A Novel Approach to detect Denial Of Service Attack in MANET

Gajendra Singh Dhakar
Department Of CSE & IT, MITS Gwalior
gajendrasingh.sati@gmail.com

Abhilash Sonker
Department Of CSE & IT, MITS Gwalior

Abstract--Mobile ad-hoc network is a growing field of research. There are lots of work done in this field. MANET can be easily threatened by many attacks, denial of service attack is one of the crucial attack by which whole network services effected, there are lots of technique regarding this attack, and they have some issues to overcome and preventing network by this attack, we propose a trust and secure base technique in which first we calculate the trust of nodes on the basis of network and node behavior and after that for securing data transfer we use hashing algorithm implementation of our work done on NS-2.35.

Keywords- *— DDOS,DOS,MANET,NS.*

I. Introduction

The advancement of the utilization of wireless networks has expanded quickly due to our requirements for mobile communications. A MANET (Mobile ad-hoc network) is a type of self-configuring, infrastructure-less wireless network that may operate independently or be associated with the Internet. A MANET comprises of a collection of devices called nodes, which may be laptops, smart phones, tablets, MP3 players, PCs, or some other sort of network enabled digital technology. This heterogeneous, dynamic architecture makes it ideal for deployment in a wide variety of situations, such as disaster relief and recovery. The capacity to react to debacles and recovery missions is an imperative element of the MANET. For instance the utilization of MANET in disastrous circumstances, for example, storms, floods, earthquakes, and snow- storms need to be examined. Availability is an important pillar of network security that should ensure data is continuously accessible to legitimate users. That MANET is useful in helping people to survive following a disaster has been demonstrated in many case studies such as Hurricane Katrina (2005) and the Haitian Earthquake (2010). Other examples include further natural disasters such as the earthquake and tsunami in Japan (2011), Hurricane Sandy (2012), and Hurricane Irene (2011). All of these instances have illustrated the importance of using MANET in monitoring the situation and providing disaster relief [1]. Trust is also an important feature of disaster recuperation and is required when reporting between nodes that have a high level of security in the network.

Fig. 1 Example Of A Typical MANET

As per the legitimate status of a node, an attack could be named external or internal. External attacks are done by utilizing nodes that don't have a place in the area and are usually not legal members of the network, in the meantime inner internal attack network. Internal attacks are extra extreme than outside attacks because of the certainty the insider traditionally is aware of useful and secret understanding, and possesses privileged access rights. These attackers are conscious of the protection techniques, and are even covered via them. In phases of interaction, an attack could be labeled as passive or active. Passive attacks don't disrupt the conversation. They intercept and seize packets to read the knowledge that they carry. Examples of passive attacks in MANETs comprise eavesdropping and site traffic

DOI- 10.18486/ijcsnt.2016.5.2.04
ISSN-2053-6283

analysis. In contrast, lively attackers inject packets into the network to intrude or interrupt network communication, overload the network traffic, fake the respectable node or packet, obstruct the operation or disconnect unique nodes from their neighbors so they cannot use the network offerings effectively any longer. A standout amongst the most customarily encountered active attacks in MANET are blackhole, wormhole, Byzantine, denial of service (DOS) attack [2].

II. DOS Attack

DOS attack makes utilization of one PC to flood a server with parcels. The goal of this attack is to overload the server's bandwidth and different resources. A DDOS attack is an extreme type of DOS, which utilizes various machines to keep the legitimate utilization of an administration. It is an active attack and powerful procedure to attack internet resources. It provides to the various-to-one dimension to the DOS problem. Making the prevention and mitigation schemes for them are extra elaborate. But the influence is proportionally severe. DDOS consists as shown in Fig.2. To begin with attacker fabricate a network of vulnerable nodes, which are utilized to incite the attack. The vulnerable nodes called zombies are then set up with attack instruments, which allow them to do attacks beneath the manage of the attacker. The zombies are isolated into experts and slave. The attacker motivates the masters to begin the attack, the masters, then move the slaves. The slaves flood the victim [3].

