ERDA: Enhanced Route Discovery Mechanism for AODV Routing Protocol against Black Hole Attacks

Kamarularifin Abd. Jalil¹, Zaid Ahmad², Jamalul-Lail Ab Manan²,

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. Due to the unique characteristic of Mobile Ad hoc Network (MANET) and lack of security in its routing protocol, MANET is vulnerable to various attacks such as Black hole. In this paper we study a Black hole attack on one of ad hoc routing protocol called AODV (Ad hoc On Demand Vector). There have been many works done to solve this problem but most of them introduced extra overheads. In this paper we proposed a novel method to address this limitation called ERDA (Enhance Route Discovery for AODV) by improving the route discovery mechanism in the AODV protocol. The first part of this method is to secure the routing table update by introducing new parameter called rt_upd in recvReply() algorithm of AODV. The second part is to analyze AODV Receive Reply messages stored in a table called rrep_tab to isolate malicious nodes by maintaining those nodes in a list called mali_list. ERDA provides secure and low latency of route discovery as compared to previous methods. We perform various simulations to evaluate AODV performance with and without ERDA method and analyse the performance in condition where the Black hole is presence and not presence in the network.

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

1 Introduction

Mobile ad hoc network (MANET), a group of mobile devices connected mostly by wireless link in temporary manner does not require fix infrastructure or centralised management like access point or based-station. It is useful in situation where creating the network infrastructure would be impossible or prohibited by certain reasons. The networks’ nodes can be static but most of the time they are mobile and dynamic - free to enter or leave the network. As a result, the network topology always frequently changed. Mobile nodes in the same communication range can communicate directly amongst them but, if they are out of range, they require cooperation from other nodes
to relay their messages which it called multi-hop network. Thus, each node in MANET plays two roles, i.e., as a host and as a router. In a multi-hop network, managing the routing path is crucial and requires standard routing protocol to facilitate the end-to-end communication. The Ad hoc On-demand Distance Vector (AODV) protocol [1] is an example of an ad hoc routing protocol [2] available today.

MANET begins to be attractive network to mobile users because of characteristics it is owned. Unfortunately, the MANET is also vulnerable to attack like any other wireless networks. This is due to the fact that wireless networks use the ether to propagate information which is also accessible by attackers. Moreover, to differentiate between normal and abnormal activities in a mobile network is not an easy task because there are no strong security features in the existing ad hoc routing protocol like AODV. Without strong security features in ad hoc routing protocol i.e. AODV, it is become easier for compromised or malicious node to inject false routing information to the network with the intention to interrupt or spy the communication channel. Black hole is one of many attacks that take place in MANET and is considered as one of the most common attacks made against the AODV routing protocol. The Black hole attack involves malicious node pretending to have the shortest and freshest route to the destination by constructing false sequence number [3] in control messages.

AODV protocol originally was created without any security considerations [4]. Thus, no protection mechanism was built to detect the existence of malicious attack. One of AODV vital task is to maintain a fresh route to destination due to the rapid change of the network topology. It is done through route discovery process. In AODV, the destination sequence number and the number of hop are important attributes to determine the freshness of the route and these attributes are easy to be manipulated by attackers. In Section 2, the detail information about the routing update in AODV discovery process will be explained. However, it was observed that the current route discovery mechanism use in AODV is not sufficient enough to handle Black hole attacks since it algorithm is based on the largest sequence number and less hops count attributes. Such algorithm would open up the opportunity for malicious nodes in Black hole to manipulate these attributes. This could be seen in a Black hole attack scenario, where a malicious node will deny the reply message from benign nodes including the reply message coming from the destination node itself.

Therefore, security in ad hoc routing protocol such as the AODV is very crucial and the researchers in MANET around the world keep searching to develop a secure and efficient routing protocol for wireless ad hoc network. In this paper, we study various methods proposed in the previous works to overcome the Black hole attack in the AODV-based MANET. Most of the works previously done which will be explained in following chapter to solve this problem have some limitations and costly in terms
of having extra overhead in the processing time during route discovery phase. We have devised a novel method to secure the network from the Black hole attack by enhancing the existing AODV route discovery process mechanism. We proposed a method by improving the algorithm of the recvReply() function in the AODV routing protocol which we called as ERDA (Enhanced AODV). As described in Section 4, the proposed algorithm will has minimum modification to the conventional AODV protocol and less delay.

