Asian Journal of Information Technology 15 (6): 1023-1031, 2016
ISSN: 1682-3915

Thwart Distributed Denial of Service Attacks (DDOS) in Manet for Medical Image Transmission in Security Issue Hospital

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

Abstract: Mobile Ad hoc network is a collection of nodes which tries to communicate each other without any fixed infrastructure. In this network, nodes can move freely and dynamically from self-organized into arbitrary topologies. Due to self-organizing, the network is vulnerable to attack by distributed denial of service who attempts to gain unauthorized access and damage data on communication medium by denial the service. This research study focuses on medical hospital, which is relay on MANET topologies for transmitting of medical images. Transmitting of medical images from source to destination is one of the greatest challenges because the image should reach the destination without disturbances like delay, packet loss and disturbances from Denial of service attackers, intruder, etc. Adhoc On-Demand Distance vector protocol is designed for transmitting of medical images by finding a new route when it's needed. Even though this protocol is creating a path on demand, protocol functionalities has limitations on route redirection, security and energy consumption. This research study is working to develop an algorithm to identify the Denial of service attacks who is playing the role of delaying the packets to the next hop, so that the emergency medical images transmission is gets delayed, as well as achieving the denial of service in on time in the network. The algorithm uses directional antenna transmission to optimize the energy consumption as energy factor is an important challenge in MANET. The developed protocol is named as directional advanced intruder handling Ad hoc on demand distance vector protocol (directional advanced intruder handling ad hoc on demand distance vector). The algorithm are simulated in NS2 and compared with Ad hoc on demand distance vector protocol. The result of analysis shown, proposed research algorithms performed 50% better than AODV protocol.

Key words: MANET, denial of service attacker, failure node, divide and conquer, directional antenna

INTRODUCTION

A Collection of nodes formed a network under the working principles of move freely, organized themselves arbitrarily and without any administration is called Mobile Ad-hoc network. In a common, a route between the source to destination through the Ad-hoc network is established by the routing protocol. The packets have followed this route to transfer the data. Packets are moved from a node to another node called the hop, until to reach the destination.

Mobile Ad Hoc Network (MANET) is assortment of Multi-hop wireless movable nodes that correspond with each other without central control or recognized infrastructure. Nodes in this network can move freely, so this network is more prone to error. The MANET architecture with three nodes communication as shown in Fig. 1. As a result, routing in MANET is a Critical task due to highly dynamic of mobile environment. In recent years, numerous routing protocols have been proposed for mobile ad hoc Networks and outstanding among them are DSR, AODV and TORA.

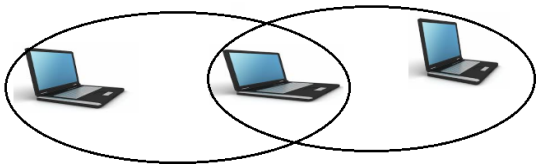

Fig. 1: The MANET

Challenges in MANET: A Mobile Ad Hoc Network (MANET) is a gathering of wireless mobile nodes form a momentary network without any fixed infrastructure. All the node are configured among them to move freely. Every node is capable of performing dual role as a router and host. This natural history of MANET leads to come across the challenges are:

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

- Dynamic network topology
- Frequency of updates or Network overhead
- Energy efficient/Power aware routing
- Secure routing

This research article is developed to provide solution for dynamic topological challenges due to failure, identify black hole attacker node and directional antenna transmission used for energy optimization.

Literature review: A Routing protocol in an Ad-hoc network is divided into two main categories of proactive and reactive protocol. In proactive protocol nodes maintain routing information for all other nodes in the network and it is stored in routing table. So this protocol is also named as a table driven protocol. In reactive protocol, route information is established when a packet is transferred between the nodes. In the table driven protocol is classified into different types Destination Sequenced Distance Vector routing (DSDV), Cluster Gateway Switch Routing protocol (CGSR), Optimization link state routing protocol, Topology dissemination Based on Reverse Path (TBRPF), Fish Eye state Routing protocol (FSR). In source initiated routing protocols are classified into different types of protocols such as Ad-hoc On-Demand Distance Vector (AODV) (Perkins and Royer 1999), Dynamic source routing protocol (DSR). In Dynamic Source Routing Protocol each node maintains a route cache contains a route learned by the node. Source node only initiates route discovery process enters into a route cache continuously updated. AODV node creates a route on demand to maintain a complete a route using DSDV algorithm. TORA is another source initiated on Demand protocol, in a concept of link reversal of directed Acyclic Graph. TORA has the capacity of routing repair. ABR routing protocol (Giannoulis *et al*., 2005) is on demand protocol route selection is based on the signal strength in the link.

