This method is faster and more reliable and has no overhead.

In [6] Hongmei Deng, Wei Li, and Dharma P. Agrawal proposed a solution for single blackhole node detection. In the proposed method, each

intermediate node to send backs the nexthop information when it sends back an RREP message. When the source node receives the reply message, it does not send the data packets right away, but extracts the nexthop information from the reply packet and then sends a Further- Request to the nexthop to verify that it has a route to the intermediate node who sends back the Further reply FRp message, and that it has a route to the destination node.

Limitation of this proposal is that it would not be able to identify that NHN works cooperatively with IN and sends back false FRp

Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng, and Shun Chao Chang [9] 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. Immediately after the conformation of black hole, the global reaction is activated to establish proper notification system to send warning to the whole network. The simulation result show the higher black hole detection rate and achieves better packet delivery. When the network is busier it achieves less overhead. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto [10] use an anomaly detection scheme. It uses dynamic training method in which the training data is updated at regular time intervals. Multidimensional feature vector is defined to express state of the network at each node. Each dimension is counted on every time slot. It uses destination sequence number to detect attack. The feature vector include Number of sent out RREQ messages, number of received RREP messages, the average of difference of destination sequence number in each time slot between sequence number of RREP message and the one held in the list. They calculate mean vector by calculating some mathematical calculation. They compare distance between the mean vector and input data sample. If distance is greater than some threshold value then there is an attack. The updated data set to be used for next detection. Repeating this for time interval T anomaly detection is performed.

Hongmei Deng, Wei Li, and Dharma P. Agrawal [11] proposed a solution for single blackhole node detection. In this method, each intermediate node is used to send backs the next hop information when it sends back an RREP message. After getting the reply message, the source node does not send the data packets but extracts the next hop information from

the reply packet and then it sends a Further- Request to the next hop to verify that it has a route to the intermediate node who sends back the Further reply message, and that it has a route to the destination node.

Latha Tamilselvan, Dr. V Sankaranarayanan[12] proposed a solution with the enhancement of the AODV protocol which avoids multiple black holes in the group. A technique is give to identify multiple black holes cooperating with each other and discover the safe route by avoiding the attacks. 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 reliability to that node. Any node having '0' value is considered as malicious node and is eliminated. The fidelity level of each RREP is checked and if two are having same level then one is selected having highest level. The responses are collected in the response table. A valid route is selected among the received based on the threshold value. After getting the acknowledgement the fidelity level of the node is updated proving it safe and reliable. The black hole node is accomplished by ALARM packets. Simulation result provides a better packet delivery ratio as the nodes are in motion.

Hesiri Weerasinghe [13] 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 a slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP). The simulation result shows that the AODV and the solution proposed by Deng et al. highly suffer from cooperative black hole in terms of throughput and packet losses. The performance of the solution is good and having better throughput and minimum packet loss percentage over other solutions.

5. COMPARISON

Few proposals assumed:

- 1) Single Black Hole node in a network
- 2) Multiple Black Hole nodes in the ad hoc network

Black hole attack detection proposals can be categorized as below:

- 1) Single non malicious nodes identifying a black hole node
- 2) Multiple non malicious nodes identifying a

black hole node

Table 1: Comparison of various black hole node detection schemes

Proposal name	Approach	Assumption	Philosophy
Dynamic learning system using DPRAODV	DPRAODV	Multiple black hole	Single non-black hole node detects
Cooperative black hole node detection using DRI and cross checking	AODV	Cooperative black hole	Single non-black hole node detects
Black hole node detection using two different solutions	AODV	Multiple black hole	Single as well as Multiple non black node detects
Distributed and cooperative mechanism	AODV	Distributed and cooperative	Cooperative detection
Detecting Black hole Attack on AODV-based Mobile Ad Hoc using dynamic anomaly detection	AODV	Multiple black hole	Single non black hole node detects
Single black hole node detection	AODV	Single black hole	Single non black hole node detects
Prevention of Black hole Attack using fidelity table	Enhancement on AODV	Multiple black hole	Multiple non- black hole node
Detection of black hole using DRI and Cross checking	Modified version of AODV	Multiple black hole	Multiple non-black hole nodes detects
Detection using neighborhood based method	AODV	Multiple black hole nodes	Multiple non black hole nodes detects
Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs	TOGBAD approach	Single black hole	Single black hole node detects

6. CONCLUSION

The various authors have given various proposals for detection and prevention of black hole attack in MANET but every proposal has some limitations and their respected solutions. The approaches leads to black hole node detection but no one is reliable procedure since all mobile nodes cooperate together to analyze and detect possible multiple black hole nodes.

Future work includes intend to develop simulations to analyze the performance of the proposed solutions and compare their performances.

7. REFERENCES

- [1] Mohammad AL-Shurman, Seon-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04, April 2-3, 2004, Huntsville, AL, USA.
- [2] Bo Sun, Yong Guan, Jian Chen, Udo, "Detecting Black-hole Attack in Mobile Ad Hoc Network", The institute of Electrical Engineers, Printed and published by IEEE, 2003.
- [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] Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network", Springer-Verlag Berlin Heidelberg, 2007.
- [5] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing security in Wireless Ad-hoc Network", IEEE Communications Magazine, Issue 40, pp 70-75, 2002
- [6] Payal N. Raj and Prashant B. Swadas, "DPRAODV: A dynamic learning system against black hole attack in AODV based Manet", International Journal of Computer Science Issues (IJCSI), Vol. 2, Issue 3, pp: 54-59, 2009
- [7] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks"
- [8] Mohammad Al-Shurman and Seong-Moo Yoon and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks"
- [9] Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", PAKDD 2007 Workshops, pp. 538-549, 2007
- [10] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, Issue 3, pp: 338-346, 2007
- [11] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, vol. 40, Issue: 10, 2002
- [12] Latha Tamilselvan, Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), 2007
- [13] Hesiri Weerasinghe, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking, vol. 02, pp: 362-367, 2007