Asian Journal of Information Technology 15 (6): 1106-1115, 2016
ISSN: 1682-3915

Implementation of DDOS Intruder Detection Using Divide and Conquer Strategy in Mobile Ad-Hoc Environment

[1]S. Hemalatha and [2]P.C. Senthil Mahesh
[1]Department of CSE, Sri Lakshmi Ammaal Engineering College,
[2]Department of CSE, Dhaanish Ahamed College of Engineering, Chennai, Tamil Nadu, India

Abstract: An ad-hoc network is an infrastructure less network with autonomous node and also the network is distributed and decentralized, Ad-hoc network are more vulnerable compared to other network, since, it's necessary to provide the security in MANET. In mobile ad-hoc networks are easily affected by Distributed Denial of Service (DDoS) intruder. Intrusion detection systems identify intrusions through continues monitoring of the network for unusual activity. Intrusion detection can be used to prevent or minimize the damage to the network and achieve possible recovery. In this proposed study, we will identify the intruder while the packet flow from the source to destination using the AIHAODV (Advanced Intrusion Handling Ad-hoc On-demand Distance Vector) protocol with the strategy of divide and conquer.

Key words: MANET, AODV, DDOS, IDS, security

INTRODUCTION

An ad-hoc network is an un-coordinated wireless network that are self-regulating deprived of any support infrastructure also the network is spread and devolved, an ad-hoc networks are more defenceless associated to other network, Since, its needed to offer the safety in MANET. In this technique, ad-hoc networks have a vibrant topology such that nodes can be simply joining or leave the network at any socket of time. They have various prospective applications are used, particularly in armed and rescue zones such as linking warriors on the battle ground or establishing a novel network in place of the network which warped later a disaster like an earth shaking. Ad-hoc networks are appropriateness for an area where it is not potential to set up a static infrastructure. To keep this connectivity, bulges practice some routing protocols such as AODV (Ad-hoc On-demand Distance Vector), Besides performing as a host, each node also performs as a router to determine a path and accelerative packets to the truthful node in the network.

Wireless links that has develop a vital to normal lives as they are more and more arranged in numerous applications (Lee and Stolfo, 2000). Still, their upward regard is faced by insecure environment of these networks. Additionally, in a truly ad-hoc wireless network area, network facilities such as routing are delivered by the nodes themselves.

The AODV routing procedure customs an on-demand method for discover the routing that is a route is recognized only when it is vital by a source node for the transferring data packets. It indicates endpoint sequence numbers to recognise the most recent track. In route judgment of AODV protocol, middle nodes are liable to invent a fresh track towards the destination. The AODV protocol is a on demand routing protocol that attempt to maintain reliable, up-to-date routing material from individual node to other node in the network. In this AODV, protocol is a source-initiated on-demand routing style. This type of routing builds paths only when preferred by the source node. When a node requires a route to a destination, it starts the route verdict procedure within the network. This process is completed once a route is found or all imaginable route variation has been examined. After a path has been recognized, it is kept by a route maintenance method till either the destination becomes remote along all paths from the source or until the route is no longer chosen. In path judgment method of AODV protocol, mid nodes are accountable to catch a fresh path to the destination. To design and progress the efficient AIHAODV protocol, it's used to detect the DDOS intruder in effective manner such as malicious behavior node. There are three possible mechanisms to be handling for AIHAODV protocol.

Literature review: In this study, researchers categorize the constructions of intrusion detection systems that have been introduced for MANETs. Current IDS's agreeing to those constructions are also studied and compared.

Corresponding Author: S. Hemalatha, Department of CSE, Sri Lakshmi Ammaal Engineering College, Chennai, Tamil Nadu, India

In this study, researcher have learned about the different type of intrusion detection techniques in MANET and then the association between numerous researches achievement will be estimated based on their parameters (Gangwar, 2012).

In this study, intrusion detection systems are security systems that gather information from variability types of system and network sources and evaluate these facts in an effort to notice motion that may comprise or intrusion on the system. This evidence also helps to the computer and systems administrators to deal with attacks, directed at their networks (Bace, 1998, 2000). In addition, the features of an intrusion detection system are to monitoring, audit and judgement of the system or network performance which is an compulsory part of security management. This type of monitoring is an ongoing process; the intrusion detection system must change according with the attacks change. As will be seen, when the monitoring system of technique and targets differ the ids will broadcast alarms and alert message to the answerable parties when behaviour of attention occur on the network. In some cases, these systems resolve users to label real-time responses to attacks (Bace and Rebecca, 2000).