Intruder detection is a one of the challenges in MANET (Anantvalee and Wu, 2007; Stamouli *et al*., 2005; Denning, 1987; Zhang and Lee, 2000). Different methodologies were proposed for identifying an intruder in MANET from the year 2001-2003, these methodologies were based on the technique of Knowledge-based intrusion detection (Anjum *et al*., 2003) signature based intruder detection, sensor based intruder detection (Kachirski and Guha, 2003), anomaly based intruder detection (Islam and Rahman, 2011) collaborative intruder detection (Marchang and Datta, 2008)and zone based intruder detections (Sun *et al*., 2003). Identification of an intruder was done by defining architecture in MANET during the year 2005 to 2007, based on corporative based intruder detection architecture and RIDAN architecture was developed. Different types of MANET attacks were identified using attacks detection techniques (Rajaram and Ranjana, 2007), warm hole attacks, critical node identification (Karygiannis *et al*., 2006; Rajaram and Palaniswami, 2010), fabrication attacks (Rajaram and Ranjana, 2007), consumption attacks, packet dropping attacks, black whole attacks were detected based on attack detection techniques. The gain (gd) of the any antenna can be defined as the product between the directivity and efficiency:

$$g_d = \eta G_d$$

When gt transmission gain of the directional antenna; Gr is a reception gain; And go is a omni-directional gain. From the property of directional antennas: gt ≥ g0; gr ≥ g0, gain is expressed in terms of decibels (dB). If g is any given gains and the equivalent gain in decibels(g_{db}) is given by:

$$g_{db} = 10 \log_{10} g$$

DdoS attacks are targeted at exhausting the victim's resources such as computing power, network band width and operating system data structures. To establish a DDoS attack, initially the attacker creates a network of computers that will be utilized to make the huge volume of traffic required to deny services to authentic users of the victim. In order to generate this attack network, the attackers identify the vulnerable hosts on the network. The vulnerable hosts are either running no antivirus or out-of-date antivirus software, or have not been correctly patched. These are explored by the attackers who utilize the vulnerability to control the access to these hosts. The next process for the attacker is to set up new programs (known as attack tools) on the compromised hosts of the attack network. The hosts which are running these attack tools are called as zombies and they can be utilized to carry out any attack under the control of the attacker host. Many zombies together form an army or botnet. In this research, a new technique called energy point analysis is used to detect DDoS attacks.

From the above literature survey, the routing protocol only performs routing the packets, none of the protocols have been proposed for identifying a denial of sevice attack in the Mobile Ad hoc network. There is need for an algorithm for efficient delivery of packet to the destination. In this research AODV protocol is modified for efficient packet delivery. Performances of AODV modified algorithms are compared with AODV and simulation results depict that proposed algorithms out performs existing AODV.

MATERIALS AND METHODS

A novel protocol is designed and implemented that incorporates identifying failure node and black hole attacker with directional antenna transmission. This algorithm is implemented by modifying existing AODV protocol as AODV lacks ability to identify failure nodes and black hole attacker nodes. The algorithm is further improved for power optimization using directional antenna transmission.

Methodology used

Divide and conquer: Divide and conquer is a recursive algorithm and it is used to give solution to a problem by working through divide the problem in to two or more sub problem. The final solution of sub problem gives solution to the original problem give solution.

There are five main steps for a divide and conquer solution:

- Step 1: Define your recursive sub-problem.
- Step 2: Define your base cases.
- Step 3: Present your recursive cases.

Common Running Times Let T (n) denote the running time of your algorithm on input of size n:
If $T(n) = 2T(n/2) + O(n)$ and $T(1) \in O(1)$ then $T(n) \in O(n \log n)$.

