Australian Journal of Basic and Applied Sciences, 5(10): 1137-1145, 2011
ISSN 1991-8178

Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol

[1]Maha Abdelhaq, [2]Sami Serhan, [3]Raed Alsaqour and [4]Anton Satria

[1,3,4]School of Computer Science, Faculty of Information Science and Technology, University Kebangsaan Malaysia, 43600, Bangi, Selangor, Malaysia.
[2]Department of Computer Science, King Abdulla II School for Information Technology, the University of Jordan, Amman, 11942, Jordan.

Abstract: Mobile Adhoc Network (MANET) is a group of wireless nodes that are distributed without relying on any standing network infrastructure. MANET routing protocols were designed to accommodate the properties of a self-organized environment without protection against any inside or outside network attacks. In this paper, we propose a Local Intrusion Detection Security Routing (LIDSR) mechanism to detect Black Hole Attack (BHA) over the Ad hoc On Demand Distance Vector (AODV) MANET routing protocol. In the LIDSR mechanism, the intrusion detection is performed locally using the previous node from the attacker node instead of performing the intrusion detection via the source node as in the Source Intrusion Detection Security Routing (SIDSR) mechanism. By performing the LIDSRmechanism, the security mechanism overhead would be decreased. Simulation results using the GloMoSim simulator show that the improvement ratio of the throughput gained by the LIDSR mechanism is 2.1%. The overall improvement reduction in the end-to-end delay and routing overhead are 14% and 5.5% respectively.

Key words: Mobile Adhoc network, Ad hoc On Demand Distance Vector, Local Intrusion DetectionSecurity Routing, Source Intrusion Detection Security Routing, Black Hole Attack.

INTRODUCTION

MANET is described as a self-configurable and rapidly deployable wireless network. The absence of centralised management makes each wireless node in MANET perform routing to its neighbours in order to maintain the connectivity and the network stability. Therefore, the routing protocol must ensure both connectivity and security to achieve network stability. Unfortunately, the widely used routing protocols which perform their algorithms over MANET routing protocols assume that all the nodes are trusted. If the routing information has been fabricated and the direction of the route has been modified, then, the attacker would perform different types of attacks such as BHA. As a result, the network will be paralysed. Furthermore, MANET properties such as mobility, frequent topology changes, limited power, decentralization, and openness make it vulnerable to different types of attacks.

Several efforts by(Al-Shurman *et al.,* 2004; Deng *et al.,* 2002; Kurosawa *et al.,* 2007; Lee *et al.,* 2002; Marti *et al.,* 2005; Gerhards-Padilla *et al.,* 2007; Wang *et al.,* 2008; Wang *et al.,* 2003) have been made to extend different routing protocols with security algorithms and functions. Adding more security algorithms and functions on the routing algorithm means adding more processing overhead and causing more network performance degradation.

The LIDSRmechanism is an improvement of the SIDSR mechanism over AODV MANET routing protocol in(Deng *et al.,* 2002). To the best of our knowledge,no one had improved on the SIDSR mechanism in (Deng *et al.,* 2002).

Both SIDSR and LIDSR mechanismsdetect BHA over MANET to prevent the threat of fabricating AODV routing information by BHA. However,the LIDSR mechanism makes AODV routing protocol effective in both security and network performance measurements. The main enhancement in the LIDSRmechanism over the SIDSR mechanism is the use oflocal intrusion detection mechanismthat are performed on the previous node of the attacker node on the route, instead of overloading the network with extra routes to perform the intrusion detection by the source node itself as in TheSIDSR mechanism(Deng *et al.,* 2002).

MATERIALS AND METHODS

AODV Routing Protocol:

The AODV routing protocol (Perkins and Royer, 1999) is the underlying routing protocol used in this paper. In abstract, AODV is a reactive self-starting, and large scale routing protocol. The AODV routing

Corresponding Author: Maha Abdelhaq, School of Computer Science, Faculty of Information Science and Technology, University Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia.

protocol has been extensively studied and developed over many years, and has proven its robustness and benefits. The main advantages of this protocol are, firstly, the connection setup delay with the destination is lower when comparing with other MANET routing protocols. Secondly, AODV avoids the congested paths in comparison with the other MANET routing protocols. Thirdly, AODV supports both unicast and multicast communications. Fourthly, it can cope with the rapid MANET topological reconfigurations that may affect the other routing protocols (Xu, 2009).

