Management Science Letters 2 (2012) 2271–2280

Contents lists available at GrowingScience

Management Science Letters

homepage: www.GrowingScience.com/msl

A new method for improving security in MANETs AODV Protocol

Zahra Alishahi[a*], Javad Mirabedini[b] and Marjan Kuchaki Rafsanjani[c]

[a]*Department of Computer, Science and Research Branch, Islamic Azad University, Kerman, Iran*
[b]*Department of Computer Science, Islamic Azad University, Central Tehran Branch, Iran*
[c]*Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran*

ARTICLEINFO

Article history:
Received May 20, 2012
Received in Revised form
July, 29, 2012
Accepted 15 August 2012
Available online
20 August 2012

Keywords:
MANETs
Ad hoc
AODV
Security
Packet drop attack

ABSTRACT

In mobile ad hoc network (MANET), secure communication is more challenging task due to its fundamental characteristics like having less infrastructure, wireless link, distributed cooperation, dynamic topology, lack of association, resource constrained and physical vulnerability of node. In MANET, attacks can be broadly classified in two categories: routing attacks and data forwarding attacks. Any action not following rules of routing protocols belongs to routing attacks. The main objective of routing attacks is to disrupt normal functioning of network by advertising false routing updates. On the other hand, data forwarding attacks include actions such as modification or dropping data packet, which does not disrupt routing protocol. In this paper, we address the "Packet Drop Attack", which is a serious threat to operational mobile ad hoc networks. The consequence of not forwarding other packets or dropping other packets prevents any kind of communication to be established in the network. Therefore, there is a need to address the packet dropping event takes higher priority for the mobile ad hoc networks to emerge and to operate, successfully. In this paper, we propose a method to secure ad hoc on-demand distance vector (AODV) routing protocol. The proposed method provides security for routing packets where the malicious node acts as a black-hole and drops packets. In this method, the collaboration of a group of nodes is used to make accurate decisions. Validating received RREPs allows the source to select trusted path to its destination. The simulation results show that the proposed mechanism is able to detect any number of attackers.

1. Introduction

A Mobile ad hoc network (MANET) is an autonomous system of wireless mobile nodes, which can be dynamically setup anywhere and anytime. MANET differs from cellular networks or conventional wired networks as there is no centralized access point (Hu & Perrig, 2004; Murthy & Manoj, 2004). MANET allows multi-hop communication among nodes, which are not in direct transmission range through intermediate nodes. Nodes are free to move randomly thus form arbitrary network topology.

* Corresponding author.
E-mail addresses: talishahi63@gmail.com (Z. Alishahi)

doi: 10.5267/j.msl.2012.08.018

The network size changes as a node can join or leave network at any time. The main problem in mobile ad hoc networks is the lack of consistency to deliver information to the intended node so, MANET is more vulnerable to security attacks than conventional wired and wireless networks due to its fundamental characteristics of open medium, dynamic topology, absence of centralized access point, distributed cooperation, lack of association (Yang et al., 2004). Authorized and malicious nodes both can access the wireless channel. As a result, there is no clear line of security in MANETs from the outside world. Routing algorithm needs mutual trust between nodes and absence of centralized access point prevents use of monitoring agent in the system. The limitation of wireless network and mobile nodes such as bandwidth of wireless channel, frequent disconnection of link, partition of network, short battery lifetime and limited computation capability poses an important challenge for implementation of cryptographic algorithms for providing security to these networks. Routing security is an important issue in MANET. In MANET, two types of messages are used: data messages and routing or control messages. Data messages need end to end authentication and can be secured using point to point security mechanism. Routing messages are used for the route establishment and route maintenance. Routing messages are processed by intermediate nodes during their propagation therefore securing routing messages is more challenging compared with data messages. A malicious node can perform many types of routing attacks such as routing table overflow, routing table and cache poisoning. Routing protocols must be robust against routing attack in order to establish correct and efficient route between pair of nodes. In this paper, we address the "Packet Drop Attack", which is a serious threat to operational mobile ad hoc networks. Although the proposed method is focused on AODV protocol, the proposed solution is applicable to other routing protocols for MANETs.

