ISSN (Print) : 2319-8613
ISSN (Online) : 0975-4024

Performance analysis of IDS for mitigation of DDOS in Wireless Networks

[1]Farhat Parveen,[2] Debendra Kumar Panda
Department of Electronics Engineering,
Medicaps Institute of Technology and Management
A.B Road Pigdamber, Rau, Indore, Madhya Pradesh 453331, India
[1]fparveenec@gmail.com,[2]debendrakumar.panda@gmail.com

***Abstract*-The security problems in Distributed System leads the researchers to find out that attacks are the major issue which outcomes the result in security problems of distributed system. Distributed Denial of Service (DDoS) attack is a attack which leads to disrupt the network by draining its resources. Network traffic is created by attackers by sending the invaluable messages to user. For every node battery capacity is important and battery draining in nodes leads to degrade the life of the node, this is a severe problem. In this paper we are discussing about the DDoS attack, which creates problem for WSN which is used in military solution, and MANET which is used in communication and is simple to use. DDoS is the major challenge for WSN and MANET, it identifies the nodes and attack on it. DDoS attacks are an attempt to make resources unavailable.**

Keyword: Distributed Denial Of Service; Wireless Sensor Network; Mobile Ad Hoc Network, Ad Hoc On-Demand Distance Vector Routing Protocol

I. INTRODUCTION

The DDoS (Distributed Denial of Service) attack, which is a reason for disrupt in life of node. This attack creates congestion into the network of communications and unwanted packets creates traffic which leads to the power consumption, the energy consumption degrade the node and also consumes the resources, even the resources are limited. Author stated about DSR Dynamic Source Routing protocol, it forms a route from source to destination on demand of request computer by preventing attacks[1].The method of security discussed by author in wireless Sensor Network is very important because the security of WSN is very weak due to limited resources. Author finds the security approaches to increase the level of protection and to reduce the overheads and the loads on node. He also implemented important features like processing, storage, energy[2]. The DDoS Distributed Denial of Service attack which attacks on the targeted node, resulting in denial of service to the targeted node. The attacker flooded the incoming messages to the targeted node resulting in congestion into the network. Many researchers have been done on DDoS attack for the detection and prevention from of it[3]. The service request attacks are repeated on targeted node as to drain the energy consumption. The user repeatedly request for the service and request was again and again denied, this denial of service is the attack on that node. Draining of battery as quickly as it can be is discussed by the author through DDOS[4]. Author proposed about Intrusion Detection System and provided solution for it. According to the solution provided by him explains if IDS is perfect then have coverage of 100% and if false then is 0% [5]. A method presented by the author which determines intrusion in MANET and is determined using intrusion detection system, also it prevent from Denial of service attack. The result analyzed is based on end-to-end delay, DDOS attack [6].

A. MANET (Mobile ad hoc network)

MANET is a Mobile ad hoc network which does not need any infrastructure to establish, It is a continuous configuration of wireless network, which is a collection of node. Security assurance is been provided during communications and all other device in MANET are free to move in any direction and also can switch the links, from one to another. It has been establish as a framework for communications and mostly uses under military solutions. A collection of node in which every node work as a source node or an intermediate node. Data are forwarded in the form of packets and these nodes are mobile nodes which can not reject to forward those packets, in it connections are maintained through radio waves.

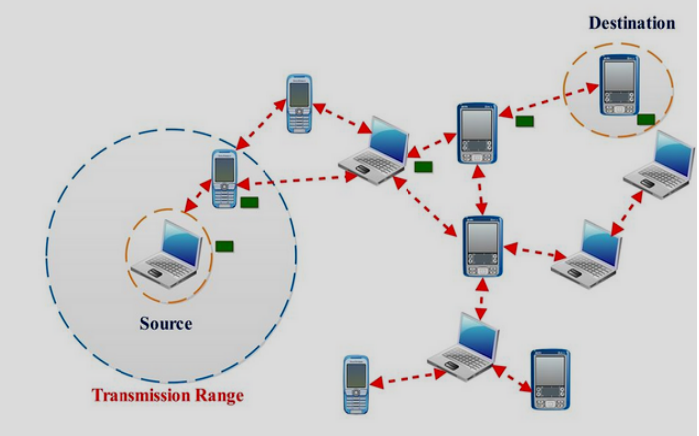

Figure 1: Architecture of MANET

B. WSN (Wireless Sensor Network):

WSN is a Wireless Sensor Network with limited resources and weak security system. Due to the limited resources the approaches in security in wireless networking is weak. WSN consists of a sensor node with transducer and are portable. It consists of battery (power source), intranet nodes, and multiprocessor with storage media, transducer, and transceiver. The transducer is used for electric signal, microprocessor processes the information, and transceiver accepts commands and transports data to centralized computer. A sensor network record every minutes/seconds of environmental condition. WSN Works as the sensing and processing of information.