In AODV, each node maintains a specific sequence number that increases monotonically each time the node sends either Route REQuest (RREQ), or Route REPly(RREP) control packet. Thesequence number ensures that a fresh enough route is selected whenever a route discovery process is performed. Fresh enough means the highest destination sequence number. If the source node has received more than one RREP packet, it will choose the one with the highest destination sequence number. If the source node has received two RREP packets with the same sequence number, it will choose the one with the smallest hop count (Perkins and Royer, 2003). In AODV routing mechanism, the AODV protocol first broadcasts RREQ packet in order to discover the paths required by a source node to destination node as shown in Figure 1. In response, once the RREQ packet reaches the destination or an intermediate node (any node on the route between the source and destination node) with a fresh enough route to destination node, the destination or intermediate node responds by unicasting a route reply (RREP) packet as shown in Figure 2. Once the source node receives the RREP packet, it starts sending its data packets through the route enclosed within the RREP packet.

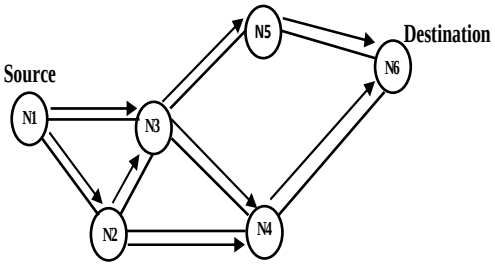

Fig. 1: Propagation of route request (RREQ).

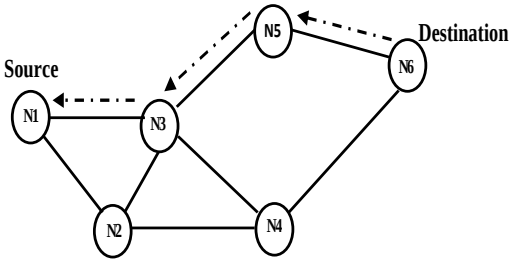

Fig. 2: The path of a routing reply (RREP).

Black Hole Attack (BHA):

MANET attacks are categorized according to their emission into two main categories: passive attacks, and active attacks (Wang *et al.*, 2008; Cayirci and Rong, 2009). In passive attacks, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information, e.g. an eavesdropping attack. In active attacks, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by causing routing disruption, network resource exhaustion, and node breaking. One of the dangerous active attacks is the BHA(Xu, 2009).

BHA in MANETs (Wang *et al.*, 2003) is a serious security problem to be solved, in which the attacker injects false routing information in the received routing packets in order to advertise itself as having the best route to the destination. If the attacker in BHA succeeds in gaining the route, it can intercept the coming and perform eavesdropping, denial-of-service, or man-in-the-middle attacks (Wang *et al.*, 2008). For example, in Figure 3, node N1 wants to send data packets to node N6 and initiates the route discovery process. We assume node N2 to be an attacker node with no fresh enough route information to the destination node N6. However, node N2 claims directly that it has the route to the destination whenever it receives RREQ packet from node N1 and sends the RREP packet response directly to source node N1. In this case, the node N2 forms a black hole in the network.Node N2can easily misroute the network traffic to itself and cause an attack to the network.

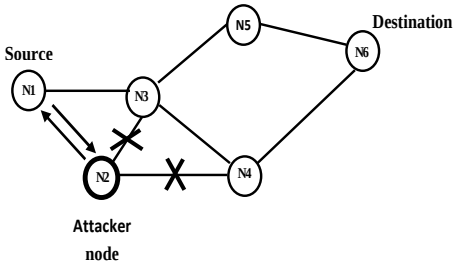

Fig. 3: The black hole attack.

In order to fake AODV using BHA, the attacker may use one of the two methods:

- Sending a RREP packet towards the source node with a high enough sequence number.
- Sending a RREP packet to the source node with a small enough hop count number.

