A Study of AODV Friendship Mechanism in Mobile Adhoc Network Trust Feature

Hatim Mohamad Tahir
School of Computing
Universiti Utara Malaysia
UUM Sintok 06010 Kedah, MALAYSIA
Email: hatim@uum.edu.my

Abas Md Said
Department of Computer Information System
Universiti Teknologi PETRONAS
Tronoh 31750, Perak, MALAYSIA
Email: abass@petronas.com.my

***Abstract*—Mobile ad hoc networks (MANETS) are mobile nodes moving rapidly and they use wireless connections to connect to various networks or nodes. The dynamic nature of MANETs, make it vulnerable to attack by intruders. The sending and passing of nodes are based on several routing protocols. The packets do not reach the destination and some form of secure mechanism based on trust or friendship are deployed to protect the network integrity. Denial of service attacks is one of the typical attack type in mobile adhoc network. In this paper, we deployed Black hole and Grey hole attack. Black hole attack absord all data packets that are sent to its node whereas grey hole attack will drop some packet for a particular network destination based on packets type, time or randomly selected portion of packets. In this experiment we simulated several routing protocol to investigate the secure mechanism in protecting from the blackhole ad greyhole attack. The findings are presented and discussed.**

***Index Terms*—AODV; MANET; Trust**

I. Introduction

Mobile adhoc network comprises autonomous and anonymous nodes roaming freely without centralize controller to determine the communication path. Each nodes can function as a router by itself. They rely on each other in forwarding packets. Communication among node exist without the need of a supporting fixed router or access point. Specific feature of MANET such as transmission range, shared resources of wireless devices, resource consumptions and the mobility of nodes may cause security and efficiency issues. MANET are not immune to false alarms cause by blackmail attacker and other potential attackers that can target the operational of a routing protocol in an adhoc network.

In this paper, AODV was chosen as the basic protocol for performance comparison due to the fact that AODV can run properly in high traffic communication and high mobility. The simulation on AODV extension namely IDSAODV and PHR-AODV mechanism under packet dropping attack is also conducted.

Adhoc network is also commonly called as Mobile Adhoc NETwork (MANET) because of its mobility function. In the ad-hoc mode, the mobile station such as a laptop or a PDA can communicate directly with one another using Independent Basic Service Set (IBSS). This communication can be established without connection to a wired backbone. In addition, adhoc network is independent because the device in this mode can act either as base station or mobile station.

II. Routing in MANET

Routing in MANET has several characteristic which are dynamic topologies, bandwidth-constrained link, energy constrained operation and limited physical security [1]. The adhoc topology network change with time as the mobile nodes join or move from the network. The routing protocol in MANET is divided into two categories based on management routing table. These two categories are proactive and reactive protocol[2]. In proactive protocol, nodes allocate resource to track routes in routing table. In reactive protocol, routes are discovered only when needed to preserve network resources. Basically, MANET is based on protocol as shown in figure 1

Fig. 1. adhoc Routing Protocol

A. AdHoc On-Demand Distance Vector (AODV) Protocol

AODV is a reactive routing protocol which creates a path to the destination when required. Routes are not built until certain nodes start to send route discovery message as an intention to communicate data with each other. The advantages of using AODV protocol are low memory overhead, minimize the use of network resource and the ablilty to run in high network

ISBN: 978-1-941968-01-7 ©2014 SDIWC

mobility. The reasons for these advantages are the routing information is only stored in source node, destination node and intermediate node which is involve in data transmission.

In AODV, there are three procedure involves in the communication which are path discovery, path establishment and path maintenance. Three types of message controls are used in AODV which are Route Request (RREQ), Route Reply (RREP) and Route Error (RRER) message[3].

The procedure of AODV protocol starts with the source node establishing the communication with the destination node by issuing route discovery procedure. The source node broadcast RREQ message to all accessible neighbours. Then, the intermediate node that receives the RREQ message will check the request. If the intermediate node is the destination, it will reply with RREP message. If not, the RREQ message from the source node will be forwarded to the other intermediate nodes. Figure 2 shows the route discovery procedure.