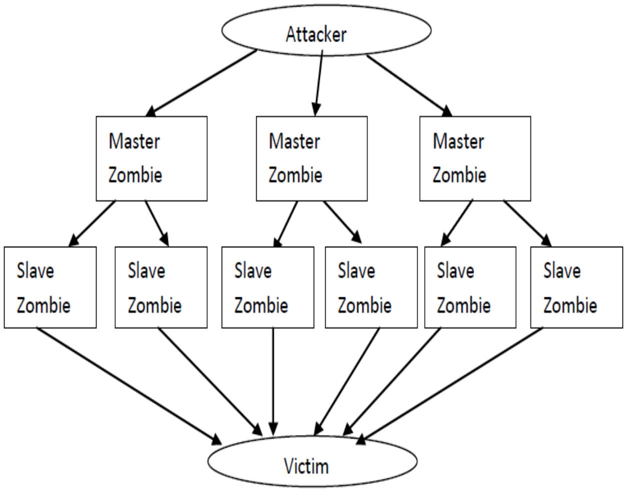


Fig.2 Block diagram of DDOS attack

III. DOS attack in Manet

DOS attacks can be propelled in two basic sorts: software makes the most and flooding, as represented in decide 1. In the instance of the application abuses attack, the attacker node will send few packets to endeavor exact software bugs within the goal node software, disabling this manner the victim. They are able to normally be addressed via ample software fixes. Flooding tends to inject a huge measure of garbage packets into the network.

Flooding attacks are additional categorized to single (DOS) and multisource (DDOS). DDOS attack is in general performed by way of zombies or reflectors. A zombie is a node compromised by using a cracker, computer virus or Trojan horse, worm, and is meant for use to participate in malicious tasks in a network or system that belongs to [2].

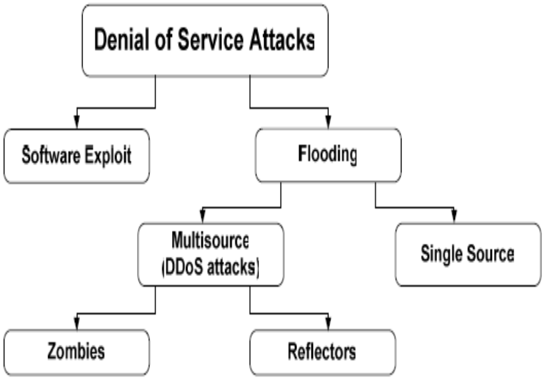


Fig.3 A Basic DOS Attack Taxonomy

IV. Literature Survey

Ahmad Lotfi [2016] et al. In this paper a proposed method called Merging Using MrDR (MUMrDR) is used to merge two MANETs in light of the Monitoring, Detection, and Rehabilitation (MrDR) technique to relieve such attacks. By adopting this method, it will be possible to detect DOS attacks when merging two MANETs, thereby maintaining network operations [4]

M. Anandhi [2015] et al. In this proposed paper, triangular vision, demonstrating structure abuses the discovery of the getting into misbehaving nodes and the selfish node in the MANET. The triangular imaginative and prescient view portrays a reasonable picture in identifying the ultimate route by means of making utilization of the conduct of nodes where it helps to discover the selfish nodes and misbehaving nodes within the MANET [5].

Adel Echchaachoui [2015] et al. In this work, present a new model to trust routing protocol's communications in MANETs against DOS attacks. We have used the box plot theory to define accurately the threshold to detect a DOS attack and to lessen the quantity of false positives [6].

Chaminda Alocious [2015]et al. This paper reasons that DOS attacks with selfish/malicious, mean can get no less than 50% better throughput with the aid of denying well-behaved nodes to receive deserved throughput, also DOS attacks with the intend of complete destruction which permit simplest less than 5% throughput for well-behaved nodes which at last prompted close down of the network. The simulation results demonstrate that presenting DOS attacks at MAC layer would gigantically influence the system throughput and data packet collision rate [7].

