Research Journal of Applied Sciences 10 (7): 256-263, 2015
ISSN: 1815-932X

Identifying Intruder in Mobile Ad Hoc Network Using AIHAODV Protocol

[1]S. Hemalatha and [2]Paul Rodrigues
[1]Department of Computer Science and Engineering, Anna University, Chennai, India
[2]DMI College of Engineering, Palanchur-Nazarethpet Post, Chennai, 602103 Tamil Nadu, India

Abstract: Mobile ad hoc network is one of the growing technology for providing communication without the need of any infrastructure. Having the limitation of infrastructure less and no access control, MANET has several possibilities to fall into attacks through intruder. The intruder is a one kind of attacker who tries to prevent the normal operations like not cooperating to forwarding the packet to the next hop. There are several methods has been proposed to identify the intruder in the network. Those methods are concentrating on the signature based, anomaly and rule based. There is none of the method is being proposed to identify the packets on data flow itself if the intruder play the role of not forwarding the packet to the next node. This study presents the implementation of AIHAODV (Advanced Intruder Handling Ad hoc on Demand Vector). This protocol is implemented using the concept of divide and conquer strategy which will help to identify the node which does not forward the packet to the next node while flow from source to destination. This protocol not only used to identify the intruder in the network also used to re-direct the packet by forming the new route.

Key words: Ad hoc network, routing protocol, intruder, divide and conquer, AIHAODV protocol

INTRODUCTION

A mobile ad hoc network is an infrastructure less and works under the principle of wireless data transmission (Perkins and Royer, 1999). Intruder detection is a one kind of the security attack who is not an authorized node but try to access the system or misuse the system or break the system (http://repository.tamu.edu/bitstream/handle/1969.1/2215/etd-tamu-2004A CPSC?sequence = 1; http://www.giac.org/paper/gsec/1377/host-vs-network-based-intrusion-detection-systems/102574). In order to identify the intruder in the MANET used an intruder detection technique which is a process of keeping track of activities among the nodes in the network. There are three different principles used in IDS are Anomaly Based IDS, Signature Based IDS and Specification Based IDS (Mukherjee *et al*., 2004; Ning and Jajodia, 2003). In this study presents the algorithm implementation of AIHAODV protocol, finally describe the performance comparison with AODV protocol.

The evolution of identifying intruder was started in the early 1987 onwards. In 1987 (Ning and Jajodia, 2003; Gangwar, 2012), the computer abuse on real time intruder detection was proposed by dinning methods able to detect, break and penetration of intruder in the MANET (Perkins and Royer, 1999). Intruder was identified by Marti, proposed that watch dog and parthrater method was used to identify the node which do not able to forward the packet. This method also checks whether node forward the packet without modification or not (Lee and Stolfo, 2000). Second method used was knowledge based IDS (Chang *et al*., 2001; Islam and Rahman, 2011) paper, different attacker patterns are updated on the IDS (Pei, 2004). Any variations on the attacker patters (Rajaram and Ranjana, 2007; Sharma and Gupta, 2009) are identified as a intruder. Third method used was sensor based (Huang and Lee, 2003; Anjum *et al*., 2003; Kachirski and Guha, 2003). They used multiple sensor for collecting data from nodes which is used to identify the intruder. Next method was a signature based intruder detection (Sun *et al*., 2003) and geographic zone based intrusion detection system (Kachirski and Guha, 2003; Sun *et al*., 2003). Next method was proposed an architecture is called cooperative intrusion detection architecture was used to detect intruders (Anjum *et al*., 2003; Rajaram and Palaniswami, 2010). This architecture (Murthy and Manoj, 2004) forms a node hierarchy on the network, top level nodes in the network were responsible for identifying an intruder. In the year 2005 knowledge based IDS proposed (Marchang and Datta, 2008) who defined finite base machine through RIDAN architecture against the AODV routing process.

From the above literature survey relies on the methods and architecture based. But none of the method is proposed to identify the intruder who plays the role of

Corresponding Author: S. Hemalatha, Department of Computer Science and Engineering, Anna University, Chennai, India

participating on the network but not cooperating to forward the packet to the next hop. By doing this kind of activity, will achieve the performance decay on the network. So, this protocol we called Advanced Intruder Handling on Demand Vector protocol is used to identify those types of intruder while the packets are flowing from sender to the receivers. This will be achieved by using the strategy of Divide and Conquer Strategy.

