Novel Paradigm: Assessment of DOS Flooding Attack through Energy Aware Routing over MANET Environment

Khushboo Sawant
PG Scholar
Computer Science Dept.
LNCT, Indore (M.P), India

Manoj Kumar Rawat, Ph.D.
Asst. Prof, HOD
Computer Science Dept.
LNCT, Indore (M.P), India

ABSTRACT
One of the most up-and- coming fields for research is mobile ad hoc network. Security is high Priority obligation in wireless ad-hoc network. In ad hoc network the communicating nodes sets new challenges for the security architecture because it doesn't necessarily feed on fixed infrastructure. In the ad-hoc network denial of service attacks (DOS) forcefully initiate through malicious nodes or attacker which is more vulnerable. In this paper, we are clarify the incident of flooding attack and their exposed to the possibility of being attacked or harmed effects which give chance to a legitimate node for doing dissimilar attacks also. So we get going towards is to recognize the presence or existence of DOS flooding attack using secure routing protocols.

This paper proposes a novel mechanism using allowable and limiting threshold for accurately measuring the flooded packets from the usual congestions. Somewhere it also prevents network being down from flooded traffic..

General Terms
Energy awareness, limiting threshold

Keywords
DOS attack, Flooding attack, Routing Protocols, Security, and Energy Aware.

1. INTRODUCTION
MANET is a wireless network consists of mobile nodes that form a short-lived network in the absence of any centralized supervision in such an environment. MANETs consist of mobile nodes that are free in moving in and out in the network [1]. Nodes can be anything like systems or devices that are participating in the network and free to moving in and out in the network. At the same time nodes can act as host as well as router and form inconsistent topologies pivot on their comparability with each other in the network. Because of their self alignment ability these nodes have the capability to reconfigure itself. Internet Engineering Task Force (IETF) has MANET working group (WG) that Develop and promotes the internet standards as well as IP routing protocols. Routing protocols is one of the worthwhile areas of research. Many routing protocols have been promote and developed for MANETS, i.e. AODV, OLSR, DSR etc. MANETs have been many mannerisms like such as o allowing access channel, revising its topography influentially, inadequacy of primary supervision & administration, cooperative algorithms which often suffer from security attacks because of its features and no clear shielding process. These factors have changed the battle field situation for the MANETs against the Security threats. The MANETs work with a decentralized administration so that on the basis of mutual trust communication occurs within the network. This features form ad hoc network more undefended to be utilize by an intruder with in An inside the network. Connections of Wireless also represent the MANETs more likely or liable to be influenced or harmed by a particular thing, which make it, trouble free for the intruder to go inside the network and gain access to the existing communication

2. BACKGROUND
Securing wireless ad hoc networks is a highly challenging issue. There are certain specific attacks to which the ad hoc context is vulnerable. Performing communication in free space exposes ad hoc networks to eavesdrop or inject messages. Ad hoc network attacks can be classified into active and passive attacks. A passive attack does not inject any message, but listens to the channel. A passive attack tries to discover valuable information and does not produce any new traffic in the network. In the case of an active attack, messages are inserted into the network; such attacks involve actions such as replication, modification, and deletion of exchanged data. In ad hoc networks, active attacks are Multilayer attacks those attacks that could exist in any layer of the network protocol stack so it is important to provide a route with secure robustness in wireless ad hoc networks likes impersonation, Denial of Service (DOS) and disclosure attack

- DOS attacks can cause a severe degradation of network performance in terms of the achieved throughput and latency.
- The performance of the wireless network is degraded by DOS depends on many factors such as location of malicious nodes, their traffic pattern, fairness provided in the network resources
- DoS attack can be launched against any layer in the network protocol stack.
- Due to the excessive number of requests, the server will be busy in testing illegal request and will be unavailable for legal users.
- These packets over carry a significant portion of network resources, and bring wireless channel & network contention in the ad hoc network
- In denial of service attack, a malicious node attempts to prevent victim and authorized node from services offered by the network and make resources or services unavailable to their intended users.

So After studying the different research papers it is identified that Flooding attack is a denial of service type of attack in which the adversaries' node broadcast the redundant false packet in the network to exhaust the available resources and reduces the throughput of the network so that valid or legitimated user can not able to use the network resources for well defined communication. The flooding attack is possible in all most all the secure on demand routing like SRP, SAODV, ARAN, Ariadne etc. Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the host's memory buffer. Once this buffer is full no further connections can be made, and the result is a Denial of Service. The number of RREQ that can be originated per second is limited.