John Haggerty [2015]et al. In this paper posits the Monitor, Detect, Rehabilitate (MrDR) method, which is applied to detect three types of DOS attacks: wormhole; greyhole; and jellyfish attacks are a successful instrument for overseeing them. The Network Simulator (NS2) was used to test the efficiency of the MrDR method and the results show that it works better for greyhole attacks, then wormhole attacks, and it works minimum well on account of jellyfish attack [8].

Albandari Alsumayt [2014] et al. In this paper, a description of the components of an ideal system to mitigate DOS attacks is presented which will help to design a new method to detect this attack with certainty in MANETs. There are many methods to mitigate this attack, such as firewalls, IDSs and filtering. Each defense method has some benefits and limitations [9].

Y. Begriche [2014] et al. In this paper, propose a novel procedure of watchdog established on two Bayesian filters Bernoulli and Multinomial. We use these two items in a complementary manner to successfully become aware of the packet shedding attacks in MANETs. Considering reproduction comes about, our channels demonstrate that these attacks can be detected with a high rate of accuracy [10].

M. Rmayti [2014] et al. In this paper a novel approach based on two Bayesian classification models: Bernoulli and Multinomial. A few tests have been performed utilizing NS2 simulator. Our channels demonstrate that purposefully dropping packets can be fully detected with a low level of false alerts [11].

Mukesh Kumar [2013] et al. In this paper, a method is proposed that may avoid a distinct type of DDOS attack, i.e. Flood attack which Disable IP Broadcast. The proposed plan is disbursed in nature, it has the capacity to anticipate distributed DOS (DDOS) attack. The execution of the proposed plan in a series of simulations shows that the proposed scheme supplies a better resolution than existing schemes [12].

Banoth Balaji [2013] et al. In this paper dissect the vulnerabilities of a pro-active routing protocol referred to as OLSR in opposition to a designated form of DOS attack known as a node isolation attack. Analyzing the attack, we propose a mechanism alluded to as enhanced OLSR (EOLSR) protocol, which is trust based method to secure the OLSR nodes in opposition to the attack. Our technique is capable of finding whether a node is advertising correct topology information or not by verifying its Hello packets, thus detecting node isolation attacks [13]

Rutvij H. Jhaveri [2012] et al. In this paper, present routing protocols, evaluate the behavior of more than a few DoS attacks at the network layer of MANET and provide a comprehensive survey of the current protection approaches to manage these attacks [14].

Fei Xing [2012] et al. In this paper, exhibit a profound recognition into DOS attacks and their impacts on MANETs. To begin with, we examine the node isolation, trouble resulting to DOS attacks and determine the probability of node isolation which proposes that the DOS attacks abusing false routing messages, for example, Black Hole attack, affects the availability much severer than different attacks [15].

Syed Atiya Begum [2012] et al. On this paper study special procedures to look after our ad hoc networks towards these DOS attacks. The mechanisms described right here seek to restrict the injury sustained by way of ad hoc networks from intrusion attacks and permit for continued network operation at an acceptable degree during such attacks [16].

S. A. Arunmozhi [2011] et al. In this paper, mentioned the DDOS attacks and proposed a safeguard scheme to strengthen the performance of the ad hoc networks. Our proposed security mechanism uses the MAC layer understanding to realize the attackers. The reputation values from MAC layer that can be utilized for detection are Frequency of receiving RTS/CTS packets, Frequency of sensing a busy channel and the quantity of RTS/knowledge retransmissions [17].

Karthikeyan Thyagarajan [2011] et al. In this paper breaks down an impressive sum of the attack mechanisms and issues in view of DDOS attack, additionally how MANET will likewise be influenced by these attacks. Moreover to this, a novel framework is proposed to security against DDOS attacks in MANETs [18].

V. Problem Statement

In existing technique author apply, trust and reputation based method to detect Denial of Service attack in mobile ad-hoc network. In this method for detecting attacks first trust calculation, in this phase if node success to send data and send back Ack to source, then this node becomes trusted node, otherwise the node is node trustworthiness, but there are lots of reasons of packet delay and dropping and network, in second phase reputation calculation on the basis of trust so that every time it's not possible that trust and reputation calculation is correct. Or existing technique only detects an attack there is no prevention technique.