AIHAODV PROTOCOL

With this AIHAODV protocol system, identify the intruder through the routing protocol. The new protocol is defined based on the ad hoc on demand distance vector protocol is named as Advanced Intrusion Handling Ad hoc on Demand Distance Vector Protocol (AIHAODV). In this new protocol introduce the concept of Divide and Conquer Strategy. In this protocol, we defined eight step by step process. First four processes are in the implementation of intruder identification stage and remaining four processes are considered for the conformation and re-direction phase. It includes:

- Decide the path using AODV protocol
- Packet transmission
- Apply Divide and Conquer Strategy
- Identification of intruder the network
- Suspect the intruder node
- Conformation intruder
- Route re-direction
- Sending alert message to other nodes about protocol

Decide the path using AODV protocol: The ad hoc on demand distance vector (Perkins and Royer, 1999) is used for decide the path between source to destination.

Steps used in route discovery:

1. Node S(source) needs a route request to D (Destination)
2. Creates a Route Request (RREQ): enters D's IP address, sequence number#, S's IP address, sequence number#, hop count (= 0)
3. Node S broadcasts RREQ to its neighbours
4. Node A receives RREQ: Makes a reverse route entry for S destination = S, next hop = S, hop count = 1 It has no routes to D, so it rebroadcasts RREQ
5. Node C receives RREQ: makes a reverse route entry for S destination = S, next hop = A, hop count = 2 It has a route to D and the sequence number# for route to D is >= D's sequence number# in RREQ

This module is processed with discover the route by using the AODV protocol (Perkins and Royer, 1999) using the NS2 simulator is shown in Fig. 1. Soure and destination nodes are shown in red color. It can be done based on the route discovery and route maintenance which includes route request and unicasting reply.

Packet transmit: Source broadcasts a packet P to all its neighbours. Each node receiving packet P and forwards packet P to its neighbours, sequence numbers help to avoid the duplication of packet (Lee and Stolfo, 2000). Moreover, the sequence number helps to maintain the freshness of the packet flow. According to the below figure, packet P reaches destination.

This module is processed with packet transmission; the packet can be transmitting via the route which is discovered by AODV protocol as in Fig. 1. Packet transmitted as in Fig. 2. If the packet is reached properly to the destination, then it indicates that, the route is perfect and the route does not have any intruder. If packet loss or any delay for packet transition occurred it consider that the route have an intruder. Identification purposes we are transmitting dummy packet.

