ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Indentifying Link Failure Attack in Distributed Denial of Service inside Mobile Ad-hoc Network

[1]P.C.Senthil Mahesh and [2]Dr.Paul Rogrigues, [3]S. Hemalatha

[1]*ResearchScholar,Annauniversity,Chennai, Tamil Nadu*
[2]*Principal,DMI college of engineering*
[3]*Associate Professor /CSE, Sri Lakshmi Ammaal Engineering College*

ARTICLE INFO

Article history:
Received 10 March 2015
Received 20 in revised form
March 2015
Accepted 25 March 2015
Available online 10 April 2015

Keywords:
MANET, AODV, DDoS ,Link Failure Attacker

ABSTRACT

Distributed denial of Service (DDoS) is kind of attack, which performing the role of degrading the performance in the network. Several types of DDoS attacks can be done in the server side and client side. Now a day the DDoS attack is slowly mitigating form LAN, WAN to temporarily networks like MANET. There are different types of DDoS attack in MANET. One of the attacks is link failure attack. Due to nature of the MANET, nodes can move that places dynamically, this causes the failure the link in the MANET. This limitation is taken into account for generating the link failure attack in MANET. This research article is defined to identify such a attacker node in MANET. The simulation is done in AODV protocol using Network simulator and compared with the existing AODV protocol. The result shown that,the performance of packet delivery ratio is increased and packet transmission energy is reduced.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: P.C.Senthil Mahesh and Dr.Paul Rogrigues, S. Hemalatha., Indentifying Link Failure Attack in Distributed Denial of Service inside Mobile Ad-hoc Network. ***Aust. J. Basic & Appl. Sci.,*** *9(11): 594-599, 2015*

INTRODUCTION

An ad hoc network is a temporary network connection created for a specific purpose. An ad-hoc network is as like LAN that is built spontaneously for devices communication. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other.

Invention of Ad-hoc network is developed from packet radio network over three generations. In the first generation before the year 1972, network was called PRNET (Packet Radio Network).when the development of packet switching radio communication, the real invention of computer communication in mobile environment was developed by the research Defence Advanced Research Projects Agency (DARPA) in 1972.

Later in the second generation improvement in the radio performance makes smallest, cheapest packet switching network was implemented by SURAN (Survivable Adaptive Radio Networks) research in 1980.

In the 1990s, the formal model of ad hoc networks is defined with nodes; with battery power arrived and nodes in the network are allowed to move freely while participating in the network, all come in handheld computers and other small portable communication equipments.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger network. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

Anad hoc network is a decentralized type of wireless network which does not rely on any pre-existing infrastructure, like a routers in wired networks or Access points in managed wireless networks. But each node relay on the principle of forwarding data for other nodes, so ad hoc networks can use flooding for forwarding data.

An ad hoc network is made up of multiple “nodes” connected by “links.”Links are influenced by the node's resources like transmitter power, computing power and memory and behavioural properties like reliability as well as link properties like length-of-link and signal loss, interference and noise. Since links can be connected or disconnected at any time, a functioning network must be able to cope with this dynamic restructuring, preferably in a way that is timely, efficient, reliable, robust, and

Corresponding Author: P.C.Senthil Mahesh, ResearchScholar, Annauniversity,Chennai, Tamil Nadu
E-mail: senthilmagesh@gmail.com

scalable. The network must allow any two nodes to communicate by relaying the information via other nodes. A "path" is a series of links that connects two nodes. Various routing methods use one or two paths between any two nodes; flooding methods use all or most of the available paths. An Ad hoc network is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires.

Palmieri *et al*. (2011) In computer and computer networks an attack is attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or makes unauthorized use of an asset.

The goal of a denial of service attack is to deny legitimate users access to a particular resource. Anincident is considered an attack if a malicious user intentionally disrupts service to a computer or network resource. Resource exhaustion (consume all bandwidth, diskspace).

Ricciardi *et al*. (2011) Distributed Denial-of-Service attack (DDoS attack) is a try to make a machineor network resource inaccessible to its deliberate users. It causes to the Internet temporarily or frequently disturb or interrupt services by sending the continues request. Denial-of-service attacks are deliberatedbreaches the architecture of internet and it also violatethe acceptable use policies Internet service providers.

