MITIGATION OF BYZANTINE ATTACK IN MANET

Jitendra Soni [1] Ashish Soni[2], Shweta Shah [3],Dr.Kirti Mathur [4]
Institute of Engineering and Technology,
DAVV , Indore

ABSTRACT :

Mobile Ad-hoc Networks (MANETs) are future wireless networks consisting entirely of mobile nodes that communicate on-the-move without base stations. MANET is one that comes together as needed, not necessarily with any support from the existing infrastructure or any other kind of fixed Stations. They are highly vulnerable as there is no presence of trusted centralized authority and dynamic network topology.[1] Due to such characteristics of MANET various kind of attacks are possible. Attack in MANET may be active or passive. Jellyfish attack is a kind of DOS(Denial of service) attack in which attackers or malicious nodes try to increase packet end-to-end delay and delay jitter. Before applying attack jellyfish attacker first gain access to the routing group in mobile ad hoc network. This can be possible by performing Rushing attack. According to change in number of senders, receivers and attack position scenarios will get change in jellyfish attack. As attacker get hold of forwarding packet, they starts delaying or dropping data packets for certain amount of time before forwarding them normally. The combination of two or more attacks is called as byzantine attack.

Keywords—Mobile ad hoc network (MANET), Jellyfish attack, byzantine attack, Rushing attack, malicious node.

I: INTRODUCTION

Mobile ad-hoc network is a collection of wireless mobile host without fixed infrastructure and centralized administration

.

Communication in MANET is done via multi hope paths. Nodes in these networks will both generate user and application traffic and carry out network control and routing protocols. Rapidly changing connectivity, network partitions, higher error rates, collision interference, and bandwidth and power constraints together pose new problems in network control—particularly in the design of higher level protocols such as routing and in implementing applications with Quality of Service Lots of challenges are there in this area: MANET contains diverse resources the line of defence is very ambiguous; Nodes operate in shared wireless medium, network topology changes unpredictably and very dynamically, Radio link reliability is an issue, Each node in MANET acts as router those forward data packets to other nodes.[2]

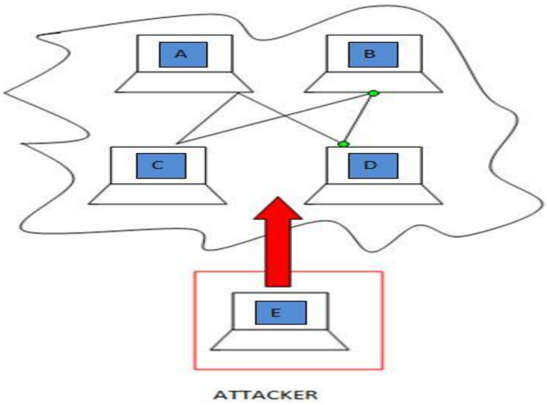
One node can communicate with another that is within its radio range or outside their radio range. It follows an infrastructure less architecture yet has a potential of service discovery, routing and packet forwarding. Communication is possible between two nodes with the help of routing protocols like AODV (Ad hoc On demand Routing Protocol), Link State Routing Protocol, WRP (Wireless Routing Protocol), ZRP (Zone Routing Protocol) etc. In these types of networks nodes can move randomly from one place to another without maintaining any topology, no static topology is there. At any time they can join the network and leave the network. These networks can be easily deployed and also setup time is very less because they do not have fixed infrastructure.

II ATTACKS CLASSIFICATION

Attacks can be classified in many categories like internal attacks, External attacks, Active Attacks Passive Attacks. Attacker can harm the network as internal, external or active, passive so this classification is very important.