This study is intended to the necessity of the execution of IDS in the activity environment (SANS Institute, 2001). The purpose of this study is indicating what are the steps to be following to maintain in the IDS. The work should also clarify what you are expecting from your intrusion detection system and what you have to anticipate for prior to deployment.

The concept behind the MDSs is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected. They can detect many or all known attack patterns (Mukherjee *et al*., 1994) but they are of little use for unknown attack methods. Misuse detection systems try to recognize known "bad" behaviour.

AODV is a routing protocol designed especially for Mobile Ad hoc Networks (MANET) (Perkins and Royer, 1999). This protocol is worked with thousands of nodes, it has the class of a demand-driven protocols. It can have the route discovery and route maintenance mechanism which includes route request, route reply, route error and hello message parameters. The routing table can be maintained by the AODV protocols which includes Source, destination and next hop, total number of hop, time stamp, etc.

AIHAODV system design: The AODV protocols are reactive routing protocols. The source node only initiated routing protocol. Since, proactive protocol routing methods to design based on cyclic updated this leads to more routing overhead. To design AIHAODV protocol is to reduce overhead. In previously no routing structure is created in AODV. The route finding process of AODV consists of two methods. First one, it is source routing. Second one is backward learning.

Source initiated means source floods the network with a route request packet when a route is required to a destination. The flooding is propagated outwards from the source. The flooding transmits the request only once. On receiving the request from the source node the destination replies to the request if it has the valid path. Reply from destination uses reversed path of route request. Since, route reply is forwarded via the reverse path which forms forward path. Thus, it uses forward paths to route data packets. AODV protocol uses hop-by-hop routing. That is each node forwards the request only once. In the meanwhile unused paths expire based on timer.

AODV uses the concept of optimization that is any intermediate nodes can reply to route request if it has valid path which makes the protocol to work faster. But the major problem with optimization causes loops in presence of link failure. Each node maintains sequence number. It acts as a timestamp. The most interesting feature of sequence number is, it signifies the freshness of the route. When a node maintains high sequence number makes it up to date in the routing. In AODV path maintenance is based on Route Error (RERR) message.

MATERIALS AND METHODS

Proposed technique: In this system, identify DDoS intruder through the routing protocol. 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. Figure 1 shows the system architecture of AIHAODV where each node has it own routing table on demand for communicating with other nodes.

In this study, includes eight step by step processes. First four processes are in the implementation of DDoS intruder identification stage and remaining four processes are considered for the confirmation and redirection phase. It includes decide the path using AODV protocol, after

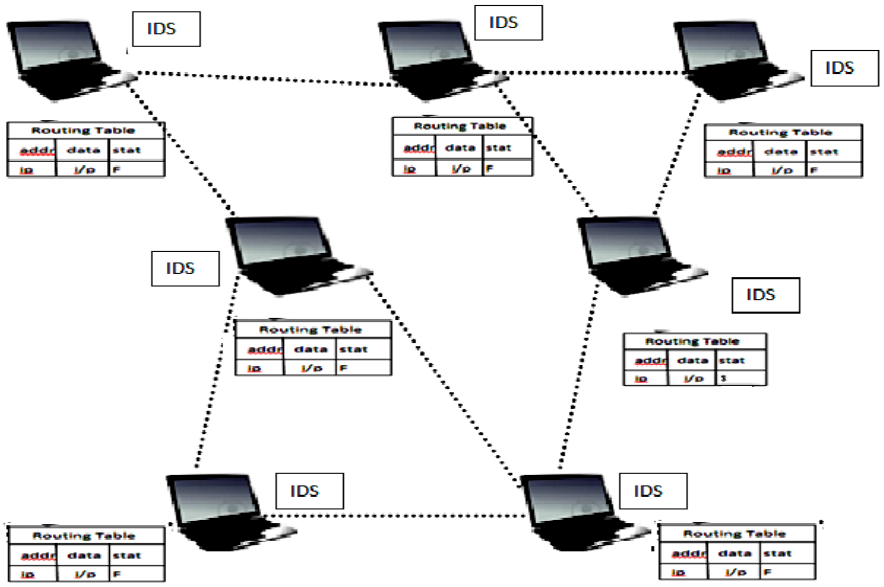

Fig. 1: System architecture

decide the path network do the packet transmition. After transmit the packet, the network do the divide and conquer strategy with the help of that strategy the network can identify the intruder. Based on the identification of intruder the network will suspect the DDoS DDoS intruder node after that suspect process network go with confirmation phase. Once, the confirmation is over network sends the alert message to entire node. Then route redirection can be taken place and source sending packet will reach to the appropriate destination.