Stephen and Ruby (2003) DDoS attacks canseriously damage the Internet service. In late June andearly July of 1999 the first DDoS attack was observed.In August 1999 the first well-documented DDoS attackoccurred, when a DDoS tool called Trinoo wasorganized in at least 227 systems, of which at least 114were on Internet2, to flood a single University ofMinnesota computer; this system was cracked off theair for more than two days. In February 2000 the firstwell-DDoS attack was publicized in the public press.

On February 7, Yahoo! Internet portal was unreachablefor three hours because of DDoS.During this attackYahoo was down, it suffered a loss of e-commerce andmarketing revenue that amounted to about $50,000.(Carl *et al*., 2006) During the DDoS attacks, Buy.comwent down from 100% availability to 9.4% and alsoCNN.com's client went down to below 10% of normalvalue. The downtime loss was huge (Bellovin *et al*.,2001).

Malan *et al*. (2000) websites of Google, Yahoo andMicrosoft was affected by DDoS attack on June 2004,vanished for hours when their servers were saturatedwith thousands of simultaneous webpage requests thatthey could not handle request. These webpage requestsare from botnet which consists of thousands of infectedmachines. Before the attack, the attacker tried to scanthe Internet to find out the vulnerable machines and fixthe bot on those machines. Internet relay chat rooms areused for communication between the attacker and thosezombie machines. After the attacker issued the attackcommand in an Internet relay chat room, the botnet startto generate a large number of web requests which bringdown the victim websites. These kinds of botnets areincreasing a crime wave against e-commerce.

1. Literature Review:

Distributed Denial of Service attacks in MANET is classified in to external and internal attack, which is based on the attack carried out by the nodes are belongs to the internal or external node. External attack is created by the nodes which is not belongs to the MANET. This attacker node sends false routing information which causes the unavailability of service. Internal attacks is created by the node which is belongs to the MANET nodes.This attacker also sendsfalse information about the route and makes the unavailability of services.

Denial of Service attack:

This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.

Impersonation:

If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.

Eavesdropping:

This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

Routing Attacks:

The malicious node make routing services a target because it's an important service in MANETs. There are two types in routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.

Black hole Attack:

In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one.

Wormhole Attack:

In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole.

Replay Attack:

An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

Man- in- the- middle attack:

An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

Gray-hole attack:

This attack is also known as routing misbehaviour attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

Problem Definition:

In the literature review, reveals that, there are different types of DDoS attacks in MANET, these attacks reduces the nodes services like energy, jamming, disruption in route and intercepts the packets etc.It is possible to create another type of attack in MANET, where the attacker node sends the route information to other network nodes.When the attacker nodes receive a router reply and it dynamically changes the position of the node to other region. This causes the link failure on the route between source to destination. This type of attack is named as Link failure attack in MANET. Due to link failure attack, packet transmission and energy utilization of the nodes from the source to destination is reduced. For identify the link failure attacker node, link failure identification attack algorithm is defined. This algorithm is an enhancement of [9]

Link Failure Attacker algorithm

Procedure(Source, Dest, G) -

Consider the ordered Set G={1……..N} .

Step 1: Initialize source = 1, dest = N .thresholdcount = 0

Step 2:Generate the route request by the source.

Step 3: if (Router reply gets by the source)

Start sending of packet to destination

Find any route failure

Step 4:if (route failure)

Increment threshold count by one for a link failed node.

Check the threshold count is in frequent and reaches the limit (say 3) for a suspected node.

Else goto step 2

Step 5:Send alert message about the link failure attacker node.

Step 7: Stop.

Implementation:

This proposed Link failure algorithm is implemented in AODV protocol using network simulator. Simulation is done with Omniantenna transmission .The simulation parameter taken for consideration is shown below.

Parameter of The Simulation:

Channel Type	Wireless Channel
Radio Propagation Model	Two Ray Ground
Antenna type	Omni Antenna
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 800 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	40,50,60
Mobility	0 or 20m/s

Sending router Request by the source:

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 link failure attacker whose role is sending aroute information to the source node.

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.