In this thesis is defined to used Divide and Conquer strategy on the packet acknowledgement for finding out Failure node and Intruder node in MANET. So the above five major steps are defined as:

Step 1: Recursive sub problem: Calculate the number of hops between the needed nodes. The number hop between the nodes is divided by two. Finding out the middle node.

Step 2: Define base cases: Case 1: Check whether the acknowledgement received from the middle node

If (Yes)

Conclude Up to the beginning to middle node packet is forwarded.

Else if (Process middle node is a failure node)

Else (Find out the new middle and repeat the process)

Step 3: Present your recursive cases Case 2: If middle node received Acknowledgment

Take the second half Check the acknowledgment received from middle node go to Step 1.

Case 3: If consecutive more than one nodes acknowledgement is not received for example I, j, k…, etc.,

Check whether the previous node of first consecutive node forwarded the packet, then conform failure node is first i node by checking following stages:

- Send router request to the acknowledgement missing nodes
- Select the failure node which router reply is not received
- If more than one Router reply missing go to (i)
- More than two chances router reply missing conform all the missing node as a failure node

Algorithm for identifying failure node:

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 whether the packet is passed through the middle node.
If (yes)
Calculate the new middle node from the middle node to the destination then go to step 2.
Else
Calculate the middle node from source node to middle node then go to step 2.
Repeat the process.
If there is no flow of data then the node may be Victim or failure node.
Process whether the middle node is victim node
If True Set Victim = Middle and initiate route discovery process.
Step 4: Process to confirm Victim node
Send route request to the Victim node.
If there is no reply then confirm Victim node.
Step 5: Process to retransmit the data through stage 1.
Step 6: Send alert message about the Victim node or failure node .
Step 7: Stop.

Algorithm for identifying black hole attacker node:

Algorithm is designed for identify an black hole attacker in the MANET by adding two more stages in algorithm of failure node identification
Procedure (Source, Dest, G)
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 whether the packet is passed through the middle node
If (yes)
Calculate the new middle node from the middle node to the destination then goto step 2
Else
Calculate the middle node from source node to middle node then go to step 2
Repeat the process
If there is no flow of data then the node may be the black hole attacker or failure node.
Process whether the middle node is black hole attacker.
If True Set attacker = Middle and initiate route discovery process.
Step 4: Process to confirm node is a black hole attacker.
Send route request to the black hole attacker node.
If there is a reply then confirm as an attacker node
Otherwise node may be the failure node.
Step 5: Process to retransmit the data through stage 1.
Step 6: Send alert message about the Intruder node.
Step 7: Stop.

Probability of failure node and attacker node: When a packet is transferred from source node to a destination node, the probability of exhasive event is whether to get the failed node or link failed node:

Probabilityof failed node = No. of failed node/
Total number of nodes

Where:
M = Number of failed node (absolutely failed node is 1)
N = A total number of nodes

The probability of failed node f = M/N:

$$f = 1/N$$

The probability of failed node is denoted by f and the probability of not failed node is denoted by a. Then:

$$N\text{-}1 = (N\text{-}m)$$

Where:
N = Total number of nodes
1 = No. of Failed nodes
N-m = No. of cases the event will not happen to failure
m = 1
N-1 = N-1

From Eq. 1:

$$a = (N\text{-}m)/N$$

Where:
a = (N/N)- (m/N)
m = 1
a = 1-(1/N)
a = Probability of not failed node
N-m = number of node which can not failed
N = Total number of node
a = 1-f
a+f = 1

Hence, $0 \leq f \leq 1$ and $0 \leq a \leq 1$. When a packet is transferred from source node to a destination node, the probability of exhasive event is whether to get the black hole attacker .

Probability of black hole attacker = No. of black hole attacker node/
Total number of nodes

b = The number of black hole attacker (absolutely failed node
1 = The one black hole attacker is possible to find
N = The total number of nodes

Then, the probability of black hole attacker node bf= b/N:

$$bf = 1/N \quad (2)$$

The probability of black hole attacker node is denoted by bf and the probability of not black hole attacker node is denoted by nb. Then:

$$N - 1 = (N\text{-}b)$$

Where:
N = Total number of nodes
1 = No. of black hole attacker nodes
N-b = No. of cases event not happen black hole attacker
m = 1
N-1 = N-1