VI. Proposed Work

In our propose work we apply trust and reputation based secure technique for data forwarding in network. For security purpose, we apply the hash algorithm. First we calculate trust of node on the basis of behavior, if node does not forward data and do not send ECN and back to neighbors node then only trust of node is decreased or if it inform neighbors about network trust neither decrease nor increase. Trust increase only when the node sends data securely to destination.

```
Step1:   initialize network
Step2:   if (node_sends_data)
           if (node_accept)
           if (Inform_neighbors_about_network)
              Trust unchanged
           Else
              Decrease trust
  Step3: if (drop_packet)
           if (dropability>threshold)
              Decrease trust
          Else
              Trust unchanged
Step4: if (trust_value >= threshold)
              Reputation built for nodes
         Else
              Reputation does not built
Step5: if ((trust<<threshold) && (reputation<< threshold))
             Malicious node
              block node
         Else
            Trusted node
Step6: exit
```

```
Algorithm for secure data forwarding
Step1: after secure path built
Step2: data forwarding happen
Step3: data = hash (data)        // encrypted
Step4: destination receive data
Step5: decrypted (data)
Step6: exit.
```

Simulation Parameter

Ns2.35 (Network Simulator) is used to simulate the MrDR method in order to detect DoS attacks in MANETs. The simulation experiments are carried out in FEDORA 15. Table I shows the computer specification which is used to do this experiment.

TABLE I. THE SIMULATION PARAMETERS

Simulation parameters	
Processor	Intel(R) Core(TM) Duo CPU P8700 @ 2.53
RAM	4.00 GB
System type	64-bit
Operating system	FEDORA 15
Routing protocol	AODV
Simulation time	6 min
No of nodes	71
Traffic type	CBR
Topology	1200*1200
Packet	512 bytes
MAC type	Mac/802_11

An example illustrates the performance of this approach

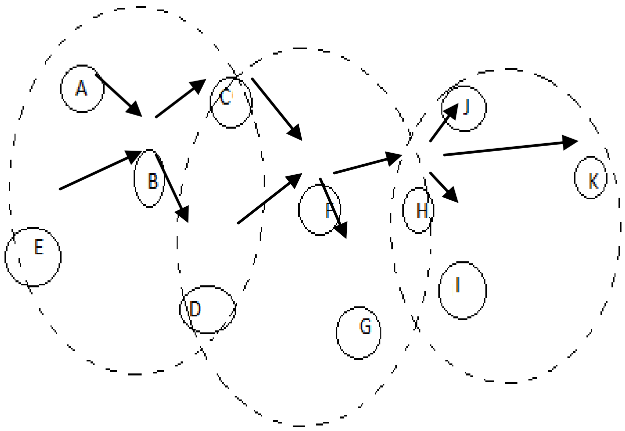


Fig.4 Observation of Other Node

From figure 3 node B monitors all its immediate neighbor nodes (A,C,D,E) and assesses them based on this observation. Table I shows the information that node B collect it from this observation.

Table I: The Information of Trust In Each Node

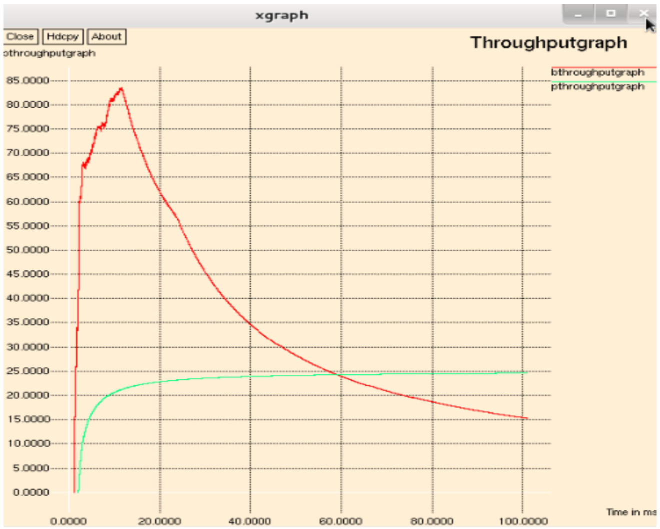
Node	Forward Packet	Drop packet	Trust Value
A	YES	NO	INCREASE
E	YES	NO	INCREASE
C	YES	NO	INCREASE
D	NO	YES	DECREASE

VII. Result Simulation

Throughput:

Per second transfer of information on bandwidth is called as throughput. The graph 1 represents a throughput graph between existing approach and the proposed approach. The proposed approach throughput is better than the existing approach.