Decide the path using AODV protocol: The Ad Hoc on demand distance vector (Perkins and Royer, 1999) is a routing protocol designed for ad hoc mobile networks. AODV is talented with both unicast and multicast routing. It is an on demand algorithm that meaning it builds routes between nodes only as favourite by source nodes. It maintains these routes as long as they are needed by the sources. AODV uses sequence numbers to guarantee the freshness of routes. It is loop-free, self-starting and scales to large numbers of mobile nodes.

AODV builds routes using a route request/route reply query cycle. When a source node desires a route to a destination, it checks if the route is already available or not if the route is available then it broadcast the packet through that route. Otherwise, the source node rebroadcast the route from the source to the destination. Nodes receiving this packet and update their information in the route tables. Routing table contains the source node's IP address, current sequence number and broadcast ID, the RREQ also contains the most recent sequence number for indicating the freshness or avoids the duplication.

As the RREP propagates back to the source, in the AODV protocols only propagate the Route Reply (RREP) through the reverse link. Once, the source node receives the RREP, it may starts to forward data packets to the appropriate destination. If the source later receives a RREP containing a same sequence number with a smaller hop count, it may update its routing information in the routing table for that destination and initiate to use the better route.

As long as the route remains active, it will continue to be maintained. For maintaining the route the AODV protocol using a technique is called route maintenance. According to the route maintenance technique if the source node moves from one location to another location then source node will again rebroadcast a new route from source to destination. If intermediate node or the destination node changes their location then its neighbour node will give a Route Error (RERR) message to the source node and the source node will reinitiate the route discovery process. If any unstable, weak or broken link is situated in the route then the intermediate node will give the RERR message to the source node. If the stranger or unknown node joins in the network then that node will broadcast a HELLO message to all the node participated

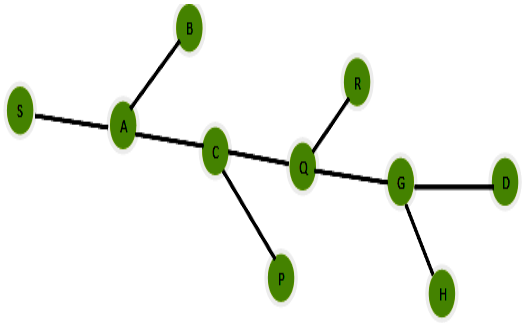

Fig. 2: Node S needs a route to D

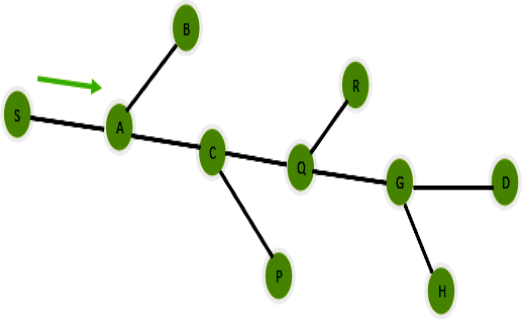

Fig. 3: Node S broadcasts RREQ to neighbours

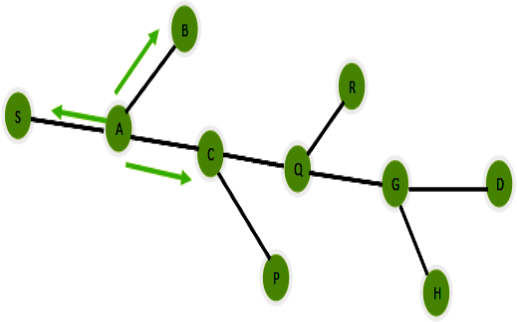

Fig. 4: Node c receives RREQ

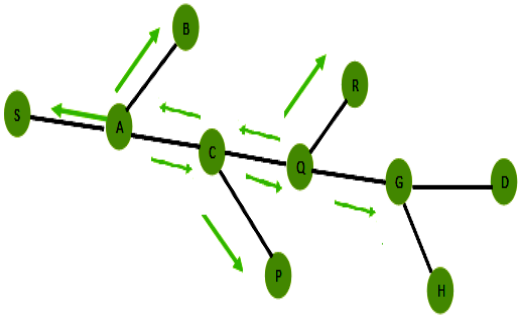

Fig. 5: NODE C broadcast RREQ and Q receive RREQbv

in the network. Figure 2 depict the router request generation from node S (Source) to D (Destination). S broad cast the router request to the neighbour A shown in Fig. 3, interns a forward the router request to C, until it reached to the destination D represented in Fig. 4. When