From Eq. 2:

$$nb = (N\text{-}m)/N$$

Where:
nb = (N/N)-(m/N)
m = 1
nb = 1-(1/N)
nb = Probability of not black hole attacker node
N-m = No. of node which can not black hole attacker
N = Total number of node

nb = 1-bfnb+bf = 1.hence 0= bf =1 and 0 = nb = 1

Directional Advanced Intruder Handling Adhoc On-Demand Distance Vector (DAIHAODV) protocol design: The stages of failure node and Denial of service attacker identification of Directional Advanced Intruder Handling AODV (AIHAODV) protocol design stages are as follows:

- Decide the path using AODV protocol
- Transmit Packet
- Apply algorithm for Identify failure or attacker node
- Suspect the Denial of service attacker node
- Confirm the Denial of service attacker node
- Route redirection
- Send alert message to other nodes about intruder

The algorithm design stages are implemented using NS2 with following simulation set up. AODV protocol is taken for adding the algorithm features. Simulation is done with directional antenna transmission and Omni antenna transmission to prove the comparison result of energy efficiency (Table 1).

Table 1: Parameter of the simulation

Channel type	Wireless channel
Radio propagation model	Two Ray Ground
Antenna type	Omni Antenna/ Directional
Interface queue type	Drop Tail /Pri Queue
Maximum packet in queue	50
Network interface type	Phy/Wireless Phy
MAC type	802_11
Topographical area	500 X 300 sq.m
txpower	0.5W
rxpower	0.1W
idlepower	0.01W
Initial energy of a node	1000.0 Joules
Routing protocol	AODV
Number of mobile nodes	10, 20,30,40,50,60,70,80
Mobility	0 or 20m/s

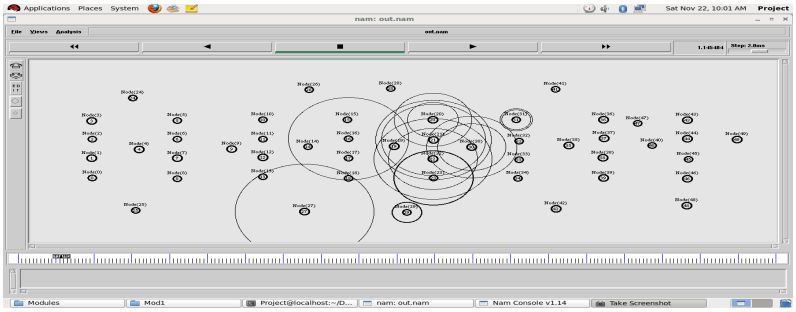

Fig. 2: Decide the path

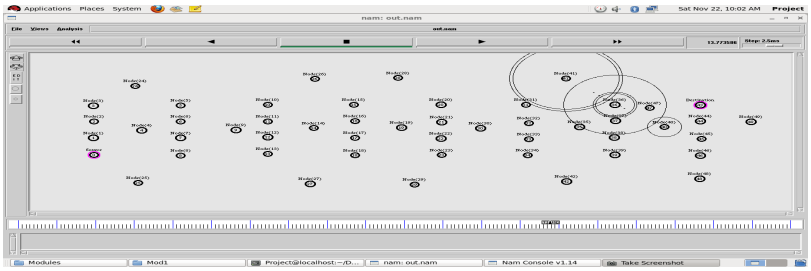

Fig. 3: Packet transmit

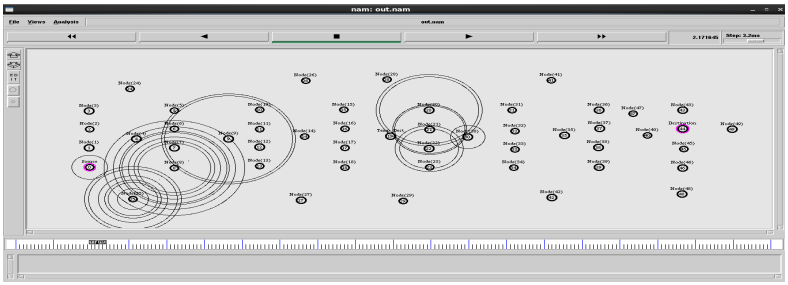

Fig.4: Send alert message about failure node/black hole attacker node

Decide the path using AODV protocol: In this stage, existing AODV protocol is used to identify route between source node to the destination node. Source node wants to transmit the packet to the destination, it send Router Request to all the nodes. Upon receiving a router Reply from black hole attacker who role is sending the a router reply to the requested node. Router Request in NS2 is shown in Fig. 2.