In most cases, the BHA attacker gains the route if the routing protocol does not protect itself. This is because the BHA attacker does not follow the routing protocol rules by responding directly to the source node. Hence,the BHA attacker replies quicker than the real destination node or any other nodes in the network.

Related Works:

On the intrusion side, the attacker must realize the routing protocol mechanism to fake the network. Furthermore, while on the security side, the researcher must understand the routing protocol mechanism to protect the network as well. This means that the attacker applies the same type of attack on different protocols using different ways; and hence the researchers use different types of intrusion detection mechanisms on different routing protocols to defend against the same attack and/or different types of attacks.

In (Lee *et al.*, 2002), the authors applied their intrusion detection method over the Dynamic Source Routing (DSR) protocol. The method requires the intermediate node to send the route Confirmation REQuest (CREQ) packet to the next hop node. When the next hop node receives the CREQ packet, it checks its cache for a route to the destination. If it has a route, it sends the route Confirmation REPly (CREP) packet to the source node with its route information. The source judges the validity of the route in the RREP packet previously received by comparing it with the one in the CREP packet.

In (Wang *et al.*, 2003), the watchdog mechanism was proposed to be implemented on top of the DSR protocol. Watchdog verifies that when a node forwards the data packet, the next node in the path also forwards the packet; otherwise the next node is misbehaving. In (Kurosawa *et al.*, 2007), the authors perform the detection process at each node. When sending a RREQ packet, each node records the destination Internet Protocol (IP) address and the destination sequence number in its list. When a RREP packet is received, the node looks over the list to see if there is a same destination IP address. If it does exist, the difference of the destination sequence number is calculated. The average of this difference is finally calculated for each time and the average of each time interval is then calculated. If it is less than or equal to a certain threshold, the node is considered as normal. Otherwise, it is considered as a malicious node and the alarm is broadcasted.

In (Al-Shurman *et al.*, 2004), the source node verifies the validity of the route caused by the node that initiates the RREP packet by finding more than one route to the destination. It waits for the RREP packets to arrive from more than two nodes. When the source node receives the RREP packets and find the routes to the destination node through shared hops, the source node can recognize the safe route to the destination. However, waiting more than two RREP packets to arrive to source node before the source node starts sending the data packets causes high data packet routing delay (Al-Shurman *et al.*, 2004).

In (Gerhards-Padilla *et al.*, 2007), the authors perform the detection operation over tactical MANET using the Optimized Link State Routing (OLSR) protocol. The intrusion detection system draws a graph for the entire network at each certain time interval. So, the truth about the number of neighbours for each node, which is the main factor for each node to win the route, appears in the graph. When any node sends a hello message that contains its information, the system compares the number of neighbours the node claims that it has with the truthful number in the system's graph. If the difference exceeds a certain threshold, the node is considered as a malicious node and the alarm message is broadcasted. Otherwise, the node is considered as normal and the route is accepted.

In (Xu, 2009), the author proposed an intrusion detection mechanism using both secure routing protocol and hardware support for reliable and efficient intrusion detection techniques. However, using hardware will be a further input into the cost of the techniques' implementation.

In (Jinsub *et al.*, 2010), the authors proposed a conceptual model for a tunnel localization system that combines timing-based algorithms for localizing in-band wormhole tunnels in MANETs for detecting the presence of a wormhole attack. However, the proposed conceptual model needs to be evaluated with a simulation study to show the effectiveness and performance of the model within the MANET network data.

Source Intrusion Detection Security Routing (SIDSR) mechanism over AODV:

In (Deng *et al.*, 2002), the authors proposed a SIDSRmechanism that detects the BHA attacker when an attacker node sends the RREP packet. In the SIDSR mechanism (Figure 4), when the source node (node N1) receives a RREP packet from the suspected attacker node (node N2), the source node sends a Further Route REQuest (FRREQ) packet to the next hop (node N4) through a new route (N1, N3, N4) to verify that node N4 has a route to the node N2,whichsent back the RREP packet and announcethat ithas a route to the destination (node N6). As soon as the next hop (node N4) receives the FRREQ packet, it sends a Further Route Reply (FRREP) packet to the source node (Figure 5). The source node (node N1) checks the FRREP Packet information and acts according to the following rules:

1. If the next node (node N4) has routes to the destination node (node N6) and intermediate node (node N2), the source node assumes that node N2 is trusted node and itestablishes the route received from node N2.