In a flooding attack, malicious node send a large volume of burst traffic to a victim node suffers from saturated network bandwidth, thereby preventing access by an authorized node. In Flooding attack, a large number of flooded packets are sent to either random or specified node on the victim node. The victim node tries to process the incoming data to determine which applications have requested data. If the victim node is not having any applications on the targeted node, it will send an RREP packet to the sending node indicating a "destination node unreachable" message.

Depending upon the type of packet used to flood the network, flooding attack can be categorized in two categories.

2.1 Flooding Of RREQ

In RREQ flooding attack the attacker selects many IP addresses which are not in the network or select random IP addresses depending on knowledge about scope of the IP address in the network. In Malicious RREQ Flooding attack an intruder broadcasts a RREQ with a destination IP address and does not wait for the ring traversal time and continuous resending the same packets with higher TTL value.

2.2 Flooding Of Data Packets

In the data flooding, malicious node flood the network by sending useless data packets. In the data flooding, first malicious node built a path to all the nodes then sends the large amount of fake data packets.

Flooding attacks can incredibly reduce the performance of reactive routing protocol and affect a node in following ways:-

- Degrade the performance in buffer
- Degrade the performance in wireless interface
- Degrade the performance in RREQ packets
- Degrade the performance in life time of MANET

Vulnerabilities in AODV is designed for use in networks where the communication is occur on the basis of mutual trust between nodes and can assume there is no malicious intruder node. Taking the operation of AODV, basically its route discovery process, it is more vulnerable to DoS attacks such as sleep deprivation and the rushing attack. In the route discovery procedure of AODV broadcasts a RREQ packet containing a broadcast id, source & destination addresses, and hops count and destination sequence number & wait for a specific time for getting a RREP or other control packet. If this time was expire; node may try same process once again for getting a valid route. AODV Provides no security mechanism so that DOS flooding attack can easily be done. Flooding attacks take place when a network or service become so balanced down with packets as well as flooded packets filled out host memory buffer so once and while this buffer is full no more ever establishment can be done & the outcome is denial of service attack. Flooding packets in the all of network will consume and exhaust lot of network resources and also disgrace the presentation of host buffer. A specific amount of energy is consumed in sending, receiving and routing the packets and with these its buffer will also full on the consume bits. So it means that processor is also busy. So at that time it recalls an autonomous host and on the name of them, it floods RREQ packets. So with whom so ever "RREQ" request will be there with destination address it will down the whole network.

Energy Conservation doesn't mean only the less power consumption, it means increasing the route request packets per nodes. Most of work have been done only in either of preventing the denial of flooding service attack or decreasing the number of route request packets in ad hoc network but none of work have been done on the preventing the whole network from denial of service flooding attack with energy awareness in flooded environment And we have to save the network being down from RREQ Flooding.

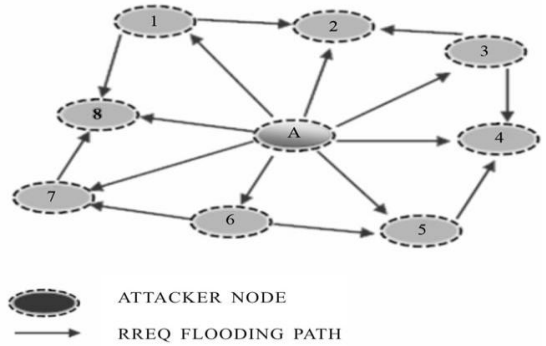

Fig 1: Flooding of RREQ Request

3. PROPOSED WORK & ALOGRITHM

This paper gives a novel method for detecting flooded packet by deriving different section in ideal condition. In ideal condition maximum of nodes flood RREQ for communicating each other. If there is no malicious node in the network then nodes can flood maximum five to seven packets on average. From that we have calculated average value of flooding packets and we know that these packets is flooded by default .After that we have also compute allowable threshold. Allowable threshold means that whatever the average is there, it will stay but rather then it there will be a variation in node is also there. For example first node send 5 pack, Second node send 7 pack, Third node send only 2 packets. So there is variation in all these 3 nodes. After that we have computed an allowable threshold, it means whatever the average is it will be, rather than it and variation is also there. So we have taken out a one more variation which is sigma and it shows packets flooding are also going on in between the gap of nodes. So now we have bind all packet flooding in one scenario. So on an average node can send five packets even two more and 2 less but it cannot send more than these. So we have derived the limited threshold that means not more packets can be sent by that amount. Now if received "RREQ" IS MORE in our new session from our limiting threshold, then in that case "RREQ" Packet will be malicious otherwise it will be honest.The work is looking forward to use Ad hoc on demand Distance Vector (AODV) protocol.