This paper is organised 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 proposed ERDA, a new method to detect and prevent the Black hole attack. Section 5 explains the evaluation method. Section 6 discusses about the simulation results and lastly, the conclusion and future work is concluded in Section 7.

2 Ad hoc On-demand Distance Vector

AODV is categorised as a dynamic reactive routing protocol [5]. In a reactive routing protocol, route will be established based on the demand (upon request by source node). The process to discover routing path to the destination node is illustrated in Figure 1. In AODV route discovery, there are two important control messages namely Route Request (RREQ) and Route Reply (RREP). Both control messages carry an important attribute called destination sequence number and has the incremental value to determine the freshness of a particular route.

2.1 Route Discovery Process

In this illustration, the source node S will broadcast control packets, RREQ message to its neighbours A, B and C in order to find the best possible path to the destination node D. Upon receiving the RREQ message, the received node either:

a) replies to the source node with a RREP message if the received node is the destination node or an intermediate node with a ‘fresh enough’ route information to the destination, or

b) updates the routing table entry which will be used in the reverse path and the rebroadcasting of the RREQ message until the destination node or intermediate node with ‘fresh enough route’ is reached.

An intermediate node is believed to have a ‘fresh enough routes’ to the destination node if the destination sequence number in its routing table is greater than or equal (with less hop count) to the destination sequence number in the RREQ message.
As mentioned in section 2.1.a above, upon receiving the RREQ message from node A, the destination node D will reply with the RREP message to node S by forwarding the message to node A. In turn, node A will forward the message to the source node S. Once the source node S received the RREP message, it will process the message by calling the AODV recvReply() function. This function will update the route entry for destination D if either one of this condition is met.

a) The destination sequence number in the routing table is less than the destination sequence in the RREP message or

b) The destination sequence number in the routing table is equal with the destination sequence number in the RREQ message but the hop count is less than the one in the routing table.

In case where node S received multiple RREP messages, this function will select the RREP message with the highest destination sequence number value. The detail mechanism of recvReply() function is explained in the Pseudo Code given in Figure 2.

Figure 1 AODV route discovery process
2.2 Black Hole Attack

A Black hole attack is a kind of denial of service attack [6] where a malicious node can falsely claiming it has a ‘fresh enough route’ information to the destination. The modus operandi of a Black hole attack in the AODV is by attacking the control message sent during the route discovery process whereby a forged RREP message is sent out to catch the attention of other nodes. Apparently, the malicious node will claim that it has the ‘fresh enough route’ information to the destination. If the other nodes fall into this trap, they will send their data packets through the malicious node. The diagram in Figure 3 demonstrates how the malicious node M pretends to be the node with a ‘fresh enough route’ to the destination node D. Upon receiving the RREQ message from node C, node M will generate the RREP message and send it immediately to source node S. The message will contain the faked destination sequence number. There will be more than one RREP massages replied and in order to be favoured against others, the destination sequence number from node M normally higher. In addition, to ensure that it is ahead from the rest of the nodes in sending out the RREP messages, the malicious node will ignore its routing table checking. The source node S will update its routing table, by assuming that the first RREP received is the shortest and freshest path to destination node D. As a result, node S will take the node C as the next hop (malicious path) to send its data to the destination node D. Node C will then forward that data packet to node M. Upon receiving the data packet,
node M either will keep or drop the packet without forwarding to the destination node D as if the packet is swallowed by a Black hole as the attack name implies.

