International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(2): 336-343
The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085)

Mitigation of Black Hole Attacks for AODV Routing Protocol

Kamarularifin Abd. Jalil[1], Zaid Ahmad[2], Jamalul-Lail Ab Manan[2],

[1]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Malaysia,
Shah Alam, Selangor, Malaysia.
kamarul@tmsk.uitm.edu.my
[2]Advanced Information Security, MIMOS Berhad
Technology Park Malaysia, Kuala Lumpur, Malaysia.
{zaid.ahmad, jamalul.lail}@mimos.my

ABSTRACT

Ad hoc On Demand Vector (AODV) is a reactive routing protocol in Mobile Ad hoc Network (MANET). Although the protocol has been around for quite some time, but there is still security issue which made it vulnerable to various attacks such as black hole which tremendously affects the network performance. There have been several works done to mitigate this problem but most of the proposed methods introduce overhead to the existing protocol i.e. extra control messages. Most of MANET devices are resource constraint and therefore a light solution is needed. For this reason, in this paper we proposed a method called ERDA (Enhance Route Discovery for AODV). The proposed method is able to mitigate the aforesaid problem by introducing new conditions in the routing table update process and also by adding simple malicious node detection and isolation process to the AODV route discovery mechanism. The proposed method does not introduce any additional control message and moreover, it does not change the existing protocol scheme. In order to test the proposed method, a simulation model was developed. The simulation results show significant improvement to the network performance after ERDA is implemented in the AODV as compared to the existing AODV protocol.

KEYWORDS

black hole attack; ad hoc on-demand distance vector; mobile ad hoc networks; route discovery; ERDA; MANET; receive reply message; AODV.

1 INTRODUCTION

A mobile ad hoc network (MANET) is a group of mobile devices connected by wireless link without require fix common infrastructure in place like wireless access point or radio based-station. MANET has dynamic topology where devices or nodes in the network can change their position or disappear from the network rapidly. One of the challenges faced by nodes in a MANET is limited resources such as battery lifetime and also the security of its routing protocol. Since MANET is formed in an ad hoc manner, cooperation amongst the nodes to establish the network path is needed. The network for nodes which are not within communication range will be established through a multi-hop link which requires every node to act as a router as well as a normal host. In router mode the node has to discover the route and deliver the data with the help of the routing protocol.

In this paper we focus on Ad hoc On-demand Distance Vector (AODV)

protocol [1] which is one of the reactive ad hoc routing protocols [2] in MANET. One of the strengths of AODV is its capability to adapt smoothly in a dynamic network environment like MANET because of its low control message overhead. However, it has a drawback i.e. the protocol was designed without any security consideration hence making it vulnerable to security attacks [4]. The condition becomes more serious as MANET uses ether to propagate the message and on the same time the communication channel is always open to various attacks.

Black hole is one of many attacks that take place in MANET and it is one of the most common attacks made against the AODV routing protocol. The black hole attack will disrupt the network and affect the whole network performance. The malicious node in a black hole will pretend to have the shortest and freshest route to the destination node by manipulating the control message [3] to attract other nodes to send their data through its node.

AODV works base on destination sequence number and hop count attribute to determine the freshness and shortest path of the route. However these two attributes are not sufficient to reduce the effect of black hole attack in the network. The existing method of routing update in AODV gives opportunity for attackers to manipulate these attributes. By manipulating those attributes. The attacker can deny Route Reply (RREP) messages from benign nodes to update the routing table.

In our review of previous works, most methods added new control message to the existing protocol scheme to overcome this problem. This approach is considered costly because it introduces overhead to the AODV process during the route discovery phase. Due to that, we devise a new method called ERDA (Enhanced Route Discovery AODV) which has less overhead in the mitigation process to overcome the effect of the black hole attacks. It works without changing the existing protocol scheme. This method improves the routing update process as well as analyzing the receive reply control messages (RREP) to isolate black hole malicious nodes. This method assumes the destination node is reachable by route request and normal black hole characteristic is high destination sequence number carried in route reply.

This paper is organized as follows. Section 2 provides an overview of the AODV route discovery process and a description of a black hole attack. Section 3 discusses about related works. Section 4 presents the ERDA, a proposed method to mitigate the black hole attack. Section 5 discusses about simulation result and lastly, plans for the future work are concluded in Section 6.

2 AODV ROUTING PROTOCOL

AODV is a dynamic reactive routing protocol [5]. As a reactive routing protocol, a route will be established on demand basis (upon request by source node). The process to discover the route to the destination node is illustrated in Figure 1. In AODV route discovery protocol, Route Request (RREQ) and Route Reply (RREP) are two important control messages. They carry two attributes i.e. destination sequence number and hop count. To determine the freshness of a particular route, both numbers are incremental value.