Transmit packet: Once the path is identified between source to destination using AODV protocol, source node starts sending packet to the destination node through the identified path. Packet transmission in NS2 is shown in Fig.3.

Apply algorithm for identifying failure and Denial of Service attacker node

Suspect the node as an attacker: In this stage, identify the whether any node is not forwarding the packet to the next hope is noted as a suspected node and it brought in to surveillance. All the activity about that node will be noted and recorded. The alert message will not be sent to the node is confirmed as a black hole attacker.

Confirmation of attacker node: In this stage, source node sends a RREQ to the suspected node, If there is no RREP from suspected node to source then confirm suspect node is attacker node and if there is False RREP from intruder to source then confirm node is black hole attacker. Otherwise the Node is failure node.

Route re-direction: The source node discovers new route to retransmit the packets when the node is identified a black hole attacker or failure node.

Send alert message: Once a suspect node is confirmed as a black hole attacker or failure node, the source node will send the alert message to the other node in the entire network. Sending alert message is shown below Fig. 4.

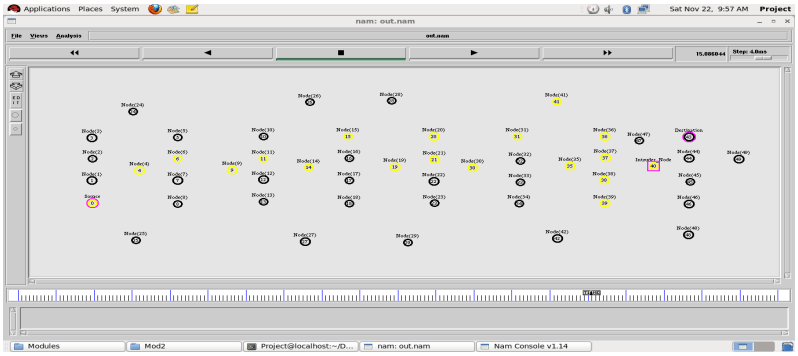

Fig. 5: Power status

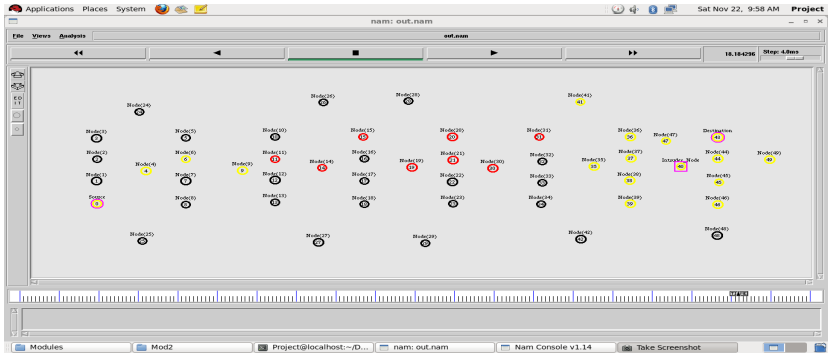

Fig. 6: Description of power status

Power identification: From the above output screen the yellow circled nodes are having residual power after identification of the black hole attacker node 40. Here, packet transmission is ba sed on the Omni-Directional Antenna. Power status is shown in Fig. 5 and 6.

From the above output screen the yellow circled nodes are having residual power after identification of the black hole attacker node. The Red circled nodes are having no power after identification of the black hole attacker node. Here, packet transmission is based on the Omni-Directional Antenna and Directional antenna.

RESULTS AND DISCUSSION

NS2 is used to simulate and compare the results with AODV. Three performance parameters such as throughput (rate of packet delivered successfully through medium), packet delivery ratio (packet send/packet received), End to End delay (total time taken/connections in channel)are considered for comparison. The algorithm is implemented in antenna transmission of Omni and directional antenna. Transmission in Omni antenna transmission performance measures are named as AIHADOV protocol for comparison. The simulation results depict that proposed DAIHADOV protocol better in all aspects. The result simulations shown in Fig. 7-9.