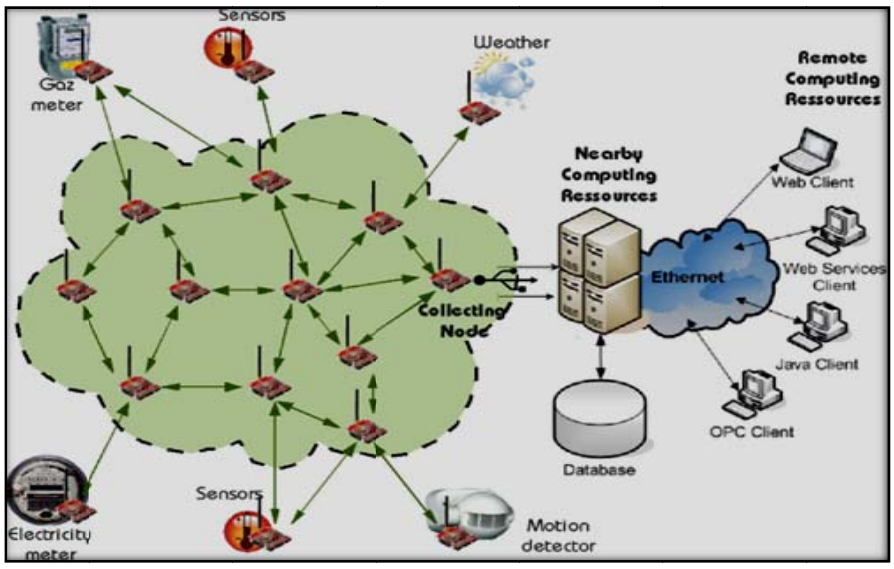

Figure 2: Architecture of WSN

C. DDoS (Distributed denial of service)

DDoS attack is a severe attack which creates traffic in network communications and consumes unnecessary energy which degrades node life and network. It identifies the targeted node and attacks on that node. When extra packets which are of no use arrive on any overload occurs on the targeted node then energy than energy. The consumption is more than regular, it decreases the processing and other function of the targeted node.

The DDoS attacks are classified in two forms:

1. Direct attack and,

2. Reflector attack.

If we will further classify them then it can in the form of congestion, flooded, smurf attack etc.

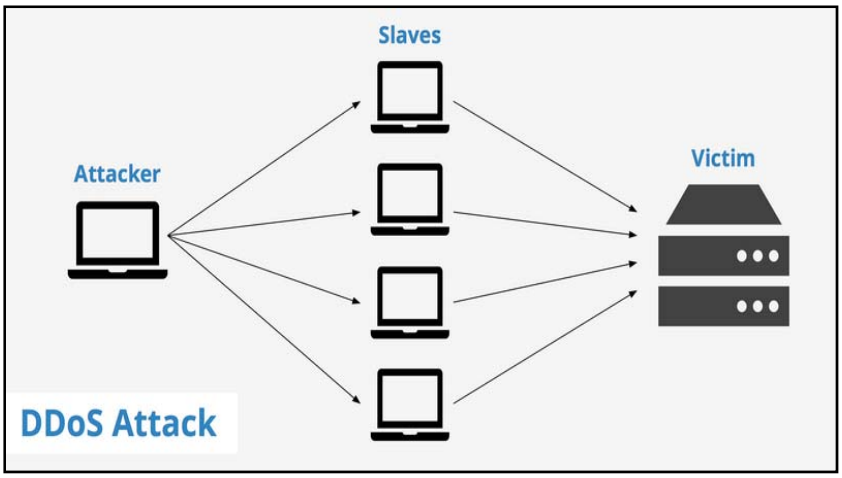

Figure 3: DDoS attack

In order to overcome the problem of DDoS we have used IDS (Intrusion Detection System) which has ability to locate and identify malicious activity on any network by examining network traffic in real time.IDS is available in HOST as well as NETWORK form. HOST IDS is installed as an agent on machine where as Network IDS examines the traffic between the nodes looking for nefarious behaviour.

The majority of IDS uses one method among the three namely signature based, anomaly or stateful protocol analysis.

II. PROBLEM DOMAIN

The major issue faced using WSN and MANET is the problem of battery, battery consumption is high during traffic and overload. A single victim node is targeted sending multiple messages repeatedly which are unwanted. The attacker node has a high capability and a fake identity which generates large packets and transmits these unwanted packets to the targeted node in network. The attacker continuously sends large packets in different interval of time which results in not getting any information that was the behaviour of the attacker. If we will further classify them in the form of congestion, flooded, smurf attack etc. The researchers also proposed solution for the detection and prevention of the attack using the Dynamic Source Routing (DSR) protocol and Ad hoc on demand distance vector routing protocol (AODV), which creates route from source to destination on the request of computer.