2. Security attacks and related work

The security attacks in mobile ad hoc network fall into two categories: passive attacks and active attacks. In passive attack, malicious node does not affect the normal operation of data so it is very difficult to detect. It includes traffic analysis, monitoring and eavesdropping. Encryption algorithms are used to prevent passive attacks. In active attack, malicious node disrupts the normal functioning of system by performing either external or internal attacks. External attacks are from malicious nodes, which would not belong to network. External attacks can be prevented by using cryptography techniques such as encryption. Internal attacks are from either compromised or hijacked nodes, which attempt to disrupt the normal routing function in order to consume the network resources. Internal attacks include modification, impersonation, jamming, sleep deprivation and denial of service attacks, which are very difficult to prevent.

There have been many studies for security of routing in MANET. Hu et al. (2002b) proposed secure efficient ad hoc distance vector (SEAD) and used a protocol, which is based on the design of DSDV (Perkins & Bhagwat, 1994). SEAD is designed to prevent attacks such as DoS and resource consumption attacks. SEAD uses one way hash function for authenticating the updates, which are received from malicious nodes and non-malicious nodes and it can be used by any suitable authentication and key distribution scheme. However, finding such a scheme is not straightforward. Ariadne (Hu et al., 2002a), by the same authors, is based on basic operation of DSR (Johnson & Maltz, 1996). Ariadne is a secure on-demand routing protocol and uses only high efficient symmetric cryptographic operations. Ariadne provides security against one compromised node and prevents many types of denial-of-service attacks. Ariadne uses message authentication code (MAC) and secret key shared between two parties to ensures point-to-point authentication of a routing message. However, it relies on the TESLA (Perrig et al., 2001) broadcast authentication protocol for secure authentication of a routing message, which requires loose clock synchronization which is, arguably, an unrealistic requirement for ad hoc networks. It is quite likely that, for a small team of nodes that trust each other and that want to create an ad hoc network where the messages are only routed by members of the teams, the simplest way to keep secret communications is to encrypt all messages (routing and data) with a "team key". Every member of the team would know the key and, therefore,

it is possible to encrypt and to decrypt every single packet. Nevertheless, this does not scale well and the members of the team have to trust each other. So it can be only used for a very small subset of the possible scenarios. Security-aware routing (SAR) (Kravets et al., 2001) is an on demand routing protocol based on AODV (Perkins & Royer, 1999). SAR defines level of trust as a metric for routing. Nodes distribute key with those nodes having equal level of trust or higher level of trust. Thus an encrypted packet can be decrypted only by the nodes of the same or higher levels of trust. The main drawback of SAR is that during the path discovery process, encryption and decryption is done at each hop, which increases the power consumption. The protocol also requires different keys for various level of security, which leads to increase in number of keys required when the number of security levels used increases.

Sanzgiri et al. (2002) proposed ARAN, authenticated routing for ad hoc networks (ARAN), which is based on AODV that uses authentication and requires the use of a trusted certificate server whose public key is known to all legal nodes in the network. In ARAN, every node, which forwards a route discovery or a route reply message must also sign it. This is very time consuming and causes the size of the routing messages to increase at each hop. On the other hand, the ARAN uses asymmetric cryptography, which causes higher cost for route discovery. The ARAN ensures secure route by end-to-end route authentication process but needs a small amount of prior security coordination among nodes. The ARAN prevents unauthorized participation, message modification attacks but prone to replay attacks if nodes do not have time synchronization. Papadimitratos and Haas (2002) proposed a protocol (SRP), which can be applied to several existing routing protocols (in particular DSR see Johnson et al., 2003 and for IERP see Haas et al., 2002). SRP requires that, for every route discovery, source and destination must have a common security association. Furthermore, the paper does not even mention route error messages. Therefore, they are not protected, and any malicious node can just forge error messages with other nodes as source. Zapata and Asokan (2003) proposed Secure AODV (SAODV), another protocol designed to secure AODV. The idea behind SAODV is to use a digital signature to authenticate the non-mutable fields of messages and hash chains to secure the hop count information. The SAODV described two methods to secure routing: Single Signature Extension and Double Signature Extension. When a node receives any message such as RREQ or RREP, it first verifies the signature before creating or updating a reverse route to that host. The SAODV is based on asymmetric key cryptographic operation therefore the nodes in MANET are unable to verify the digital signatures quickly enough as they have limited battery life as well as processing power. Moreover, if a malicious node floods messages with invalid signatures then verification can be very expensive.