2. If the next hop node (N4) has a route to the destination node (Node N6) but does not have a route to the intermediate node (node N2), the source node assumes that N2 is an attacker node. Then, the source node initiates the route using the new route to the next hop (node N4) and broadcasts an alarm message to isolate the intermediate attacker node (node N2).
3. If the next hop (node N4) does not have routes to the intermediate node (node N2) and the destination node (node N6), the source node will initiate a new route request.

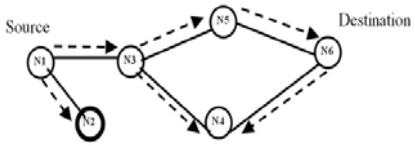

Fig. 4: FRREQpacket. N2 attacker node.

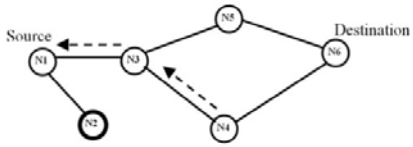

Fig. 5:FRREP packet, N2 attacker node.

The SIDSR mechanism is efficient in detecting a BHA attacker, but there is more than one drawback. Firstly, re-sending a FRREQ packet from the source node towards the next hop and waiting for the FRREP packet from the next hop means increasing routing overhead packets between the source and the next hop node, especially when this mechanism is applied on a large-scale MANETand the distance between the source node and the attacker node is long. Secondly, if the distance between the source node and the attacker node is long, the delay in the discovery period of the routewill be high, which causes an overall network performance degradation.

RESULTS AND DISCUSSION

The Proposed Local Intrusion Detection Security Routing (LIDSR) Mechanism:

In order to mitigate the drawbacksin the SIDSR mechanismproposed in (Deng *et al.*, 2002),we propose a newmechanism called the Local Intrusion Detection Security Routing (LIDSR) mechanism. The mechanism is shown in Figure 6 and its algorithm pseudo-codes are given in Algorithm 1 and Algorithm 2. LIDSR mechanism allowsthe detection of the attacker to be locally done, which means that when the suspected attacker node (node N5) unicasts the RREP towards the source node (node N1) the previous node (node N4)to the attacker node performs the process of detection, and not the source node (node N1) as in SIDSR mechanism. First, the previous node (node N4) buffers the RREP packet. Second, it uses a new route to the next node (node N6) and sends a FRREQ packet to it. When the previous node (Node N4) receives the FRREP packet from the next node (Node N6), it extracts the information from the FRREP packet and behaves according to following rules:

1. If the next node (N6) has a route to the attacker node (N5) and the destination node (N7). In this case, N4 assumes that N5 is trusted node and it discards the FRREP packet, then unicasts the RREP packet which received from N5 to the source node (N1).
2. If the next node (N6) has no route to the destination node (N7) or the attacker node (N5) or both of them (N5 and N7), the previous node (N4) discards the buffered RREP and the FRREP as well, at the same time broadcasting the alarm message to announcethat there is no secure enough route available to the destination node (N7).

The last case includes another scenario, such as the case in which the previous node (N4) does not receive any FRREP packet from the next node (N6). Here,N6 will discard the RREP packet and inform the source node to initiatea new route discoveryprocess to the destination.

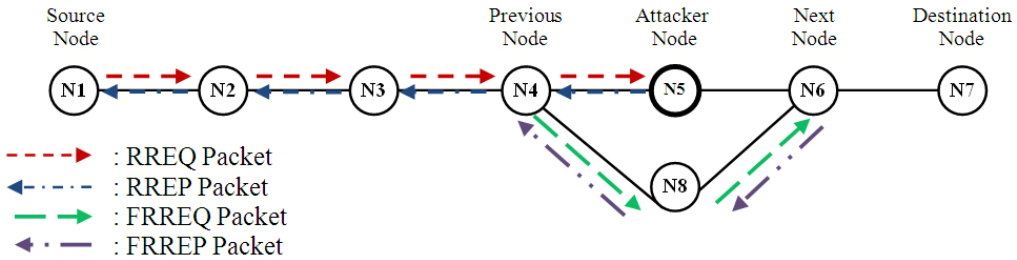

Fig. 6: Proposed Local Intrusion Detection Security Routing (LIDSR) Mechanism

Algorithm 1: *Pseudo-code for LIDSR mechanism. Source node.*

Broadcasts RREQ packet
If RREP packet received**then**
Sends data packets
Otherwise
Reinitiates a new RREQ packet
End If