Apply Link failure attack algorithm:

In this stage, identify the whether any link failure node in the MANET .If any link failure node

Australian Journal of Basic and Applied Sciences, 9(11) May 2015, Pages: 594-599

appears, then the threshold count of the link failure is incremented by one. The source node sends a router request to all other nodes. All the activity about that node will be noted and recorded. The alert message will not be send until the node is confirmed as a link failure attacker node.The node performs a frequent link failure ,then the node is confirmed as link failure attacker node.

Send Alert Message:

Once a link failure attacker node is identified, the source node will send the alert message to the other node in the entire network.

Result:

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), and End to End delay (total time taken /connections in channel)are considered for comparison. The algorithm is implemented in antenna transmission of Omni antenna. Transmission. Energy utilization and residual energy is calculated and compared with AODV protocol.

Fig1. Through Put is shown below.

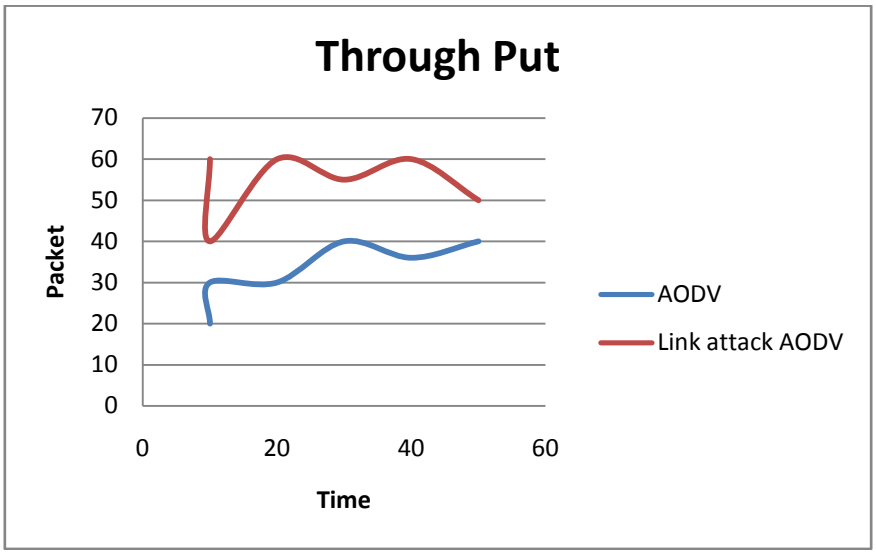

Fig. 1: Throughput

Packet Delivery Ratio is defined as The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

∑ Number of packet receive / ∑ Number of packet send

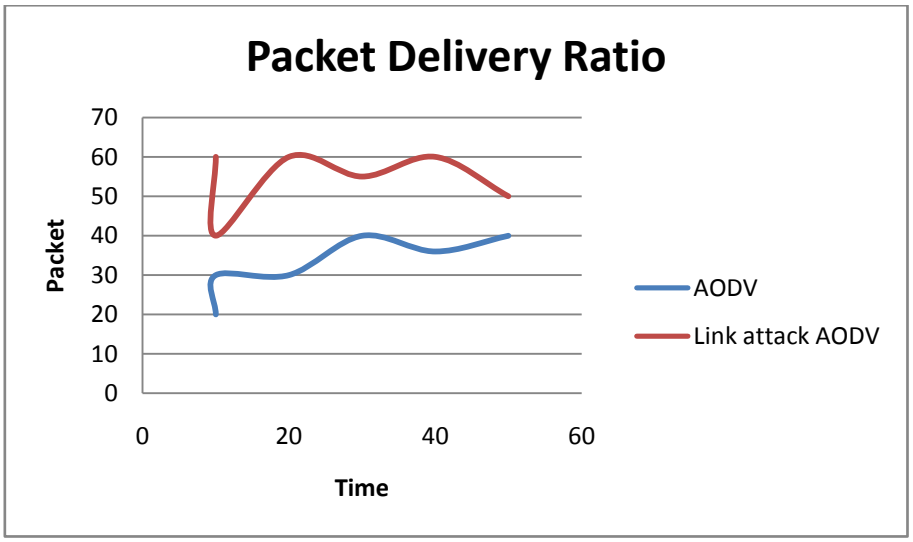

Fig. 2: Packet Delivery Ratio

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.