3. Ad-hoc On-Demand Distance Vector Routing (AODV) protocol

3.1 Overview

Ad Hoc On-Demand Vector Routing (AODV) protocol (Perkins et al., 2003) is a reactive routing protocol for ad hoc and mobile networks, which maintains routes only among nodes, which need to communicate. The routing messages do not contain information about the whole route path, but only about the source and the destination. Therefore, routing messages do not have an increasing size. It uses destination sequence numbers to specify how fresh a route is (in relation to another), which is used to grant loop freedom. Whenever a node needs to send a packet to a destination in which it has no ‘fresh enough’ route (i.e., a valid route entry for the destination whose associated sequence number is at least as great as the ones contained in any RREQ that the node has received for that destination) it broadcasts a route request (RREQ) message to its neighbors. Each node, which receives the broadcast sets up a reverse route towards the originator of the RREQ, unless it has a ‘fresher’ one. When the intended destination (or an intermediate node that has a ‘fresh enough’ route to the destination) receives the RREQ, it replies by sending a Route Reply (RREP). It is important to note that the only mutable information in a RREQ and in a RREP is the hop count, which is being

monotonically increased at each hop. The RREP is uncast back to the originator of the RREQ. At each intermediate node, a route to the destination is set (again, unless the node has a 'fresher' route than the one specified in the RREP). In the case that the RREQ is replied to by an intermediate node (and if the RREQ had set this option), the intermediate node also sends a RREP to the destination. In this way, it can be granted that the route path is being set up bidirectionally. In the case that a node receives a new route (by a RREQ or by a RREP) and the node already has a route 'as fresh' as the received one, the shortest one will be updated.

4. Packet Drop Attack

A packet may be dropped under various reasons, which in turn can be grouped into the following categories,

1) Unsteadiness of the medium,

- A packet may be dropped due to contention in the medium
- A packet may be dropped due to congestion and corruption in the medium
- A packet may be dropped due to broken link

2) Genuineness of the node,

- A packet may be dropped due to overflow of the transmission queue
- A packet may be dropped due to lack of energy resources

3) Selfishness of the node,

- A packet may be dropped due to the selfishness of a node to save its resources

4) Maliciousness of the node,

- A packet may be dropped due to the malignant act of a malicious node

The unsteadiness of the medium generally causes errors in the packet, which forces the begin node to drop the packet even if the node aspires to forward it. On other hand, a genuine node with zero options may drop the packets when it runs out of its resources. Though a packet may be dropped in the similar manner by a selfish or a malicious node, they distinctly differ from the others because the packets are dropped intentionally. From the above examination, it is obvious that the intentional packet drop events have to be tackled, which we generalize as "Packet Drop Attack". Generally, there are two types of attackers: The type-1 attacker drops all the received packets. The type-2 attacker is smarter and drops only data packets and exchanges control packets normally. In this paper, we will investigate type-2 attackers (Abdalla et al., 2011).

