Academic Science

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 3, Issue 1
April 2014

An implementation of security policy by using ID in Adhoc routing for mobile network

Naincy Juneja
(M.TECH C.S.E)
IFTM University,
Moradabad, India
naincy.juneja@gmail.com

Abhishek Mishra
(Assistant.Professor in C.S.E)
IFTM University,
Moradabad, India
abhimishra2@gmail.com

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 Tropical Intrusion Detection (TID) security policy to detect Packet Drop Attack (PDA) over the Ad hoc On Demand Distance Vector (AODV) MANET routing protocol. In the TID security policy, 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 Root Intrusion Detection Security Policy (RID) mechanism. By performing the TID security policy, the security mechanism overhead would be decreased. Simulation results using the GloMoSim simulator show that the improvement ratio of the throughput gained by the TID mechanism is 2.1%. The overall improvement reduction in the end-to-end delay and routing overhead are 14% and 5.5% respectively.

Keywords
MANET, AODV ,Ad Hoc Network , TID security policy, Packet drop attack

INTRODUCTION
Wireless technology allows users to access information and services electronically irrespective of geographical position. Wireless technology has become tremendously popular due to its usage in various new fields of applications in the domain of networking. One such important field is Mobile Ad-hoc Networks (MANET's) where the nodes of the network do not have a specific infrastructure and they are connected dynamically in an arbitrary manner. Nodes within each other's radio range communicate directly via wireless links, while those that are further apart use other nodes as relays. Nodes in an ad-hoc network move dynamically; consequently keeping track of the network topology is a difficult task to achieve. There are many security issues associated with these kinds of networks. Security in wired networks can be applied to some extent but ad-hoc networks have their own Vulnerabilities which cannot be always plugged using wired security issues. Although security has been achieved to some extent, attacks keep increasing in the form of malicious nodes which may jam or spoof the channel or drop the packets. Many routing protocols have been proposed for Ad hoc networks. Recently secure routing protocols have also been proposed [3] Zapata , Deng et al. . If the introduction of secure mechanisms into routing degrades the performance significantly, the network designer has to evaluate the trade-offs in introducing security into routing. However, to the best of our knowledge no one has investigated the overheads associated with introducing security into routing protocols. This thesis concentrates on one such routing protocol namely Ad hoc On Demand Vector Routing Protocol (AODV) [Perkins and Royer 10]. We compare AODV with secure AODV and study the impact of security on routing overhead and on other performance metrics.

MATERIALS AND METHODS

1. AODV Routing Protocol

AODV is an on demand distance vector routing algorithm. In AODV each mobile host acts as a specialized router and routes are obtained as needed (i.e., on demand). Routes are maintained only between the nodes which need to communicate. It is suitable for dynamic self-starting networks. It also provides loop free routes and even repairs broken links by notifying the nodes so that they can invalidate the route using the lost link. The overall bandwidth required for this protocol is smaller compared to other protocols since it doesn't require any global periodic advertisementsPath discovery is initiated when a source node communicates with another node for which it has no routing information in its table. Each node maintains two counters, node sequence number and broadcast ID. Path discovery is initiated by broadcasting route request (RREQ) packets to its neighbors. The source broadcasts the route request packets to its neighbors. The neighbors in turn sends the packets to their neighbors until the packet reaches an intermediate node which has recent route information for the destination or it till reaches the destination itself. Nodes discard the packets which

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 3, Issue 1
April 2014

they had already seen. The RREQ packet contains the following fields:

<source_addr, source_sequence#, broadcast_id, dest_addr, dest_sequence#, hop_count>

The pair <*source_addr, broadcast_id* > uniquely identifies a RREQ packet.

RREP packet contains the following fields:

<source_addr, dest_addr, dest_sequence#, hop_count, lifetime>

Each node either satisfies the RREQ packet by sending a route reply (RREP) back to the source (only when the RREQ packet reaches an intermediate node which has route to the destination node) or rebroadcasts the RREQ packet to its neighbors after increasing the *hop_count*.