A) EXTERNAL ATTACK

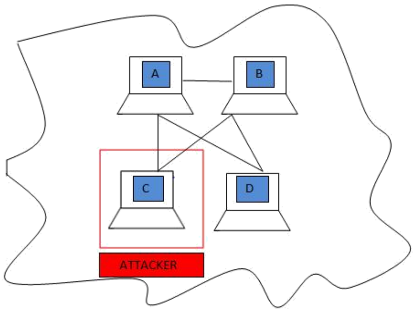
These attacks are basically used by the person who is outside the network and want to get access to the network. And if they get entry to the network then they misuse it, they send spoofed packets and due to which the whole network gets down.[3]



In figure 1, there are four computers or nodes i.e. A, B, C and D and they belongs to a single network. Every computer is connected to each other. Any external computer say computer E which does not belongs to the same network tries to get access to the network and will do malfunctioning in the network.

Internal Attack

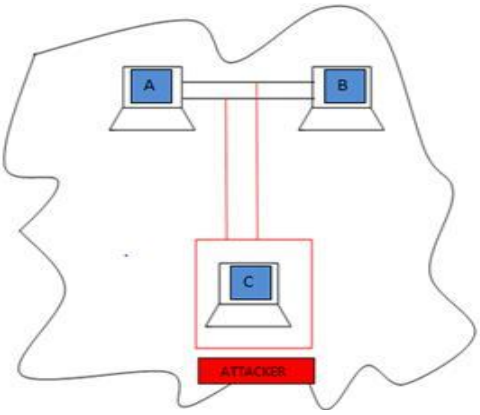
This attack is usually occurs inside the network. The attacker can normally involve in the communication. A new node that is added to the network can act as an attacker that has gain the access to a network.



In figure, initially there are three nodes A, B and D, they all are connected with each and belongs to the same network. Suppose C node came into existence and join the network and hence can participate in the communication. As C node is malicious one so it can hamper the communication by sending spoofed packets to other nodes or by dropping all the packets

B) PASSIVE ATTACKS

In this attack, Attackers can easily get all the information about the network that is useful in hijacking or injecting an attack in the network. It is quite hard to detect passive attacks as compared to active attacks Examples of passive attacks are eavesdropping and Traffic Analysis.



In figure 3, there are two computers A and B which are communicating with each other. Suppose they are sharing or transferring some confidential information and while doing so one more computer i.e. computer C comes into play and it will acts as a sniffer and will listen each and every thing that is going on between computer A and computer B. In this type of attack attacker only listens the information and later on display it to others.

I. EAVESDROPPING

In this the attacker listen all the information that is being transmitted between the two parties in order to find some useful data like passwords, secret codes, confidential information etc.

II. TRAFFIC ANALYSIS

In this the attacker keeps track of the traffic flow so that he is able to detect the location of the hosts. By using this method the attacker can determine the patterns, frequency and length of the message.

C) Active Attack

In active attack the attackers modify the data. It is basically used to reduce the performance of the network. Some of the examples of active attacks are masquerade attacks, replay attacks, DOS attacks.

In figure 4, there are two computers A and B which are communicating with each other and computer C which acts as an attacker will modify or change all the data coming from computer A and then sent the modified data to computer B.

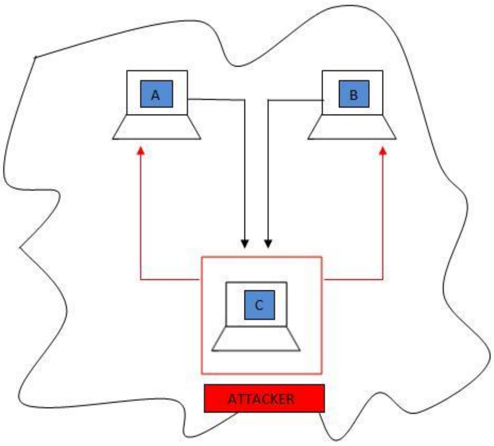
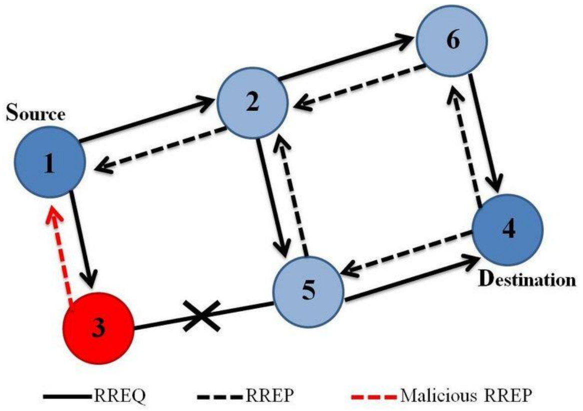