III. METHODOLOGY

Following steps are proposed for implementation and evaluation purpose:

1. Initially, two different scenarios for MANET and WSN have been developed for creation of proposed platform.

2. Afterwards, little malicious attack with extra flooding attack has been deployed to drain the network battery or another resource.

3. To diagnose the attack, a monitoring mechanism has been used i.e IDS technique to collect the information of initial battery and remaining battery.

4. This value would help to calculate the draining rate of each node. Every attack has very significant symptoms for detection.

5. This work will consider this value as the input and it will compare with previously supplied value of threshold to observe whether this consumption is genuine or not.

6. It crosschecks the remaining value with higher threshold value. It only forwards the packet when node's remaining power is higher than threshold value. In case of less value it considers the node as victim node and executes the *detection* mechanism.

7. This step executes detection mechanism and start collecting the remaining node power. If any node found with higher battery power, mechanism consider this node as attacker node. As per the study observed that, malicious node always carry extra ordinary battery capacity, its power will be higher than maximum capacity of sensor node. Mechanism will consider such node as suspicious node and alarm with message on console. Afterwards, it forward the suspected node detect to prevention mechanism.

IV. RESULTS ANALYSIS

This section represents the result analysis of the solution proposed for the detection and prevention of nodes from DDoS attack in WSN (mobile), WSN (static), MANET (mobile) and MANET(static) using throughput, end to end delay, total energy consumed and protocol energy consumed as the parameters.