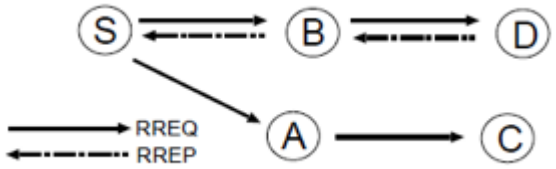

Fig. 2. Route Discovery Procedure [4]

B. PHR-AODV and IDSAODV

PHR-AODV was proposed by [5] to enhance the security aspect on Reverse-AODV (R-AODV) protocol. PHR-AODV performed multipath communication by using path hoping routing mechanism. The number of paths from the source node to the destination node is determined based on the number of edges from the source node. In this protocol, the message is delivered through multipath route. When a path is broken during the communication process, that path will be eliminated from the path list. When there is no path in the list, the node sends back RREQ message to establish new path.

IDSAODV was proposed by [6] to eliminate the effect of black hole attack by implementing RREP caching on existing AODV protocol. The authors of IDSAODV examine when simulation under black hole attack, there is a second RREP message come to source node from the destination node. Thus, this method is invented to create RREP caching to count the second RREP message.

In both of the studies for PHR-AODV and IDSAODV, the authors do not evaluate their protocols under grey hole attack. In this paper, these two protocols will be evaluate under black and grey hole attack to determine its performance. Besides, IDSAODV only evaluate its performance on packet loss. The other performance metrics like end to end delay and throughput is ignored. The significant of this research is to compare which protocol can successfully eliminate or reduce the attack.

III. Type of Attack

Mobile adhoc network faced vulnerabilities from various attacks due to high number of nodes involve in the communication process. The attacks that always occur in adhoc network are black hole attack, grey hole attack, impersonation and modification attack.

A. Packet Dropping Attacks

Basically, packet dropping attack is categories as Denial of Service attack [7], [8], [9], [10] . This situation occurs when node does not forwards the requests message to destination nodes by dropping all or some of the packets. The packet dropping attack consists of two types which are black hole attack and grey hole attack.

B. Black Hole Attack

Black hole is a malicious node or attacker node that attempts to absorbs the network traffic and drops all packets. It is also forging route replies to create fake routes with it as an intermediate node.

The black hole will divert and intercept all the traffic and subsequently drop packets that it received. The source node considers the message has arrived and the communication has been successfully established. The attacker node absorbs all the messages itself and in fact the message did not arrive at the destination node. The black hole node sends the false RREP message to the sender. Therefore, the requesting nodes (sender) assume that route discovery process is completed and ignore other RREP messages and begin to send packets over black hole node [11], [4].

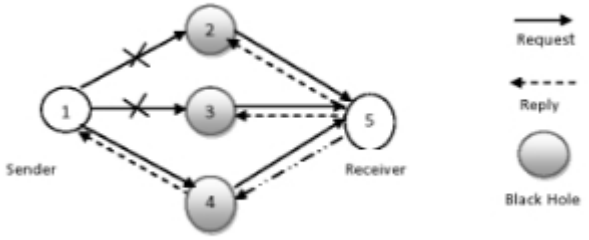

Fig. 3. Scenario of black hole attack

Based on the figure 3 above, node 1 acts as sender node, node 5 as destination node while node 2, 3 and 4 acts as black hole node. Node 4 receives a request message, and send reply message to the source node. In this case, source node which is node 1 assumes the message has arrived and assume that the communication has been successfully performed. Actually, the message did not reach at the destination node (node 5) and the communication between node 1 and node 5 failed.

C. Grey Hole Attack

Grey hole can be classified as faulty node rather than explicitly malicious. Grey hole does not falsify route replies

but periodically drop the packets. This kind of dropping against black hole, grey hole does not drop all packets. This means that grey hole sometimes act as a normal node and other times act like a malicious node [4], [12], [13].

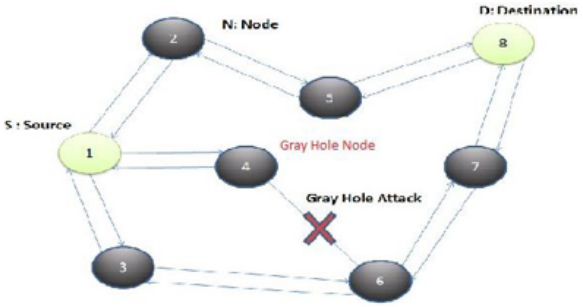

Fig. 4. Scenario of grey hole attack

Based on the figure 4 above, the node 1 act as sender broadcasting RREQ message to the destination node 8. The grey hole node which are node 4 and 5 refuse to forward RREQ message and simply drop them.