∑ (arrive time – send time) / ∑ Number of connections. End to End Delay is shown in fig3.

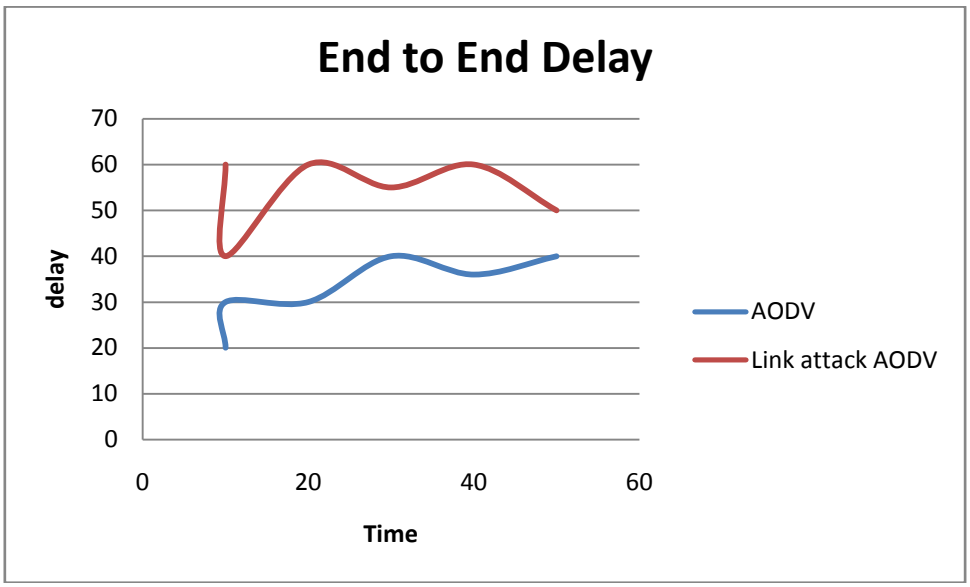

Fig. 3: End To End Delay

simulate and compare the results with AODV. The performance parameters are based on energy consumption and residual energy. The simulation results depict that proposed algorithm better in all aspects. The result simulations are shown in figure 4 and 5.