3 Related Works in Black Hole Attack Solution

There have been quite a number of works done in securing the routing protocol in MANET from the Black hole attack. One example is by S. Yi [7] which looked at the Security-Aware Ad hoc Routing (SAR) using the security attributes such as trust values and relationships. Another example is the work done by Kimaya [8] which has proposed the used of Authenticated Routing for Ad hoc Networks (ARAN) i.e. a standalone protocol that uses cryptographic public-key certificates in order to achieve the security goals. Y.C Hu [9] on the other hand, has worked on the Secure Efficient Ad hoc Distance Vector Routing Protocol (SEAD) which employs the hash chains to authenticate hop counts and sequence numbers in the Distance Sequence Distance Vector (DSDV) protocol. Y.C Hu has also worked on Ariadne [10], which happen to be another secure routing protocol and it uses a shared secret key between two nodes based on the Dynamic Source Routing (DSR) Protocol.
The above mentioned protocols use cryptographic as base method to solve the Black hole problem. Cryptography can be a burden because of processing time involved in it which will cause an extra overhead to the protocol. As a result, the protocols are not scalable and have latency. Although in cryptographic method, mostly the packets are normally authenticated, it is suitable for external attacks, but if the attacks are from inside such as Black hole where the packets are assumed authenticated, they can simply takeover the routing path and drop the packet passing through. Therefore, cryptographic methods cannot avoid such attacks from internal.

Reactive method is another way to trigger an action to protect the network from the malicious nodes. Zhang and Lee [11] present an intrusion detection technique for wireless ad hoc networks that uses cooperative statistical anomaly detection techniques. By using this technique, many numbers of false positives have been encountered. According to S. Lee in [12], the method requires the intermediate node to send Route Confirmation Request (CREQ) to the next hop towards the destination. This operation can increase the routing overhead which will then result in the performance degradation. 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. Due to this, Dokuer [15] has proposed a solution based on ignoring the first established route to reduce the adverse effects of the Black hole attack. 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 has some limitations. For instance, the second RREP message received at a source node may also come from malicious node if the real destination node is nearer to the source node than the malicious node. This method also does not address how to detect and isolate the malicious node from the network.

In a related work by N.R. Payal [16], the source node 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. The ALARM packet will then be sent to the neighbours which contains the information of 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
analysing the RREP messages which arrived within the predefined waiting period by using the heuristic method. 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.

Generally, most methods discussed in [8] – [18], put some overhead on the intermediate and the source node. Therefore, the proposed algorithm for route discovery should consider the following objectives:

- Minimum routing overhead
- Low latency time
- Efficient processing

4 ERDA: The Proposed Method for Black Hole Attack

Based on the facts discussed in Section 2 and limitations highlighted in Section 3, a protocol which is the enhancement of the AODV is proposed. The ERDA (Enhanced Route Discovery AODV) is designed to improve the previous methods in terms of the overhead incurred during the route discovery. The proposed solution will employ minimum modification to the existing AODV algorithm. There are three new elements introduced to improve the existing AODV in recvReply() function namely are 1) the rrep_table to store incoming RREP packet, 2) mali_list to keep the detected malicious nodes identity and 3) the rt_upd, parameter to control the routing table update. Generally, the proposed method is divided into two parts, 1) Securing routing table update. 2) Detecting and isolating the malicious node. The Pseudo Code for the improved recvReply() function is shown in Figure 4.

