Evaluation of Performance of Flooding attack in Ad hoc Network

Dharmeshkumar M Mistry
Department of IT Engineering, D.J.Sanghvi College of Engineering
Vile Parle-W, Mumbai, India

Shilpa Verma
Departments of Computer Engineering, Thadomal Shahani College of Engineering
Bandra-W, Mumbai, India

***Abstract*— Ad hoc networks are new paradigm of networks offering unrestricted mobility without any underlying infrastructure. The ad hoc networks have salient characteristics that are totally different from conventional networks. These cause extra challenges on security. In an ad hoc network, each node should not trust any peer. In this paper, A injection of Flooding attack on ad hoc networks is made and the network performance parameter is analyzed and evaluated based on different scenarios.**

I. INTRODUCTION

A mobile ad hoc network is a dynamically self organizing network without any central administrator or infrastructure support. It is composed of mobile terminals that communicate one to the other through broadcast radio transmissions, i.e., transmissions that reach all the terminals within the transmission power range, if two nodes are not within the transmission range of each other, other nodes are needed to serve as intermediate routers for the communication between the two nodes. In ad hoc wireless networks, communicating data is vulnerable to lots of potential attacks due to their characteristics of having dynamic topology, limited bandwidth and energy constraints indeed, data security is an important issue in such environment. In general, the attacks are classified as passive and active. In passive attacks, the attackers attempt to discover valuable information within their transmission range. On the other hand, active attacks attempt to d disrupt the operation of communication. Ad hoc nodes are mobile and the underlying communication medium is wireless, in which case the network is called mobile Ad hoc network (MANET). Mobility is not, however a requirement for nodes in Ad hoc networks, and there may exist static and wired nodes, which may make use of services offered by fixed infrastructure. This infrastructure-less network means that no fixed routing backbones are present and nodes must assume the roles of routers and deliver packets on a multi-hop basis. This lack of infrastructure, dynamic network topology, and distributed operation makes Ad hoc networks appealing for use in personal area networks, meeting rooms and conferences, disaster relief and rescue operation as we as battlefield operations. Due to high requirements of Wireless communication in diverse application areas there is a high probability of threats/attacks to be encountered in a mobile network and these attacks affect the performance parameters of a network.

II. MOTIVATION

Use of wireless links renders an Ad hoc network susceptible to attacks ranging from passive flooding to other attacks too. Flooding might give an attacker a chance to avoid receiver from receiving valid packets means this attack will flood the receiver with syn packets because of which many packets will be dropped, hence evaluating performance of such Mobile Wireless Network has become very important to assess the impact of these attacks to boost network performance. [3, 4]

III. LITERATURE REVIEW

A. Ad hoc Networks

Wireless communication enables information transfer among a network of disconnected, and often mobile, users. Popular wireless networks such as mobile phone networks and wireless LANs are traditionally infrastructure-based, i.e. base stations, access points and servers are deployed before the network can be used. In contrast, ad hoc networks are dynamically formed amongst a group of wireless users and require no existing infrastructure or pre-configuration.Maintaining the Integrity of the Specifications.

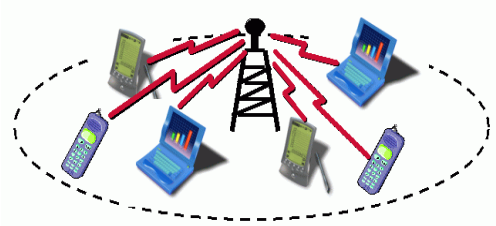


Fig 1.Infrastructure-based wireless network

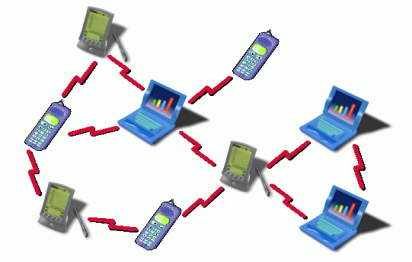


Fig 2.Ad hoc network

B. *Flooding Attack*

In this attack a Malicious node i.e. the attacker node injects false packets into the network or create ghost packets which loop around due to false routing information, efficiently using bandwidth and processing resources along the way. This attack severely affects ad hoc networks causing a huge packet loss to receiver.

IV. SECURITY CHALLANGES

Due to vulnerability in ad hoc networks there are many security challenges to be faced in networks like in flooding attack the initiated malicious nodes tries to hinder or affect the network performanec of the ad hoc network and since its ad hoc network the attacker node keeps changing his position due to which at various postions the attack level differs.If the attacker is near the receiver than its affect will be different and if far than it will again differ in its impact on ad hoc network performance.