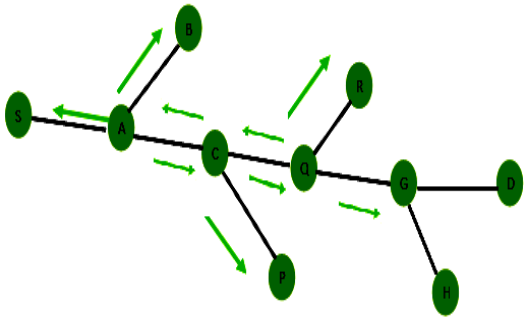

Fig. 6: Node Q broadcast RREQ and NODE G receive RREQ

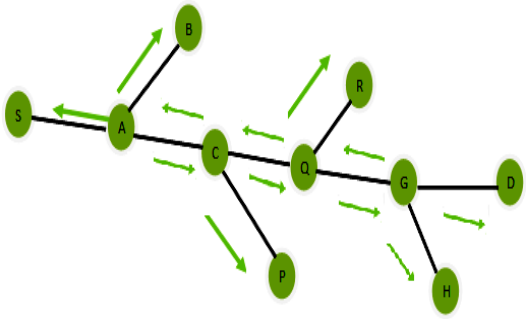

Fig. 7: NODE G broadcast RREQ and NODE D receive RREQ

D receives RREQ, it sends Router Reply RREP to the Source S shown in Fig. 5. This router reply forwarded via the same path Fig. 6 and 7.

Algorithm A; Steps used in route discovery

Node S needs a route to D
Creates a Route Request (RREQ):
Enters D's IP address, sequence
Number#, S's IP address, sequence
Number#, hop count (= 0)
Node S broadcasts RREQ to its
Neighbours.
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.
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.

Packet transmit: Sender 19 broadcasts a p-acket P to all its neighbours shown in Fig. 8. Each node receiving packet P and forwards packet P to its neighbours, sequence numbers help to avoid the duplication of packet. More over the sequence number helps to maintain the freshness of the packet flow. According to Fig. 8, Packet P reaches destination 4 provided that sent by the node 19 to

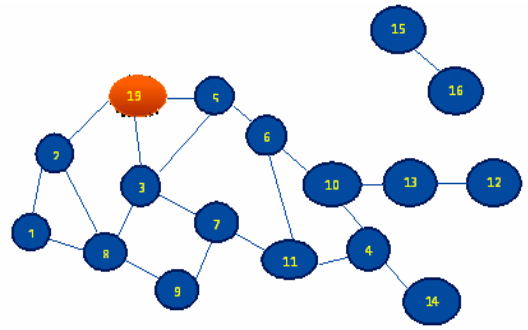

Fig. 8: Represents node that has received packet P

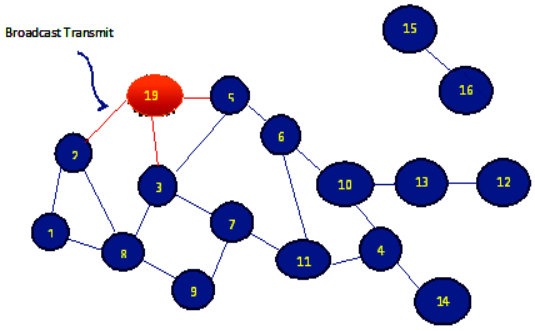

Fig. 9: Represents a node receives packet P for the first Time

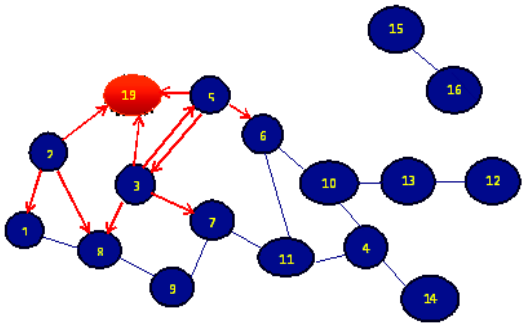

Fig. 10: Node H receives packet P from two neighbours

destination 4 shown in Fig. 9. Then destination 4 does not forward the packet. Because that, node 4 is the destination node.

Suppose node receives multiple copies of packets from the neighbour nodes like in Fig. 10. It forward only one copy to the next hop node. When I reached to the destination is called flooding represented in Fig. 11.