Figure 4: Active Attack

I. BLACK HOLE ATTACK

The black hole attack is one of the well-known security threats in wireless mobile ad hoc networks. The intruders utilize the loophole to carry out their malicious behaviors because the route discovery process is necessary and inevitable. Many researchers have conducted different detection techniques to propose different types of detection schemes. In this paper, we survey the existing solutions and discuss the state-of-the-art routing methods.

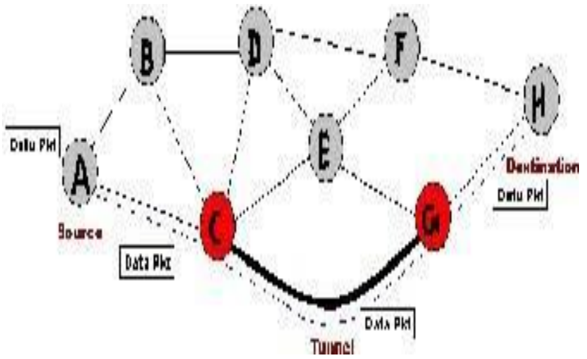
We not only classify these proposals into single black hole attack and collaborative black hole attack but also analyze the categories of these solutions and provide a comparison table. We expect to furnish more researchers with a detailed work in anticipation.[4]



.

II. WORMHOLE ATTACK

This attack belongs to network layer and it one of the most dangerous attack. It basically records information or traffic form one point, tunnels it and then broadcast it to other point. Packet Leases is one of the technique by which wormhole attack can be detected, Packet Leases can be geographic or temporal, and the reason of using leases method is that it will put a limit on greatest amount of transmission distance of a packet. With the help of some of some techniques wormhole techniques can be created for example packet encapsulation, high power transmission capability, packet relay, protocol distortion etc



III. MISROUTING ATTACK

In this attack a selfish node reroute all the traffic originating from a source node and destined for a particular destination node to wrong destination. Hence when a packet does not find its destination, packet is dropped.[5]

IV. SELFISH NODE

Mobile Ad-Hoc Networks special categories of wireless networks that are attracting attention of industry and academia for quite some time due to its Low cost, low power, low bandwidth, multi-functional networks, and design and implementation issues. New algorithms for media access and routing are being designed to optimize the performance. MANETS use multi-hop radio relaying and are capable of operating without the support of any fixed infrastructure. Security is a challenge for implementing Ad-hoc networks. In this paper we are proposing mathematical model for the detection of selfish node in MANETs using k-nearest neighbor technique that classify the nodes into two classes and improves the efficiency.[6]

V.BYZANTINE ATTACK:

A compromised intermediate node or a set of compromised intermediate nodes works in collusion and routing loops, carries out attacks such as creating routing packets on non optimal paths, and selectively dropping packets as in .[7] This module provides the capability to simulate the black hole attack hole, Byzantine wormhole, and Byzantine overlay network wormhole attacks without modifying the routing protocol. It was not possible to simulate the flood rushing attack using this technique because it requires timing changes in the routing protocol code. Because this attack simulation.[8]

III RELATED WORK

[1] Md. AMIR KHUSRU AKHTAR^1 & G. SAHOO^2 et.. al In this paper we have presented the K-Nearest Neighbor technique that can detect selfish nodes with a good confidence as shown by our simulation results. In an adhoc Network, the K-nearest Neighbor classifies an unknown sample on the “votes” of k of its nearest neighbors. It classifies the network into classes and a selfish node is detected easily, then this is a good indication for excluding the node from the network.

