ISSN:0975-9646

Impact of Flooding Attack on MANET: A Survey

Sheetal Jatthap[#1], Priya Saxena[*2]
[#1]*M.Tech Scholar, Sanghvi Innovative Academy Indore*
[2]*Asst.Professor,Sanghvi Innovative Academy Indore*

***Abstract*— MANET is widest range of protocol working towards security however their needs some Enhancements over the dynamic and active Kind of attacks. Out of those the flooding attacks can tested to be to be devastating in terms of resource consumption in terms of information measure and battery power of the nodes. Because the MANET isn't having any infrastructure and if all of an sudden due to such flooding affect the networks performance gets degraded and also the actual operations of communication are going to be terminated. This research paper investigates the impact of flooding attack on MANET and also proposed a method to mitigate the same. Complete work is proposed to simulate with NS-2.35 simulator using AODV routing protocols.**

***Keywords*— Flooding Attack, MANET, AODV , NS-2.35.**

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) formed by a set of mobile hosts that perform basic networking functions like packet forwarding, routing, and repair detection without the help of a conventional infrastructure. Nodes of an ad hoc network supported each other in forwarding a packet to its final node, due to the restricted range of every mobile host's wireless transmission. The ad hoc network uses no central superintendence. It ensures that the network won't stop functioning simply because one in all the mobile nodes moves off from the vary of the others. Nodes should be able to enter and leave the network after they need. Due to the mounted transmitter vary of the nodes, multiple hops square measure typically needed to succeed in different nodes within the network [2].

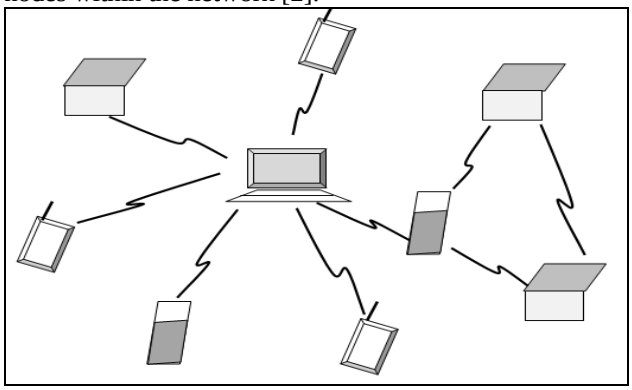

Figure 1: Ad hoc network architecture

There are various types of attacks which try to degrade the performance of the network. Flooding attacks occur when a network becomes so heavily traffic loaded with unnecessary packets initiating requests for link that it can no longer process authentic connection requests. Flooding is reason for traffic and congestion in the network and thus incompleteness of legal connection. Once this buffer is full with request packet traffic become uncontrolled no extra connections can be made, and the result is a Denial of Service [3].

In an ad hoc wireless network wherever wired infrastructures don't seem to be likely, energy and information determine conservation are the two key parts presenting analysis challenges. Restricted information determines make a network simply overcrowded by management signals of the routing protocol. Routing scheme developed for wired networks uncommonly acquire into account limitations of this type. as an alternative, they suppose that the network is in general steady and also the overhead for routing messages is slight. Considering these variations between wired and wireless network, it's essential to develop a wireless routing protocol that restricts congestion within the network.

The mobile unintended networks have many salient characteristics, like Dynamic topologies, Bandwidth-constrained, variable capability links, Energy-constrain operation, limited physical Security [4]. Owing to these options, mobile unintended networks are notably susceptible to denial of service attacks launched through compromised node.

MANET has several significant properties. Some of them present below:

1. *Mobility*: Nodes are free liberated to travel arbitrarily. Hence, the topology could modify accidentally and quickly at uneven times, and should accommodates each bidirectional and unidirectional links

2. *Bandwidth Constrained, Variable Capacity Links*: Wireless links resolve the considerably lower capability than their hardwired counterparts. In accumulation, the complete turnout of wireless communications, once accounting for the consequences of multiple access, fading, noise, and interference conditions, is usually abundant but a radio's most transmission rate.