V. ATTACK APPROACH(METHODOLOGY)

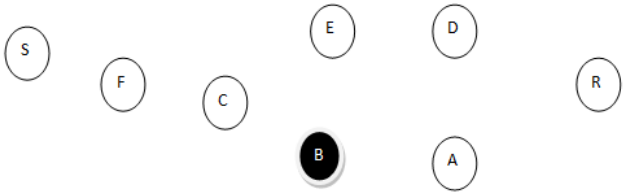
The attack approach discussed in this paper follows following steps:

a) Selection of attacker postion: Here the attacker node will be assigned intial postion before actual transmission begins and then it starts moving.

b) Change number of flooding Packets: Here number of attacking packets will be changed to see their affects on ad hoc network.

*c) Analyze the performance parameters:*In this paper network parameters like Transmisssion time, Packet drop count and Throughput will be evaluated.

d) Network Architecture:



In the network structure nodes S and R are the sender and the receiver nodes respectively. Here node B is the attacker node which performs the attack. This attack is denial of service attack. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes affecting network performance.

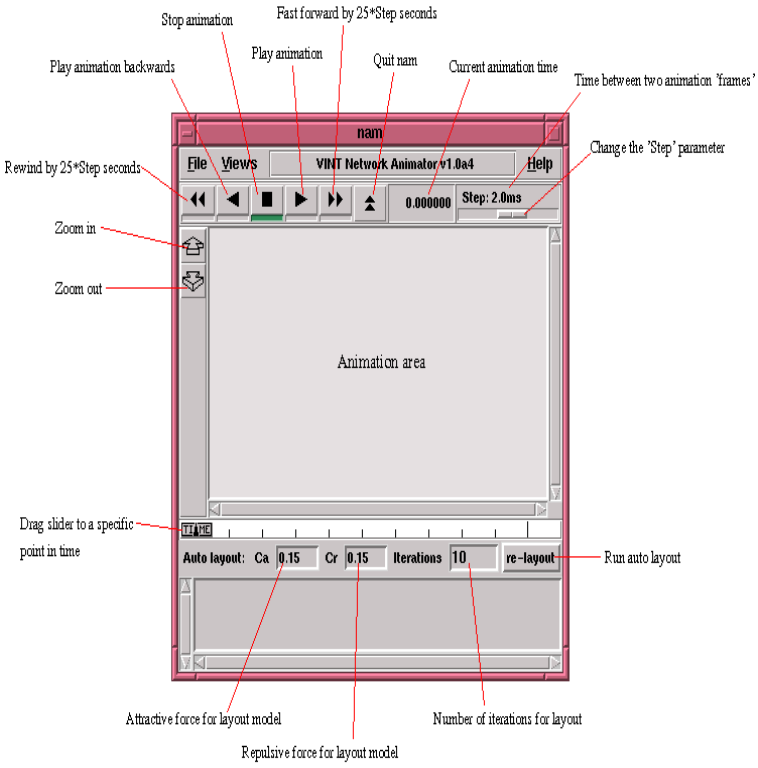
VI. SIMULATION ENVIORNMENT

A. *NS-NETWORK SIMULATOR*

NS is a discrete event simulator targeted at networking research. Ns provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks.

NS began as a variant of the REAL network simulator in 1989 and has evolved substantially over the past few years. In 1995 ns development was supported by DARPA through the VINT project at LBL, Xerox PARC, UCB, and USC/ISI. Currently ns development is support through DARPA with SAMAN and through NSF with CONSER, both in collaboration with other researchers including ACIRI. Ns has always included substantial contributions from other researchers, including wireless code from the UCB Daedelus and CMU Monarch projects and Sun Microsystems,Using NS-2 Simulator the Flooding attack is simulated.

B. *NS-nam (Network Animator)*



VII. SIMULATION PARAMETERS

We conducted our simulation using NS-2 simulator, a scalable simulation environment for wireless network systems. Our simulated network consists of 000 nodes placed randomly with in 1500x300m area. Each node has a transmission range of 250m and moves at a speed of 10m per second.

PARAMETER	VALUES
Channel Capacity	2 Mbps
Packet Size	512 bytes
Traffic Model of Sources	Constant bit rate
Queuing policy for routers	First In First Out

A. *PERFORMANCE METRICS*

- Transmission Time

  It is the amount of time from the beginning until the end of a message transmission. In the case of a digital message, it is the time from the first bit until the last bit of a message has left the transmitting node. The packet transmission time in seconds can be obtained from the *packet size* in bit and the bit rate in bit/s as:

  Packet transmission time = Packet size / Bit rate

- Packets Dropped

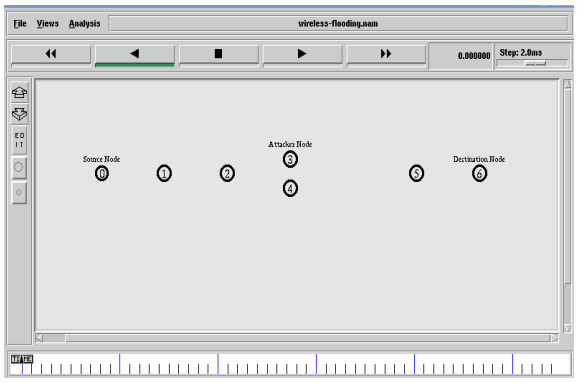
  It's the number of data packets dropped during transmission by a node.