5. Proposed Method

We investigate the attacks in which malicious node forward the control packets such as normal node, but it discards data packets when receives them. We also address the malicious nodes that drop control packets and send fictitious RRAPs to source node. We raise the security in the way that we distinguish invalid paths from valid paths and discard invalid paths and just send our data packets through valid path. Security mechanism is used both at the time of route discovery and route reply process. The proposed model of this paper investigates validity of intermediate node, which forward RREQ or RREP packets in each hop. At the time of route discovery process, each intermediate when a node receives RREQ or RREP packet, it will identify the node through the packet received. Intermediate node performs this operation by sending CM packet (a small data packet) towards the previous node and it waits for a reply. The previous node, which has forwarded the RREQ or RREP packet is required to acknowledge back to the intermediate node with a ACK packet to verify the validity of the path along which the data packets are transmitted as shown in Fig. 1.


```
1  Any intermediate node send CM packet to before node in path
2  Increment CM counter
3  If  receiver node is normal node  then
4      send ACK packet back to intermediate node
5  Else
6      drop CM packet and send no ACK packet to source
7  End if
8  If  CM counter >3 and intermediate node receive no ACK packet  then  discards RREQ or RREP
   packet
9  End if
10 If  CM counter <3 and intermediate node received no ACK packet  then
11    Send CM packet again
12   Increment CM counter
13 End if
14 If  intermediate node received ACK packet  then
15    Forward RREQ or RREP packet
16 End if
```

Fig. 1. (a)Validate of RREQ /RREP packets at the time of Route Discovery (b)validate algorithm

If the previous node i.e. the recipient node of the data packet is a normal node it sends reply (ACK packet) for intermediate node. However, if it is a malicious node it drops the data packet and sends no reply as shown in Fig. 2. If the ACK packet fails to reach back to the intermediate node, then the source node increases the number of times of sending CMs. The operations of validation repeats for three times and each time intermediate node waits for a reply. A normal node may be not able to send a reply because of ruined of connective link or its sources. In both cases received RREQ or RREP packet will be discarded and it is not processed because the method assumes that this packet probably has come from a malicious node, which looks to attracts all the packets towards itself by altering the routing information and then drops those packets.

Fig. 2. Attacker drops CM packet (data packet)

Each time that an origin node broadcasts a RREQ packet in network for finding a route towards a distinguished destination it may receive several RREP from various nodes but the origin node must choose only the path for sending the data, which passes from credible nodes so we start this security mechanism for the selection of the creditable RREP. As soon as an origin node receives a RREP packet, it sends a CM packet (a small data packet) to the sender of the RREP (destination) through the first node where the origin node has received RREP from and waits for a reply. If receiver node of data packet is a normal node, it searches its routing table to find the sender of RREP (destination) and next node towards the destination and then sends information about next node towards the destination(NNTD) for origin node as a reply(ACK packet). However, if receiver node of data packet is a malicious node, it discards the packet and sends no reply. Each time origin node sends CM packet to destination through NNTD the operations will be continued till the receiver node will be a malicious node, which drops the data packet and stops the operations as shown in Fig. 3. Alternatively, it will be at the destination that if it is not a malicious node and it sends intended reply for origin node. In case it is malicious node, it drops the data packet, so the origin node itself decides that path is creditable or not. Discarding packets have come from malicious node(s) enable the source to select another trusted path to their destination.


```
1   Source node send CM packet to destination
2   If   receiver node = attacker  then
3      drop CM packet and send no ACK packet to source
4   Else
5      If  receiver node=destination then
6         Send ACK packet to source
7      Else
8         send ACK packet to source with information about next node toward destination(NNTD)
9        forward CM packet
10     End if
11  End if
12  If  source node received ACK packet   then
13       Waits for ACK packet from NNTD
14  Else
15       attacker is detected and source discard RREP packet
16  End if
17  If  source received ACK packet came from destination  then
18  no attacker is detected and transmit data through the RREP packet
19  End if
```

Fig. 3. (a) Validate of RREP packet at the time of Route reply (b)Validate Algorithm

In the proposed security mechanism, we do not isolate malicious node from the network and discard only RREQ and RREP packets which have come from malicious node (the paths that pass from malicious nodes) because the security in sending data is in priority for us.

6. Simulation and comparison

Fig. 4 and Fig. 5 present the proposed CPN model for modified AODV protocol based on the implementation of CPN Tools to run the simulation.