The source sequence number in RREQ maintains the freshness information about the reverse route to the source whereas the destination sequence number specifies the information of the fresh route to the destination which is accepted by the source. Reverse path is automatically setup when RREQ packet travels from source to various destinations. These reverse path entries are preserved until a reply is sent back to sender.

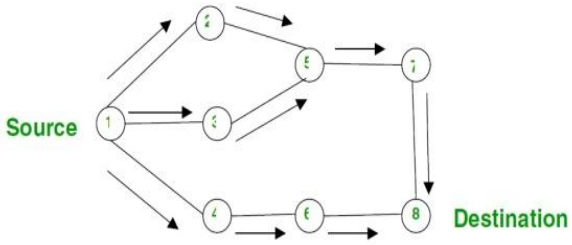

Fig 1.Propagation of a Route Request (RREQ) Packet

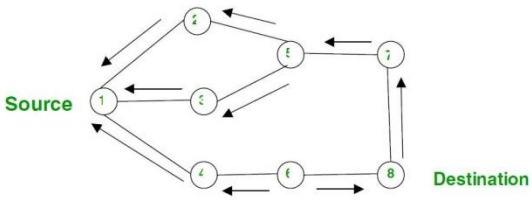

Fig 2 Reverse Path Formation

2. Packet Drop Problem

AODV is an important on-demand routing protocol that creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a *route discovery* process within the network. It broadcasts a route request (RREQ) packet (Fig. 1) to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located. In this process the intermediate node can reply to the RREQ packet only if it has a fresh enough route to the destination. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or intermediate node responds by unicasting a route reply (RREP) packet (Fig. 2) back to the neighbor from which it first received the RREQ. After selecting and establishing a route, it is maintained by a *route maintenance* procedure until either the destination becomes inaccessible along every path from the source or the route is no longer desired. In this article we address one routing attack that could easily happen in wireless MANETs, the packet drop problem. According to the original AODV protocol, any intermediate node may respond to the RREQ message if it has a fresh enough route, which is checked by the destination sequence number contained in the RREQ packet. This mechanism is used to decrease the routing delay, but makes the system a target of a malicious node.The malicious node easily disrupts the correct functioning of the routing protocol and makes at least partof the network crash.for example, node 1

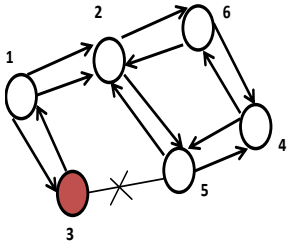

Fig 3Packet Drop Problem

Wants to send data packets to node 4 in Fig. 3, and initiates the route discovery process. We assume node 3 to be a malicious node with no fresh enough routeTo destination node 4. However, node 3 claims that it has the route to the destination whenever it receives RREQ packets, and sends the response to source node 1. The destination node and any other normal intermediate nodesthat have the fresh route to the destination may also give a reply. If the reply from a normal node reaches the source node of the RREQ first, everything works well; but the reply from malicious node 3 could reach the source nodefirst, if the malicious node is nearer to the source node. Moreover, a malicious node does not need to check its routing table when sending a false message; its response is more likely to reach the source node first. This makes the source node think that the route discovery process is complete, ignore all other reply messages, and begin to send data packets. As a result, all the packets through the malicious node are simply consumed or lost. The malicious node could be said to form a packet drop in the network, and we call this

the packet drop problem. In this way the malicious node can easily misroute a lot of network traffic to itself, and could cause an attack to the network with very little efforts on its part.

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 [7] (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 [14] (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 [6] (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 [9] (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. In [4] (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 neighbor's 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 neighbors 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 [16](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 afurther input into the cost of the techniques' implementation. In [5] (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.

1.Tropical Intrusion Detection Security Policy(TIDSP) over AODV

This paper proposes the TID security policy over the AODV MANET routing protocol. The TID security policy performs its intrusion detection mechanism locally in the previous node of the attacker node in contrast with the RID security policy, which performs its intrusion detection mechanism by means of the route node. End-to-end delay, routing overhead, and throughput of the RID security policy and TID security policy will be compared by varying the number of nodes, network size, and the transmission range. The proposed TID security policy 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, I will perform more enhanced intrusion detection mechanism that could perfectly detect a group attack if applied on the MANET. Subsequently, the new enhanced security policy will be evaluated using the same performance metrics and simulation parameters. To achieve this, the following objectives were identified:

1) To develop and implement the AODV routing protocol.

