AODV-UI with Malicious Node Detection and Removal for Public MANET

Ruki Harwahyu, Boma Anantasatya Adhi, Harris Simaremare, Abdusy Syarif, Abdelhafid Abouaissa, Riri Fitri Sari, and Pascal Lorenz

***Abstract*: A node in Mobile Ad-hoc Network (MANET) solely depends on neighbor nodes for its connectivity to the outer networks. It is completely different with fixed network connection where a central infrastructure is providing connectivity to the outside network for all mobile nodes there. This kind of situation makes MANET easier to build rather than fixed network with certain infrastructure. However, this nature of MANET makes it very vulnerable to various attacks, especially by nodes within the MANET that is called malicious nodes. This paper provides a preliminary result for MANET security enhancement based on AODV-UI routing protocol. In this work we implement an algorithm to detect and remove malicious nodes in AODV-UI routing protocol. We evaluate our work in different scenarios by varying the number of nodes, the number of malicious node, the sending rate of the node in concern, and the type of the attack i.e. route poisoning, black hole, packet spoofing. Our experiment shows that on average, an attack can be completely removed within 0.48 seconds in the worst case, with the traffic rate of 100 kbps, and 0.04 seconds in the best case, with the sending rate of 10 kbps.**

***Index terms:* AODV-UI, Malicious Node, MANET Security**

I. INTRODUCTION

MANET is a non-infrastructure network that consists of a collection of nodes that can communicate each other independently [1]. MANET enables ubiquitous and omnidirectional connection. It is designed for ease of setup and mobility. MANET is expected to be very useful in an urgent situation where infrastructure communication facilities are absent or difficult to install. For instance, MANET may be used in different situations e.g. a military communications network in a war field, an urgent rescue communication network when a disaster occurs, or a communications network in a temporary meeting.

In MANET, the connection is made available for every node by such a relay mechanism that is done by every node there. This mechanism is mainly maintained by an ad-hoc routing protocol. Ad-hoc routing protocol should be able to create multi-hop routing between participating mobile nodes and forming continuous ad-hoc network without much user intervention.

However, MANET is considered as a non-secure network to be relied on in several case of communication. Compared to fixed wired network, aside from its easy-to-setup advantage, MANET has some drawbacks especially in terms of network security. MANET is more vulnerable due to its physical configuration that is basically open; its topology that likely will change rapidly; its power and resources limitation of the node; and the absence of centralized management and monitoring unit. The problem complexity is increased by the fact that each node should actively discover the other, learn the topology and ensure the end-to-end connection.

MANET implies that the underlying protocol relies on a mutual trust among all nodes. Every node in MANET has to work together with the others faithfully, whoever it is. This cooperation mechanism makes MANET easy to disrupt since there is no guarantee that the neighboring nodes will always forward one's packet correctly. MANET is different from the wired network which has its connection governed directly by the legitimate device that is dedicated and fixed as the infrastructure. MANET's connectivity is strongly depends on the other nodes.

MANET uses wireless channel that is by default shared and accessible by all nodes, whether it is a legitimate member node or malicious node. Technically speaking, a node that is already acknowledged as the member of a MANET can disrupt the network. It can also play prank to the other node that relies its connection on this node by simply altering the packet forwarding path. All of these security drawbacks emerge because basically it is unknown whether malicious nodes exist in a sending path.

Since the MANET is weaker to attack compared to the wire network, it is required to immediately detect and take measures for an attack against the MANET [2]. It is important to ensure all the nodes within a MANET to behave properly. Some approaches have been proposed. Ensuring node's behavior basically can be achieved by membership registration. Although this is important, membership management in MANET is hard to implement without central management device. The other way is by limiting the access, but this approach is not a good practice for public MANET since it should be open and easy to setup. To mitigate this kind of security threat while maintaining MANET's open nature, the

Manuscript received September 25, 2012; revised December 24, 2012.

This work is part of International Joint Collaboration and Scientific Publication project between Universitas Indonesia, Indonesia and Universite Haute-Alsace, France, 2011-2013.