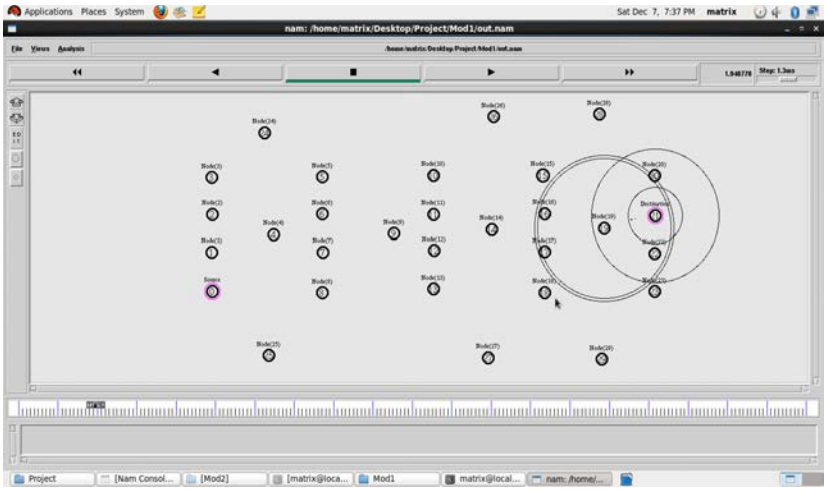

Fig. 1: Decide the path using AODV protocol

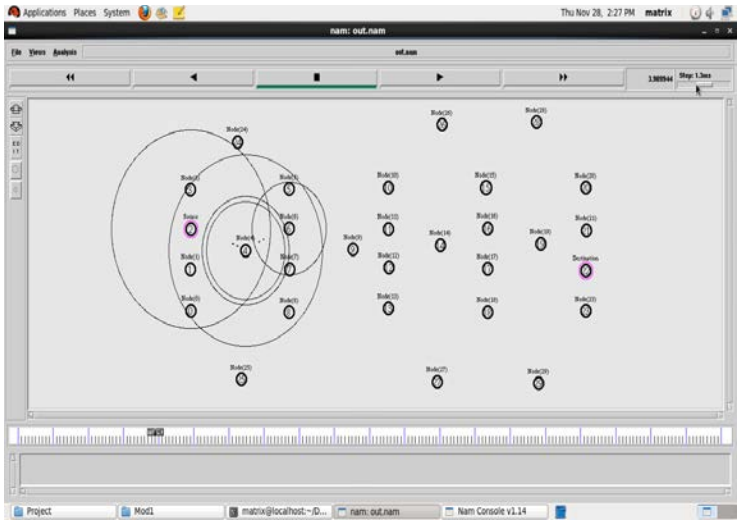

Fig. 2: Packet transmit

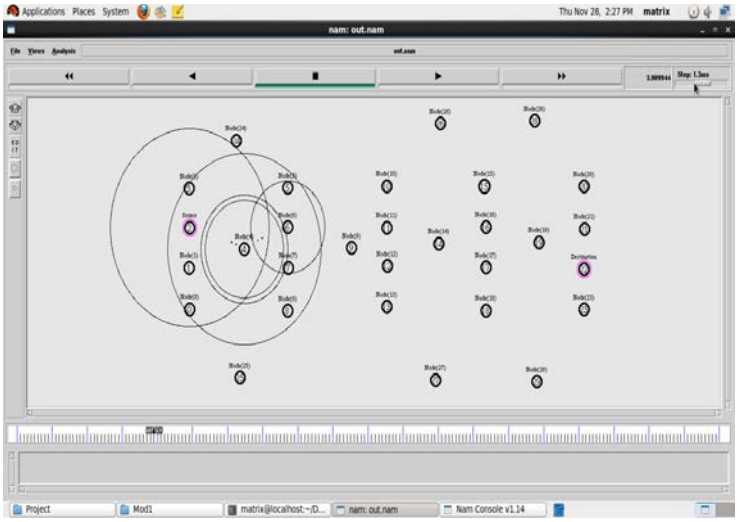

Fig. 3: Route discovery and No. of node calculation

Establish the divide and conquer strategy: Customized protocol forwards the packet from source to the approved destination. Then, calculate the number of node and do the operation of the divide and conquer strategy. In this strategy, the network can calculate the number of nodes and then it takes the middle node that middle nodewill act as the temporary destination. Then, the packet can be transmitted from the source to the temporary destination. If the temporary destination receives the packet then that node will not consider as an intruder. Else middle node considers as the destination do the middle node calculation again. And do the process, until identifying the intruder.

Divide and Conquer Strategy algorithm:

Procedure (Source, Dest, G)-Divide and Conquer strategy
Consider the ordered Set G = {1, ..., N}
Step 1: Initialize source = 1, dest = N
Step 2: Calculate middle = No of hops (source to dest)/2
Step 3: (i) check the packet is passed the middle node if yes the calculate the new middle form old middle (source = old middle) to dest, go to step 2
(ii) other wise calculate the new
middle for source to middle (Dest = middle)
(iii) repeat the process
//assume there is no flow of data then suspect the node may be the intruder.
Process whether the middle node is intruder

This module is processed under the strategy of divide and conquers; the packet can transmit via the route which is discovered by the AODV protocol as in Fig. 1. It can calculate the number of nodes in the route as in Fig. 3. It can send the packet to the destination. If the

