Performance Evaluation of AODV variants on DDOS, Blackhole and Malicious Attacks

Harris Simaremare† and Riri Fitri Sari††,

Universitas Indonesia, Depok, Indonesia

Summary
This paper reviews security issues on Adhoc network and Ad hoc On-Demand Distance Vector (AODV) protocol. In Adhoc network, active attack i.e DDOS, blackhole and malicious nodes attack can easily occur. These attacks can decrease the performance of the communications protocol. In this paper, AODV was chosen as the basic protocol to perform simulations due to the fact that the AODV protocol can run well in high mobility and high traffic communication. Many AODV protocol variants have been developed. Currently, AODV protocol has been developed to improve the performance in terms of efficiency and security. To improve the performance of the AODV protocol, we proposed AODV-UI. AODV-UI has been developed by adopting a reverse request method introduced by R-AODV protocol, and it can run on the gateway modes. To improve the security in AODV, Path Hopping based on Reverse AODV (PHR-AODV) have been developed. In this paper we will evaluate the performance of AODV-UI protocol and PHR-AODV protocol under DDOS, blackhole and malicious nodes attacks using NS-2 simulator. The topology is fixed, and the attacks come from inside the network. The performance evaluation performed includes the packet delivery ratio, packet lost and end to end delay. The result of the simulation shows that the performance of AODV-UI protocol is better than PHR-AODV in terms of packet delivery ratio, packet lost and end to end delay under malicious and DDOS attack. The simulation shows that under blackhole attack, PHR-AODV gives a better performance than AODV-UI.

Key words:
AODV, blackhole attack, DDOS, Malicious nodes, protocol routing, security

1. Introduction

Mobile Ad hoc Network (MANET) is a non-infrastructure network that consists of a collection of nodes that can communicate each other independently. In MANET, there are no administrative nodes to control the network. Every node participating in the network is responsible for the reliable operation of the whole network. Each node acts as a router for other nodes, because on the execution of communication process between nodes in the network, each node must be able to forward and route packets to other nodes. So every node in the network are responsible for the continuity of communication that run on the network.

AODV routing protocol is a routing protocol that can run on MANET and in present developed extensively by many researchers. Currently many AODV protocol variant has been developed, due to the fact the AODV protocol can run well in high mobility and high traffic communication. The development of this variant aims to cover weaknesses in AODV protocol. One of the disadvantages of AODV protocol is the source node must re initiate communications by running route discovery procedure, and try to find new path communication, when communication between nodes is lost due to the high mobility of nodes. AODV-UI [4] was developed to overcome this problem. In this work we will evaluate AODV-UI for its security performance.

The next challenging issue that many investigated in MANET is about the security. The high level of mobility, no central coordination mechanism and open network makes the MANET more vulnerable from various types of attack. AODV routing protocol, assumes that there are no malicious nodes participating in routing operations. This assumption cannot be applied in the MANET, because of the nature of MANET. MANET is an open network, in which any nodes can be involved in communicating and collaborating.

Attacks on MANET can be classified as active attacks and passive attacks [1, 5, 6]. Passive attacks do not disrupt the operation of a routing protocol or influence the functionality of connection, but only attempt to discover valuable information by listening to the routing traffic. Passive attacks are difficult to detect. Active attacks attempt to improperly modify data, destroy data, gain authentication, or procure authorization by inserting false packets into the data stream or modifying packets transition through the network. Some examples of active attacks are malicious nodes, distributed denial of service (DDOS) and blackhole attack, which will be used in this work.

Many secure protocol based on AODV have been developed. Improvement of security in AODV protocol is generally done by three methods i.e. the signature method, trust based method and disjoints multipath methods.

Securing with the signature method is performed by providing a key mechanism for securing the data packets during transmission to destination node. This method

Manuscript received June 5, 2011
Manuscript revised June 20, 2011

guarantees the security of data. The data cannot be changed or read by the attacker, since the key mechanisms and authentication mechanisms have been applied. Several protocols are developed with this method, i.e. SAODV [16], AODV-SEC [17], A-SAODV [15], SA-AODV [18], CAODV [19], One time signature secure AODV [20], and ID based on-line / off-line authentication AODV [21].

The second method is the trust-based method. This method implements a trust mechanism between nodes. Nodes that communicate on the network are nodes that has guaranteed the trust. There are several protocols using this method, i.e TAODV [22], trust-based AODV [23], Trustworthy AODV [25], the Trust AODV [26], Adaptive Trust AODV [28], the Trust framework AODV [27], and Simple Trust Framework AODV [24].

The last method is a multipath and disjoint method. This method secures the communication between nodes by creating many paths of communication when data exchange occurs. This method secures data from the eavesdropping and guarantees that the data will arrive to destination. Several protocols which have been developed with this method are SDSMR [29], PHR-AODV [3], MP-SAR [30], SecMR [31], and SAODVMAP [32].

We evaluate PHR-AODV [3] as an example of secure AODV protocol. This protocol secures the communication between nodes from malicious nodes attacks using path hopping method.

In this paper, we conduct the performance evaluation of the AODV-UI and PHR-AODV protocol by inducing DDOS, blackhole and malicious nodes attacks. We carried out the simulation using NS-2 simulator. Evaluation criteria in this simulation are the performance of average packet delivery ratio, end to end delay and packet lost when a number of attacks are carried out simultaneously.