2.1 Route Discovery Process

In Figure 1 illustration, the source node S start broadcasting its control message RREQ to reachable neighbors A, B and C to request for best possible path to the destination node D. Upon receiving the RREQ message, node A, B and C either:

a) Reply RREP message to the source node if the node is the destination node or the node is an intermediate node with a 'fresh enough' route information to the destination, or
b) Update the routing table entry as the reverse path and rebroadcasting the RREQ message until the destination node or intermediate node with 'fresh enough route' is received the RREQ message.

Upon receiving the RREQ message from node A, the destination node D generates RREP and forwards the message to node A. Node A updates its routing table and forwards the RREP message to node S. Source node S calls AODV recvReply() function to update the route entry in routing table for destination node D if one of these conditions is met.

a) The destination sequence number in RREP message is higher than the one in routing table or
b) The hop number in RREP message is less than the one in routing table if both destination sequence number is equal.

The explanation of normal recvReply() mechanism is described in Figure 2.

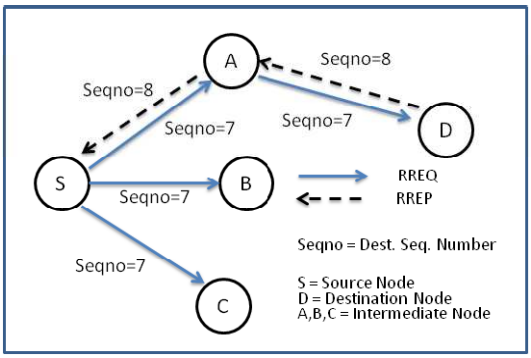

Figure 1. AODV route discovery process

```
AODV
1   RecvReply(Packet P) {
2   if (P.dst no entry in Routing Table RT) {
3      Add entry of P.dst to RT
4   }
5   select dst_seqno from RT
6   if (P.dst_seqno > RT.dst_seqno or
7     P.dst_seqno = RT.dst_seqno and P.hops < RT.hops) {
8        update RT entry with P
9        send data packets to the route in RT
10  }
11  else  if (routing is UP for P)  {
12        forward packet P
13        else  discards   P
14        }
15  }
```

Figure 2. Normal AODV recvReply() function

2.2 Black hole Attack

The black hole attack is a kind of denial of service attack [6] where it will disrupt the network and the result affects the whole performance of the network. The attack is made by malicious node which attacks the AODV control message. The diagram in Figure 3 is the attack model on how the malicious node M pretends to be a node with attractive route to the destination node D. Upon receiving the RREQ message from node C, node M immediately generates RREP message and send it to source node S. In large network, there is a possibility to have more than one reply of RREP massage. In order to be favored against others, the destination sequence number sent by

node M normally higher and it is sent ahead from the rest. Characteristic of AODV will make Node S will believe that the first RREP received (through node C) is the shortest and up-to-date path to destination node D. As a result, node S updates its routing table by taking node C as its next hop to send out data to node D. Node C with infected route entry forwards the data packet to node M. Node M either keeps or drops the packet without forwarding it to the destination node D as if the packet is disappeared in a black hole as the attack name implies.

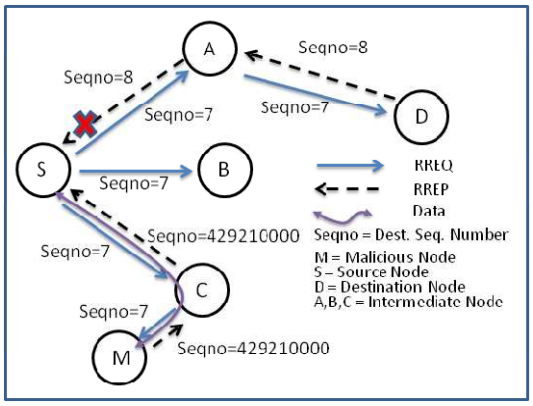

Figure 3. Black hole attack model in AODV

3 RELATED WORKS

A lot of attention is given by researchers to find a method to defeat the effect of black hole attack in AODV. One example is by S. Jain [7] which using a technique based on sending data equally but in small blocked size and the message is monitored independently at neighborhood. Another example is the work done by A. Baadache [8] which has proposed a method based on Merkle tree which requires hashing technique to detect malicious node. E.A Mary [9] has proposed certificate based authentication to counter the effect of black hole attack. S. Deswal [10] worked on SAODV by using password security for each routing node and updates the routing table timeliness. Zhang and Lee [11] present an intrusion detection technique for wireless ad hoc networks that uses cooperative statistical anomaly detection techniques. S. Lee in [12], uses the method which requires the intermediate node to send Route Confirmation Request (CREQ) to the next hop towards the destination.