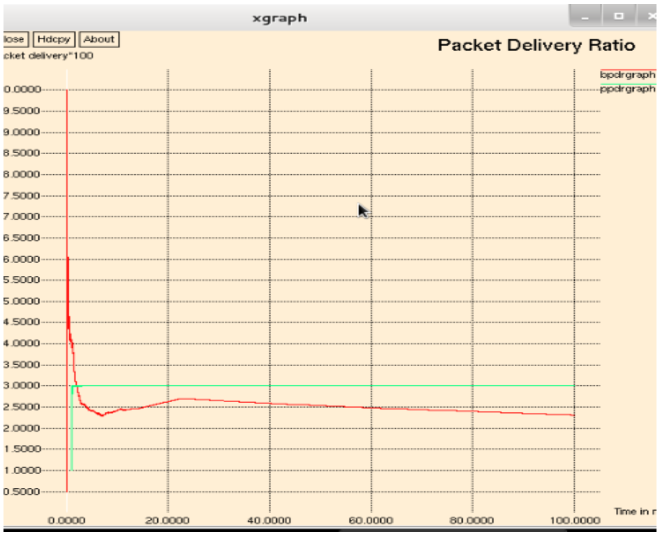
:



Graph 1. Throughput

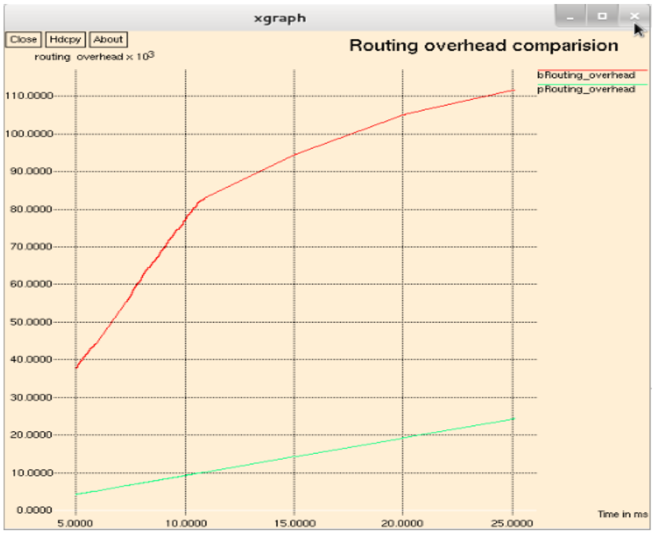
Packet delivery ratio:

Defined as packets delivered ratio from source to destination. The graph 2 represents a graph of PDR between the proposed approach and existing approach. The PDR of the proposed approach is better than the existing approach.



Graph 2. Packet delivery ratio

Routing Overhead:
The routing overhead is described as information on data and data flooding in network transmitted through application, which uses accessible transfer rate bit of communication protocols. The graph 3 represents a routing overhead graph between existing approach and the proposed approach. The overhead of the proposed approach is more than the base approach. Since overhead should be minimum, but as the routing growths in proposed work the overhead also growths.



Graph 3. Routing Overhead

DOI- 10.18486/ijcsnt.2016.5.2.04
ISSN-2053-6283

VIII. Conclusion

Above discussion show that denial of service attack is a crucial attack of the network and by which network performance down by graph we conclude that our propose work is better as compared to existing techniques and secure also in the future we apply a differential evaluation technique to get better results.