Ruki Harwahyu, Boma Anantasatya Adhi, Abdusy Syarif and Riri Fitri Sari are with the Universitas Indonesia, Indonesia (e-mails: {ruki.harwahyu11, boma.anantasatya11, abdusy.syarif, riri}@ui.ac.id).

Harris Simaremare, Abdelhafid Abouaissa and Pascal Lorenz are with University of Haute-Alsace, France (e-mails: {harris.simaremare, pascal.lorenz}@uha.fr).

other approach is to secure the sending path between nodes. Such a security adjustment should be working together with the routing protocol.

There are two types of ad-hoc routing protocols [3], namely:

- Proactive: Destination Sequenced Distance Vector (DSDV), Cluster Switch Gateway Routing (CSGR), Wireless Routing Protocol (WRP), Optimized Link State Routing (OLSR).
- Reactive: Dynamic Source Routing (DSR), Ad-hoc On-demand Distance Vector (AODV), Temporally Ordered Routing Algorithm (TORA), Associativity-Based Routing (ABR), Signal Stability Routing (SSR).

Routing protocols in ad-hoc networks becomes a challenging problem to be investigated since a node can move freely, coming and leaving the coverage area, connect and disconnect to the network, as well as extending the coverage area and increasing the hop.

This work incorporates a security measure on the AODV routing protocol, i.e. to detect and remove malicious node. This work concerns on how to secure the sending path. The primary focus of this mechanism is to guarantee that the forwarding path consist of legitimate nodes only. We review some similar works in section 2. Section 3 gives a brief review on AODV and AODV-UI. Section 4 explains the implementation of the proposed algorithm into AODV-UI. The simulation is conducted under various scenarios as discussed in section 5 along with the result. Section 6 presents the conclusions and future works.

II. MANET SECURITY

Routing in MANET has two important steps, i.e. discovering the neighbors and route management. In MANET, neighborhood may rapidly change due to mobility. Neighbor discovery is very crucial since route formation uses the information gathered on this step. Taking this into account, the first security method is to secure neighbor discovery.

Basically, security threat in MANET can be caused by a node that either does not forward other's packet, does not forward packet to the correct route or altering the packet's content. Other kind of threat could also be routing information manipulation and many kind of DoS that can be done both by flooding and signal jamming.

In the ITU-T recommendation no. X.805 there are 8 security dimensions that should be taken into account in security architecture for systems providing end-to-end communication [4]. Some of them are required to be addressed in MANET. There are some proposed methods to secure MANET in term of access control and authentication approach. This approach aims to control user's access to the network and apply a proof of identity. In term of data confidentiality and privacy, some approaches have been introduced by performing encryptions. In term of communication security and data integrity there are some approaches introduced to mitigate packet spoofing and route poisoning.

There are various ways to secure MANET. Reciprocal authentication between the sender and receiver based on the public key has been introduced in [5]. It invokes session key to further ensure that both nodes are legitimate. This method reduces the number of packets dropped compared to the normal AODV and DSR when malicious nodes exist. It requires a cluster head to manage keys and authentication service. Other security measures employing authentication have also been used such as in SAODV [6] and TAODV [7]. However, for authentication to be happened, one should aware how the key should be distributed and who should manage the process.

Secure routing mechanism using control and confidence value has been proposed in [8]. In this work, a watchdog judges whether a node has an abnormal behavior in forwarding other packet. IN addition, node's credence value is maintained for each node. In principle, this proposed method can detect black hole attack without much routing overhead.

Another a trustworthiness measure is also employed in security adaptive protocol suite. This protocol suite introduces a certain level of security for each route that is attained through Ranked Neighbor Discovery (RND). It then judges the security level required by the application and route the packet accordingly. This Security-Aware Ad-hoc Routing (SAR) approach provides enhancement in its route discovery for including security attributes [9]. SAR enables the use of security as a negotiable metric to improve the relevance of the routes discovered by ad-hoc routing protocol.

An approach based on fairness and trust has been introduced in CONFIDANT protocol [10]. The method is implemented on DSR protocol by employing 4 functionalities: (1) to monitor the neighbor for malicious behaviors, (2) to manage neighbor's trust level using similar mechanism that is used in Pretty Good Privacy (PGP), (3) to calculate node's reputation based on its behavior and (4) to manage the path, classify it and determine whether it contains malicious node or not. However, there is no similar approach implemented in AODV protocol.