2) To study the attacks which can be launched on AODV network such as attacks on routing messages and control messages. Attacks concerning the impersonation of nodes should also be identified.

3) To develop and implement the SAODV routing protocol which provides authentication, integrity and non-repudiation.

4) To study the impact of security on AODV routing and control messages.

5) To generate test scripts with and without attacks and test the above mentioned protocols performances on those test scripts.

6) To compare the performance of all the protocols with and without attacks in the network.

7)To suggest some measures to improvise these protocols.

In order to mitigate the drawbacks in the RID mechanism proposed in [3] (Deng *et al.*, 002), we propose a new mechanism called the Local Intrusion Detection Security Routing (TID) mechanism. The mechanism is shown in Figure 4 and its algorithm pseudo-codes are given in Algorithm 1 and Algorithm 2. TID mechanism allows the 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 RID 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 announce that 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 initiate a new route discovery process to the destination.

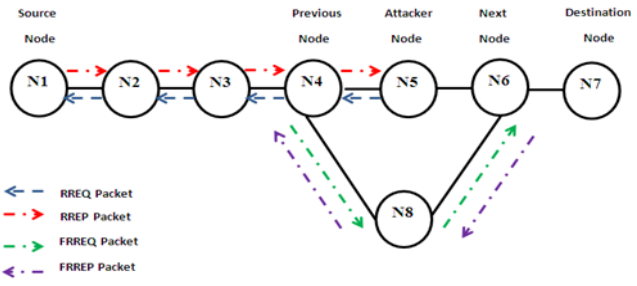

Fig.4 Proposed Local Intrusion Detection Security Routing (TID) Mechanism

Algorithm 1: Pseudo-code for TID 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 TID 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

4 Simulation Results and Evaluation

To simulate the performance of the TID mechanism, we use the GloMoSim 2.03 network simulator [7] (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.

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 3, Issue 1
April 2014

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 RID and the TID 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.

In order to study the effect of the number of nodes in RID and TID mechanisms 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 5, Figure 6, and Figure 7 compare between the network throughput, average end-to-end delay, and routing overhead respectively in both RID and TID mechanisms while varying the number of nodes. It is clear from the figures that the TID mechanism outperforms the RID mechanism. This is because the TID mechanism uses local intrusion detection compared with the RID mechanism that uses source intrusion detection. The TID 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.

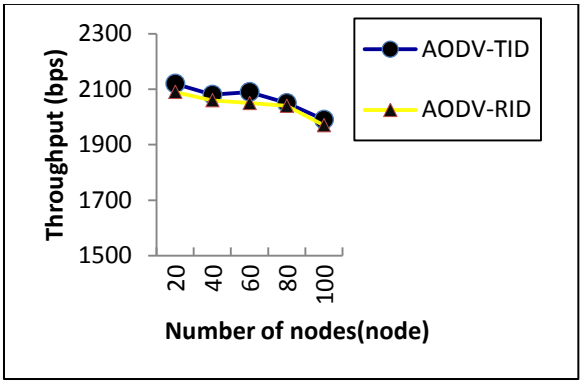

Fig 5 Throughput vs. Number of nodes

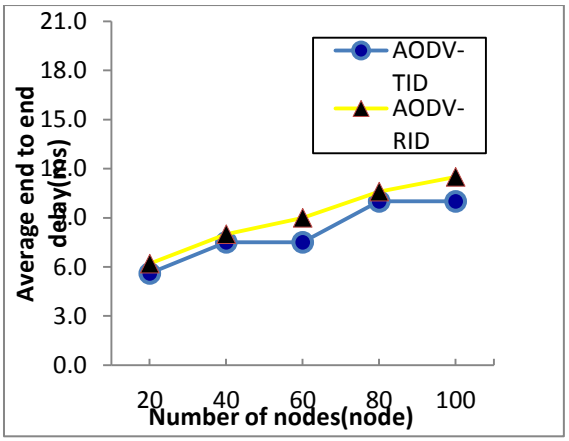

Fig 6 Average end-to-end delay vs. Number of nodes.