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 node

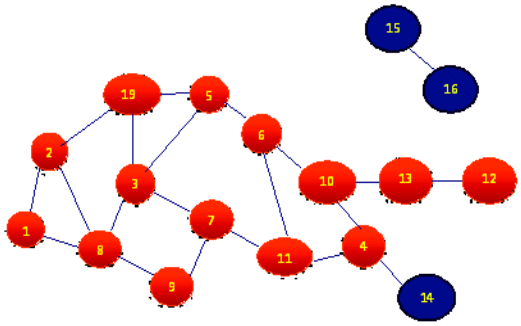

Fig.11: Flooding completed

and then it take the middle node that middle node will act as the temporary destination. Then, the packet can be transmitting from the source to the temporary destination. If the destination receives the packet then that node will not consider as a DDoS intruder. Else middle node consider as the destination do the middle node calculation again. And do the process, until identifying the DDoS intruder.

Alogrithm B: divide and conquer strategy:

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: 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
Other wise calculate the new middle for source to middle (Dest = middle)
Repeat the process
assume there is no flow of data then suspect the node may be the DDoS intruder. Process whether the middle node is DDoS intruder

Identify the DDoS intruder using AIHAODV: Using AIHAODV routing protocol divide and conquer strategy can be done. Based on this strategy, it can identify the DDoS intruder. DDoS intruder node can be stored or drop the packet from the network.

DDOS intruder suspect: According to the DDoS 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.

DDOS intruder confirmation: In this phase, DDoS intruder node is confirmed based on the identification phase as well as the suspect phase. It includes the phenomenon that source node send a packet to the suspect node for the confirmation process. In that time suspect node replied appropriate to the sender with in

time period as well as in the original reply then that suspected node is consider as good node, else that node will consider as the DDoS 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 give the reply message in proper time period (Algorithm C).

Algorithm C; Procedure (source, H, DDoS intruder)

Consider the ordered Set H = {1...M)

Step 1: Initialize source = 1, DDoS intruder = M
Step 3: If there is no RREP from DDoS intruder to source
confirm M is DDoS intruder
Else if there is False RREP from DDoS intruder to source and confirm M is DDoS intruder
Step 4: Otherwise the Node M is not a DDoS intruder node
Step 5: Stop

Send alert message: Once the node is confirmed that, suspect node as DDoS 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 DDoS intruder node id and ip address.

Route re-direction: Once the alert message sends to the entire node, again divide and conquers strategy process happen and redirection can be happen without passing with the DDoS intruder node. That route will make the direction to source the destination directly. For the same time the message or the packet can reach in the destination (Algorithm D).

Algorithm D; Procedure(Source, Dest, G, DDoS 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(DDoS 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

RESULTS AND DISCUSSION

Implementation phase

Decide the path using AODV protocol: This module is processed with discover the route by using the AODV protocol as in Fig 12. It can be done based on the route discovery and route maintenance, which includes route request and unicasting reply.

Packet transmit: This module is processed with packet transmition; the packet can be transmitting via the route which is discovered by AODV protocol as in Fig. 12. Packet transmitted as in Fig. 13. If the packet is reached properly to the destination, then it indicates that, the route is perfect and the route does not have any DDoS intruder. If packet loss or any delay for packet transition occurred it consider that the route have an DDoS intruder. Identification purposes we are transmitting dummy packet.

Establish the divide and conquer strategy: This module is processed under the strategy of divide and conquers; the packet can be transmit via the route which is discovered by AODV protocol as in Fig.12. It can be calculate the number of node in the route as in Fig. 14. It can send the packet to the destination. If the packet is not reached to