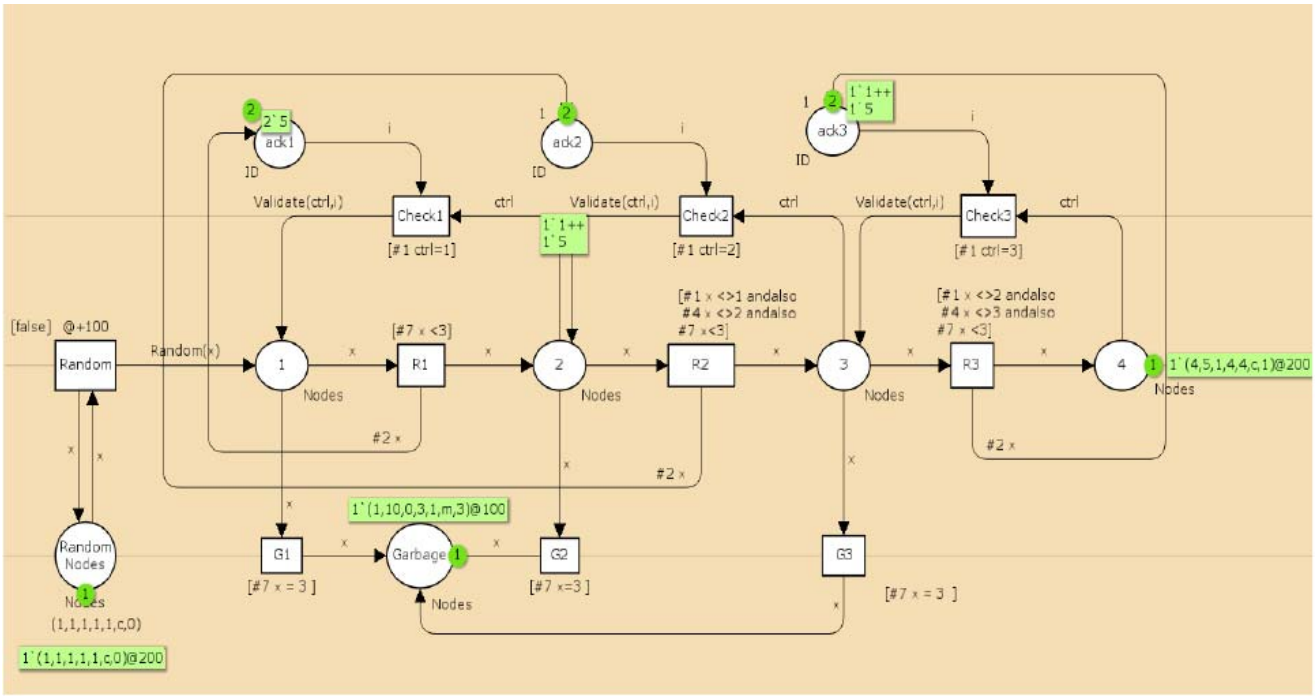

Fig. 4. CPN model for validate process at the time of Route Discovery

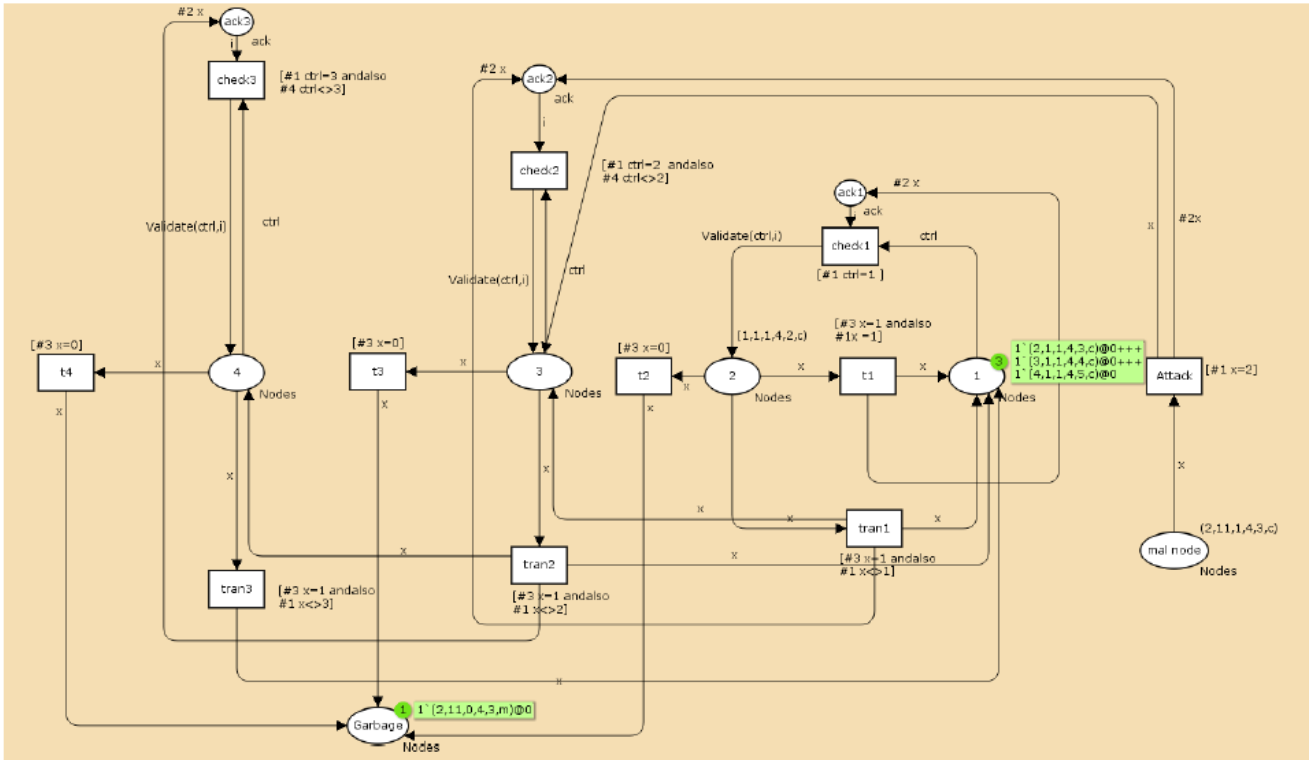

Fig. 5. CPN model for validate process at the time of Route Reply

Table 1 shows the number of packets which broadcasted in network .Table 2 shows the number of discarded packets (discarded paths) in modified protocol where the variable parameter is time, showing that modified AODV protocol can detect the invalid packets that come from malicious nodes.

Table 1
Broadcasted Valid/Invalid Packets (RREQ /RREP)

Total time	2800	5800	8600	11300	14300	17200
Invalid packets	15	32	46	62	78	93
Valid packets	13	24	40	51	63	78

Table 2
Discarded Packets (RREQ /RREP)

Total time	2800	5800	8600	11300	14300	17200
Invalid Packets	15	32	46	62	78	93
Discarded Packets	16	35	49	66	83	100

Table 3
Packets distinguished as valid ones (RREQ /RREP)

Total time	2800	5800	8600	11300	14300	17200
Typical AODV Protocol	28	56	86	113	141	171
Modified AODV Protocol	12	21	37	47	58	71

Table 3 shows the number of the packets, which are distinguished as valid packets (valid paths for transmit data). The result of simulation shows that from the different RREQ and RREP packets that are distributed in network, the valid packets only will be forwarded and all of invalid packets will be discarded. Also, by assessment of the receiver RREPs by origin node, only the safe paths for sending of the data will be chosen and RREPs that pass from a malicious node or a normal node with a broken link or ruined sources will be discarded. Therefore, safe paths for sending of the data is chosen all the time and in this way the security to find paths and transmit of data both at the time of route discovery and reception route reply will be raised.