III. AODV AND AODV-UI

A. AODV

AODV is a reactive distance vector routing protocol. It only requests a route when needed. The standard AODV was developed by C. E. Perkins, E.M. Belding-Royer and S. Das in RFC 3561 [11]. AODV nodes rely on control messages namely Route Requests (RREQs), Route Replies (RREPs) and Route Errors (RERRs) to communicate with others. All of this control messages are sent with UDP and IP encapsulation to manage the route on the routing table.

The routing table stores information about the next hop to the destination and indicates the latest information. Routing tables managed by every node in AODV contains the following fields [11]:

- Destination IP Address
- Destination Sequence Number
- Valid Destination Sequence Number flag
- Other state and routing flags (e.g., valid, invalid, repairable, being repaired)
- Network Interface
- Hop Count (number of hops needed to reach destination)

- Next Hop
- List of Precursors
- Lifetime (expiration or deletion time of the route)

Since it works on demand, AODV node does not maintain any route entry except for some seconds after the use of corresponding route entry. This timer ensures every node to serve only a 'fresh' route and to invalidate old route entry by itself. If a route to a destination exists, the node will use it to forward the packet. If the route does not exist, the sending node initiates path discovery by broadcasting the RREQ message. This type of message is used to enquiry route that satisfy the destination. The broadcast of RREQ message is limited by the TTL in the IP header. The RREQ message format can be seen in Fig. 1

RREP message is used to propagate route information. This message serves as the reply for RREQ message. RREP message is sent unicastly along the way back to the RREQ's sender. Nodes who can reply RREQ message with RREP message are either the destination node itself or any intermediate nodes that has a valid route to the destination that is asked by the RREQ message. If the nodes who receive the RREQ message is unable to give a reply, it must rebroadcast the RREQ to its neighboring nodes. Thus, when intermediate nodes receive a RREQ message, they update their routing table and forward the message. When the intermediate nodes receive Route Reply (RREP), they will forward it to the destination. The route reply message contains some fields as shown in Fig. 2.

Byte 1	Byte 2	Byte 3	Byte 4
Type	Flags + Reserved		Hop Count
RREQ ID			
Destination IP Address			
Destination Sequence Number			
Originator IP Address			
Originator Sequence Number			

Fig. 1. RREQ message format

Byte 1	Byte 2	Byte 3	Byte 4
Type	Flags + Reserved + Prefix Size		Hop Count
Destination IP Address			
Destination Sequence Number			
Originator IP Address			
Lifetime			

Fig. 2. RREP message format

Byte 1	Byte 2	Byte 3	Byte 4
Type	Flags + Reserved		Dest. Count
Unreachable Destination IP Address			
Unreachable Destination Sequence Number			
… <more unreachable destination & sequence> …			

Fig. 3. RRER message format

Byte 1	Byte 2	Byte 3	Byte 4
Type	Reserved		Hop Count
R-RREP ID			
Destination IP Address			
Destination Sequence Number			
Originator IP Address			
Reply time			

Fig. 4. RRER message format

RERR message is used to notify other nodes to remove a certain route. Each node monitors the next hop nodes noted in the valid routing entry. If the next hop for a certain route entry is no longer reachable, possibly because of node's movements, this node will invalidate the route entry in its own routing table and send RRER message to the other node that is concerned about this route. By doing this, any other nodes that use this route will be aware that this route is no longer available. This reporting mechanism is made possible by a "precursor list" containing IP address for each its neighbors who are likely to use this node as a next hop towards other destination. The route error message contains some fields as shown in Fig 3.

The special characteristic of AODV is the use of destination sequence number in each route entry. This value is calculated along the way as the RREP message being propagated. This value is to ensure loop-free route. When there are more than one route to a destination exists in routing table, the sender supposed to choose the one with the greatest sequence number.