Packet delivery ratio: The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination:

$$\Sigma \text{ Number of packet receive} / \Sigma \text{ Number of packet send}$$

The average time taken by data a packet to arrives 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:

$$\Sigma \text{ (arrive time} - \text{send time)} / \Sigma \text{ Number of connections}$$

The AIHAODV algorithm is further modified for optimization of congestion in traffic, delay and power consumption using directional antenna transmission. NS2 is used to simulate and compare the results with AODV and AIHAODV directional transmission and Omni antenna transmission. The performance parameters are b ased on energy consumption and residual energy. The simulation results depict that

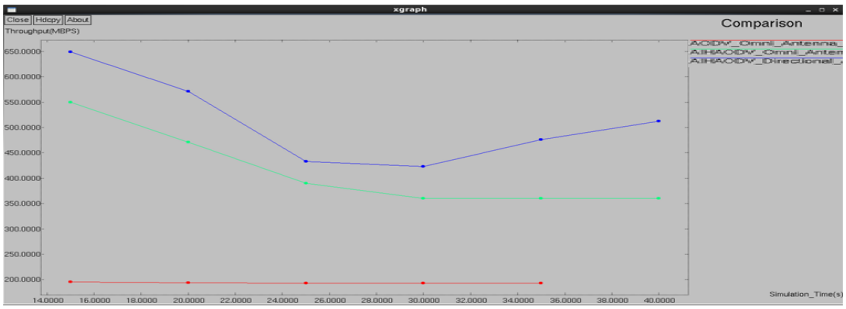

Fig. 7: Through put

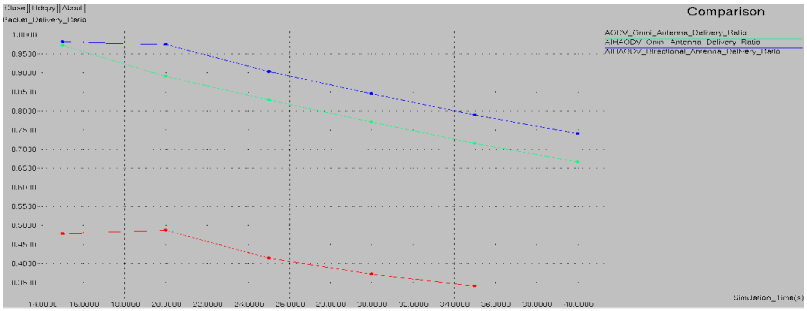

Fig.8: Packet delivery ratio

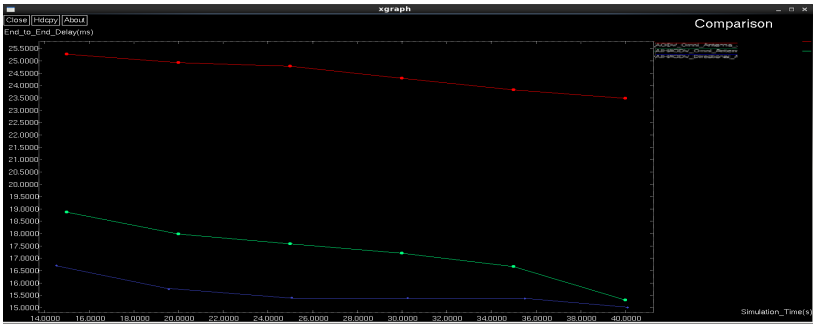

Fig. 9: End to end delay

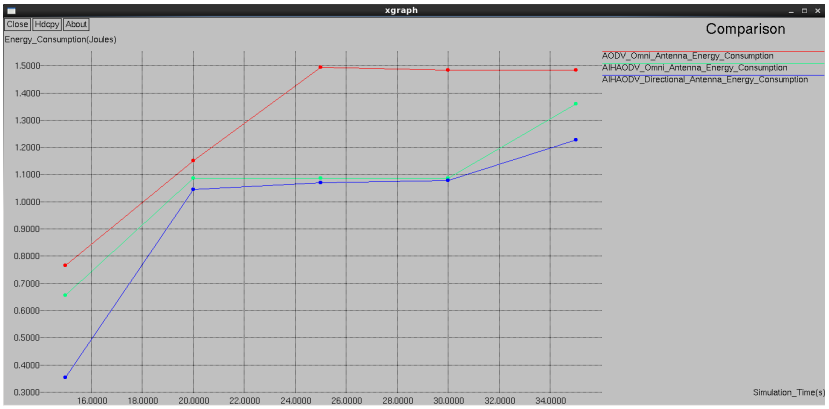

Fig. 10: Energy consumption

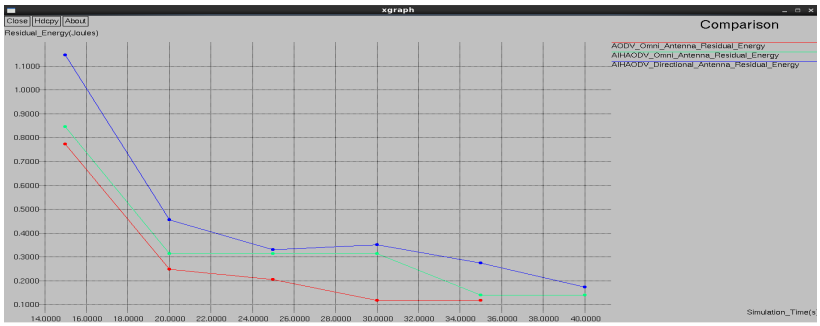

Fig. 11: Residual energy

proposed DAIHADOV algorithm better in all aspects. The result simulations are shown in Fig. 10 and 11.

CONCLUSION

An Adhoc network is a combination of different nodes, created for communicating each other without any infrastructure. Transmitting of packet from source to destination is one of the greatest challenges because the packet should reach the destination without disturbances like delay, packet loss and security breach. Adhoc On-Demand Distance vector protocol is designed for transmitting packet by finding a new route when it's needed. Even though, this protocol is creating a path on demand, protocol functionality limits on route redirection, security and energy consumption.

AAODV algorithm designed to identify failure node overcome it limitation of reliable packet delivery. Simulation results show that the algorithm performs better than exiting AODV.