The proposed methods above require additional control message either by using cryptographic technique or introducing extra messages to existing protocol. Those techniques can increase the routing overhead which will then result in the performance degradation especially in presence of the black hole during route discovery process.

In a related research, Stamouli [13] has proposed the architecture for Real-Time Intrusion Detection for Ad hoc Networks (RIDAN). The detection process relies on a state-based misuse detection system. As a result, each node would require extra processing power and sensing capabilities. M.A. Shurman [14] in his work has proposed for the source node to verify the authenticity of the node that initiates the RREP messages by finding more than one route to the destination, so that it can recognize the safe route to the destination. This method can cause routing delay, since a node has to wait for a RREP packet to arrive from more than two nodes. Dokurer [15] has proposed a solution based on ignoring the first established route. His assumption is based on the fact that the first RREP message that arrived at a node normally would come from a malicious node. Unfortunately, this method does not cater if the second RREP message received at a source node may also come from malicious node.

This method also does not address on the isolation of malicious nodes in the network.

In a related work proposed by N.R. Payal [16], the method checks the RREP destination sequence number against a threshold value which is dynamically updated [17] at every time interval. If the value is higher than the threshold, the RREP is suspected to be malicious. This method introduces ALARM packet to be sent to the neighbor nodes which contains the black list (malicious) node as a parameter. An overhead of updating threshold value at every time interval along with the generation of ALARM packet will considerably increase the routing overhead. N.H. Mistry in [18] has proposed for the source node to verify the RREP destination sequence number by analyzing the RREP messages using the heuristic method which is collected within the predefined waiting period. If the sequence number is found to be exceptionally high, the sender of the respective RREP will be marked as malicious node. The major issue in this method is the latency time during the route discovery process since the source node has to wait until the waiting time period expired before the routing table can be updated. In the event where there is no attack in the network, the node still suffers with the latency time.

4 ERDA: THE PROPOSED MITIGATION METHOD

The ERDA is designed to improve AODV protocol with minimum modification to the existing route discovery mechanism recvReply() function. There are three new elements introduced in modified recvReply() function namely: table rrep_table to store incoming RREP packet parameter mali_list to keep the detected malicious nodes identity and parameter rt_upd to control the process of updating the routing table. The pseudo code of modified recvReply() function is shown in Figure 4.

Unlike the conventional AODV protocol, ERDA will secure the routing update by imposing an additional condition controlled by parameter rt_upd. This parameter only receives either true or false value. By default, the value is set to true which means the routing table is allowed to be updated regardless of what value the existing two conditions have e.g. the destination sequence number in the RREP message is less than the one in the routing table.

Explanations on how the ERDA works is described in Figure 5. When route request (RREQ) message is sent out by the source node S to find a fresh route to the destination node D, all nodes that have “fresh enough route” information will response to the request including the destination node D as shown in Figure 5(a). RREP messages received by node S will be captured into rrep_tab table. Figure 5(b) shows the information stored in the rrep_tab table, node_id and destination sequence number. Since the malicious node M is the first node to response, the routing table of node S is updated with RREP information from node M as depicted in Figure 5(c). Since the value of parameter rt_upd is ‘true’, node S accepts the next RREP messages from node A to update the routing table although it arrives later and with a lower destination sequence number than the one in the routing table. As a result, the current route entry in routing table will be overwritten by the later RREP coming from node A as shown in Figure 5(d). ERDA method offers a simple

solution by eliminating the false route entry and replaced the entry with later RREP. Based on possibility of later RREP is came from the actual destination node D, the rt_upd parameter value is then set to false when reply from destination node is received. Any RREP message that comes after when rt_upd is false will be ignored until the process of detecting malicious node complete.

```
ERDA
1   RecvReply(Packet P) {
2    save P.srcIP and P.dst_seqno to rrep_tab
3    if (rt_upd = false) {
4       detect malicious node and save in mali_list
5       flush rrep_tab
6       set rt_upd to true
7    }
8    if (P.dst no entry in Routing Table RT) {
9       Add entry of P.dst to RT
10  }
11  select dst_seqno from RT
12  if (rt_upd = true) or
13    (P.dst_seqno > RT.dst_seqno or
14    P.dst_seqno = RT.dst_seqno and P.hops < RT.hops) {
15       if (P is from request destination node)
16          set rt_upd to false
17       update RT entry with P
18       send data packets to the route in RT
19  } else if (routing is UP for P)  {
20              forward packet P
21          else discards  P
17          }
18 }
```