3. *Energy Constrained Operation*: each and every one node in a MANET possibly will rely on batteries or other exhaustible means for their energy. For these nodes, the foremost vital system style optimization criteria could also be energy conservation [3]. Our work is on economical energy consumption.

4. Self-Configuration: Nodes have capability to reconfigure network topology and discover new path when path breaks or node moves due to dynamic nature of networks.

5. *.Absence of Centralized Router*: In ad-hoc networks, each node play role as router that process route discovery techniques because specific coordinator does not designated as router.

II. RELATED WORK

Singh, N. et. al. [4] in this paper the author studied and evaluated flooding attacks that is usually recommended by giving some detection parameters. Here the variety of parameters can work as one mechanism for detection of DDOS attacks and distributive flooding attacks. During this plan its later section additionally suggests inexplicit query based detection and prevention technique for DDOS. The parameters are: sequence number, battery power, RTT, threshold values, packets forwarded at each node, total time taken by any packet, black-list and a notification mechanism (EAN). At the first level of simulation study the approach is proving its effectiveness. It is recommended to deal with attack impact and later on offer some enhancements over the detection environments.

Kim, H.[4] In this paper, the author address a unique defence mechanism using the amount of legitimate packet processing at every node by that collaborative flooding.

attacks detection rates are improved. The work additionally resolves a network conditions and confirms that flooding attacks not solely causes network down however additionally limit the method of legitimate nodes. The work additionally estimates the standard of the packets by using two specific buffer corresponding sizes of control packets buffer and the data packets buffer. The local density of a node is outlined because the variety of near nodes lying underneath its transmission range. The simulation results show that the proposed scheme additionally improves the end-to-end packet delivery ratio.

III. PROBLEM STATEMENT

The Flooding is that the active class primarily based network attack whose aim is to create the network overcrowded by some forged route request (RREQ) packets. During this state of affairs once a route initiated route discovery, then the supply node sends RREQ packet to its neighbors and waits for a time for its reply.

The node isn't having any data regarding the behavior of its neighbors. The neighbor distance is taken as a hop count. Thus, if the node has smallest hop count the packet is forwarded thereto. Throughout this method of ancient routing the verification of legitimate node condition isn't concerned and therefore some new node can destruct the particular operating of the network by flooding the pretend RREQ packets to the network. By these packets the particular packet route discovery gets affected and that later makes denial of service (DOS) attacks. Thus, within the absence of any malicious packet removal schemes the network is obtaining engorged with these pretend packets.

Ancient schemes don't seem to be capable of distinctive these packets. Therefore anon many enhancements over the AODV protocol is projected. This paper studies varied techniques projected for overcoming the flooding attack state of affairs and measured that there square measure some problems that remains unsettled. [5]

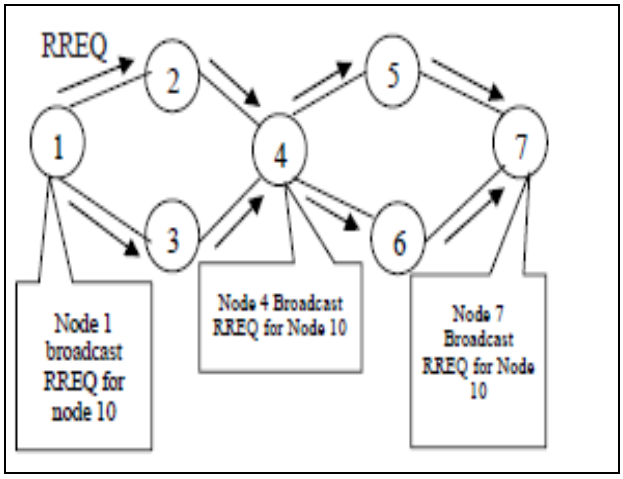

Figure 2. RREQ Flooding Attack

The node isn't having any data regarding the behavior of its neighbors. The neighbor distance is taken as a hop count. Thus, if the node has smallest hop count the packet is forwarded thereto. Throughout this method of ancient routing the verification of legitimate node condition isn't concerned and therefore some new node can destruct the particular operating of the network by flooding the pretend RREQ packets to the network. By these packets the particular packet route discovery gets affected and that later makes denial of service (DOS) attacks. Thus, within the absence of any malicious packet removal schemes the network is obtaining engorged with these pretend packets.