References

[2] Albandari Alsumayt, John Haggerty and Ahmad Lotfi "Performance, Analysis, and Comparison of MrDR Method to Detect DoS Attacks in MANET" 2015 European Intelligence and Security Informatics Conference.

[1]. Mirjana Stojanovic,Valentina Timcenko and Slavica Boštjancic Rakas "INTRUSION DETECTION AGAINST DENIAL OF SERVICE ATTACKS IN MANET ENVIRONMENT" PosTel 2011, Beograd, 06. i 07. December 2011.

[2]. A. Anna Lakshmi and Dr. K. R. Valluvan" A Survey of Algorithms for Defending MANETs against the DDOS Attacks" Volume 2, Issue 9, September 2012.

[3]. Albandari Alsumayt, John Haggerty and Ahmad Lotfi "Detect DoS attack using MrDR method in merging Two MANETs" 2016 30th International Conference on Advanced Information Networking and Applications Workshops

[4]. M. Anandhi and Dr. T. N. Ravi "A Novel Framework for Prevent The Denial Of Service Attacks in MANET" IJRITCC | May 2015

[5]. Adel ECHCHAACHOUI, Abdellatif KOBBANE and Mohammed ELKOUTBI "A New Trust Model to secure Routing Protocols against DOS attacks in MANETs" 978-1-4799-7560-0/15/$31 ©2015 IEEE.

[6]. Chaminda Alocious, Hannan Xiao and Bruce Christianson "Analysis of DOS Attacks at MAC Layer in Mobile Adhoc Networks" 978-1-4799-5344-8/15/$31.00 ©2015 IEEE.

[7]. Albandari Alsumayt , John Haggerty and Ahmad Lotfi "Comparison of the MrDR method against different DoS attacks in MANETs" ISBN: 978-1-4673-6832-2©2015 IEEE

[8]. Albandari Alsumayt and John Haggerty" A survey of the mitigation methods against DoS attacks on MANETs" Science and Information Conference 2014

[9]. M. Rmayti, Y. Begriche, R. Khatoun, L.Khoukhi and D. Gaiti "Denial of Service (DoS) Attacks Detection in MANETs Using Bayesian Classifiers" 978-1-4799-8030-7/14/$31.00 ©2014 IEEE.

[10]. M. Rmayti_, Y. Begrichey, R. Khatouny, L. Khoukhi and D. Gaiti_"Denial of Service (DOS) attacks detection in MANETs through statistical models" 978-1-4799-5490-2/14/$31.00 ©2014 IEEE

[11]. Mukesh Kumar & Naresh Kumar "DETECTION AND PREVENTION OF DDOS ATTACK IN MANET'S USING DISABLE IP BROADCAST TECHNIQUE" Volume 2, Issue 7, July.

[12]. Banoth Balaji , Mohammed HasanKhan and R. Prathap Kumar" Enhanced OLSR for Defense against Node Isolation Attack in Ad Hoc Networks"International Journal of Computer Science and Information Technologies, Vol. 4 (6), 2013, 1004-1009.

[13]. Rutvij H. Jhaveri, Ashish D. Patel and Kruti J. Dangarwala "Comprehensive Study of Various DOS Attacks, and Defense Approaches in MANETs" 2012 - International Conference on Emerging Trends in Science, Engineering and Technology.

[14]. Laxmi Shrivastava, G.S. Tomar & Sarita Bhadoria, "Secure and Congestion Adaptive Mechanism with Load Balancing for MANETs", International Journal of Communication Systems and Networks, Vol.1 No.1, pp41-51, Feb 2012.

[15]. Fei Xing and Wenye Wang "Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks" January 27-31,2012.

[16]. Syed Atiya Begum " Techniques for resilience of Denial of service Attacks in Mobile Ad Hoc Networks" International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -201.2

[17]. S. A. Arunmozhi and Y. Venkataramani "DDOS Attack and Defense Scheme in Wireless Ad hoc Networks" Vol.3, No.3, May 2011.

[18]. Karthikeyan Thyagarajan and Arunkumar Thangavelu " An Integrated Defense Approach for Distributed Denial of Service Attacks In Mobile Ad-Hoc Network" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11,