The remainder of this paper is structured as follows. In section II we discuss related work and literature review. This section will explain the work process of AODV, AODV-UI and PHR-AODV protocols. In section III we will discuss the evaluation criteria applied in our experiments. Section IV discussed the security issue in AODV protocol. Next in section V we explain the simulations, and in section VI we discuss the result of the simulations and perform some analysis. Lastly, Section VII contains the conclusion and future work.

2. Related Work

One of the most protuberant communication protocol in MANET is AODV protocol. However this protocol still has many weaknesses, which attract many researchers to develop new variants protocol based on AODV protocol to improve its performance.

2.1 AODV Overview

Ad hoc On-Demand Distance Vector (AODV) [2, 7, 8, 9] is a reactive routing protocol which creates a path to destination when required. Routes are not built until certain nodes send route discovery message as an intention to communicate or transmit data with each other. Routing information is stored only in the source node, the destination node, and the intermediate nodes along the active route which deals with data transmission. This scenario decreases the memory overhead, minimize the use of network resources, and run well in high mobility situation.

In AODV, the communication involves main three procedures [1], i.e. path discovery, establishment and maintenance of the routing paths. AODV uses 3 types of control messages to run the algorithm, i.e. Request (RREQ), Route Reply (RREP) and Route Error (RERR) messages. The format of RREQ and RREP packet are shown in Fig. 1 and Fig.2.

Source_ address	Source_ sequence	Broadcas t_ id	Destination_ address	Destination_ sequence	Hop_ count

Fig. 1 RREQ field [4].

Source_ad dress	Destination_ address	Destination _ sequence	Hop_ count	Lifetime

Fig.2 RREP field [4]

When the source node wants to establish the communication with the destination node, it will issue the route discovery procedure. The source node broadcasts route request packets (RREQ) to all its accessible neighbours. The intermediate node that receive request (RREQ) will check the request. If the intermediate node is the destination, it will reply with a route reply message (RREP). If it is not the destination node, the request from the source will be forwarded to other neighbour nodes. Before forwarding the packet, each node will store the broadcast identifier and the previous node number from which the request came. Timer will be used by the intermediate nodes to delete the entry when no reply is received for the request. If there is a reply, intermediate nodes will keep the broadcast identifier and the previous nodes from which the reply came from.

The broadcast identifier and the source ID are used to detect whether the node has received the route request message previously. It prevents redundant request receive in same nodes. The source node might get more than one reply, in which case it will determine later which message will be selected based on the hop counts.

When a link breaks down, for example due to the node mobility, the node will invalidate the routing table. All destinations will become unreachable due to the loss of the

link. It then creates a route error (RERR) message which lists all of these lost destinations. The node sends the RERR upstream towards the source node. Once the source receives the RERR, it reinitiates route discovery if it still requires the route. AODV is slow at reacting to route breakdowns, which are frequent in an ad hoc network. Further, to get a route, AODV refers to the first RREP received. This is one of the disadvantages of AODV.

R-AODV Algorithm :

1 The Source broadcast RREQ
2 Node received RREQ
3 If it is redundant RREQ, then Ignore or drop
4 If node is a gateway, then perform gateway mode procedure
5 If a local repair procedure is in progress, then en-queue the packets
6 If node is the destination, then
Node create reverse route request (R-RREQ)
Node generate R-RREQ
Node sends R-RREQ
7 if it is not in the route table, then create an entry for the reverse route
8 if there is a fresher Seq_No or less hop_count, then update the route table
else do not bother
9 If node is not the destination but it is a gateway, then forward the R-RREQ

Gateway mode Algorithm :

1 if gateway discovery = 0 , then proactive gateway mode ON
Agent send advertisement (Network_Diameter)
interval = advertisement_interval x random
2 if gateway discovery = 1 , then hybrid gateway mode ON
Agent send advertisement (Advertisement_Zone)
interval = advertisement_interval x random
3 if gateway discovery = 2 , then reactive gateway mode ON

Fig.3 AODV-UI Algorithm

As explained before, AODV protocol only build one path to find the destination node on the network. Inefficiencies occur in AODV protocol when the path is lost. Source node will repeat the process from initial discovery to find the destination node.

To solve this weakness, Chonggun et.al [11] developed a method of reverse request and proposed R-ODV protocol. Reverse mechanism provides an alternative path when the discovery process is done. As the consequence, it will build an alternative path of communication. The path that is used to establish communication is the shortest path. When one path of communication is broken, the alternative route will be used directly without reinitiating discovery procedure. AODV-UI uses this mechanism to improve its communications performance. Fig.3 shows the algorithm of AODV-UI which uses the reverse method of R-AODV and the gateway mode of AODV+.

2.3 PHR-AODV

Elmurod [3] proposed PHR-AODV protocol as a secure protocol against malicious nodes. Malicious nodes are nodes that attack inside the network during the communication process. Many type of attack can be done by malicious nodes. In this experiment the malicious nodes will drop all packets that have been received. The malicious node does not forward the request message (RREQ) to intermediate node in the network.