Ancient schemes don't seem to be capable of distinctive these packets. Therefore anon many enhancements over the AODV protocol is projected. This paper studies varied techniques projected for overcoming the flooding attack state of affairs and measured that there square measure some problems that remains unsettled. [5]

IV. SOLUTION APPROACH

The purpose of this study is to deploy flooding attack and develop a technique to detect & prevent flooding attack in the wireless network. Application of wireless networks such as military battle field is used to transmit the confidential data via wireless medium. Wireless networks are also used in national security applications such as monitoring and tracking the borders, nuclear attacks detection etc. Since all the transmission take place through wireless medium where security risks are major so the security of sensitive information is important part thus the security of data is important aspects.

Mobile nodes send data packets to its neighbour node in networks using standard routing protocol like AODV but the existing routing protocols in wireless network are not designed for security purpose. AODV routing protocol is vulnerable to many kinds of threats.

DDOS attacker node easily becomes a part of network and creates conjunction on targeted node either to disable receiver / intermediate node or decrease performance by creating deadlock condition. In such case the AODV

routing algorithm needs of some mechanism to detect and prevent network from attacker nodes.

Security is a primary need of the real time scenarios based on wireless networks. The basic assumption of this study is that mobile nodes are normal and non-malicious nodes in the network deployment. Mobile nodes have low transmission power range due to this nodes are deployed in the transmission range of its neighbor nodes[6]. All mobile nodes deployed in the networks are static means there is no mobility in the nodes. This study is based on the routing attack called DDOS attack, so all nodes in the networks are fully functional device (FFD). The results of this study are measured at different scenarios which consist less number of nodes.

A. Expected Benefits

1. The scheme is capable of timely malicious behavior detection and continuous monitoring which saves network resources efficiently.
2. The flooded nodes and packets are detected and removed using conditional threshold based rate limiter.
3. Alerting mechanism makes the distinction between the actual node and attackers node by which categorization is made easy.
4. Collaborative flooding is also detected by the approach and gets isolated by other nodes preventing DOS, and DDOS attacks.
5. No further overhead is involved with the Proposed Algorithm and it makes minimal modifications to the existing data structures and functions related to blacklisting a node in the existing version of pure AODV.

Also, the proposed scheme is a lot of efficient in terms of its resultant routes established, resource reservations and its computational complexity.

V. SIMULATION STRATEGY

The simulation of the work completed in three scenarios. The configuration of scenarios is based on the number of nodes are deployed and the position of the source node and destination node. Initially all nodes in each scenario are normal and no malicious node is present in the scenario. The standard AODV routing algorithm is used at routing protocol on network layer. The scenarios are differentiated as per normal scenario, scenario with malicious nodes and scenario with proposed technique;

Scenario 1: It describes the normal situation of mobile ad-hoc networks with normal AODV routing protocols.

Scenario 2: It described impact of flooding attack using high capacity method and impact of flooding attack on performance of ad-hoc networks.

Scenario 3: Battery Capacity Based proposed technique to detect and prevent flooding attack in mobile ad-hoc networks.

The following metrics are used in this work for comparing the performance of AODV, AODV under attacks and Modified AODV routing protocols.

- ✓ **Throughput (bytes/sec)**
- ✓ **Packet Delivery Ratio (PDR)**
- ✓ **End to End Delay**
- ✓ **Energy Consumption**

VI. CONCLUSION

At this level of the analysis work isn't finished. The creators are taking an effort at verity execution and are clear that within the close to future the approach is sort of effective whereas detection intruders at terribly early stages of knowledge transfer. at first the simulation setting is taken into account is recovering result than existing approaches.