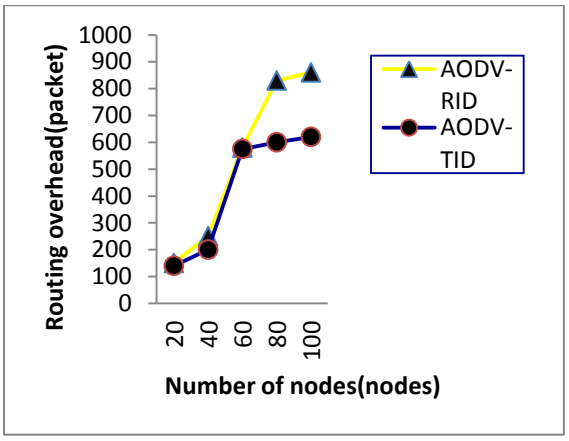

Fig 7 Routing overhead vs. Number of nodes.

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 3, Issue 1
April 2014

1. 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 8, Figure 9, and Figure 10 compare between the network throughput, end-to-end delay, and routing overhead of The TID and RID 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[13] (Shanudin *et al.*, 2005), collisions, and hence data packets dropping. Figure 8, Figure 9, and Figure 10 state clearly the better performance of the TID mechanism over the RID mechanism. The local TID 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 RID 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.

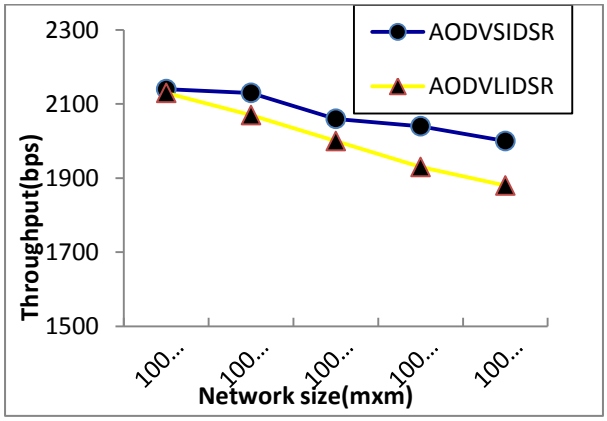

Fig 8 Throughput vs. Network size.

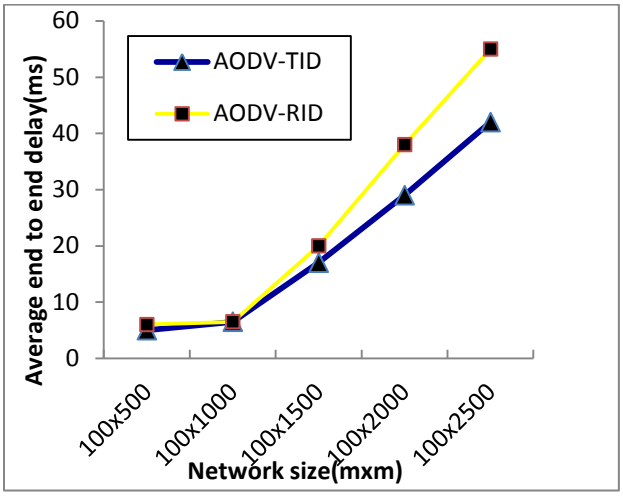

Fig 9 Average end-to-end delay vs. Network size.

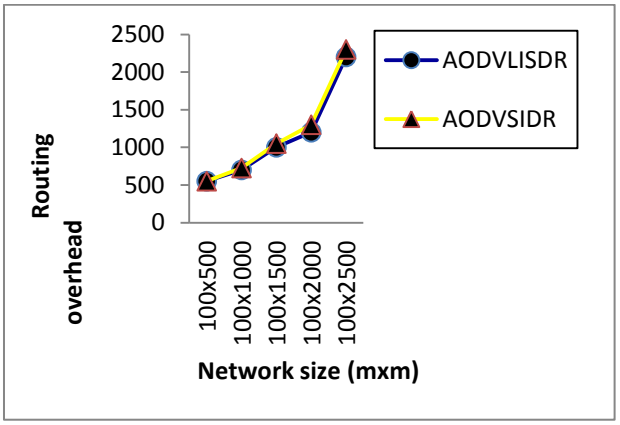

Fig 10 Routing overhead vs. Network size

2. Varying the Transmission Range

In order to study the effect of transmission range in the RID and TID mechanisms, 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 11, Figure 12, and Figure 13 compare between the network throughputs, end-to-end delay, and routing overhead of the RID and TID 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 neighbors while the nodes are moving and reduces the data packet dropping (Saqour *et al.*, 2007).