Figure 4. Modified recvReply() function in ERDA

As pointed out in section 4.1 above, the RREP's information like node id and destination sequence number is saved in the rrep_tab table without change the flow of AODV protocol scheme. If the parameter rt_upd is 'false', ERDA start triggering the process of analyzing the information in the rrep_tab table using heuristic method. Node id which has exceptionally high destination sequence number will be suspected as a malicious node [18]. The identity of those nodes will be kept in the mali_list list. All nodes listed in the mali_list will be isolated from participating in future route discovery updates. Any RREP messages that come from those nodes will be discarded. In order to ensure that this process consumes less memory, the rrep_tab table will be flushed and the parameter rt_upd is set back to 'true' once the process of identifying malicious node is completed.

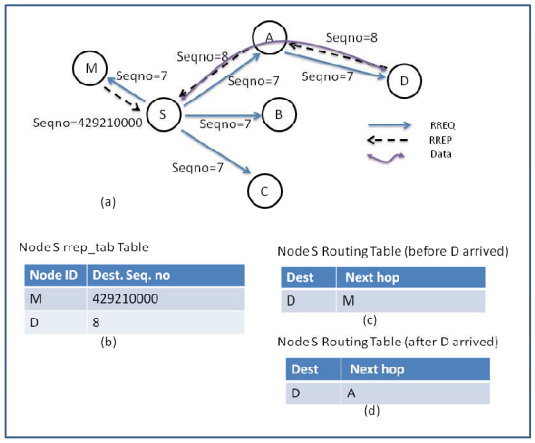

Figure 5. ERDA method .in AODV Route Discovery process

5 EVALUATION METHOD

5. 1 Simulation Setup

A simulation model was developed using NS-2 (version 2.34) where the evaluation was done by analyzing the performance result of two conditions 1) using normal AODV protocol and 2) using AODV protocol built with ERDA method.

Overall simulation parameters were summarized in Table 1. In order to ensure consistency and uniformity in the simulation, the same connection pattern was used throughout all experiments.

Table 1. Simulation Parameters

Parameter	*Value*
Simulator	*NS-2 version 2.34*
Simulation Time	*100s*
Number of nodes	*10 to 80*
Routing Protocol	*AODV*
Traffic Model	*CBR*
Pause time	*5 s*
Mobility	*Up to 3 m/s*
Terrain	*800 x 800m*
Transmission Range	*250m*
Malicious nodes	*1 - 3*

5.2 Simulation Results and Analysis

We simulated the black hole attack in five different scenarios. The simulation model was developed in order to see the effect of such attacks on the performance of both Normal AODV as well as AODV with ERDA method. Packet Delivery Ratio (PDR) was used as a performance metric to evaluate the performance of both methods.

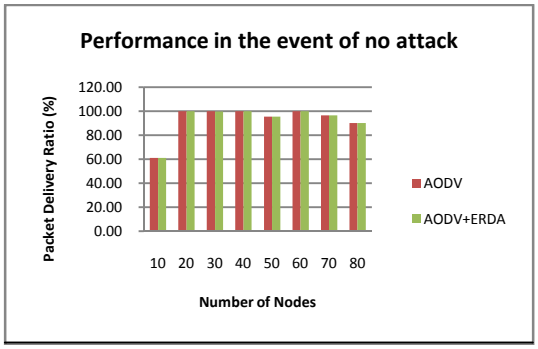

Figure 6. Packet delivery performance in absence of Black hole in different network sizes.

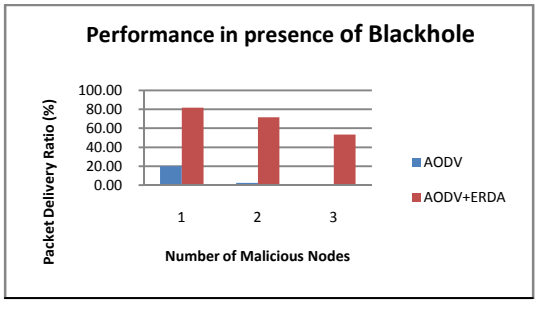

Figure 7. Packet delivery performance in presence of varies number of malicious nodes.

There was no significant performance change to the AODV during the absence of black hole although ERDA was added to the protocol. It shows that there is no overhead in this method. The result in Figure 6 shows that the performance was consistent even though the network size was varied.