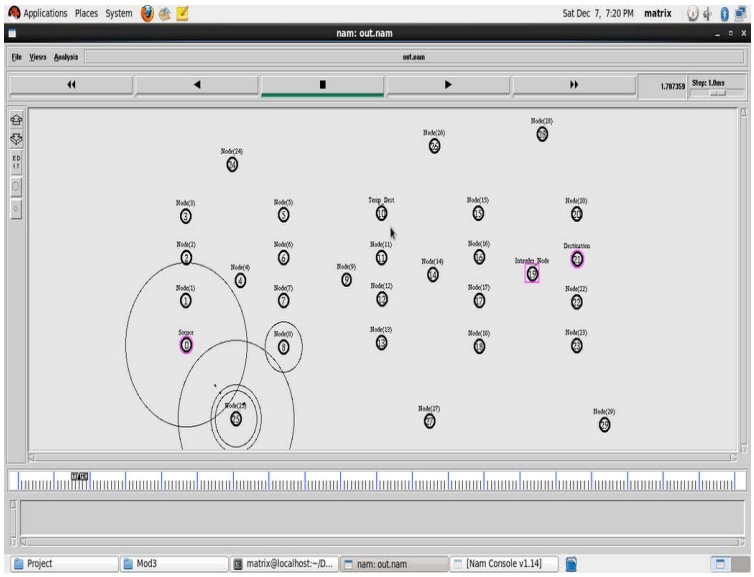

Fig. 4: Divide the route into two half

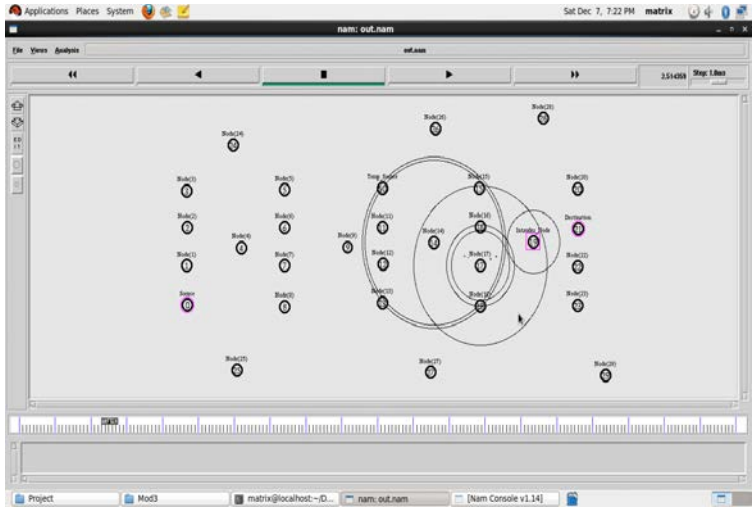

Fig. 5: Temporary destination becomes temporary source

packet is not reached to the destination then the route is divided and calculate middle node that node will act as the temporary destination as in Fig. 3. After a transmition that temporary destination receives the packet, then that node act as the temporary source Fig. 4. Continue the process until we got the idea of which node is an intruder as in Fig. 5.

Identify the intruder using AIHAODV: Using AIHAODV routing protocol divide and conquer strategy can be done. Based on this strategy it can identify the intruder. Intruder node can be stored or drop the packet from the network. This module is focused for intruder identification as in Fig. 6, using divide and conquer strategy.

Intruder suspect: According to the intruder identification process, we are suspecting or doubtful about the node and that node will get a special caution. That node will be under surveillance. All the activity about that node will be noted and recorded. This process must be confidential and furtive.

This module is processed to help the intruder conformation as a result of intruder identification. The result of the suspect module is reflected in conformation phase. It is shown in Fig. 7, intruder node is highlighted and suspect.

Intruder conformation: In this phase, intruder node is conformed based on the identification phase as well as