IV. Network Simulation

In this simulation, 20 nodes are used to evaluate the impact of malicious attack (black hole and grey hole) using three protocols which are IDSAODV, PHR-AODV and AODV. In every simulation, UDP connections are established between even numbered nodes (0 (zero) included) and odd numbered nodes. Node 18 and Node 19 did not have a connection to any other node in the network [6]. In the scenarios, even numbered nodes (Node 0 - Node 16) are functioned as the sending nodes and odd numbered nodes (Node 1 - Node 17) are functioned as the receiving nodes. The even numbered nodes send the packets to the next odd numbered nodes, for example Node 0 to Node 1, Node 2 to Node 3, Node 4 to Node 5 and so on. In the scenarios, UDP agents are attached to the even numbered nodes and NULL agents are attached to odd numbered nodes. NULL agents act as traffic sink and attached at the destination nodes [14]. As a result, there are 9 total connections have been implemented between the 18 nodes and all of these connections are always between the same nodes. A scenario between 20 nodes that move from a random starting point to a random destination with a speed that is randomly chosen, during 500 seconds, in a 750 x 750 meter flat space is simulated. The simulation topology is illustrated in figure 5.

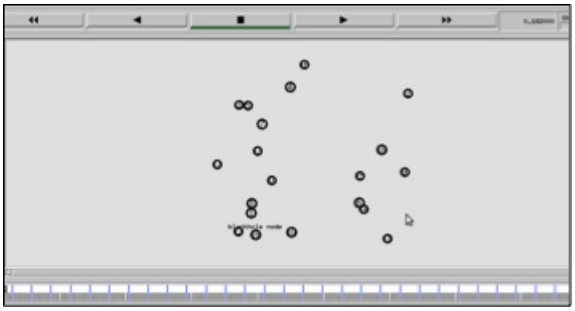

Fig. 5. Simulation Tapology

A. Simulation Setting

The Constant Bit Rate (CBR) application that generates constant packets are attached through the UDP connection. The duration of network simulation is 500 seconds and the CBR connections started at the first second of the scenario and lasts until 450 seconds. The packet size for CBR is 512 bytes and its data rates are 10 Kbits as shown in the table I.

TABLE I
Simulation Parameter

Parameter	Value
Simulation Time	500 s
Topology	750 x 750 m
Number of nodes	20
Number of attacks	1
Traffic type	CBR
Packet rate	10 Kbits
Packet size	512 bytes

Nodes in the simulation are generated by “for” loop statement of the Tcl language. These statements that create the nodes are shown in figure 6. “$ns_ node-config - adhocRouting blackholeAODV” statement changes routing protocol of the node configuration as “blackholeAODV” that we implemented in NS. After this statement, the second loop creates the last node. Changing the “$val(nnaodv)” variable we can create AODV in Black Hole and AODV in Grey Hole nodes as we wish.

```
# Creating mobile AODV nodes for simulation
puts “Creating nodes...”
for {set i 0} {$i ¡ $val(nnaodv)} {incr i} {
set node_($i) [$ns_ node]
$node_($i) random-motion 0 ;#disable random motion
}
# The last node act as attacker node (Black/grey hole attack)
# Creating Black/Grey Hole nodes for simulation
$ns_ node-config -adhocRouting blackholeAODV
for {set i $val(nnaodv)} {$i ¡ $val(nn)} {incr i} {
set node_($i) [$ns_ node]
$node_($i) random-motion 0;#disable random motion
$ ns_ at 0.01
}
```

Fig. 6. Implementation of attacker node in wireless environment

V. Performance Metric

According to [15], selecting performance metric is an important step to evaluate the result of experiments. The metrics used in this research have been used widely by the other researchers in computer network [15], [16], [17].

A. Packet delay

The packet delay is the average time in order to traverse the packet inside the network. This includes the time from generating the packet from sender up till the reception of the packet by receiver or destination and expressed in seconds. In this research, end to end delay is used, which means the average time taken for the packet sent from the source node to the destination node. End to end delay means the amount of time of packets takes to transmit from sender to the destination. Packet end to end delay formulated in equation 1 as:

$$End\,to\,end\,delay = \frac{time_{packet\_arrived(destination)} - time_{packet\_sent(s}}{No.\,of\,connection} \quad (1)$$

B. Throughput

Throughput is the ratio of the total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is represented in bits per second or packets per seconds. In MANETs throughput is affected by various changes in topology, limited bandwidth and limited power. Unreliable communication is also one of the factors which adversely affect the throughput parameter. Throughput can be defined in equation 2 as:

$$Throughput = \frac{Packet\_received}{Packet\_forwarded} \quad (2)$$

VI. Results

The performance metric considered in this research are packet end to end delay and throughput. A simulation model was developed using NS-2 (version 2.34) to analyze the performance results under of three conditions below:

i. Packet dropping attack using normal AODV protocol
ii. Packet dropping attack using PHR-AODV protocol
iii. Packet dropping attack using IDSAODV protocol

A. Packet End to End Delay

Packet end to end delay for AODV, PHR-AODV and IDSAODV under black hole attack, grey hole attack and without any attack are evaluated.