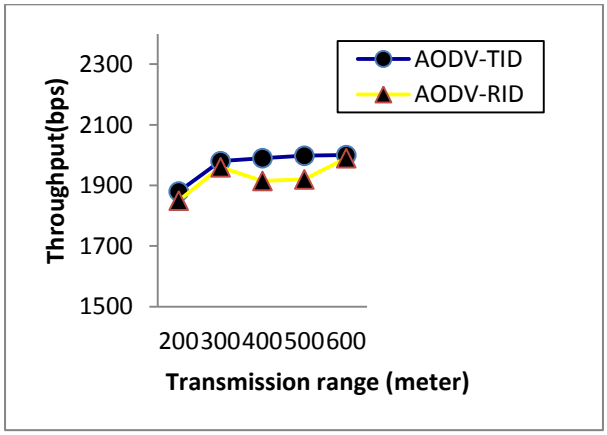

Fig 11 Throughput vs. Transmission range

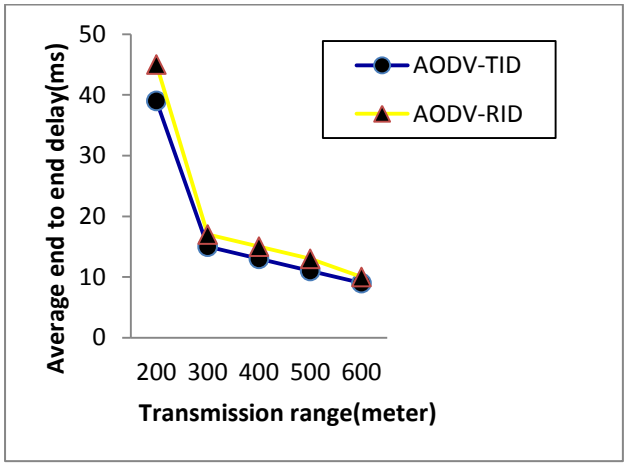

Fig 12 Average end-to-end delay vs. Transmission range

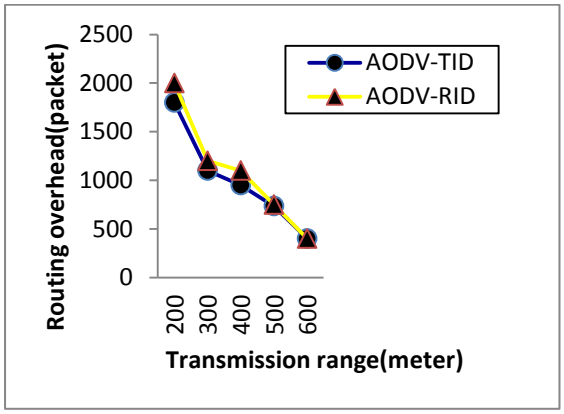

Fig 13 Routing overhead vs. Transmission range

It is clear from Figure 11, Figure 12, and Figure 13 that the TID mechanism outperforms the SID mechanism. The TID mechanism in 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 RID mechanism. 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 AND FUTURE WORK

This paper proposes the TID mechanism over the AODV MANET routing protocol. The TID mechanism performs its intrusion detection mechanism locally in the previous node of the attacker node in contrast with the RID mechanism, which performs its intrusion detection mechanism by means of the source node. End-to-end delay, routing overhead, and throughput of the RID and TID 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 TID mechanism 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 mechanism that 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

[1] 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.

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

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

[4] 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.

[5] 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.

[6] 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.

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

[8]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.

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

[10]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.

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

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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