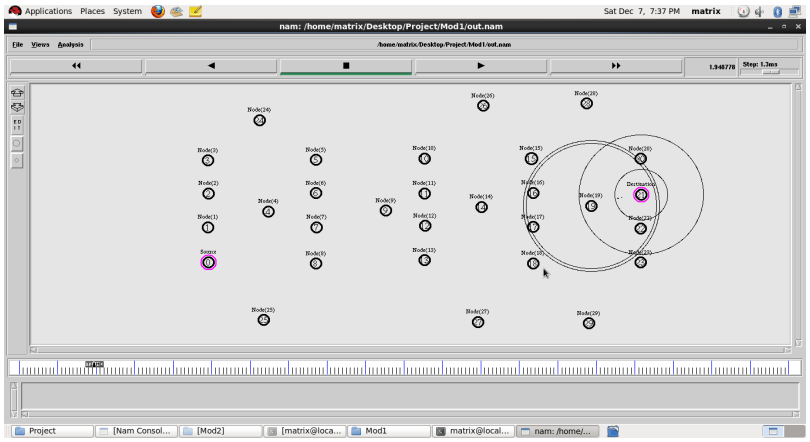

Fig. 12: Decide the path using AODV protocol

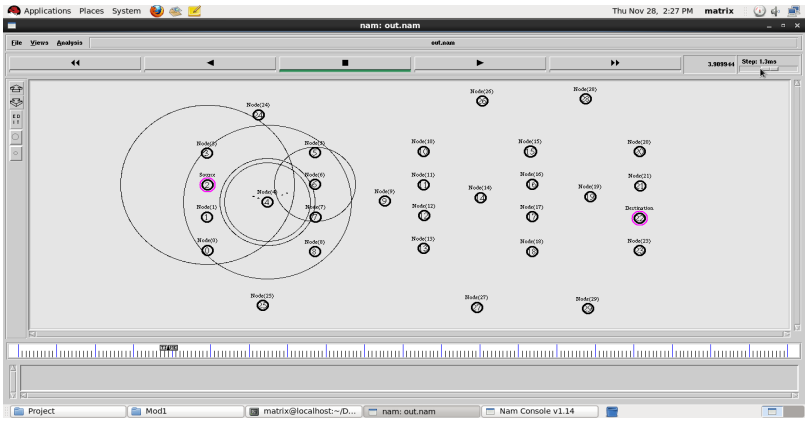

Fig. 13: Packet transmit

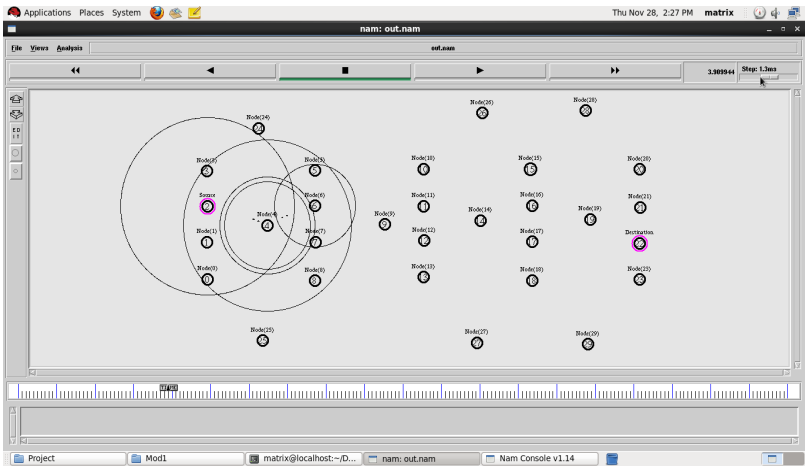

Fig. 14: Route discovery and number of node calculation

the destination, then the route is dividing and calculate middle node that node will act as the temporary destination as in Fig. 14. After a transmit ion that temporary destination receive the packet, then that node act as the temporary source. Continue the process until we got the idea of which node is an DDoS intruder, as in Fig. 15 and16

Identify the DdoS intruder using AIHAODV: This module is focused for DdoS intruder identification as in Fig. 17, using divide and conquer strategy.

DdoS intruder Suspect: This module is processed to help the DdoS intruder confirmation as a result of DDoS intruder identification. The result of the suspect module is reflected in confirmation phase. It shows in Fig. 18.

DDoS intruder confirmation: This module is processed with the basis of DDoS intruder suspect phase. DDoS intruder Confirmation is used to confirm the identified DDoS intruder is original DDoS intruder. The result of the confirmation phase is reflected in Fig. 19.

Send alert message: This module is processed with the basis of DdoS intruder confirmation phase. After using the confirmation phase, network send the DdoS intruder information to the entire node as well as it gives the updation to the routing table.

Route re-direct: This module is processed with the basis of DDoS intruder confirmation phase. After using the confirmation phase, source node will redirect the route to the destination. The message will reach to the destination send by the source through the new redirected route. This diagram representation is shown in Fig. 20.