PHR-AODV protocol was developed from R-AODV. To enhance the security aspect of the R-AODV protocol, Elmurod added path hopping routing mechanism. In general, these mechanisms perform a multipath communication. In PHR-AODV, the number of paths from the source node to the destination node is determined based on the number of edges from the source node [3]. Messages will be delivered through multipath. The selection process is conducted in sequential path. During the communication process, when a path is broken, that path will be eliminated from the list. When no path remains in the list, the source node sends back the RREQ for establishing new paths.

The path hopping method in PHR-AODV assumes that the malicious node will not succeed to disrupt communication between the source and the destination nodes.

AODV-UI and PHR-AODV are both developed from R-AODV protocol. In previous studies, Elmurod did not evaluate the PHR-AODV protocol under the attack. In this study, we examine the two protocols that have the same basic development on having DDOS, blackhole and malicious nodes attacks. We assess the performance of both protocols while being attacked simultaneously.

3. Evaluation Criteria

In this paper we focus on evaluating the protocols under DDOS, blackhole and malicious nodes attack with following criteria [2, 3, 8, 9, 13]:

Packet Delivery Ratio (PDR): the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

$$\text{Packet delivery ratio} = \frac{\sum \text{Number of packet receive}}{\sum \text{Number of packet send}} \quad (1)$$

The greater value of packet delivery ratio means the better performance of the protocol.

End-to-end Delay: the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in

data packet transmission. Only the data packets that successfully delivered to destinations that counted.

$$\text{End to end delay} = \frac{\sum (\text{arrive time} - \text{send time})}{\sum \text{Number of connections}} \quad (2)$$

The lower value of end to end delay means the better performance of the protocol.

Packet Lost: the total number of packets dropped during the simulation.

Packet lost = Number of packet send – Number of packet received. (3)

The lower value of the packet lost means the better performance of the protocol.

4. Security Issue

MANET is very vulnerable from various attacks [1]. This is because of number of nodes involved in the network and each node has a role in the communication process.
The following are some of eminent attacks that have been addressed in literature [1, 2, 6, 10, 14] which happens in MANET:

4.1 Black-hole attack:

Malicious node sends a forged RREP packet to a source node that initiates the route discovery in order to pretend to be a destination node itself or a node of immediate neighbour the destination. Source node will forward all of its data packets to the malicious node; which were intended for the destination.

4.2 Wormhole attack:

A malicious node uses a path outside the network to route messages to another compromised node at some other location in the net.

4.3 Denial of Service Attack:

An adversary tries to disturb the communication in a network, for example by flooding the network with a huge amount of packages. Services offered by the network are not working as usual, slow down, or even stop. Wireless adhoc network are more affected than wired networks, because there are more possibilities to perform such attack. Depending on the layer an adversary starts an attack, it could disturb transmissions on physical layer, manipulate the routing process on network layer, or bring down important service on application level.

4.4 Rushing attack:

A malicious node will attempt to tamper with route request packets, modifying the node list, and hurrying this packet to the next node.

4.5 Byzantine attack:

Two or more nodes will attempt to drop, fabricate, modify, or misroute packets in an attempt to disrupt the routing services.

4.6 Detour attack:

An attacker attempt to cause a node to use detours through suboptimal routes. Compromised nodes also try to work together to create a routing loop.

4.7 Packet replication:

The replication of stale packets, to consume additional resources, such as bandwidth.

4.8 Impersonation attack:

also called spoofing attacks. The attacker assumes the identity of another node in the network, thus receiving messages directed to the node it fakes. Usually this would be one of the first steps to intrude a network with the aim of carrying out further attacks to disrupt operation.
In this research, the evaluation focused on DDOS, blackhole and malicious nodes attacks. The attacks scenarios implemented on the evaluation are as follows.
DDOS attack: nodes that have been defined will deliver the massive request to the destination node. To initiate the attack, we performed modifications in the file aodv.cc. Fig.4 shows the scenario of the DDOS attacks

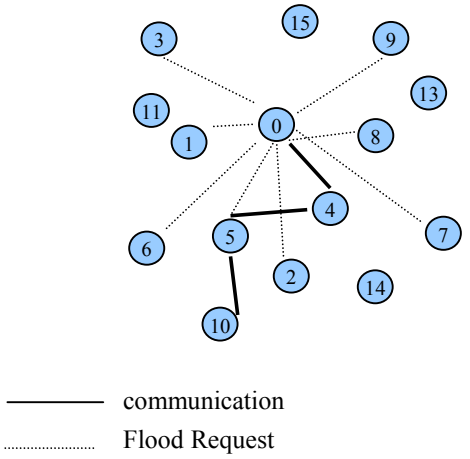

Fig. 4 Scenario of the DDOS attack.