Based on figure 7, 8 and 9, the delay for all protocol is high except in the case where there is no attack on the network. As we can see, delay on black hole attack is lower compared to others. This is because during the black hole attack, there is no need to send RREQ and RREP packet due to black hole node already sent its RREQ packets to the sender before the destination node reply RREP packet. All the RREQ packets are absorbed by the black hole node. Thus, the delay is less.

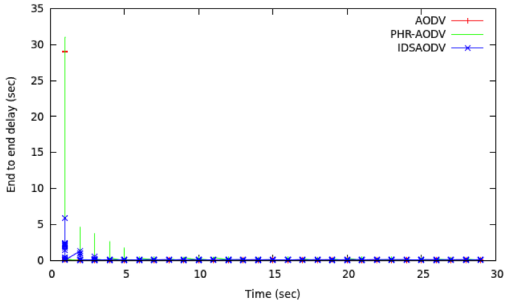

Fig. 7. End to end delay under black hole attack

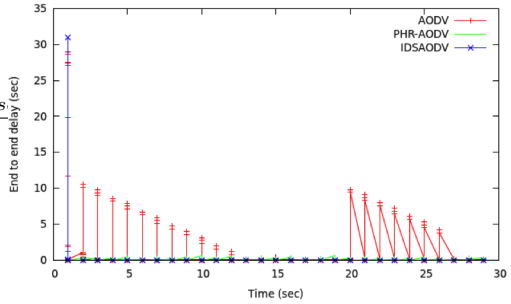

Fig. 8. End to end delay under grey hole attack

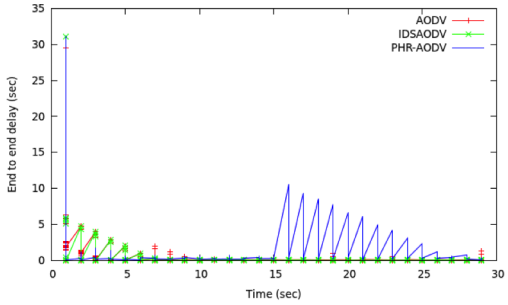

Fig. 9. End to end delay without attack

Based on the three protocols, we can conclude the performance of IDSAODV protocol is better than PHR-AODV and basic AODV in term of lower delay. This is because IDSAODV have a special mechanism which is RREP caching to count the number of RREP message. For PHR-AODV protocol, the delay time of packet data to reach destination increases due to many alternative paths to send packet data to the destination node. However, in term of simulation without attack, AODV is better compared to others. The reason is that AODV is created to adapt normal network environment. There is no need to use alternative path mechanism in packet transmission because it will consume more delay.

B. Throughput

Throughput is the number of packet received over the amount of time. From the table below, it can be seen that the throughput value under black hole attack is worst compared to grey hole. From the previous analysis, the value of packet loss under black hole attack is high because black hole node discards the packet rather than forwarding it to the destination. As the result, low number of packet received at the receiver and thus the value of throughput is also low.