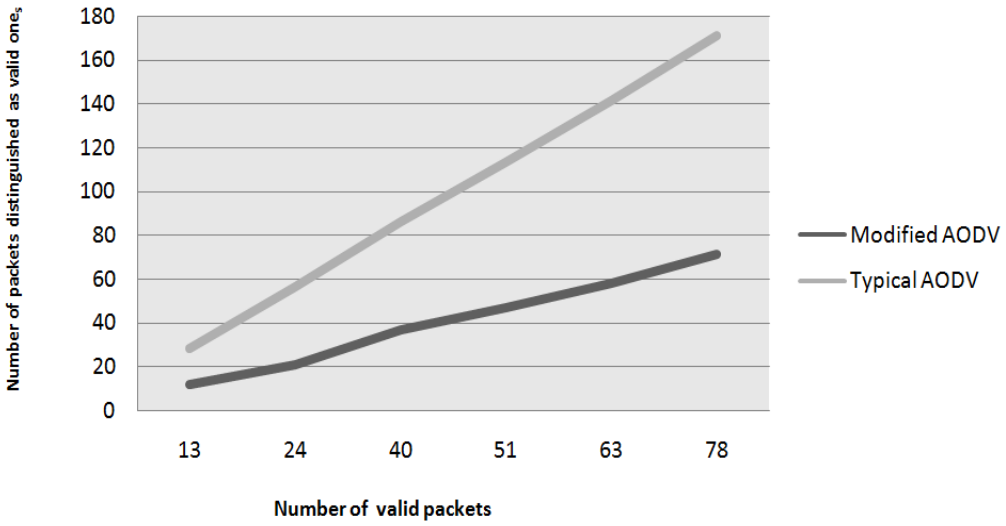

Fig. 6. improvement rate recognition of valid packets

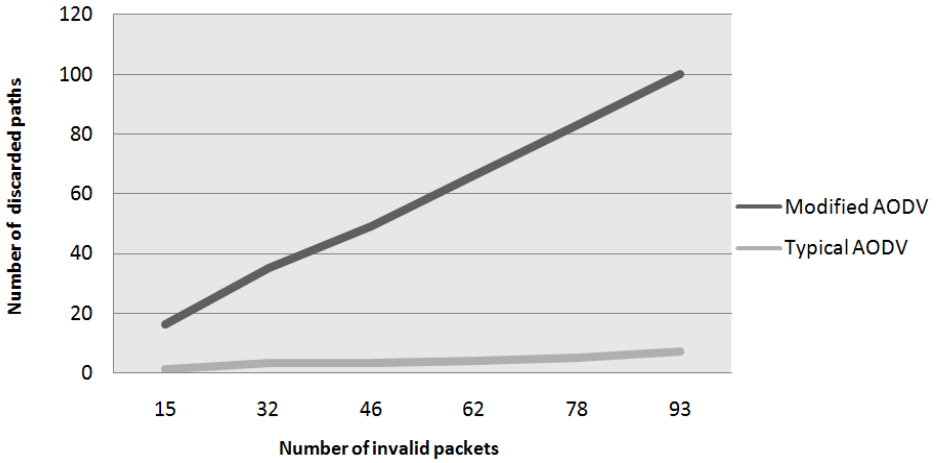

Fig.7. Performance improvement at ignore invalid paths

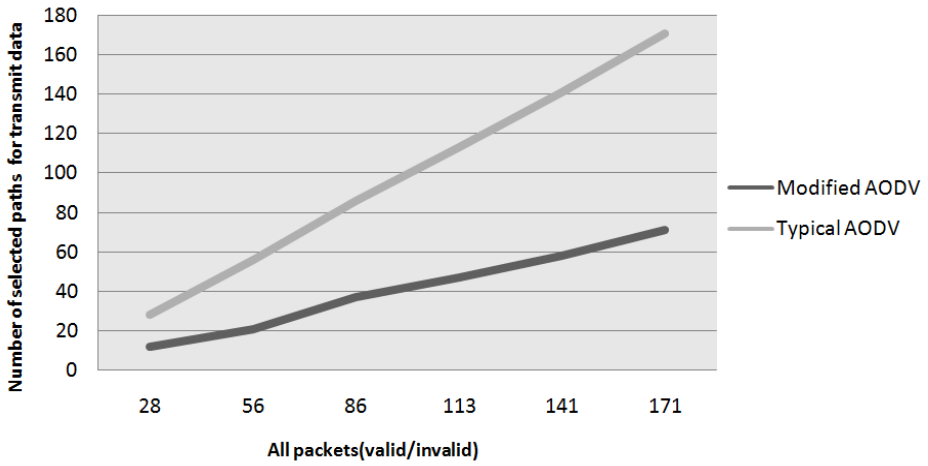

Fig. 8. Performance improvement at select of valid paths for transfer data

Fig. 6 shows the improvement rate recognition of valid packets. Fig. 7 and Fig. 8 show the improvement rate routing security when comparing modified AODV with Typical AODV, indicating that improvement become more significant when number of invalid paths increases by attackers.

7. Conclusions and future works

We have presented a method based on End-to-End connection for securing the AODV protocol. Our method can detect many types of malicious node(s) that drop packet through the path between the source and the destination. The collaboration of a group of nodes is used to make accurate decisions. Discarding packets have come from malicious node(s) enables the source to select another trusted path to its destination. We achieved better performance results when action was taken to detect malicious nodes by validation operations.

The simulation results showed that our method is able to detect any number of attackers and fictitious packets.

Our future work will be focused on how to apply the proposed IDS on other MANET routing protocols methods.

Acknowledgment

The authors would like to thank the annonymous referees for their constructive comments on earlier version of this paper.

References

Abdalla, A.M., & Saroit, I.A., & Kotb, A., & Afsari, A.H.(2011). Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol. *Procedia Computer Science*, 115–12.

Haas, Z. J., Pearlman, M. R., & Samar, P. (2002). The inter zone routing protocol (IERP) for ad hoc networks. INTERNET DRAFT, MANET working group.

Hu, Y., Johnson, D.B., & Perrig, A. (2002b). Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, 3-13.