- Throughput

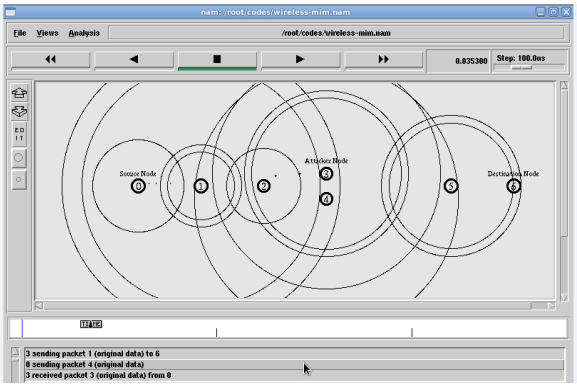
  It is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

VIII. SIMULATION RESULTS

A. *NEWORKS ARCHITECTURE*



B. *PACKET TRANSMISSION*



In this scenario the nodes in the network perform routing and exchange their routing table information with each other and then the source node (node 0) initiates transmission and sends the data to the destination node i.e. node no 6.

C. *PERFORMANCE EVALUATION RESULTS*

After the traffic starts flowing through the network the attacker node start attacking the destination node with flooding packets due to which the receiver is not able to receive correct data i.e. the original data sent from the source node. Because of the attacker node the network performance is affected and using some performance parameters the networks performance is evaluated in terms of transmission time, Packets dropped and throughput.
The evaluated results using NS-2 is obtained as follows

- For Transmission time

Case	Source Node	Destination Node	Sent Time	Received Time	Transmission Time
1	0	6	0.043416501	0.056100201	0.012683700
2	0	6	0.012739688	0.096995885	0.084211172
3	0	6	0.012740012	0.099662316	0.086922304

In the above scenario there are 3 cases implemented. In
Case1: The results are obtained without attacker node.
Case2: The results are obtained with attacker node.
Case3: The results are obtained by increasing the number of attacking packets.

- For Packets dropped

Case	Source Node	Destination Node	No of Packets Sent	No of Packets Received	Packets Dropped
1	0	6	51	51	0
2	0	6	51	38	13
3	0	6	51	26	25

In the above scenario there are 3 cases implemented. In
Case1: The results are obtained without attacker node.
Case2: The results are obtained with attacker node.
Case3: The results are obtained by increasing the number of attacking packets.

- For Throughput

Case	Source Node	Destination Node	Throughput
1	0	6	10511
2	0	6	5311
3	0	6	6589

In the above scenario there are 3 cases implemented. In
Case1: The results are obtained without attacker node.
Case2: The results are obtained with attacker node.
Case3: The results are obtained by increasing the number of attacking packets.

IX. CONCLUTION AND FUTURE DIRECTIONS

Conclusion

The goal of the paper is to evaluate network performance parameters in order to know the impact of attack in adhoc network, while simulating this attack it can be concluded that flooding attack affects the network performance very adversely and disallows the original packet from reaching the destination. The flooding attack adversely affects the packets dropped parameter as the attacker node is sending flooding packets due to which the sending packet cannot reach the destination node because of buffer overflow or all resources occupied by it, hence original packets fail to reach receiver.

Future Direction

This paper deals with one sender and one receiver in adhoc network. Apart from this there are chances to enhance it to have multiple senders and multiple receivers in multicast adhoc network. In this paper it is assumed to have only one attacker node in the network, for future it can be extended by adding more attacker nodes in the network.

REFERENCES

[1] Ali Ashraf Suyyagh, Department of Computer Engineering, University of Jordan IEEE AD HOC Networks Security Challenges, Amman,Jordan, 2009.
[2] Mobile Ad hoc Networks IETF Chapter http : // www.ietf.org / html.charters / manet charter.html
[3] N.SHANTI,DR.LGANESAN and DR.K.RAMAR Study Of Different Attacks in Multicast Ad Hoc Network,JATIT 2009., Department of Computer Science, Tamilnadu, India.
[4] V.Palanisamy,P.Annadurai,S.Vijaylakshmi"Impact of Black hole attack on Multicast in Ad Hoc Network".IEEE Network,2010.Tamilnadu,India.
[5] Priyanka Goyal, Sahil Batra,Ajit Singh,"Literature review of security attack in mobile Ad hoc networks"Nov-2010,Department of Computer Science.Haryana,India.
[6] M.J.Mayer,J.R.Rao and P.Rohatgi.A survey of security issues in Multicast Communications 17(8)(1999) 1380-1994.