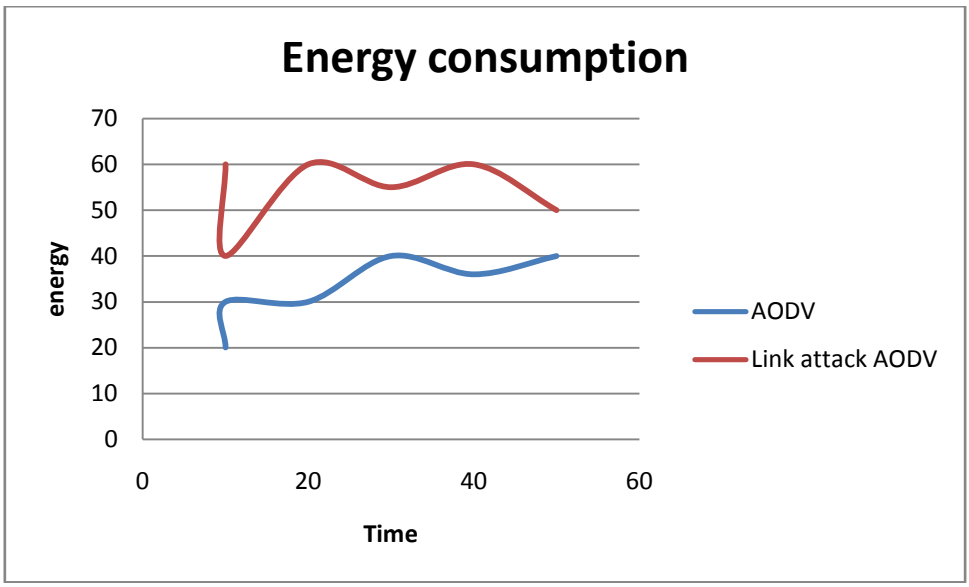

Fig. 4: Energy Consumption

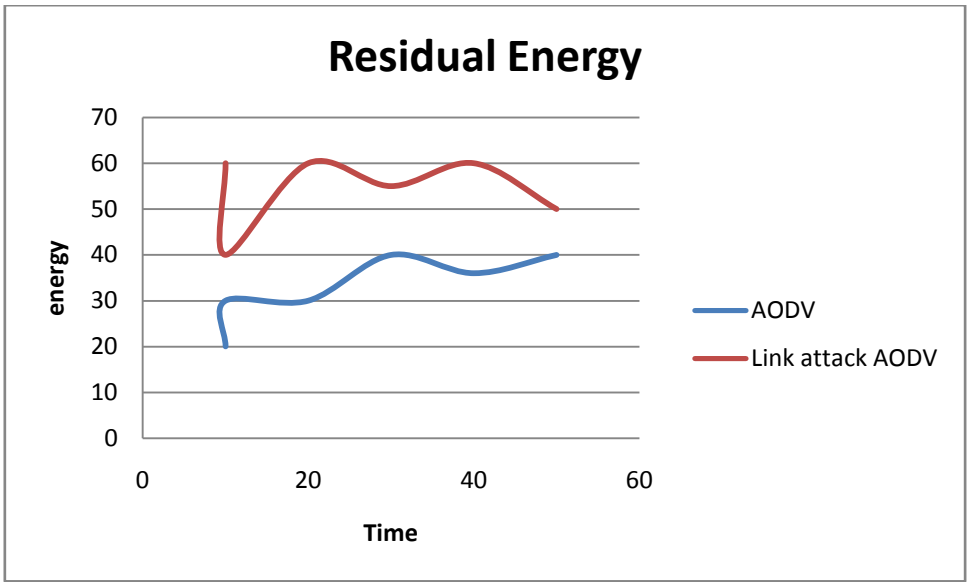

Fig. 5: Residual Energy

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 security..

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

Comparative analysis with existing algorithm shows the modified algorithm proves better. Efficient energy consumption shows that algorithm outperforms existing AODV algorithm. The Proposed research article modifies an existing AODV protocol and gives solution to identify failure and attacker node in MANET with directional antenna transmission. The proposed algorithm is simulated by NS2 and outperforms the existing ADOV.

REFERENCES

Abadi, M., M. Burrows, M. Manasse and T. Wobber, 2003. Moderately hard, memory-bound functions. Proceedings of NDSS 2003 (Networks and Distributed Systems Security), pp: 25-39.

Abdelsayed, S., D. Glimsholt, C. Leckie, S. Ryan and S. Shami, 2003. An e-cient-lter for denial-ofservice bandwidth attacks. Proceedings of IEEE Global Telecommunications Conference (GLOBECOM '03), 3: 1353-1357.

Bellovin, S., M. Leech and T. Taylor, 2001. ICMP Traceback Messages. Internet Draft, Work in Progress. Retrieved form: http:// search. ietf. org/ internet-drafts/draft-ietf-itrace-01.txt. (Accessed on: October 2001)

Carl, G., G. Kesidis, R.R. Brooks and S. Rai, 2006. Denial-of-service attack-detection techniques. IEEE Internet Comput., 10(1): 82-89.

Malan, G.R., D. Watson, F. Jahanian and P. Howell, 2000. Transport and application protocol scrubbing. Proceedings of INFOCOM 2000, pp: 1381-1390.

Palmieri, F., S. Ricciardi and U. Fiore, 2011. Evaluating network based Dos attacks under the energy consumption perspective. Proceeding of the International Conference on Broadband and Wireless Computing, Communication and Applications, pp: 374-379.

Ricciardi, S., D. Careglio, U. Fiore, F. Palmieri, G. Santos-Boada and J. Solé-Pareta, 2011. Analyzing local

strategies for energy-efficient networking. Proceeding of the SUNSET 2011, IFIP NETWORKING, Valencia, Spain, LNCS 6827, pp: 291-300.

Stephen, S. and L. Ruby, 2003. Taxonomies of Distributed Denial of Service Networks Attacks, Tools and Countermeasures. Retrieved form: http:// www.ee.princeton.edu/ ~rblee/DdoS %20 Survey% 20 Paper_v7final.doc.

Hemalatha, S and Dr Paul Rodrigues, 2014. Advanced AODV protocol for identifying a victim node in MANET.