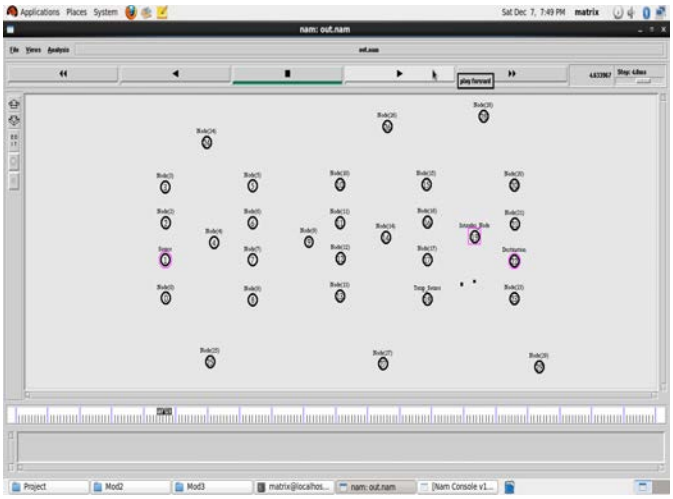

Fig. 6: Intruder is identified

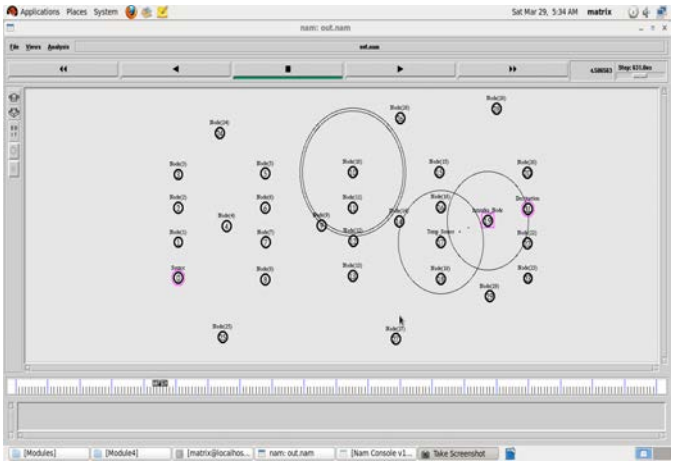

Fig. 7: Intruder suspect

the suspect phase. It includes the phenomenon that source node sends a packet to the suspect node for the conformation process. At that time suspect node replied appropriately to the sender within the time period as well as in the original reply, then that suspected node is considered as good node, else that node will consider as the intruder node. The strategy will process with the help of neighbour node. Neighbour node will give the message to the sender node that the suspect node is giving the reply message in proper time period.

Procedure (Source, H, Intruder)
Consider the ordered set H = {1, ..., M)
Step 1: Initialize source = 1, Intruder = M
Step 3: If there is no RREP from intruder to source and conform M is intruder
Else if there is false RREP from intruder to source and conform M is intruder
Step 4: Otherwise the node M is not a intruder node
Step 5: Stop

This module is processed with the basis of intruder suspect phase. The intruder confirmation is used to conform the identified intruder is original intruder. The result of the confirmation phase is reflected in Fig. 8.

Route re-direction: Once the alert message is send to the entire node, again divide and conquers strategy process happens and re-direction can happen without passing with the intruder node. That route will make the direction to source the destination directly. In the same time, the message or the packet can reach in the destination.

Procedure (source, Dest, G, Intruder)
Consider the ordered set G = {1, ..., N}
Step 1: Initialize source = 1, dest = N
Step 2: In set G, find the route by passing router request. Alter source = prev (intruder)
Step 3: Find the route discovery process from alter source based on AODV protocol
Step 4: Finally establish the network from source to destination

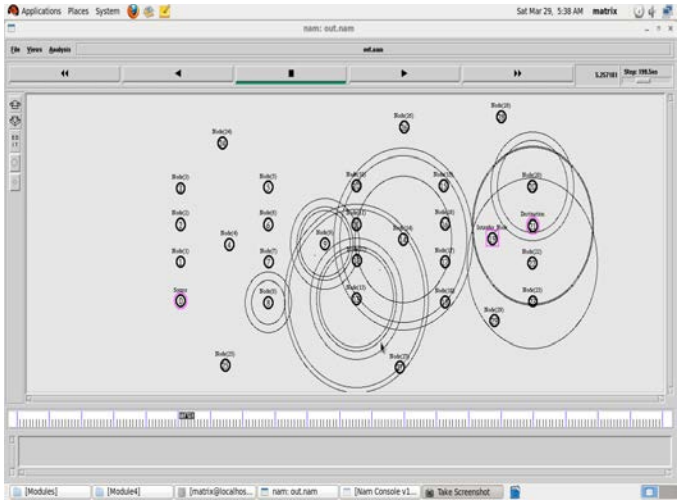

Fig. 8: Intruder conformation

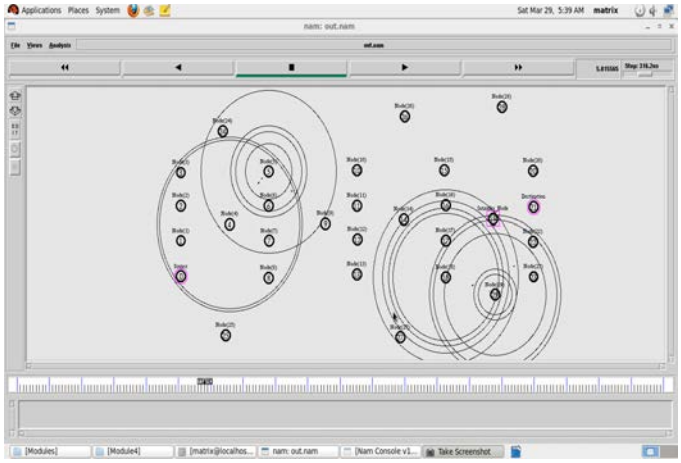

Fig. 9: Route re-direct

This module is processed with the basis of intruder conformation phase. After using the confirmation phase, source node will re-direct the route to the destination. The message will reach to the destination send by the source through the new re-directed route. This diagram representation is shown in Fig. 9, source node identified a new path and retransmit the packet through the new path.