DOS attack is performed by sending request continuously to the victim node, in this case node 0. Nodes that do requests flooding are node 2, 5, 9, 11, 14, and 16. When the communication starts between node 10 to 0, the attacker will flood the node 0 with the request message. Fig.5 shows the modification script of aodv.cc to perform DDOS attack.

```
void
 BroadcastTimer::handle(Event*) {
 agent->id_purge();
 if (agent->malicious == true ) {
   agent->sendRequest(0);
   }
Scheduler::instance().schedule(this,    &intr,
BCAST_ID_SAVE);
}
```

Fig.5 Script DDOS attack

Malicious Nodes attack: every request that is accepted by the malicious nodes will be dropped. The goal is to make communication from the source to the destination cannot be done. Process of dropping request packet is done by modifying the file aodv.cc on the protocol. Fig.6 shows the modifications to execute malicious nodes.

```
// if I am malicious node
        if (malicious == true ) {
           drop(p,
DROP_RTR_ROUTE_LOOP);
           //  DROP_RTR_ROUTE_LOOP  is
added    for no reason.        }
```

Fig.6 Script malicious node attack

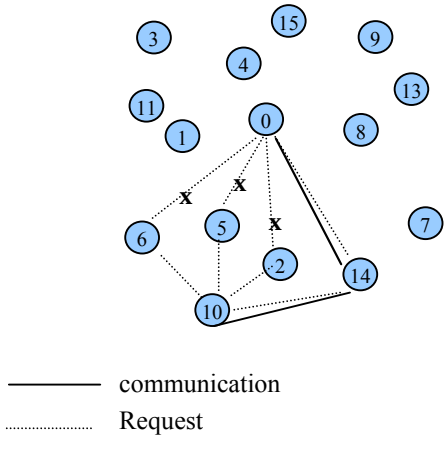

Fig. 7 Scenario of the malicious nodes attack

Fig.7 shows the scenario of the malicious nodes attacks. The attacker node will drop all requests, which cause the communications between nodes 10 to 0 failed. Attacker nodes are node 2, 5, 9, 11, 14, and 16.

Blackhole attack: attacker nodes receive a request message, and send reply message to the source node. So that the source node considers the message has arrived and the communication has been successfully performed. In fact, the message did not reach the destination node. To implement this attack, we modify aodv.cc in the protocol. Fig.8 shows the script of blackhole attack added to aodv.cc.

```
Blackhole  attacker  always  say  that
have the route to be a sink.
 else if ((rt && blackhole == 1)) {
   assert(rq->rq_dst == rt->rt_dst);
   sendReverse(rq->rq_src);
   rt->pc_insert(rt0->rt_nexthop);
   rt0->pc_insert(rt->rt_nexthop);
               Packet::free(p);}
```

Fig.8 Script blackhole attack

Fig.9 shows the scenario of the blackhole attack that performed in our simulations.

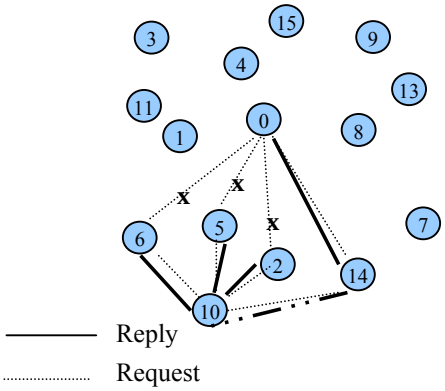

Fig.9 Scenario of the blackhole attack

5. Simulation

Simulation has been performed using NS-2 simulator version 2.34. The number of nodes was varied from 10 to 30 nodes. The traffic are Constant Bit Rate (CBR), with fix topology and position of nodes. Nodes that perform communication are between the node 10 and 0. The nodes attackers are node 2, 5, 9, 11, 14, and 16. These nodes will perform DDOS, blackhole and malicious nodes attack.
The scenario and the environmental setting are fixed, in order to enable comparison. Simulation scenario is depicted in Fig.10.

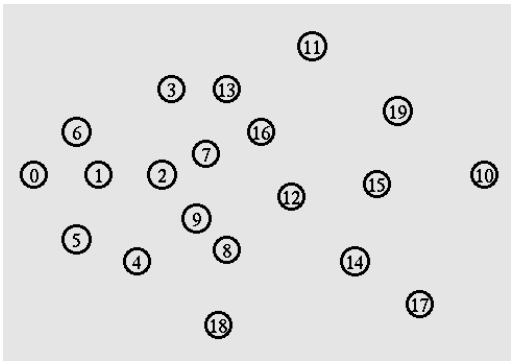

Fig.10 Simulation scenario

Table 1 shows the detail of the parameter for the simulation scenario.

Table 1: Simulation parameter

Parameter	Value
Simulation time	1000 s
Topology	1000 x 1000 m
Number of nodes	10 - 30
Number of attacks	01/05/11
Sources	1
Traffic type	CBR
Packet rate	0.1 Mb
Packet size	50 bytes

6. Result and Analysis

Simulation is performed with two conditions, first condition are under malicious and DDOS attacks, we compare the protocols performances when the number of attacks and the number of nodes changes. The second situations are when the network under blackhole attacks. We compare AODV-UI and PHR-AODV performances when the number of attacks and the number of nodes changes.
Fig.11, Fig.12, Fig.13 shows the performance comparison of AODV-UI and PHR-AODV on the malicious node and DDOS attack. We observe the impact of the number of nodes to the average packet delivery ratio, packet lost and end to end delay. The number of nodes was increased gradually from 10 to 30 with 5 attacker nodes.