When the number of malicious node increases, as depicted in Figure 7, the AODV with ERDA method provided significant improvement in terms of packet delivery. Even though there was a ~~it~~ decrease~~d~~ when the malicious node increases but the drop is not as drastic as compared to the normal AODV.

6 CONCLUSIONS AND FUTURE WORKS

In this paper, the issue of black hole attack and its affect on the AODV-based routing protocol has been discussed. A few methods to overcome this problem have been proposed. The route discovery process in the AODV is susceptible to black hole attack and therefore, it is vital to have an efficient security method built into the AODV protocol in order to mitigate the effect of such attacks. ERDA is designed to isolate and mitigate the effect of black hole attacks in MANET. ERDA enhances recvReply() function in the AODV protocol to improve the network performance by improving routing update condition. The enhancement only involves a minimum modification and does not change the existing AODV protocol scheme. The solution is also light and suitable for most resource constraint devices.

As future work, we intend to perform more extensive simulation test on ERDA method. Research areas potentially to be examined in the future 1) Exploring a

new method for the ERDA to identified malicious node based on outlier detection algorithm [19][20]. 2) Performance and effectiveness of the ERDA to combat collaborative black hole and non-black hole attack in MANET. 3) Information sharing protection and privacy preservation in MANET using trusted ERDA.

6 REFERENCES

1. Perkin, C.E., Royer, E.M.: Ad-hoc on demand distance vector routing. In: Proceedings of 2nd IEEE Workshop on Mobile Computer Systems and Applications, New Orleans (1999)
2. Abolhasan, M., Wysocki, T., Dutkiewicz, E.: A review of routing protocols for mobile ad hoc networks. Elsevier, Amsterdam (2004)
3. Mahmood, R.A., Khan, A.I.: A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks. In: International Symposium on High Capacity Optical Networks and Enabling Technologies (2007)
4. Perkin, C.E.: Ad hoc On Demand Distance Vector (AODV) Routing. Internet draft, draft-ietf-manetaodv-02.txt (November 1988)
5. Kumar, V.: Simulation and Comparison of AODV and DSR Routing Protocols in MANETs, Master Thesis (2009)
6. Xing, F., Wang, W.: Understanding Dynamic Denial of Service Attacks in Mobile Ad hoc Networks. In: IEEE Military Communication conference, MILCOM (2006)
7. Shalini Jain, Mohit Jain, Himanshu Kandwal, Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks, International Journal of Computer Applications Volume 1 (2010)
8. Abderrahmane Baadache, Ali Belmehdi, Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010
9. E. A .Mary Anita, V. Vasudevan, Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining, International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 12 (2010)
10. Suman Deswal and Sukhbir Singh, Implementation of Routing Security Aspects in AODV, International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010
11. Sanzgiti, K., Dahill, B., Levine, B.N., Shields, C., Elizabeth, M., Belding-Royer: A secure Routing Protocol for Ad hoc networks. In: Proceedings of the 10th EEE International Conference on Network Protocols, ICNP 2002 (2002)
12. Hu, Y.-C., Johnson, D.B., Perrig, A.: SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks. In: Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, pp. 3–13 (June 2002)
13. Hu, Y.-C., Perrig, A., Johnson, D.B.: Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks. In: Proc. 8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom 2002), Atlanta, Georgia, pp. 12–23 (September 2002)
14. Zhang, Y., Lee, W.: Intrusion detection in wireless ad – hoc networks. In: Proceedings of the 6th annual international Mobile computing and networking Conference (2000)
15. Lee, S., Han, B., Shin, M.: Robust routing in wireless ad hoc networks. In: ICPP Workshops, p. 73 (2002)
16. Stamouli, I.: Real-time Intrusion Detection for Ad hoc Networks. Master's thesis, University of Dublin (Septermber 2003)
17. Shurman, M.A., Yoo, S.M., Park, S.: Black hole attack in wireless ad hoc networks. In:ACM 42nd Southeast Conference (ACMSE 2004), pp. 96–97 (April 2004)
18. Dokurer, S.: Simulation of Black hole attack in wireless Ad-hoc networks. Master's thesis, Atılım University (September 2006)
19. Raj, P.N., Swadas, P.B.: DPRAODV: A Dynamic Learning System Against Blackhole Attack In Aodv Based Manet. International Journal of Computer Science Issues 2, 54–59 (2009)
20. Kurosawa, S., Nakayama, H., Kat, N., Jamalipour, A., Nemoto, Y.: Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. International Journal of Network Security 5(3), 338–346 (2007)