B. AODV-UI

One of the disadvantages of AODV protocol is that the sender node must re-initiate the connection by running route discovery procedure to find new path when the connection between nodes is lost. Hence, AORV will introduce a lot of routing overhead as te mobility of nodes inside the MANET increase. AODV-UI [12] was developed to overcome this problem. AODV-UI is developed by Universitas Indonesia by Abdusy Syarif et al and was introduced in 2011.

This proposed protocol combines gateway mode and reverse rote. AODV-UI can be used in hybrid ad-hoc networks and it has some improvement in routing overhead and energy consumption. This protocol has an algorithm to determine which nodes as an intermediate node. This protocol also includes energy as a parameter in selecting node.

The gateway mode enables a node to be set as a gateway. In real implementation, this gateway node can be a stationary device backed with wired connection. Other mobile node on the MANET will use this gateway to connect to the outside network such as internet. This gateway mode is adopted from AODV+ [13].

AODV+ has been designed to achieve routing communication between node in ad-hoc network to node in wired network or infrastructure. This variant of AODV uses hybrid gateway discovery mode. It combines two gateway discovery models, i.e. reactive and proactive. The reactive gateway discovery is initiated by ad-hoc node to create or update a routing table to the gateway. In this discovery mode, mobile node will broadcast a route request (RREQ) message with "I" flag (RREQ_I). Only the gateway(s) addressed by this message will process it. In the contrary, the proactive gateway discovery is initiated by the gateway itself. This gateway can be a mobile node or other static terminal with wireless interface. It broadcasts a gateway advertisement (GWADV) message periodically to ad-hoc network, so a mobile node that receives the GWADV will update its route entry and recognize it as the gateway.

The reverse route in AODV0UI is adopted from R-AODV [14, 15]. R-AODV provides solutions for the MANET topology that is changing rapidly. Frequent change of network topology is a tough challenge for many important issues, such as routing protocol robustness and resilience performance degradation. This variant of AODV provides reverse route by trying multiple route replies. This protocol has been proved in reducing path fail correction message, reduce routing overhead, and shorten the time required for path recovery process.

In R-AODV, RREQ message has additional 4-bytes field for timestamp. During the route discovery, immediately after receiving the first RREQ message, the node broadcast reverse request (R-RREQ) message rather than sending unicast RREP. The format of R-RREP message is illustrated in Fig 4.

The processing procedure of this message is same as the RREP message in AODV. However, the nodes who send RREQ will receive multiple R-RREQ suggesting a valid path toward the destination. This originating nodes will chose the best path to forwarding the packet.

By broadcasting R-RREQ, this protocol has more control packet overhead. Nevertheless, this overhead is smaller compared to the original AODV that uses only single reply message in high-mobility MANET. For instance, in ad-hoc network has N number of terminals with M nodes participate in discovering a routing path, the required number of control messages to discover routing path for AODV (*P*) if it does not fail in first try is expressed in equation (1)

$$P = M - 1 + t \quad (1)$$

where *t* is the number of nodes forwarding RREP message.

If source node fails in the first try, since it does not receive any RREP message during a certain interval time, the node will re-initiates path discovery process. It means that the number of control messages will be increased by the number of attempts, as expressed in equation (2)

$$\mathrm{P} = \mathrm{c}(\mathrm{M} - 1 + \mathrm{t}) \quad (2)$$

where *c* is the number of attempt for route discovery.

If we assume that R-AODV has at least one stable path that satisfies the RREQ, the number of control messages for R-AODV (*Q*) is expressed in equation (3).

$$\mathrm{Q} = 2\mathrm{M} - 2 \quad (3)$$

Hence, we can conclude when c>1, standard AODV causes more packet overhead than the case of c=1 on R-AODV routing. This condition is likely to be experienced in MANET. As mentioned in [16], when the number of nodes is 100 and the number of flows is 50, 14% of total RREP messages are lost in standard AODV.

IV. AODV-UI FOR SECURING PUBLIC MANET

Most of the security measures that have been introduced for MANET are conducted by limiting node's access to the network. We consider this kind of preventive security measure is not the best practice for public MANET where everyone is supposed to share and support other connectivity. In public MANET, the more nodes joined, the wider area can be covered, and the more people can be served without much sacrifice on their mobility. It is preferred to conduct detection and curative treatment assuming that the level of security required by users in public MANET is not too urgent. Hence, we mostly focus on mitigating the attack in MANET.