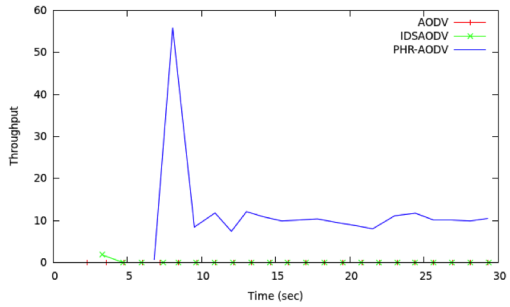

Fig. 10. Throughput with black hole attack

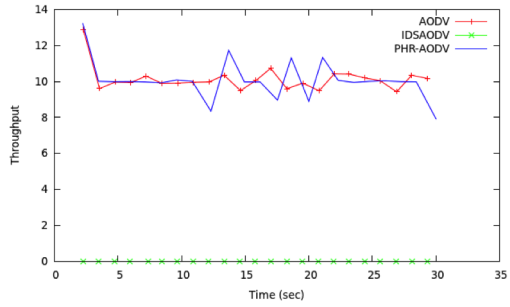

Fig. 11. Throughput with grey hole attack

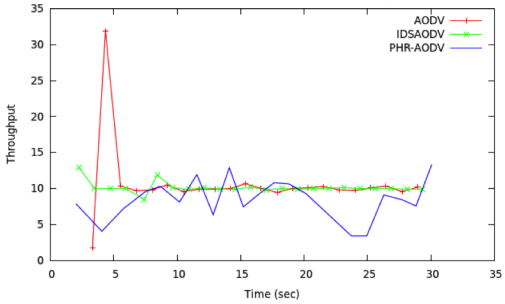

Fig. 12. Throughput without any attack

Refering to the figure 10 , 11 and 12, it can be seen that the throughput of PHR-AODV is good under all conditions. This is because when the amount of packet loss is low, the value of throughput is high because the number of successful packet received at the receiver is high.

VII. Conclusion

The experiments are conducted to show which protocols can performed efficiently under black hole and grey hole attack. Performance metrics such as end to end delay and throughput have been used for the purpose of evaluation. From the analysis, it can be seen that the performance of PHR-AODV is better than the others in term of high throughput, and low delay under attack.

Acknowledgment

The authors would like to express our gratitude to the Ministry of Science, Technology and Innovation (MOSTI), Government of Malaysia under e-Science Grant No. 01-01-07-SF0018 and Research & Innovation Management Center (RIMC), Universiti Utara Malaysia Grant Number S/O 12121

References

[1] Nur Ziadah Harun, Osman Ghazali, and Baharudin Osman, "Impact of weight values in hybrid and adaptive fec mechanism over wireless network", in *Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on*. IEEE, 2010, pp. 42–47.

[2] AF Farhan, D Zulkhairi, and MT Hatim, "Mobile agent intrusion detection system for mobile ad hoc networks: A non-overlapping zone approach", in *Internet, 2008. ICI 2008. 4th IEEE/IFIP International Conference on*. IEEE, 2008, pp. 1–5.

[3] H. Simaremare and R.F. Sari, "Performance evaluation of aodv variants on ddos, blackhole and malicious attacks", *IJCSNS*, vol. 11, no. 6, pp. 277, 2011.

[4] 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.", *IJ Network Security*, vol. 5, no. 3, pp. 338–346, 2007.

[5] Chonggun Kim, Elmurod Talipov, and Byoungchul Ahn, "A reverse aodv routing protocol in ad hoc mobile networks", in *Emerging Directions in Embedded and Ubiquitous Computing*, pp. 522–531. Springer, 2006.

[6] Semih Dokurer, *Simulation of Black hole attack in wireless Ad-hoc networks*, Atılım University, 2006.

[7] P. Albers, O. Camp, J.M. Percher, B. Jouga, L. Mé, and R. Puttini, "Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches", in *Proceedings of the First International Workshop on Wireless Information Systems (WIS-2002)*, 2002, pp. 1–12.

[8] T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks", *Wireless Network Security*, pp. 159–180, 2007.

[9] P. Brutch and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks", in *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*. IEEE, 2003, pp. 368–373.
[10] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research", *Wireless communications and mobile computing*, vol. 2, no. 5, pp. 483–502, 2002.
[11] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", *Wireless Communications, IEEE*, vol. 14, no. 5, pp. 85–91, 2007.
[12] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks", *Wireless Communications, IEEE*, vol. 11, no. 1, pp. 48–60, 2004.
[13] R. Puttini, J.M. Percher, L. Mé, and R. De Sousa, "A fully distributed ids for manet", in *Computers and Communications, 2004. Proceedings. ISCC 2004. Ninth International Symposium on*. IEEE, 2004, vol. 1, pp. 331–338.
[14] N. Griffiths, A. Jhumka, A. Dawson, and R. Myers, "A simple trust model for on-demand routing in mobile ad-hoc networks", *Intelligent Distributed Computing, Systems and Applications*, pp. 105–114, 2008.
[15] R. Jain, *The art of computer systems performance analysis*, John Wiley & Sons, 2008.
[16] Venkata Giruka, Mukesh Singhal, James Royalty, and Srilekha Varanasi, "Security in wireless sensor networks", *Wireless Communications and Mobile Computing*, vol. 8, no. 1, pp. 1–24, 2008.
[17] E. Fonseca and A. Festag, "A survey of existing approaches for secure ad hoc routing and their applicability to vanets", *NEC network laboratories*, 2006.