Hu, Y.C., Johnson, D.B., & Perrig, A. (2002a). Ariadne: A secure on-demand routing protocol for ad hoc networks. *Proceeding of 8th Annual International Conference on Mobile Computing and Networking*, ACM Press, 12-23.

Hu, Y.C., & Perrig, A. (2004). A survey of secure wireless ad hoc routing. *IEEE Security and Privacy*, 2(3), 28-39.

Kravets, R., Yi, S., & Naldurg, P. (2001). A security-aware routing protocol for wireless ad hoc networks. *Proceedings of ACM MOBIHOC*, 299-302.

Murthy, C.S.R., & Manoj, B. (2004). *Ad hoc Wireless Networks: Architectures and Protocols*. Prentice Hall.

Johnson, D.B., & Maltz, D.A. (1996). The dynamic source routing protocol in ad hoc wireless networks. *Mobile Computing, Kluwer Academic Publishers*, 353, 153-181.

Johnson, D. B. et al. (2003). The dynamic source routing protocol for mobile adhoc networks (DSR). INTERNET DRAFT, MANET working group.

Papadimitratos, P., & Haas, Z. J. (2002). Secure routing for mobile ad hoc networks. *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*.

Perkins, C.E., & Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. *Proceeding of ACM SIG-COMM*. 24, 234-244.

Perkins, C.E., & Royer, E.M. (1999). Ad hoc on-demand distance vector (aodv) routing. *Proceeding of IEEE Workshop on Mobile Computing System and Applications*. 90-100.

Perkins, C. E, Belding-Royer, E. M, & Das, S. R. (2003). Ad hoc on-demand distance vector (AODV) routing. *Internet Request for Comments*, RFC3561.

Perrig, A., Canetti, R., Song, D., & Tygar, D. (2001). Efficient and secure source authentication for multicast. *Network and Distributed System Security Symposium* (NDSS01).

Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C., & Royer, E.M.B. (2002). A secure routing protocol for ad hoc networks. *Proceedings of IEEE ICNP*, 78-87.

Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks: challenges and solutions. *Wireless Communications*, IEEE, 11, 38-47.

Zapata, M.G., & Asokan, N. (2003). Securing ad hoc routing protocols. *Proceeding of ACM Workshop on Wireless Security (WiSe)*, ACM Press, 1-10.