3.1 Algorithm for RREQ Flooding Attack

1. Suppose in an ideal conditions there are N sessions are performed
2. Thus we have an average value of RREQ control message exchange. there for allowable RREQ=

   Allowable RREQ = $\frac{1}{n}\sum_{i=0}^{n} si$
3. In addition of that sometimes router flood packets due to unreachable host. Thus it can be exceed for in a route of ɠ.where

   $$ɠ=\sqrt{\frac{1}{n}\sum_{i=0}^{N}(Si - Allowable\ RREQ)}$$
4. Thus we find a limiting threshold for detecting the malicious behaviour

   Limiting Threshold = Allowable RREQ + ɠ
   Where ɠ is a variance
   If Received RREQ > Limiting Threshold
   Then
   (Node is malicious)
   Else
   (Node is honest)
   End " if"
   End " if"

4. SIMULATION SCENARIO

The Routing protocols AODV is under the analysis for this paper. The Linux UBUNTU OS 12.04 LTS is used to run the Simulation Software NS2 (Network Simulator 2) version 2.35 for the performance appraisal. The performance is observed at various pause time and intervals with the number of nodes. In our work we used AODV routing protocol and 06 nodes with random way point mobility model. During the simulation some parameters are defined which are stated in the table below:

Table 1. Simulations Parameters

Simulation Property	Value
Number of nodes	06
Routing Protocol	AODV
Time of simulation	60sec
Transmitting power	1W
Receiving power	2W
Initial power	100J
X coordinates	750
Y coordinates	550
Chanel propagation	Two Way
Antenna	Omni Antenna
MAC layer	802.11
Wireless	Physical Channel

5. PERFORMANCE SUMMERY

The Figure 2 & 3 compares the Energy loss over flooded packet of AODV routing protocols with fixed node speed with fixed number of nodes. AODV includes both legitimate and malicious nodes. Table 2 Conclude that Energy Loss over the proposed approached is 10% and remains Energy is 90 %.where as under attack approached energy Loss is 35% & remains Energy is 65%. It decreases the Energy loss control over head by only by 10 % with the presence of attackers.

5.1 ROUTE REQUEST

In ad hoc network sender sends route request message to destination with the help of intermediate nodes to set up a communication path. So flooding of request occur because of same request

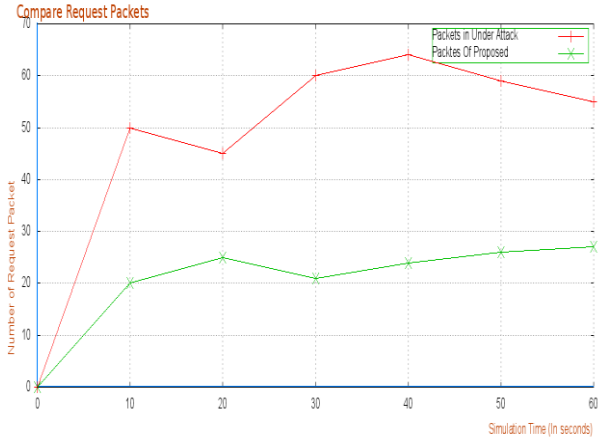

Fig 2: Comparison of RREQ

5.2 ENERGY CONSUMPTION

In wireless network every nodes wants to communicate with every other nodes within the network. So before staring the communication nodes send route requests message to every nodes and got the route reply message with valid path. So energy is consumed in sending or receiving the request or reply.