Our proposed method enhances AODV-UI with the ability to detect and remove malicious nodes. It is accomplished by so called 'hear' and 'compare' mechanism. We define malicious nodes as a node that does not forward other packet; modify other packet in forwarding, and sending some kind of forged routing control packet. This algorithm is designed to overcome black hole attack, packet spoofing, and routing message flooding.

In this proposed method, every node has a 'hear' mechanism that will capture the transmission even if it is not for this node. This capture is possible in 802.11 standards, since naturally every packet sending can be considered as a broadcast in physical level on the same wireless channel. This happens after the node sends a packet to a neighboring node to be relayed to the 'unseen' destination.

Referring to the simple topology shown in Fig 5, when node_a wants to send a packet to node_c which is unseen from node_a, after node_a send the packet to node_b, node_a will keep 'hearing' node_b, whether this intermediate nodes relaying the packet to the other node. If node_b is not relaying node_a's packet within a certain amount of time, node_a will consider node_b as a malicious node since it does malicious behavior, i.e. not forwarding other's packet.

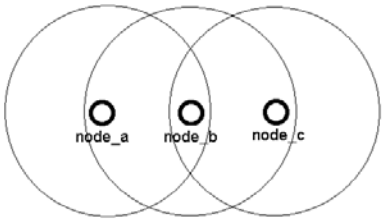

Fig. 5. Simple configuration with sender, intermediate, and receiver node

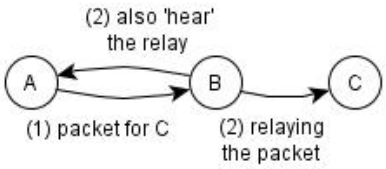

Fig. 6. Sender 'hears' if the intermediate node is relaying the packet

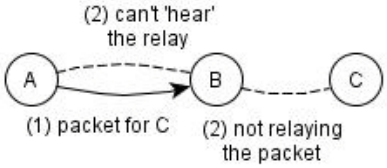

Fig. 7. Sender mark the neighbor as malicious if sender cannot 'hear' the relay

To accompany this 'hearing' mechanism, each sending node also keeps its sent packet for a while. This is then compared to the packet captured by 'hearing'. If the captured packet content is different, this node will consider the

forwarding node as a malicious node. Every malicious node is remembered and removed from the routing table and neighbor management.

For this to be done, an interval where the node is supposed to wait for the echoed packets by its neighbor is applied. We call this a Wait interval. If the delay is larger than this interval, the neighbor node is considered as malicious. The size of this interval is significant since it will give additional latency to every packet transmission.

We consider propagation delay in defining this interval. If D is time required for a packet to travel from its origin until the direct neighbor, it may take the same amount of time for the echo packed to be broadcasted by the neighbor to be received by the sender. Thus, 2D is the minimum interval for waiting for echo packet. In this scenario, we use 3D for the maximum interval allowed. The proposed mechanism works as pseudo code shown in Fig. 8.

```
Foreach packet sent
{
 save packet information
 waiting for Wait interval
 {
  If hear neighbor do forwarding the packet
  {
   If saved pkt info == heard pkt info
   {
    Neighbor normal
   }
   Else
   {
    Neighbor malicious
  }
  Else
  {
   If neighbor still reachable
   {
    Neighbor malicious
   }
   Else
   {
    Route error //topology change
   }
  }
 }
}
```

Fig. 8. Pseudocode of the proposed algorithm

This 'hear' and 'compare' scheme is only applied for data packet. Our proposed method does not apply any encryption to the AODV message. It is kept in plain to make it accessible for public. However, we apply some delay timer to appropriately mitigate the flooding attack that can keep the node busy and further exhaust node's battery.