Algorithm 2: *Pseudo-code for LIDSR mechanism. Previous node.*

If RREP packet received from suspected attacker node **then**
Buffers the RREP packet
Initiates a route to next node
Sends FRREQ packet to next node
If FRREP packet received **then**
Extract FRREP packet information
If next node has a route to (destination &attacker nodes)**then**
Discards FRREP packet
Unicasts RREP to source node
Otherwise
Discards both RREP and FRREP packets
Broadcasts alarm message
End If
End If
End If

Simulation Results and Evaluation:

To simulate the performance of the LIDSR mechanism, we use the GloMoSim 2.03 network simulator (Lokesh *et al.,* 1999). GloMoSim is network protocol simulation software that simulates wireless and wired network systems. Our choice of GloMoSim is based on its ability to run under the Windows environment and its use of a layers approach as is currently used by most network systems.

Table 1 shows the simulation parameters that are used along with all of our simulation experiments.

Table 1: Simulation parameters.

Parameter	Value
MANET routing protocol	AODV
Simulation time	15 minutes
Connections	10 CBR
Node placement	random
Mobility speed	0-10 m/s
MAC protocol	802.11
Data packet size	512 bytes

This study adopted the following performance metrics to evaluate the performance of the SIDSRand the LIDSR mechanisms.

- ***Network Throughput:*** Throughput is the number of data packets delivered from source node to destination node per unit of time.
- ***Routing Overhead:*** The routing overhead is measured as the average number of routing control packets (RREQ, RREP, FRREQ, and FRREP packets) exchange by all the nodes in the network during the AODV routing process. This metric affects the robustness of the network in terms of nodes' battery power consumption, and bandwidth utilization.
- ***Average end-to-end Delay:*** The end-to-end delay is the average time elapsed for all data packets delivered successfully from the source node to the destination node.

Varying the Number of Nodes:

In order to study the effect of the number of nodes in SIDSR and LIDSRmechanisms over the AODV routing protocol, the combination of 20, 40, 60, 80, and 100 network nodes are simulated using 50×1000 terrain dimensions and 376.782 transmission range, keeping all of the other simulation parameters in Table 1 as constants.

Figure 7, Figure 8, and Figure 9 compare between the network throughput, average end-to-end delay, and routing overhead respectively in both SIDSR and LIDSRmechanisms while varying the number of nodes. It is

clear from the figures that the LIDSR mechanism outperforms the SIDSR mechanism. This is because the LIDSR mechanism uses local intrusion detection compared with theSIDSR mechanism that uses source intrusion detection. The LIDSR mechanism reduces routing information overhead (RREQ, RREP, FRREQ, and FRREP packets) that results in a less congested network and less utilized bandwidth which decreases the dropping of data packets and an increase in network throughput with a decrease in both end-to-end delay and routing overhead. According to this experiment, the improvement ratio of throughput, average, end-to-end delay, and routing overhead gained by the LID security routing are1.2%, 10.3%, and 3.4% respectively.

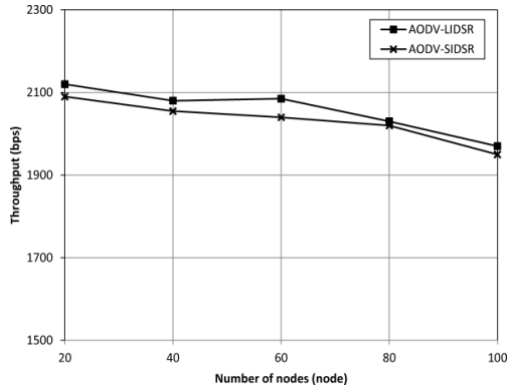

Fig. 7: Throughput vs. Number of nodes.