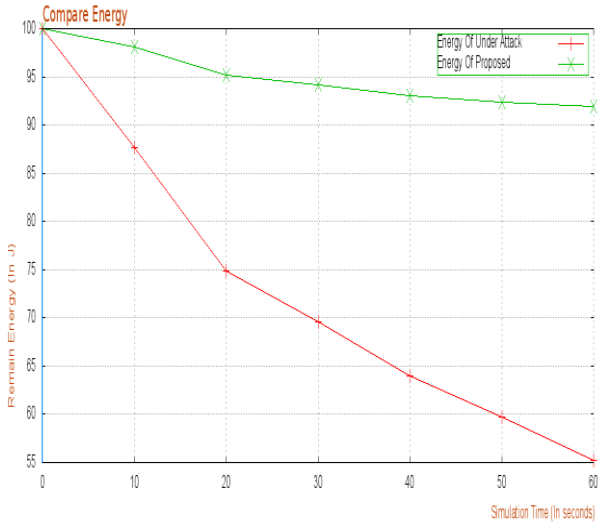

Fig 3: Comparison of Energy consumption in the network

5.3 LOSS OF ENERGY

In ad hoc wireless network the RREQ Packets as well as RREQ Request consume the lots of energy, while performing the communication within the network. The loss of energy conservation is unbalanced between all the nodes in the network in flooded network.

Table 2. Energy Loss

Total Energy	Remain Energy	Loss Energy
Proposed Approached	90%	10%
Under Attack	65%	35%

6. CONCLUSTION & FUTURE WORK

In these paper we briefly discussed one of the crucial security attack in MANET i.e. DOS Flooding. In these paper we proposed a novel mechanism by using two threshold values that is allowable and limiting threshold that deals with flooded request and provides the mechanism to reduces or overcome the flooded request as well as overall conservation of energy in flooded environment .simulation analysis conclude that proposed approached has a good energy consumption in the presence of attack in flooded environment

Some mechanism would be propose in future work like congestions windows on each node to identify core nodes of flooded packets in well founded communication to detect Dos flooded attack to increases the life time of network .

7. ACKNOWLEDGMENTS

The author would like to thank Prof. Dr. M.K. Rawat for his help. This work was supported in part by the LNCT, Indore.

8. REFERENCES

[1] Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong, "New Routing Attack in Mobile Ad Hoc Networks", Journal of Information Technology, 83−94.

[2] Abhay Kumar Rai, Rajiv Ranjan Tewari and saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet", Journal of Computer Science and Security, 265-274.

[3] Bhupandith Kannhavong, Hideshisa Nakayama, Yoshiaki Nemoto And Nei Kat, "IEEE Wireless Communication, 2007, 85-91.

[4] Yi-an Huang and Wenke LeeE. Jonsson , "Springer-Verlag Berlin Heidelberg" 2004RAID 2004, LNCS 3224, 125–145.

[5] Kavuri Roshan1 , K.Reddi Prasad2 , Niraj Upadhayaya3 & A.Govardhan4, Journal of Computer Science, 2012, 25-34

[6] YihChun Hu , Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network routing Protocols", 2003, San Diego, California, USA University of Washington.

[7] Shishir K. Shandilya, Sunita Sahu,, "A Trust Based Security Scheme for RREQ Flooding Attack in MANET", Journal of Computer Applications (0975 – 8887) , 2010 , 4-8.

[8] Ujwala D. Khartad & R. K. Krishna, "Route Request Flooding Attack Using Trust based Security Scheme" , I Journal of Smart Sensors and Ad Hoc Networks, 2012, 27-33.

[9] Panagiotis Papadimitratos, Zygmunt J. Haas; Secure Link State Routing For Mobile Ad Hoc Networks

[10] Mach. Adnan Nadeem , Michael Howarth, "Adaptive Intrusion Detection & Prevention of Denial of Service attacks in MANETs".

[11] Khushboo sawant, Dr. M.k Rawat, "Survey of dos flooding attak over manet Environment", Journal of Engineering Research and Applications, 2014, 110-115.

[12] Sapna Choudhary, Alka Agrawal, "Threshold Based Intrusion Detection System for MANET using Machine Learning Approach", l Journal of Advance Electrical and Electronics Engineering, 2278-8948, 2014, 1-*6*.

[13] Sitesh kumar sinha Krishna kumar pandey Mukesh kumar sahu, "Survey of different types of attack and prevention scheme", Journal of Computer Technology and Electronics, 2320 – 0081, 19-24.

[14] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack", Journal of Engineering and Advanced Technology, 2249 – 8958, 2012.

[15] D.karun Kumar Reddy, Journal of Research in Computer and Communication technology, 228-237.

[16] Aarti, "A Study of MANET: Characteristics, Challenges, Application and Security Attacks", Journal of Advanced Research in Computer Science and Software Engineering, 2013, 252-257.