4.1 Securing the Routing Table Update.

In the normal AODV as described in section 2, the forward path routes in the node’s routing table will be updated based on a) the destination sequence number in the routing table is lower than the one in RREP’s message or b) the destination sequence number in the routing table and in RREP message is equal but number of hop in RREP packet is lower. In our proposed method, ERDA has imposed an additional condition by introducing a third parameter called rt_upd. This parameter can receive either true or false value. By default, the value is set to true which means the routing table is allowed to be updated and it is not necessary from the first RREP message received by the node.
In Figure 5, it explains how the ERDA works during route discovery phase and how it updates the routing table. In AODV route discovery process, the route request (RREQ) message is sent out by the source node S to find a fresh route to the destination node D. All neighbour nodes that have received this request and got “fresh enough route information” in their routing will response to node S including the destination node D as illustrated in Figure 5(a). RREPs received by node S are stored in rrep tab table. Figure 5(b) shows the information contained in the rrep tab table for node S. The information stored in the rrep tab table includes the node_id and the destination sequence number. Since the network is under Black hole attack, malicious node M is assumed to be the first node to response to node S, the routing table of node S is updated with the information provided by node M as depicted in Figure 5(c). However, since the value of the rt_upd parameter in the ERDA is set to ‘true’, the routing update does not stop but allows next RREP messages to update as well. Thus, when node S received the RREP message from node A, the message will be accepted although the destination sequence number is smaller than the one in the routing table. As a result, in Figure 5(d) the former route entry is overwritten by the later RREP coming from node A. Once the updating receives the RREP message from the destination node D, the rt_upd parameter value is then set to false. Any RREP message that comes after this point will be denied from updating the routing table until the process of detecting malicious node is completed.

```
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
22    }
18}
```

Figure 4 Pseudo code for ERDA recvReply() function
4.2 Detecting and Isolating the Malicious Node

ERDA is seamlessly integrated into AODV with no change to existing flow of AODV protocol. One additional feature that ERDA provides to AODV is to save RREP’s information like node id and destination sequence number into the rep_tab table as pointed out in section 4.1 above without cause any processing overhead. In the ERDA, the process of updating the route entry will continue until the value of rt_upd parameter is set to ‘false’. During rt_upd in a ‘false’ state, the information in the rep_tab table start to be analysed using the heuristic method whereby the node id which has exceptionally high destination sequence number will be isolated as a malicious node and the identity of those suspected nodes will be kept in the mali_list [18]. Our proposed mali list can handle more than one suspected nodes as compared to mali_node in [18]. Purpose of mali_list is to inform the node to isolate those listed nodes from participating in route discovery updates. Thus, any control messages (e.g. RREP or RREQ) that come from those listed nodes will be discarded by the node. In order to ensure that this process does not consume memory, the rep_tab table will be flushed once the process of identifying malicious node is completed and the rt_upd parameter value again is set back to ‘true’.

Figure 5 Routing update in the ERDA.
5 Evaluation Method

5.1 Simulation Environment

For evaluations and experiments, network simulator NS-2 (version 2.34) is used as a tool for simulation works. NS-2 is a discrete event network simulator for simulating different types of network i.e. wired or wireless and various network protocols. In our simulation setup, Two Ray Ground radio propagation model for Wireless Channel together with the IEEE 802.11 standard is used at the physical and data link layer. At the network layer AODV is used as the routing protocol. We consider two AODV conditions 1) normal AODV and 2) AODV with ERDA method. UDP is used at the transport layer and for data packet transmission at application layer, CBR (continuous bit rate) packets is used. The size of the packet is 512 bytes and transmission rate is set at 0.2 Mbps.

To create the simulation models, we use NS-2 utilities provided in the package to ease the works. The connection patterns are generated using cbrgen and the mobility models are generated using setdest utility. Setdest provides random positions of the nodes in the network and provide required mobility models. The terrain area is fixed to 800m x 800m for all simulations but the number of nodes involve in the experiments are varied from 10 to 80 and for mobility model the nodes movement is varied from 10 to 70 m/s. Overall simulation parameters are summarized in Table 1.

Each data point represents graphs below are an average of ten different scenarios. To ensure the consistency of the experiment result, the same connection pattern and mobility model is used for uniformity in simulations.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulator</td>
<td>NS-2 version 2.34</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>100s</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>10 to 80</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Traffic Model</td>
<td>CBR</td>
</tr>
<tr>
<td>Pause time</td>
<td>2 s</td>
</tr>
<tr>
<td>Mobility</td>
<td>10 to 70 m/s</td>
</tr>
<tr>
<td>Terrain</td>
<td>800 x 800m</td>
</tr>
<tr>
<td>Transmission Range</td>
<td>250m</td>
</tr>
<tr>
<td>No. of malicious node</td>
<td>1</td>
</tr>
</tbody>
</table>
5.2 Simulation Metrics

To create the scenarios, various model based on different network topology are created and simulated to analyze the proposed method. Data is collected based on different network sizes and different nodes mobility by varying the number of nodes and the speed of nodes respectively. Three important metrics are used to evaluate the result of the experiments and the details are as follows.