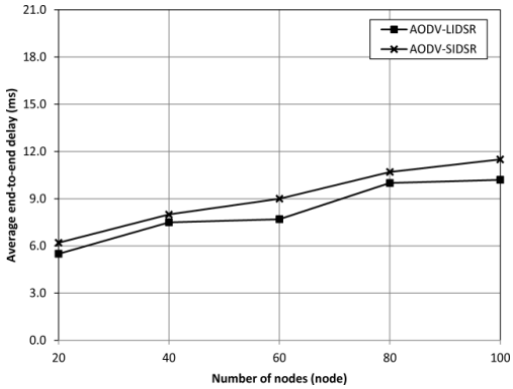

Fig. 8: Average end-to-end delay vs. Number of nodes.

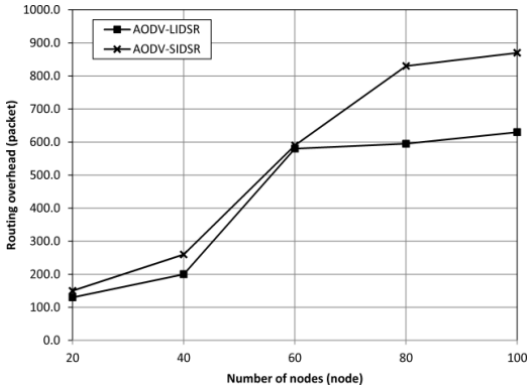

Fig. 9: Routing overhead vs. Number of nodes.

Varying the Network Size:

In this experiment, a combination of network sizes of 100m×500m, 100m×1000m, 100m×1500m, 100m×2000m, and 100m×2500m are simulated using 100 nodes and 376.782 transmission range, keeping all other simulation parameters as mentioned in Table 1.

Figure 10, Figure 11, and Figure 12 compare between the network throughput, end-to-end delay, and routing overhead of The LIDSR and SIDSR mechanisms while varying the network size. In both mechanisms,

as the network size increases the throughput decreases while the average end-to-end delay and the routing overhead increase. This is due to the fact that an increment in the network size increases the number of routing hops the data packets needs to use in order to reach the intended destination and this increases the route length to destination, resulting in an increase of breaking links(Shanudin *et al.,* 2005), collisions, and hence data packets dropping. Figure 10, Figure 11, and Figure 12 state clearly the better performance of the LIDSR mechanism over the SIDSRmechanism. The local LIDSR mechanism in intrusion detection reduces the route length and the number of routing hops from source to destination by relaying the intrusion detection to be performed by the attacker's previous node rather than source node as currently used by the SIDSR mechanism. According to this experiment, the improvement ratio of throughput, end-to-end delay, and routing overhead gained by the LID security routing protocol are 2.7%, 17.8%, and 5.4% respectively.

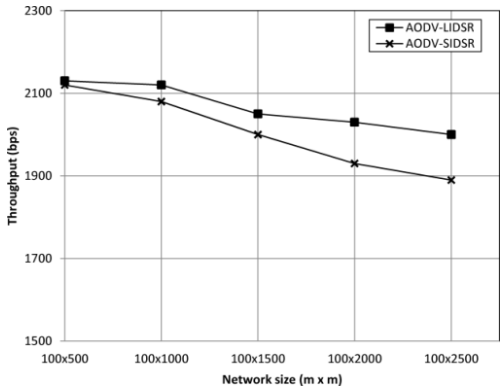

Fig. 10: Throughput vs. Network size.

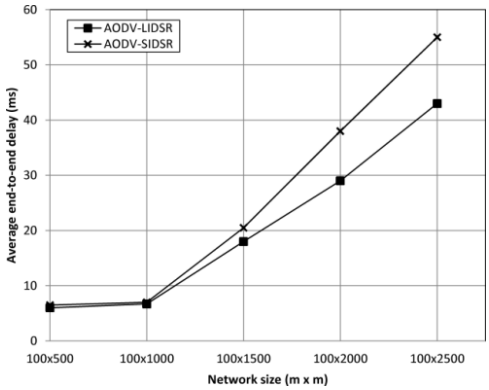

Fig. 11: Average end-to-end delay vs. Network size.