REFERENCES

[1]. Khushboo Sawant, Manoj Kumar rawat, Akans Jain "Implementation Of Energy Aware Secure Routing Protocol Over Flooding Enviroment In MANET " communication and control IEEE International Conference On Computer 2015

[2] Muhammad Aamir and Muhammad Arif, "Study and Performance Evaluation on Recent DDoS Trends of Attack & Defense", in I.J. Information Technology and Computer Science, DOI: 10.5815/ijitcs.2013.08.06, July 2013.

[3] BounpadithKannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Neikato "Asurvey of routing attacks in mobile ad hoc networks",ieee wireless communications • october 2007 85 1536-1284/07/2007 ieee.

[4]. HyoJin Kim, RamachandraBhargavChitti and Jose Song, "Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks", in Journal o f Information Processing Systems, DOI : 10.3745/JIPS.2011.7.1.137, Vol.7, No.1, March 2011.

[5] Mohan K Mali and Pramod A Jadhav, "Review of DDoS and Flooding Attacks in MANET", in International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 3, Issue 5, May 2013

[6]. Muhammad Aamir and Muhammad Arif, "Study and Performance Evaluation on Recent DDoS Trends of Attack & Defense", in I.J. Information Technology and Computer Science, DOI: 10.5815/ijitcs.2013.08.06, July 2013.

[7] S. Corson,J. Macker,Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations，RFC 2501，January 1999

[8]. Rashid Hafeezkhokhar, MD Asringadi, Satria mandala "A review of current routing attacks in mobile ad hoc networks", international journal of computer science and security, volume (z) issue (3).

[9]. S.Corson,J. Macker ,Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations，RFC 2501，January 1999.

[10]. Yi-an huang and wenke " Attack analysis and detection for adhoc routing protocols" e. jonsson et al. (eds.): raid 2004, lncs 3224, pp. 125–145, 2004.springer-verlag berlin heidelberg 2004.

[11]. Venkatesan Balakrishnan, Vijay Varadharajan, Udaya Kiran Tupakula "Defense against Flooding and Packet Drop Attacks in MANET" INSS Research Group, Department of Computing, Macquarie University,North Ryde, Sydney, NSW Australia 2109.

[12]. Abhay Kumar, Rai Rajiv Ranjan Tewari, Saurabh Kant Upadhyay "Different types of attacks on integrated manet"-internet communication international journal of computer science and security (ijcss) volume (4): issue (3) 265.

[13]. V.Kaviyarasu and S.Baskaran, "Security in MANET Against DDoS Attack", in International Journal of Computer Trends and Technology (IJCTT), Volume 7,Number 1, Jan 2014.

[14]. Meghna Chhabra, Brij Gupta and Ammar Almomani, "A Novel Solution to Handle DDOS Attack in MANET", in Journal of Information Security, July 2013.

[15]. Mohammed Alenezi and Martin J Reed, "Methodologies for detecting DoS/DDoS attacks against network servers", in ICSNC 2012 at IARIA, ISBN: 978-1-61208-231-8, 2012.
[16]. Shuyuan Jin and Daniel S. Yeung, "A Covariance Analysis Model for DDoS Attack Detection", in IEEE Communications Society, ISSN: 0-7803-8533-0/04, 2004.
[17]. Fasheng Yi, Shui Yu, Wanlei Zhou, Jing Hai and Alessio Bonti, " Source-Based Filtering Scheme against DDOS Attacks", in International Journal of Database Theory and Application,2005.
[18]. PyungKoo Park, HeeKyoung Yi, SangJin Hong and JaeCheul Ryu, "An Effective Defense Mechanism against DoS/DDoS Attacks in Flow-based routers", in ACM Conference, ISSN: 978-1-4503-0440-5, 2010
[19]. Jian-Hua song1, 2, Fan Hong1, Yu Zhang1 "Effective filtering scheme against rreq flooding attack in mobile ad hoc networks " proceedings of the seventh international conference on parallel and distributed computing, applications and technologies (pdcat'06)0-7695-2736-1/06 2006.
[20]. MS Neetu Singh Chouhan, MS Shweta Yadav "Flooding attack prevention in manet" international journal of computer technology and electronics engineering (ijctee) volume 1, issue 3.