DAIHAODV algorithm modified AODV algorithm in safer delivery of packets when nodes are under threats by an DDoS attackers. Comparative analysis with existing algorithm shows the modified algorithm proves better. Efficient energy consumption show that DAIHAODV outperforms existing AODV algorithm. The Proposed research articles modifies an existing AODV protocol and gives solution to identify failure and attacker node in MANET with directional antenna transmission. The proposed algorithms are simulated by ns2 and outperform the existing ADOV.

REFERENCES

Anantvalee, T. and J. Wu, 2007. A Survey on Intrusion Detection in Mobile Ad Hoc Networks. In: Wireless Network Security, Xiao, Y., X. Shen and D.Z. Du (Eds.). Springer, New York, ISBN: 9780387331126, pp: 159-180.

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.

Denning, D.E., 1987. An intrusion-detection model. IEEE Trans. Software Eng., SE-13: 222-232.

Giannoulis, S., C. Antonopoulos, E. Topalis and S. Koubias, 2005. ZRP versus DSR and TORA: A comprehensive survey on ZRP performance. Proceedings of the 10th IEEE Conference on Emerging Technologies and Factory Automation, Volume 1, September 19-22, 2005, Catania, Italy -.

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 -.

Karygiannis, A., E. Antonakakis and A. Apostolopoulos, 2006. Detecting critical nodes for MANET intrusion detection systems. Proceedings of the 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, June 29-29, 2006, Lyon, France -.

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

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.

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

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

Stamouli, I., P.G. Argyroudis and H. Tewari, 2005. Real-time intrusion detection for ad hoc networks. Proceedings of the 6th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, June 13-16, 2005, Taormina, Italy, pp: 374-380.

Sun, B., K. Wu and U.W. Pooch, 2003. Zone-based intrusion detection for mobile ad hoc networks. Int. J. Ad Hoc Sensor Wireless Networks, Vol. 2, No. 3.

Zhang, G.Y. and W. Lee, 2000. Intrusion detection in wireless ad-hoc networks. Proceedings of the 6th International Conference on Mobile Computing and Networking, August 6-11, 2000, Boston, MA., USA., pp: 275-283.