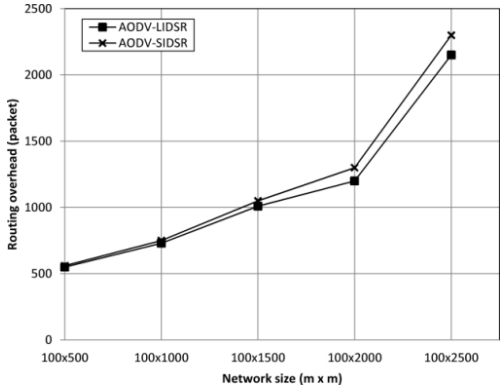

Fig. 12: Routing overhead vs. Network size

Varying the Transmission Range:

In order to study the effect of transmission range in the SIDSRand LIDSRmechanisms, the combination of 200, 300, 400, 500, and 600 m transmission ranges are simulated, using 100 nodes and 50×1000m terrain dimensions, while maintaining all other simulation parameters as mentioned in Table 1. Figure 13, Figure 14, and Figure 15 compare between the network throughput, end-to-end delay, and routing overhead of the SIDSR and LIDSR mechanisms while varying the transmission range. In both mechanisms, as the transmission range increases, the throughput increases while the average end-to-end delay and the routing overhead decrease. Hence, the transmission range does not express the movement of nodes, but it affects the mobility of nodes from the view of connectivity between the nodes. In the AODV routing protocol, increasing the node's transmission range reduces the number of routing nodes (hops) needed to reach the intended destination and enhances overall network connectivity. In addition, it will reduce the chance of nodes breaking the link with its neighbours while the nodes are moving and reduces the data packet dropping(Saqour *et al.*, 2007).

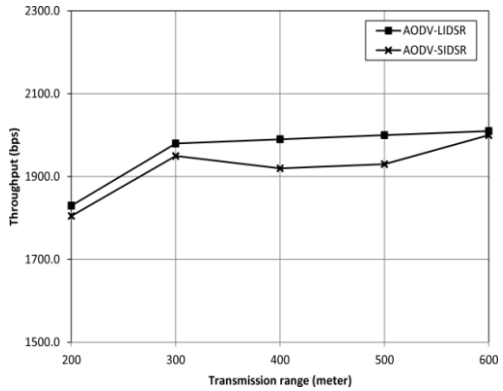

Fig. 13: *Throughput vs. Transmission range.*

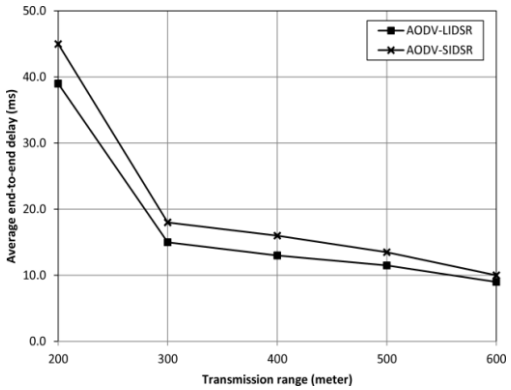

Fig. 14: *Average end-to-end delay vs. Transmission range*

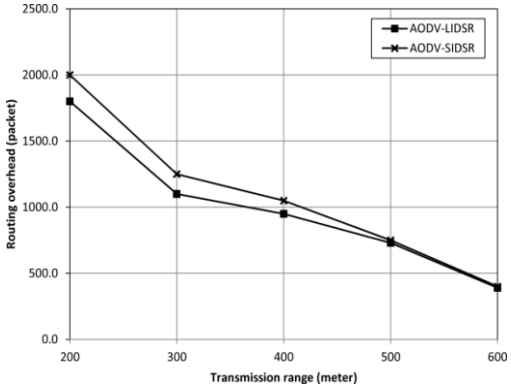

Fig. 15: *Routing overhead vs. Transmission range*

It is clear from Figure 13, Figure 14, and Figure 15 that the LIDSRmechanism outperforms the SIDmechanism. The LIDSR mechanismin intrusion detection reduces the route length and number of routing nodes (hops), from source to destination by relaying the intrusion detection to be performed by the attacker's previous node rather than the source node as currently used by the SIDSRmechanism. According to this experiment, the improvement ratio of throughput, end-to-end delay, and routing overhead gained by the LID-RS protocol are 2.4%, 14.1%, and 7.7% respectively.