This module is processed with the basis of intruder conformation phase. After using the conformation phase, network send the intruder information to the entire node as well as it gives the updating to the routing table.

Send alert message: Once the node is conformed that suspect node as an intruder. Then, the network will give the message to the entire node in the network. Then, the entire node should be prepared with that system and alert with that. That node should contain the routing table that routing table contains source IP address, destination IP address, broad cast ID, number of hop, total number of hop along with that the routing table contain an intruder node ID and IP address.

PERFORMANCE EVOLUTION

This study discuss the performance comparisons with the AODV protocol. We have taken three parameters are throughput, packet delivery ration and end to end delay.

Through put between AODV and AIHAODV: Throughput refers to how much data can be transferred from one location to another in a given amount of time. Comparing AIHAODV with AODV, AIHAODV give better performance shown in Fig. 10.

Packet delivery ratio between AODV and AIHAODV: The ratio of the number of delivered data packets to the destination. This illustrates the level of delivered data to the destination:

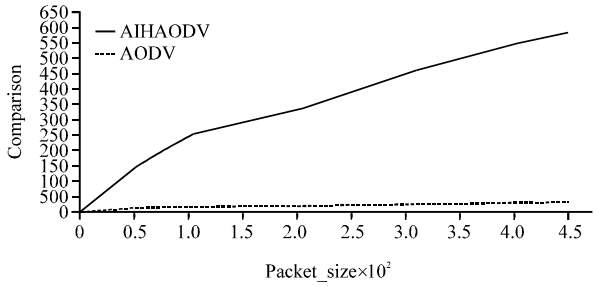

Fig. 10: Graph for throughput evaluation

ΣNo. of packet receive/Σ No. of packet send

Comparing with AODV protocol, AIHAODV protocol shows more packet delivery ratio shown in Fig. 11.

End to end delay between AODV and AIHAODV: The average time is taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted:

Σ(arrive time-send time)/ΣNo. of connections

Comparing with AODV protocol, AIHAODV protocol shows less end to end delay is shown in Fig. 12.