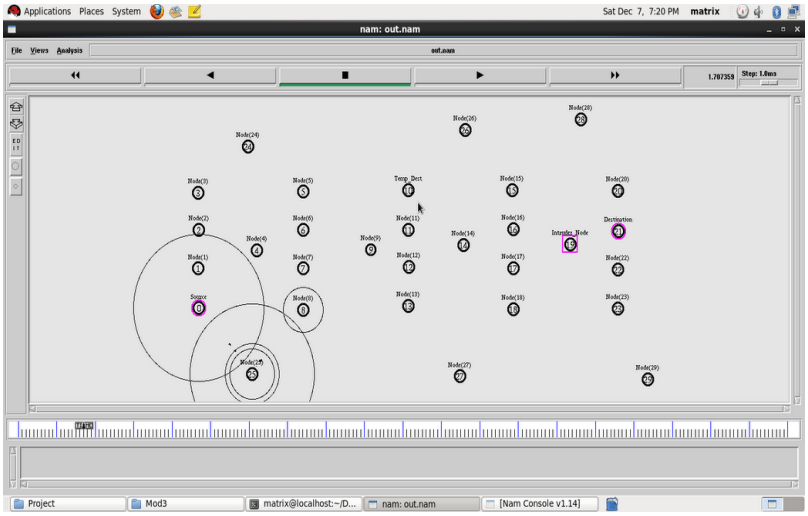

Fig. 15: Divide the route into two half

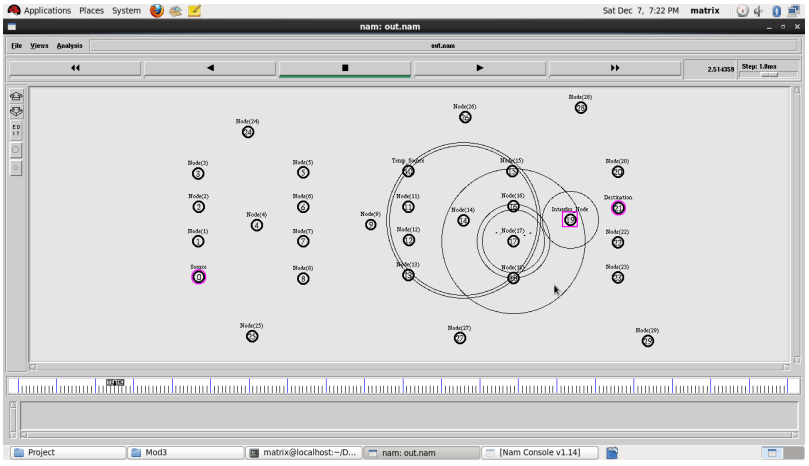

Fig. 16: Temporary destination becomes temporary source

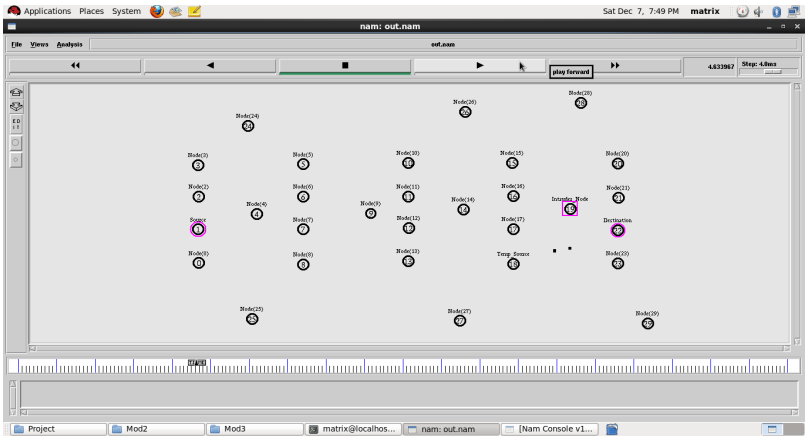

Fig. 17: DDoS intruder is identified

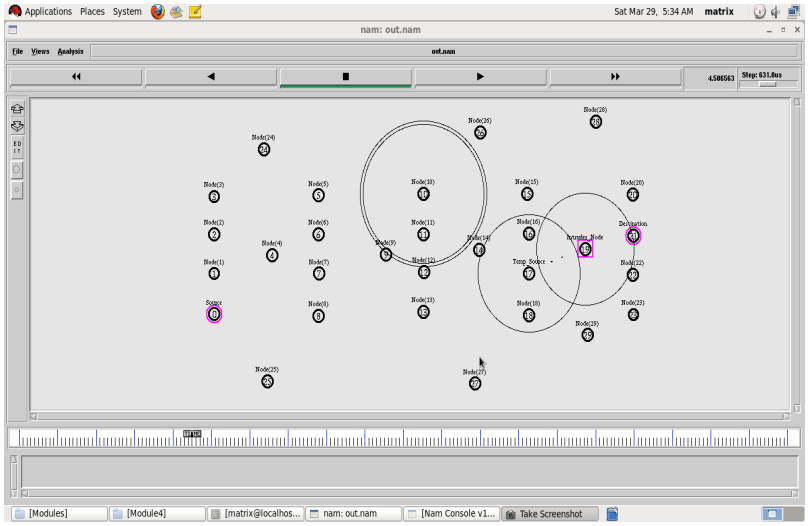

Fig. 18: DDoS intruder Suspect

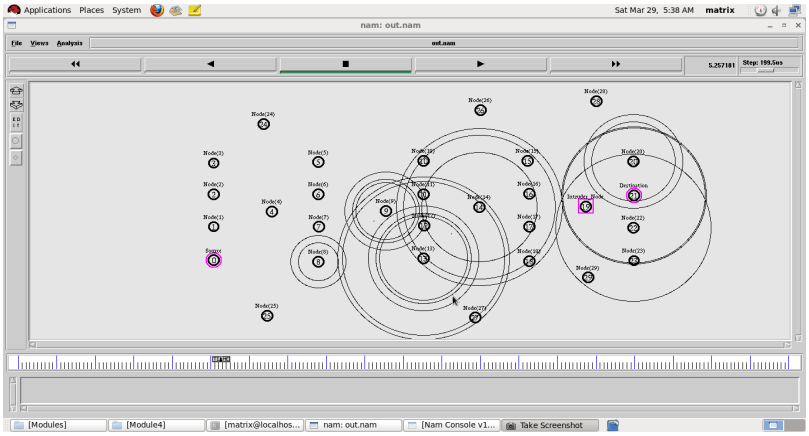

Fig. 19: Intruder confirmation

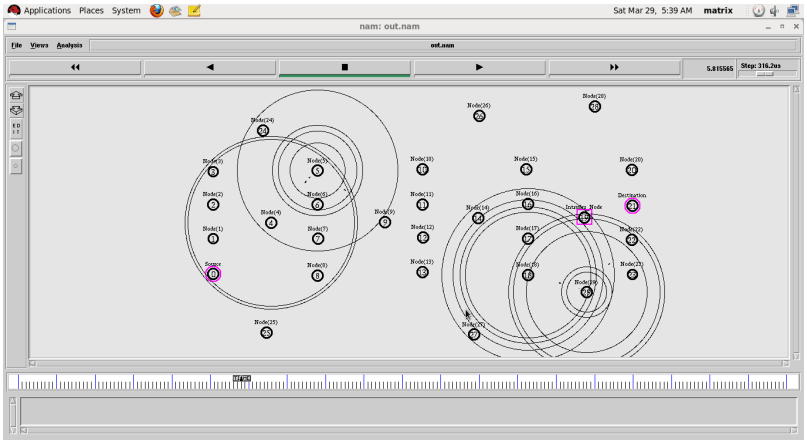

Fig.20: Route re-direct

CONCLUSION

In Mobile Ad hoc Network (MANET) is a self-configuring network that is created automatically by a group of mobile nodes without any help of fixed infrastructure or centralized organization. Each node is able to have a wireless transmitter and receiver, which allow it to communicate with other nodes help of radio communication range. Therefore, each node must act as both a host and a router at the same time. The network topology regularly changes due to the mobility of mobile nodes as they move within, move into, or move out of the network. Wireless networks that have become an essential to an everyday lives as they are more and more deployed in numerous applications. However, their growing esteem is challenged by insecure environment and characteristics of these networks. Moreover, in a truly ad-hoc wireless network domain, network services such as routing are provided by the nodes themselves. In such a scenario, a malicious entity can deny network services by dropping packets that need to be forwarded, by misrouting packets or by initiation other attacks. All these intrusion detection system have some collections of data set or the training set, they are performing based on the reference or experience, now introducing for improve the performance by using the AIHAODV routing protocol and it can be identify the DDoS intruder by using packet flow.

RECOMMENDATIONS

In the future, this proposed protocol will identify DDoS intruder node while transfer the packet from source to destination itself and do the redirection procedure in the same way it self. In future, this protocol will do the power and energy consumption along with no loss of performance.

REFERENCES

Bace, R., 1998. An introduction to intrusion detection and assessment. ICSA., Inc. http://www.iss.net/documents/whitepapers/intrusion.pdf.

Bace, R.G., 2000. Intrusion Detection. Sams Publishing, USA., ISBN: 1578701856, Pages: 339.

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

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

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

Perkins, C.E. and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing. Proceedings of the 2nd Workshop on Mobile Computing Systems and Applications, February 25-26, 1999, New Orleans, LA., pp: 90-100.

SANS Institute, 2001. Understanding intrusion detection systems. https://www.sans.org/reading-room/whitepapers/detection/understanding-intrusion-detection-systems-337.