Conclusion:

This paper proposesthe LIDSRmechanismover the AODV MANET routing protocol. The LIDSR mechanism performs its intrusion detection mechanism locally in the previous node of the attacker node in contrast with the SIDSR mechanism, which performs its intrusion detection mechanism by means of the source node. End-to-end delay, routing overhead, and throughput of the SIDSR and LIDSR mechanisms were compared by varying the number of nodes, network size, and the transmission range. The improvement ratio of increasing throughput, decreasing average end-to-end delay, and decreasing routing overhead are 2.1%, 14%, and 5.5% respectively. The proposed LIDSRmechanism takes into consideration the fact that the previous node of the attacker node is trusted node and there is no group attack in the network.

As a piece of future work, we will perform more enhanced intrusion detection mechanismthat could perfectly detect a group attack if applied on the MANET. Subsequently, the new enhanced security mechanism will be evaluated using the same performance metrics and simulation parameters.

REFERENCES

Al-Shurman, M., S. Yoo and P. Seungjin, 2004. Black hole attack in mobile ad hoc networks.In ACM 42nd southeast conference (ACMSE'04), pp: 96-97.

Cayirci, E. and C. Rong, 2009. Security in wireless ad hoc and sensor networks.United Kingdom; WILEY.

Deng, H., W. Li and D. Agrawal, 2002. Routing security in wireless ad hoc networks. IEEE communications magazine, 40(10): 70-75.

Gerhards-Padilla, E., N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle, 2007. Detecting black hole attacks in tactical MANETs using topology graphs. In the 32nd IEEE conference on local computer networks, pp: 1043-1052.

Jinsub, K., S. Dan, H. Rommie, K.T. Roshan and T. Lang, 2010. Timing-based localization of in-band wormhole tunnels in MANETs. Proceedings of the third ACM conference on Wireless network security, pp: 1-12.

Kurosawa, S., H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto, 2007. Detecting black hole attack on AODV-based mobile ad hoc networks by dynamic learning method.International journal of network security, 5(3): 338-346.

Lee, S., B. Han and M. Shin, 2002. Robust routing in wireless ad hoc networks.Proceedings of international conference onparallel processing workshops, pp: 73-78.

Lokesh, B., T. Mineo, A. Rajat, T. Ken, B. Rajive and G. Mario, 1999. GloMoSim: A Scalable Network Simulation Environment. Technical Report 990027, University of California.

Marti, S., K. Lai and M. Baker, 2005. Mitigating routing misbehavior in mobile ad hoc networks.Proceedings ofthe 6th annual international conference on mobile computing and networking, Boston, USA, ACM press, pp: 255-265.

Perkins, C.E. and E.M. Royer, 1999. Ad hoc On-demand distance vector routing.Proceedings of the 2nd IEEE workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA, pp: 90-100.

Perkins, C.E., E.M. Royer, 2003. Ad hoc on-demand distance vector routing. IETF MANET Internet Draft.

Saqour, R., M. Shanudin and M. Ismail, 2007. Prediction schemes to enhance the routing process in geographical GPSR ad hoc Protocol. Mobile information systems, 3(3): 203-220.

Shanudin, M., M. Ismail and R. Saqour, 2005. Impact of mobility metrics on geographical greedy ad hoc network routing protocol and improvement using angular prediction model. Proceedings of the IEEE malaysia international conference on communications (MICC) and the IEEE international conference on networks (ICON), pp: 262-267.

Wang, D., M. Hu and H. Zhi, 2008. A survey of secure routing in ad hoc networks.Proceedings of the IEEE 9th international conference on web age information management, pp: 482-486.

Wang, W., Y. Lu and B. Bhargava, 2003. On vulnerability and protection of ad hoc on-demand distance vector protocol. The 10th international conference on telecommunications 2003(ICT2003), pp: 375-382.

Xu, S., 2009. Integrated prevention and detection of byzantine attacks in mobile ad hoc networks. PhD thesis, The University of Texas at San Antonio.