Packet Delivery Ratio (PDR): The percentage of send and receive packets ratio between sender and recipient in predefined simulation time.

Network Routing Load (NRL): The percentage of total routing packets and total data packet ratio that are completely transmitted in the network.

Average End-to-End Delay (Delay): The average time taken in second by one packets to travel from the sender to recipient. It includes all the delays caused during route discovery, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc.

6 Simulation Results and Analysis

In the experiment, we simulate normal AODV and AODV with ERDA method in order to evaluate the performance during the network is under Black hole attacks (attack time) and without Black hole attacks (safe time). To evaluate the PDR, NRL and Delay, all simulations are done with a source node transmitting maximum of 10000 packets to the destination node over various size and mobility speeds of the network. Fig. 6 shows the performance graphs when network size (number of nodes) is varied. This result can be seen from Fig. 6 (a), where the average of PDR in normal AODV has drop to 1% (which is about 90% decrease) during attack time as compared to safe time. By implementing ERDA method to AODV, the result shows improvement where the average PDR increases from 1% to 74% (during attack time) as shown in the same graph. At the same time, in Fig. 6(b) and Fig. 6(c) show no significant changed in NRL and Delay between normal AODV and AODV with ERDA method during safe time which means no overhead. During attack time the NRL and Delay is low if AODV with ERDA method is used in the network.

Fig. 7 shows the AODV performance in various mobility speeds. The graph from Fig. 7(a) shows the average PDR in the network using normal AODV during attack time has drop 81% in average as compare during safe time. With ERDA method, AODV PDR has increased 77% from its drop level 2.2% during attack time. In Fig 7(b) and 7(c), the average NRL and Delay of normal AODV and AODV with ERDA is almost
at par. As in network size performance, when in attack time, the NRL and Delay of AODV with ERDA will increase but not more than 10%.

The improvement in both condition (size and mobility) are quite significant to AODV either during safe time or attack time.

Fig. 6(a) PDR performance in different network size

Fig. 6(b) NRL performance in different network size
Fig. 6(c) End-to-end delay performance in different network size

Fig. 7(a) PDR performance in different mobility speed
Fig. 7(b) NRL performance in different mobility speed

Fig. 7(c) End-to-end delay performance in different mobility speed
7 Conclusions and Future Work

In this paper, the issue of Black hole attack on AODV routing protocol in MANET and various methods to overcome this problem has been discussed. In our study, the existing route discovery mechanism in the AODV is so susceptible to Black hole attack and therefore, it is important to have an efficient security method built seamlessly into AODV protocol in order to secure from such attacks. Based on the limitation of the previous proposed methods, we presented our novel method, called ERDA, to prevent, detect and isolate the Black hole nodes in MANET.

ERDA method enhances existing recvReply() function in the AODV protocol by improving the process of updating the routing entry and implementing a simple mechanism to detect and isolate malicious nodes. The enhancement only involves a minimum modification and does not change the existing AODV protocol flows. Moreover, the ERDA does not incur high cost in terms of routing overhead (NRL) and delay overhead (Delay).

In evaluating ERDA performance, various simulations have been performed and the results show there is significant improvement to AODV and yet no overheads are incurred in terms of NRL and Delay in the event of Black hole is not present in the network. In the event where Black hole is presence in network, ERDA provides protection to AODV and successfully maintains high PDR in the network. This has been proved by simulating ERDA method in various network sizes and mobility speeds and the results show the substantial improvement of AODV performance.

For future works, there are few research areas remaining which can be explored. 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.
References

12. S. Lee, B. Han, and M. Shin, “Robust routing in wireless ad hoc networks,” in ICPP Workshops, pp. 73, 2002.