We perform modification in AODV UI to implement our proposed mechanism as follows:

- Adds the 'hear' and 'compare' mechanism at AODV::recv() routine to be executed toward every packet received with similar packet unique ID with buffered packet (packet that has been sent before by the current node).
- Adds a MAL packet for propagating malicious node information.
- Set layer 2 broadcast as the default forwarding method in AODV::forward(). It is important to make NS explicitly simulate layer 2 broadcasts for the packet. It is required for 'hearing' by the other node. This is only necessary for simulation purpose.
- Adds a timer for 'compare' mechanism, called Wait interval. 'Hear' mechanism will active during this timer interval and when it hears an echoed packet, it 'compares' it with buffered packet.

V. Experiment and Result

A. Experimental Setup

Several parameters were evaluated and analyzed during our simulations. CBR is used to generate data traffic between the user and receiver with various sending rate. TCP is used for the transport protocol. The ACK from TCP is used to evaluate the round-trip latency. The MANET condition is varied by the number of malicious node and its position. Simulation parameter shows in Table I.

TABLE I
Simulation parameter

Parameter	Value
Simulation time	30 seconds
Topology	2D random mobility (1st scenario) & linear (2nd scenario)
Wait interval	0.3 seconds
Number of node	3 (1st scenario) and 10 (2nd scenario)
No. of malicious node	1
Sources	Tahoe TCP
Traffic type	CBR

B. Result and Discussion

There are two main evaluation conducted to evaluate our proposed method. The first is round-trip latency and the second is the recovery time. We define the recovery time as the amount of time required to remove malicious node(s) from the routing table.

Round-trip latency is measured by comparing timestamp of the packet sent and its ACK that is received back on the sender. The first scenario consists of three nodes: sender node, normal (legitimate) node who acts as intermediate node, and receiver node. The result from this scenario is depicted in Fig.9 and Fig.10 for original AODV and our proposed method respectively. Compared to the original AODV, the proposed secured AODV-UI has additional latency. This additional latency is proportional to the Wait time required for 'hearing' mechanism and it is inevitable. This implies that our proposed algorithm works as fine as AODV does in the normal environment excluding the mentioned additional latency.

From 60 times of trials, on average, the best latency that TCP can deliver with AODV is approximately 24.09 ms, and with AODV-UI is 44 ms. As displayed in Fig.11, the latency

between secured AODV-UI is about 20 ms greater than the latency on the normal AODV. This is because of the drawbacks of the 'hearing' method. However, this additional latency is not much interference with overall performance of MANET. While introducing the drawback in term of latency, AODV-UI can handle attacks from malicious nodes.