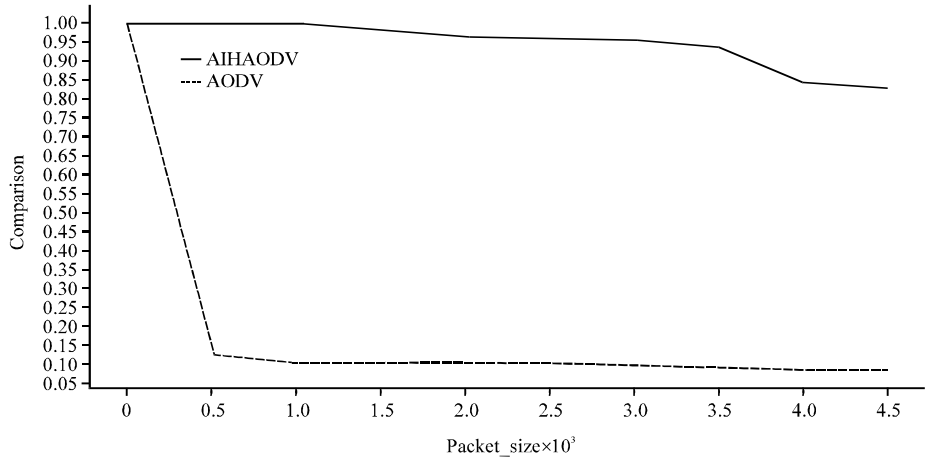

Fig. 11: Graph for packet delivery ratio

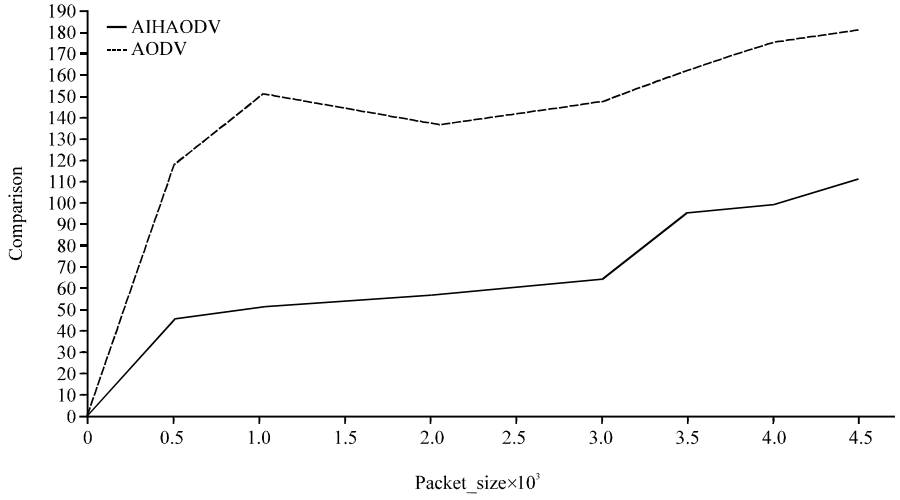

Fig. 12: Graph for end to end delay

CONCLUSION

Finally, we conclude that the AIHAODV protocol can be used for identifying the intruder who play the role of not forwarding the packet to the next hop. Comparing with the AODV protocol this produces a better performance ratio. In future, this protocol can be done power saving in packet transmission implemented by by using a directional antenna.

REFERENCES

Anjum, F., D. Subhadrabandhu and S. Sarkar, 2003. Signature based intrusion detection for wireless Ad Hoc networks: A comparative study of various routing protocols. Proceedings of the IEEE 58th Conference on Vehicular Technology, Oct. 6-9, Morristown, New Jersey, USA., pp: 2152-2156.

Chang, H.Y., S.F. Wu and Y.F. Jou, 2001. Real-time protocol analysis for detecting link-state routing protocol attacks. ACM Trans. Inf. Syst. Secur., 4: 1-36.

Gangwar, S., 2012. Mobile ad hoc network: A comprehensive study and survey on intrusion detection. Int. J. Eng. Res. Appl., 2: 607-612.

Huang, Y. and W. Lee, 2003. A cooperative intrusion detection system for ad hoc networks. Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, October 31, 2003, New York, USA., pp: 135-147.

Islam, M. and S.A. Rahman, 2011. Anomaly intrusion detection system in wireless sensor networks: Security threats and existing approaches. Int. J. Adv. Sci. Technol., 36: 1-8.

Kachirski, O. and R. Guha, 2003. Effective intrusion detection using multiple sensors in wireless ad hoc networks. Proceedings of the 36th Annual Hawaii International Conference on System Sciences, Volume 2, January 6-9, 2003, Hawaii, USA.

Lee, W. and S. Stolfo, 2000. A framework for constructing features and models for intrusion detection systems. ACM Trans. Inform. Syst. Security, 3: 227-261.

Marchang, N. and R. Datta, 2008. Collaborative techniques for intrusion detection in mobile ad hoc networks. Ad Hoc Networks, 6: 508-523.

Mukherjee, B., L. Hebedein and K.N. Levitt, 2004. Network intrusion detection. IEEE Network, 8: 26-41.

Murthy, C.S.R. and B.S. Manoj, 2004. Ad Hoc Wireless Networks: Architectures and Protocols. Pearson Education India, New Delhi, India, ISBN-13: 9788131706886, Pages: 878.

Ning, P. and S. Jajodia, 2003. Intrusion detection techniques. Internet Encycl., 10.1002/047148296X. tie097.

Pei, J., S.J. Upadhyaya, F. Farooq and V. Govindaraju, 2004. Data mining for intrusion detection: Techniques, applications and systems. Proceedings of the 20th International Conference on Data Engineering, March 30-April 2, 2004, Boston, MA., USA.

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, February 25-26, 1999, New Orleans, LA., USA., pp: 90-100.

Rajaram, A. and D.S. Palaniswami, 2010. Malicious node detection system for mobile ad hoc networks. Int. J. Comput. Sci. Inf. Technol., 1: 77-85.

Rajaram, M. and R. Ranjana, 2007. Detecting intrusion attacks in ADHOC networks. Asia J. Inform. Technol., 6: 758-761.

Sharma, S. and R. Gupta, 2009. Simulation study of blackhole attack in the mobile ad hoc networks. J. Eng. Sci. Technol., 4: 243-250.

Sun, B., K. Wu, and U.W. Pooch, 2003. Zone-based intrusion detection for mobile ad hoc networks. Int. J. Ad Hoc Sens. Wirel. Netw.