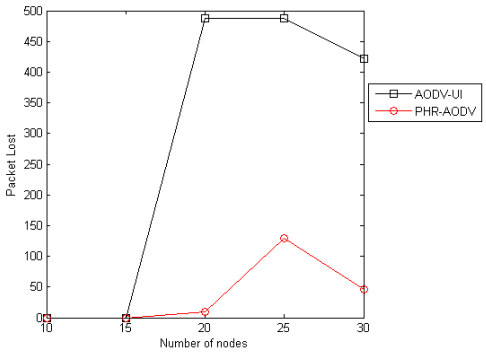

Fig.11 Packet delivery ratio vs number of nodes on malicious and DDOS attack

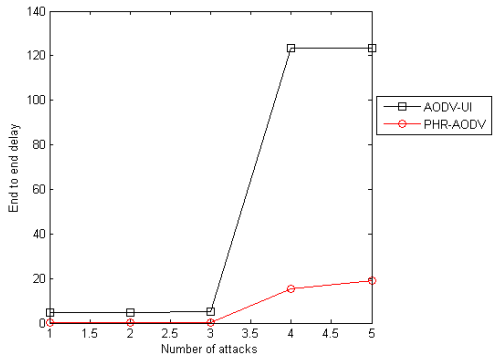

Fig.12 Packet lost vs number of nodes on malicious and DDOS attack

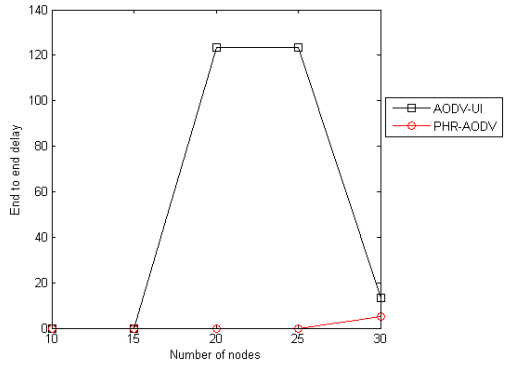

Fig.13 End to end delay vs number of nodes on malicious and DDOS attack

In Fig.11 we can see that for both protocols, the average of packet delivery ratio increase for increasing the number of nodes. This means that the level of guaranteed packet data that arrive at the destination is high. When the number of node increases, average packet lost increases. For the average end to end delay, we found different trend between PHR-AODV and AODV-UI. In AODV-UI, the average of end to end delay will increase when the number of nodes increases. In PHR-AODV, the average end to end delay decreased for increasing the number of nodes. In general, we can conclude the performance of AODV-UI protocol better than PHR-AODV. For PHR-AODV, the delay time of packet data to reach destination increases due to many alternative paths to send packet data to destination node. It makes the performance of PHR-AODV decreases.

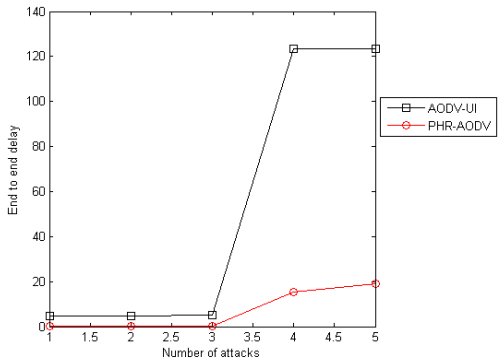

Fig.14 Packet delivery ratio vs number of attacks on malicious and DDOS attack

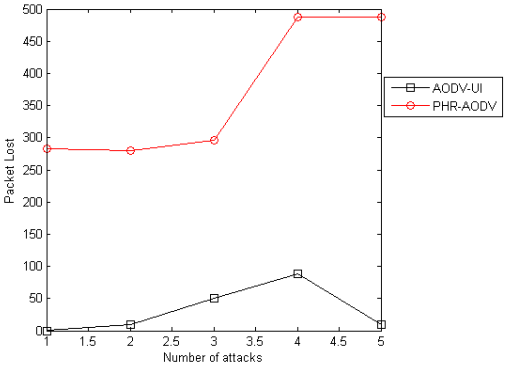

Fig.15 Packet lost vs number of attacks on malicious and DDOS attack

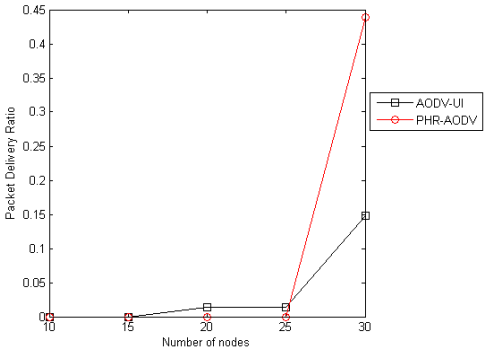

Fig.16 End to end delay vs number of attacks on malicious and DDOS attack

Fig.14, Fig.15, Fig.16 shows the impact of the number of attacks to the average packet delivery ratio, packet lost and end to end delay when malicious nodes and DDOS attack simultaneously. The test conditions are the number of nodes is set 20, and the number of attacker nodes varies from 1 to 5. The attacker nodes are node 1, 2, 5, 9, 11, 14, and 16.

We can see that the performance of AODV-UI is better than PHR-AODV in terms of packet delivery ratio, packet lost and end to end delay. In general, for both protocols, we can see that when the number of attacks increases, the average of packet lost and end to end delay increases, otherwise the average of delivery ratio decreases. Its means that, when many attacks happened, the possibility of packet data to reach the destination is low. Many packet data lost in network, and time consumed to perform communication is long.