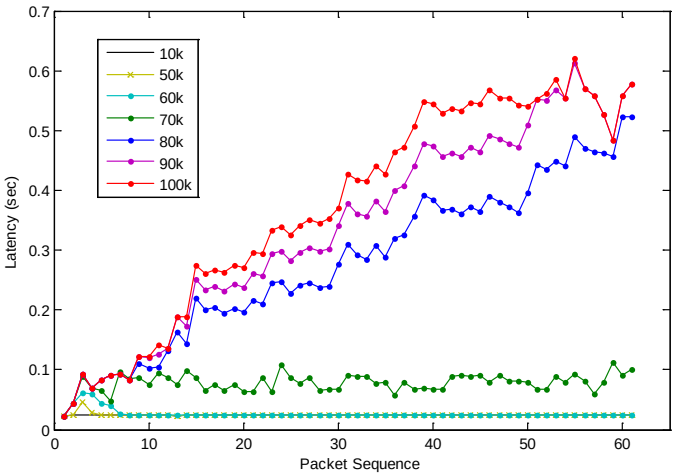

Fig. 9. Per-packet latency on various rate of CBR on AODV

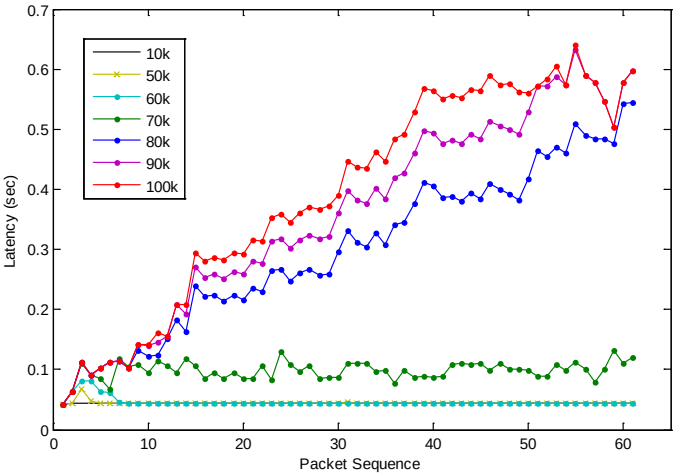

Fig. 10. Per-packet latency on various rate of CBR on secured AODV-UI

The recovery time is measured by sending the packet to an 'unseen' remote node, by relying to some intermediate nodes on a line. We set one of the intermediate node (in random position) to be a malicious node on a certain time, and compare this time to the timestamp when the sending node detect this malicious behaviors and remove this node from the routing table. Fig.12 shows that the recovery time is varied by sending rate, and most of them are twice as its latency.

VI. Conclusion and Future Work

Our proposed method to mitigate the common attacks on public MANET has been successfully implemented on ns2 network simulator. This enhanced AODV-UI is proven for being robust against malicious node. The improvement that has been made on AODV-UI now has made it closer to be implemented on public MANET. However, for further MANET-specific security threat, we still do not prevent detour attack. This will improve gradually along with the implementation of public MANET as security requirements rises on the user side. Cross layer security measure may also be considered to overcome attacks on the lower layer. In the future work, we will implement a new trust mechanism as an early detection and prevention from various attacks.

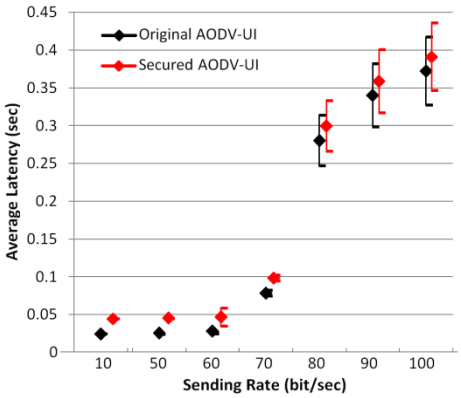

Fig. 11. Average latency on various rate of CBR

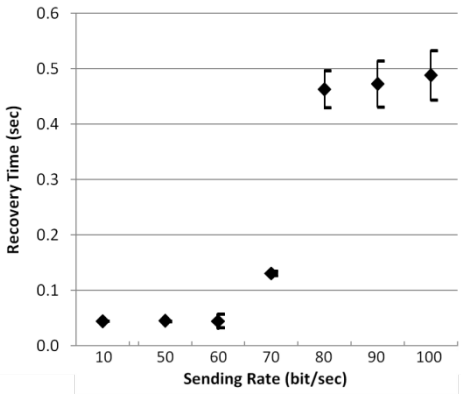

Fig. 12. Recovery time on various rate of CBR on secured AODV-UI

References

[1] Harris Simaremare, Riri Fitri Sari, "Performance Evaluation of AODV variants on DDOS, Blackhole and Malicious Attacks" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.6, June 2011.

[2] Jongoh Choi, Si-Ho Cha, GunWoo Park and JooSeok Song, "Malicious Nodes Detection in AODV-Based Mobile Ad-hoc Networks" GESTS Int'l Trans. Computer Science and Engr.,Vol.18, No.1, 2005.

[3] C. Kopp, "Ad-hoc Networking", Background Article, Published in 'System', (2002) p.33-40.

[4] Zachary Zeltsan, Security Architecture forSystems Providing End-to-End Communications, ITU-T Recommendation X.805, 2003.

[5] G.Varaprasad, S. Dhanalakshmi, M. Rajaram3, "New Security Algorithm for Mobile Adhoc Networks Using Zonal Routing Protocol", 2008.

[6] M. G. Zapata, "Secure Ad-hoc On-Demand Distance Vector (SAODV) Routing", ACM SIGMOBILE Mobile Computing and Communications Review, p.106-107, Volume 6 Issue 3, July 2002.

[7] Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu, "A Trust Model Based Routing Protocol for Secure Ad-hoc Networks", IEEE Aerospace Conference Proceedings, 2004.