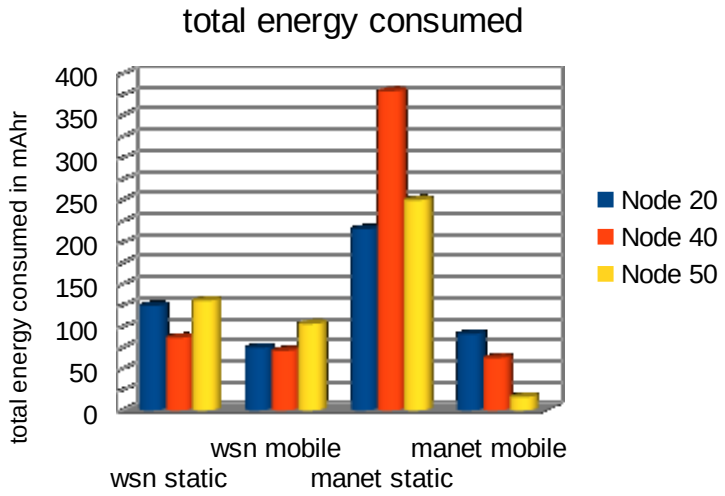

Figure 4. Comparison of total energy consumed

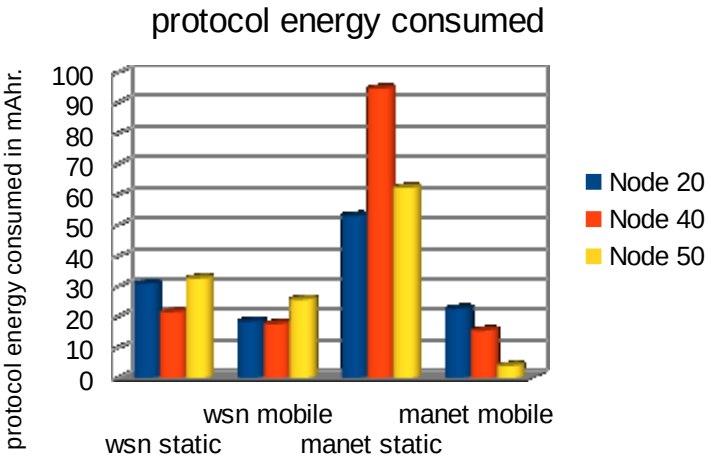

Figure 5. Comparison of protocol energy consumed

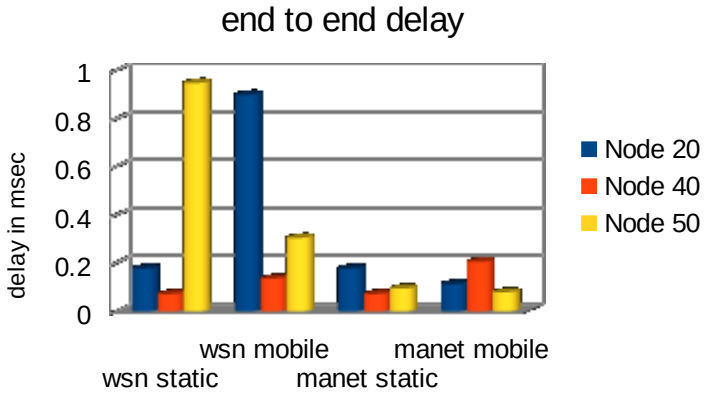

Figure 6. Comparison of end-to-end delay

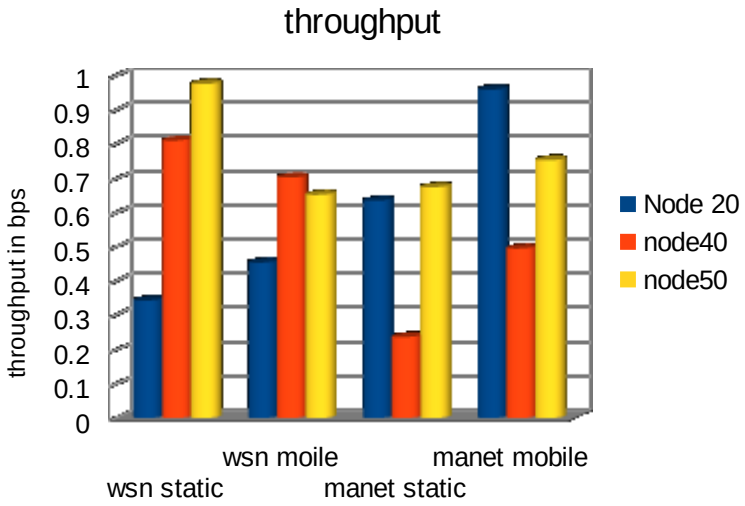

Figure 7. Comparison of throughput

V. CONCLUSION

The complete work observes that DDoS attack is one of the severe resource draining attack leads to reduce the life of node. Here, mitigation technique has been developed to diagnose and mitigate malicious node. Simulation with NS2 has been performed. The complete work has been observed on the basis of following parameters end to end delay, throughput, total energy consumed and protocol energy consumed. The study of result concludes high energy drain has been observed in attacking and preventive technique is capable to overcome circumstances and diagnose the attacker node and provides the best result for MANET mobile network in most of the case when compared to other three wireless network.

REFERENCES

[1] Raksha Upadhyaya, Uma Rathore Bhatta , Harendra Tripathi “DDOS Attack Aware DSR Routing Protocol in WSN”, International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA available on ELSEVIER.
[2] Jaydip Sen, “A Survey on Wireless Sensor Network Security”, In proceedings, International Journal of Communication Networks and Information Security (IJICNIS), Vol 1, No 2, Augest-2009.
[3] Sonali Swetapadma Sahu, Manjusha Pandey “Distributed Denial of Service Attacks: A Review” In proceedings, MECS I.J. Modern Education and Computer Science, 2014, 1, 65-71.
[4] Thomas Martin, Michael Hsiao, Dong Ha, Jayan Krishnaswami “Denial-of-Service Attacks on Battery-powered Mobile Computers” In proceedings, MECS I.J. Modern Education and Computer Science, 2014, 1, 65-71.S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.
[5] Mirjana Stojanovic, Valentina Timcenko, Slavica Boštjancic Rakas, Intrusion Detection Against Denial Of Service Attacks In Manet Environment, XXIX Simpozijum, 0, decembar 2011.
[6] Ramratan Ahirwal, Leeladhar Mahour,” Analysis of DDoS Attack Effect and Protection Scheme in Wireless Mobile Ad-hoc Network”, International Journal on Computer Science and Engineering (IJCSE)-06 June 2012

AUTHORS PROFILE

Farhat Parveen was born in Madhya Pradesh in 1991. She graduated in Electronics and Communication from V.I.T.S(satna) in year 2013 and pursuing M.E in electronics and communication from Medi-caps institute Indore. Her research interests are in embedded system and different networking concepts especially in networking security.

D.K Panda was born in Orissa, in 1970. He graduated in Chemistry from Utkal University in year 1992 and became an Associated Member of IETE in 1997. He did his ME in Digital System and Instrumentation from BEC (DU), Howrah, and West Bengal, India in the year 2003. He has obtained his Ph D from IIT Kharagpur, in 2010. He worked as a Lecturer in the Dept. of Electronics and Communication Engg. of JIS college of Engineering, Kalyani in 2003. Currently he is working as Dean, Faculty of Engineering at Medi-Caps University, Indore. His research interests are Numerical Techniques in Electromagnetic, waveguide power dividers and waveguide slot antennas, beam forming algorithms, different networking concepts especially in networking security.