AODV-UI is better than PHR-AODV due to the fact that AODV-UI protocol applies reverse mechanism that can guarantee data to arrive at destination. In the PHR-AODV, the data is transmitted using multipath and divided on several paths. Maintaining many paths makes the performance of PHR-AODV low.

Under Blackhole Attack

We use the same scenario to implement the simulation of blackhole attack. In this experiment, we compare the performance of AODV-UI and PHR-AODV under blackhole attacks with 10 – 30 nodes and 5 attacker nodes. The result shows the effect of the number of nodes and the number of attacks against the performance of average packet delivery ratio, packet lost and end to end delay.

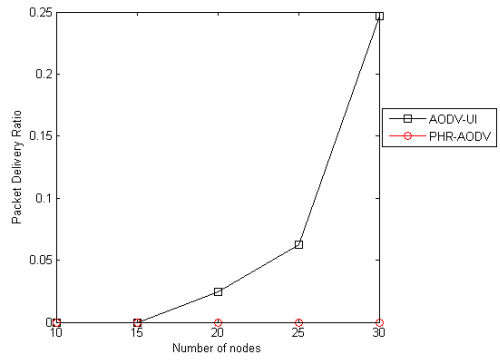

Fig.17 Packet delivery ratio vs number of nodes on blackhole attack

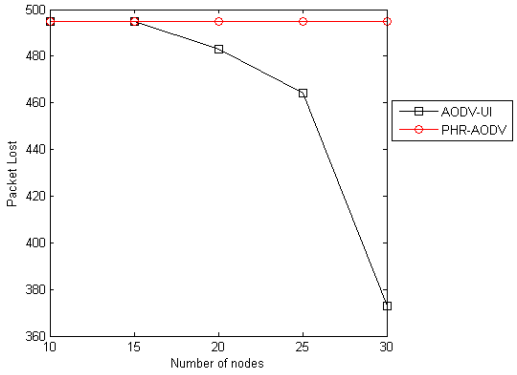

Fig.18 Packet lost vs number of nodes on blackhole attack

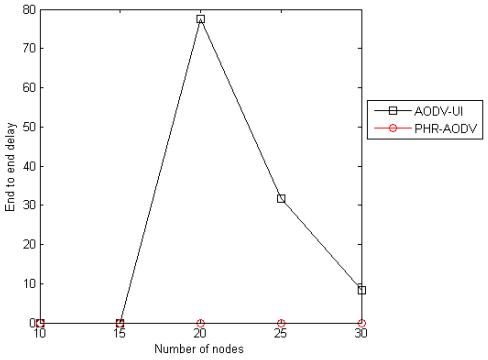

Fig.19 End to end delay vs number of nodes on blackhole attack

Fig.17, Fig.18, Fig.19 depict the impact of the number of nodes to the average packet delivery ratio, packet lost and end to end delay. The number of attacker nodes is set 5 and the number of nodes varies from 10 to 30. The result shows that for PHR-AODV, the average packet delivery ratio decreases for increasing the number of nodes. In contrast, the average of packet lost increases for increasing number of nodes. It means that for PHR-AODV, the larger the number of nodes in the network, the better the performance. For AODV-UI, all communications are failed under blackhole attack.

In blackhole attack, the source node receive reply message from attacker nodes that indicate the data packet have reach the destination, so the source node does not send packet request again, and the communication is failed.

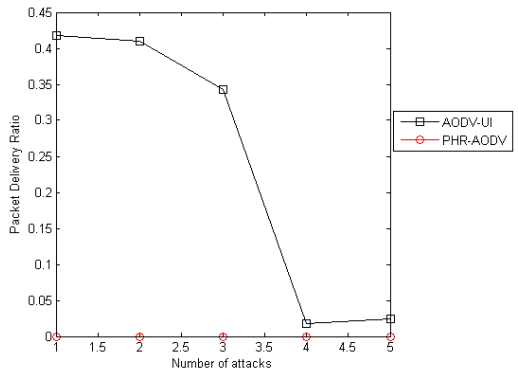

Fig.20 Packet delivery ratio vs number of attack on blackhole attack

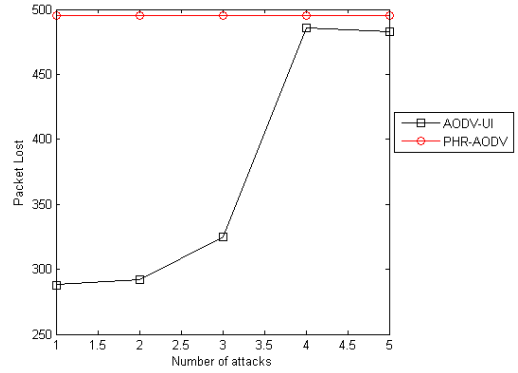

Fig.21 Packet lost vs number of attack on blackhole attack

Fig.20, Fig.21, Fig.22 shows the impact of the number of blackhole attacks to the average packet delivery ratio, packet lost and end to end delay. The number of nodes in the simulation under blackhole attack is 20, and the numbers of attacks increase gradually from 1 to 5 nodes.