[8] Liu Jinghua, Geng Peng, Qiu Yingqiang, Feng Gui, “A Secure Routing Mechanism in AODV for Ad-Hoc Networks”, Proceedings of 2007 International Symposium on Intelligent Signal Processing and Communication Systems Nov.28-Dec.1, 2007.

[9] Seung Yi, Prasad Naldurg, Robin Kravets, “A Security-Aware Routing Protocol for Wireless Ad-Hoc Networks”, MobiHoc '01 Proceedings of the 2nd ACM international symposium on Mobile ad-hoc networking & computing, proceeding of, p.299-302, 2001.

[10] Buchegger, Sonja, and Jean-Yves Le Boudec. "Performance analysis of the CONFIDANT protocol." In Proceedings of the 3rd ACM international symposium on Mobile ad-hoc networking & computing, pp. 226-236. ACM, 2002.

[11] C. Perkin, E.M. Belding-Royer, S. Das, Ad-hoc On Demand Distance Vector (AODV) Routing, IETF Internet Draft, 2002.

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

[13] A. Hamidian, ”Performance of Internet Acces Solutions in Mobile Ad-hoc Networks”, Master Thesis, Lund University, 2001

[14] C. Kim, E. Talipov, B. Ahn , ”A Reverse AODV Routing Protocol in Ad-hoc Mobile Networks”, IFIP-International Federation for Information Processing, Seoul, Korea, August 2006

[15] E. Talipov, D. Jin, J. Jung, I. Ha, YJ Choi, C. Kim,”Path Hopping based on Reverse AODV for Security”, APNOMS, Busan, Korea, September 2006

[16] Rendong Bai and Mukesh Singhal, “Salvaging Route Reply for On-Demand Routing Protocols in Mobile Ad-Hoc Networks” in MSWIM 205, Montreal, Quebec, Canada. Oct 2005.

BIBLIOGRAPHY

Ruki Harwahyu receives his Bsc degree at Departement of Electrical Engineering Universitas Indonesia in 2011. He is currently undergoing his dual degree master study at Information and Multimedia Network, Universitas Indonesia and Electronic & Computer Engineering, National Taiwan University of Science and Technology. He has been conducting research around the topic of Internet of Things.

Boma Anantasatya Adhi receives his Bsc degree at Departement of Electrical Engineering Universitas Indonesia in 2010. He is currently undergoing his dual degree master study at Information and Multimedia Network, Universitas Indonesia and Computer and Communication Engineering University of Duisburg-Essen. His interests include hi-performance computing, embedded and operating system and intelligent control.

Harris Simaremare received the B.Sc. and Master degrees in Electrical Engineering from Universitas Gadjahmada. He is currently pursuing his PhD research at University of Haute-Alsace in Colmar France. He is working on security in wireless ad-hoc network.

Abdusy Syarif receives his BSc degree in Informatic Engineering from Universitas Mercu Buana, Indonesia. And his Master degree in Electrical Engineering from Universitas Indonesia. He is currently pursuing his PhD research on ad-hoc hybrid routing protocol and wireless sensor networks.

Abdelhafid Abouaissa is an Associate Professor at the University of Haute-Alsace, in Colmar France. He received the BS degree from Technical University of Wroclaw, Poland, in 1995, and the MS degree from Franche-Comté University of Besançon, France, in 1996. He obtained the PhD at Technical University of Belfort, France in January 2000. His interests include multimedia synchronization, group communication systems, QoS routing in Ad-Hoc, MPLS, DiffServ, and QoS management.

Riri Fitri Sari, PhD. is a Professor at Electrical Engineering Departement of Universitas Indonesia. She received her Bsc degree in Electrical Engineering from Universitas Indonesia. She receive 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).

Pascal Lorenz is a professor at the University of Haute-Alsace and responsible for the Network and Telecommunication Research Group. His research interests include QoS, wireless networks, and high-speed networks. He is a member of many international program committees and has served as a guest editor for a number of journals, including Telecommunications Systems, IEEE Communications Magazine, and Lecture Notes in Computer Science.