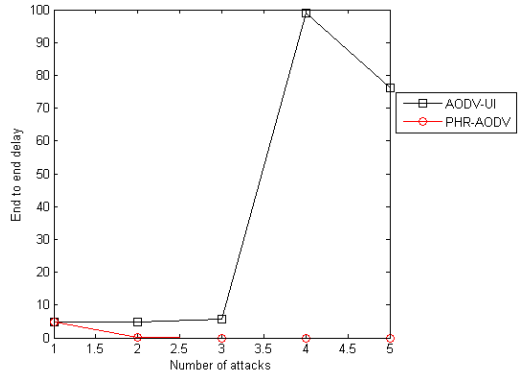

Fig.22 End to end vs number of attack on blackhole attack

With the variation of the attacker nodes under blackhole attack, for PHR-AODV, the average of packet delivery ratio decreases and the average of packet lost and end to end delay increases, when the number of attacker nodes increases. It means that more attackers in the network will lower the performance of PHR-AODV protocol. For AODV-UI, all communication failed. It means AODV-UI cannot perform communication under blackhole attack due to the minimum number of nodes inside the network.

7. Conclusion

Experiment results show that the performance of AODV-UI is better than PHR-AODV in terms of average packet delivery ratio, packet lost and end to end delay under DDOS and malicious nodes attacks. In the blackhole attack, PHR-AODV have a better performance than AODV-UI for the average packet delivery ratio, packet lost and end to end delay. AODV-UI cannot perform good communications under blackhole attack due the fact that AODV-UI does not have mechanism to generate an alternative communication path to destination.

Under malicious nodes and DDOS attack, the performance of the protocol that is not using secure method are better than protocol that is using secure method. In the future, we will develop a security mechanism in an efficient AODV protocol in which the secure algorithm does not degrade the performance of communication protocols. We plan to use bio inspired algorithm such as genetic algorithm to optimize the security mechanism.

References

[1] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, “A Survey of Secure Mobile Ad Hoc Routing Protocols,” IEEE communications surveys & tutorials, Vol. 10, no. 4, pp. 78-93, 2008.

[2] Arshad, J.; Azad, M.A.; , "Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks," Sensor and Ad Hoc Communications and Networks, SECON '06. 2006 3rd Annual IEEE Communications Society on , vol.3, no., pp.971-975, 28-28 Sept. 2006.

[3] Elmurod Talipov, Donxue Jin, Jaeyoun Jung, Ilkhyu Ha,YoungJun Choi, and Chonggun Kim, “Path Hopping Based on Reverse AODV for Security,” Proceedings 9th Asia-Pacific Network Operations and Management Symposium, APNOMS Busan, Korea, September 27-29, 2006.

[4] Abdusy Syarif, Harris Simaremare, Sri Chusri Haryanti, Riri Fitri Sari, "Adding Gateway Mode for R-AODV Routing Protocol in Hybrid Ad Hoc Network " tobe published at the IEEE Tencon conference, Bali, 2011.

[5] Abhay K. R, Rajiv Ranjan, Sauratbh Kant U, “Different types of attacks on integrated MANET – Internet Communication”, International Journal of Computer and Security (IJCSS, vol. 4, pp. 265-274, 2010.

[6] Ye Tung; Alkhatib, M.; Rahman, Q.S.; , "Security Issues in Ad-Hoc on Demand Distance Vector Routing (AODV) in Mobile Ad-Hoc Networks," Proceedings of the IEEE , vol., no., pp.339-340, 2005.
[7] Mohd Anuar Jaafar, Zuriati Ahmad Zukarnain, "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment," European Journal of Scientific Research ISSN 1450-216X, pp.430-443 Vol.32 No.3, 2009.
[8] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri,"Improving AODV Protocol against Blackhole Attacks," Procedings of the international multi conference of engineer and computer science Vol 2, 2010.
[9] Juwad, M.F.; Al-Raweshidy, H.S.; , "Experimental Performance Comparisons between SAODV & AODV," Modeling & Simulation, AICMS 08. Second Asia International Conference on , vol., no., pp.247-252, 13-15 May 2008.
[10] Payal N. Raj, Prashant B. Swadas. "DPRAODV: A Dyanamic Learning System Against Blackhole Attack In Bodv Based Manet." In: International Journal of Computer Science Issues, Vol.2, pp 54-59, 2009.
[11] C. Kim, E. Talipov, and B. Ahn, "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks", in Proc. Emerging Directions in Embedded and Ubiquitous Computing, EUC 2006 Seoul, Korea, pp.522-531, 2006.
[12] A. Hamidian, "Study Of Internet Connectivity For Mobile Ad Hoc Networks In NS-2", Masters Thesis, Departement Of Communication Systems, Lund Institute Of Technology, Lund University, Sweden, January 2003.
[13] R. F. Sari, A. Syarif, K. Ramli, B. Budiardjo, "Performance Evaluation Of Aodv Routing Protocol On Adhoc Networks Testbed Using PDA", *IEEE Malaysia International Conference On Communications And IEEE International Conference On Networks*, Kuala Lumpur, Malaysia,16 -18 November 2005.
[14] Kettaf N, Abouaissa H, Lorenz P, "An efficient heterogeneous key manajement approach for secure multicast communication in ad hoc network", Springet Telecommunication Syatem, vol 37, pp.29-36, 2008.
[15] Davide Cerri and Alessandro Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype," Communications Magazine, IEEE In Communications Magazine, IEEE, Vol. 46, No. 2. pp. 120-125, February 2008.
[16] M.G. Zapata, "Secure adhoc on-demand distance vector (S-AODV) Routing," in proceeding of ACM workshop on wireless security (WISE), Atlanta, 2002.
[17] Stephan Eichler; Christian Roman; , "Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC," Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on , vol., no., pp.481-484, Oct. 2006.
[18] Rasib Hassan Khan , K. M. Imtiaz-ud-Din , Abdullah Ali Faruq , Abu Raihan Mostofa Kamal , Abdul Mottalib, "A Security Adaptive Protocol Suite: Ranked Neighbor Discovery (RND) and Security Adaptive AODV (SA-AODV)," 5th International Conference on Electrical and Computer Engineering ICECE,Dhaka, Bangladesh. December 2008.
[19] Monis Akhlaq, M. Noman Jafri, Muzammil A. Khan, Baber Aslam, Addressing Security Concerns of Data Exchange in AODV. Transactions on Engineering, Computing and Technology, Volume 16 ISSN 1305-5313, pp. 29-33, November 2006.
[20] Shidi Xu, Yi Mu and Willy Susilo, "Authenticated AODV Routing Protocol Using One-Time Signature and Transitive Signature Schemes," Journal of Networks (JNW) Vol. 1 Issue 1, Academy Publisher, ISSN:1796-2056, pp. 47-53, May 2006.
[21] Shidi Xu, Yi Mu and Willy Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," Information Security and Privacy (ACISP), 11th Australasian Conference, Lecture Notes in Computer Science, Springer-Verlag, , pp. 99 – 110, 2006.
[22] Xiaoqi Li; Lyu, M.R.; Jiangchuan Liu; , "A trust model based routing protocol for secure ad hoc networks," Aerospace Conference, 2004. Proceedings. IEEE , vol.2, no., pp. 1286- 1295 Vol.2, 6-13 March 2004.
[23] A.Menaka Pushpa M.E, "Trust Based Secure Routing in AODV Routing Protocol," IMSAA'09 Proceedings of the 3rd IEEE international conference on Internet multimedia services architecture and applications IEEE Press Piscataway, NJ, USA , 2009.
[24] Raza, I.; Hussain, S.A.; , "A Trust based Security Framework for Pure AODV Network," Information and Emerging Technologies, ICIET 2007. International Conference on , vol., no., pp.1-6, 6-7 July 2007.
[25] A.A. Pirzada, A. Datta, and C.S.McDonald,"Trustworthy Routing with the AODV Protocol," the International Networking and Communications Conference (INCC'04), IEEE Communications Society, Lahore, Pakistan, pp 19-24, June 2004.
[26] Zhiyuan Liu; Shejie Lu; Jun Yan; , "Secure Routing Protocol based Trust for Ad Hoc Networks," Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on , vol.1, no., pp.279-283, July 30 2007-Aug. 1 2007.
[27] Kamal Deep Meka, Mohit Virendra and Shambhu Upadhyaya. "Trust Based Routing Decisions in Mobile Ad-hoc Networks", Proceedings of 2nd Workshop on Secure Knowledge Management, Brooklyn, New York, September.,2006.
[28] Anis Ben Arbia, Hedi Hamdi, Habib Youssef, "Wireless Routing Protocol Based on Trust Evaluation," icsnc, pp.329-334, 2008 Third International Conference on Systems and Networks Communications, 2008.
[29] Sebastien Berton; Hao Yin; Chuang Lin; Geyong Min; , "Secure, Disjoint, Multipath Source Routing Protocol(SDMSR) for Mobile Ad-Hoc Networks," Fifth International Conference Grid and Cooperative Computing (GCC), pp.387-394, Oct. 2006.
[30] In Sung Han, Hwang-Bin Ryou, Seok-Joong Kang, "Multi-Path Security-Aware Routing Protocol Mechanism for Ad Hoc Network," ichit, vol. 1, International Conference on Hybrid Information Technology , pp.620-626, Cheju Island, Korea 2006.
[31] Kotzanikolaou, P.; Mavropodi, R.; Douligeris, C.; , "Secure Multipath Routing for Mobile Ad Hoc Networks," Wireless

On-demand Network Systems and Services, 2005. WONS 2005. Second Annual Conference on , vol., no., pp. 89- 96, 19-21 Jan. 2005.

[32] Binod Vaidya, JaeYoung Pyun, JongAn Park, SeungJo Han, "Secure Multipath Routing Scheme for Mobile Ad Hoc Network," dasc, pp.163-171, Third IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC 2007), 2007

Harris Simaremare received the B.Sc. and Master degrees in Electrical Engineering from Universitas Gadjahmada. He is currently pursuing his PhD research on security in wireless ad-hoc networks.

Riri Fitri Sari, PhD. is a Professor at Electrical Engineering Department of Universitas Indonesia. She received her Bsc degree in Electrical Engineering from Universitas Indonesia. She receives her MSc in Computer Science and Parallel Processing from University of Sheffeld, UK. And she received her PhD in Computer Science from University of Leeds, Leeds. Riri Fitri Sari is a senior member of the Institute of Electrical and Electronic Engineers (IEEE).