[2] K.Mohanaprakash^1, N.Dhanaraj^2, K.Dinakaran^3, T.Mani^4 et.al. In this paper it concludes Ad Hoc on demand distance vector routing algorithm (AODV) in the mobility models of MANET are implemented and analyzed the energy consumption of the mobile nodes and also calculated different parameters namely control overhead, delay, packet delivery ratio and throughput.

[3] Pooja Chahal, Gaurav Kumar Tak, Anurag Singh Tomar **et al.** Sensors are small device that are deployed in a particular are for sensing the data or information. Micro sensors are used in military, health industries, food industries, used for environmental and weather information gathering.

[4] Mai Abdelhakim^1, Leonard E. Lightfoot^2, Jian Ren^3, et.al. In this paper author has concluded that Both static and dynamic attack strategies were discussed. Author proposed sim-plified q-out-of-m fusion schemes by exploiting the linear relationship between the scheme parameters and the net-work size. Author also derived a near-optimal closed-form solu-tion for the fusion threshold based on the central limit theorem.

[5]***MR.HEPIKUMARR.*** KHIRASARIYAThe performance of a connection in a MANET under Jellyfish attack depends heavily on many factors such as the number of flows, node mobility, traffic load, and the number of attackers as well as their positions. Our simulation results confirm an intuitive claim: the more attackers there are in the network, the more damage they inflict on a flow in terms of packet delivery ratio, or delay and delay jitter (jellyfish attack).

[6] Shweta Shah[1], Madhu Sharma[2] and Ashish Jain[3]

Jellyfish Attack exploits the end-to-end communication and creates congestion in transmission protocols. Arbitrary network failure or node failure is the natural phenomena and may vary as per real life deployment, but intentional failure or compromising network may lead to information leakage. Security in mobile networks is a challenging task.

[6] Shweta Shah[1], Madhu Sharma[2] and Ashish Jain[3]

Jellyfish Attack exploits the end-to-end communication and creates congestion in transmission protocols. Arbitrary network failure or node failure is the natural phenomena and may vary as per real life deployment, but intentional failure or compromising network may lead to information leakage. Security in mobile networks is a challenging task.

IV Technology used for implementation

A. Working Environment

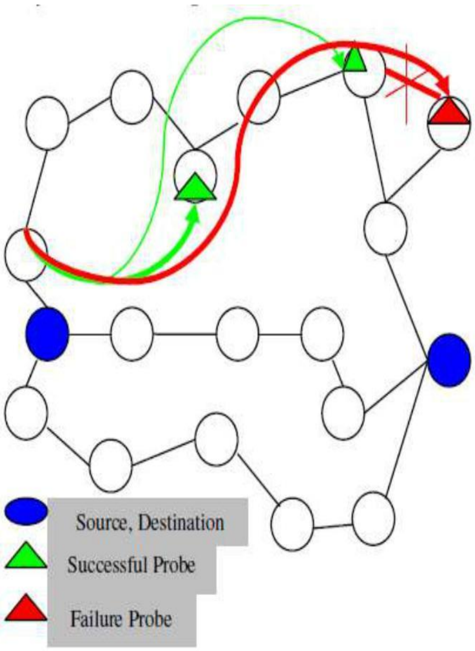
- Qual Net 5.0

B. Simulation Settings and Parameters

No. of Nodes	**100 nodes**
Area Size	**1000 X 1000**
Mac	**802.11**
Radio Range	**250m**
Simulation Time	**50 sec**
Traffic Source	**CBR**
Packet Size	**512 bytes**
Mobility	**Random Way Point**
Protocol	**AODV**

IV IMPLEMENTATION OF PROPOSED ALGORITHM:

In the byzantine attack, A compromised intermediate node or a set of compromised intermediate nodes works in collusion and routing loops, carries out attacks such as creating routing packets on non optimal paths, and selectively dropping packets as in. By selecting secured multiple paths with the removal of faulty links only and not the entire path, the reliability is enhanced and congestion gets reduced. Adaptive probe signals are used to find out the Byzantine Faults. Threshold is set based on the normal behavior of the network. When the loss rate exceeds the threshold, probing will start to find the adversaries. The paths from source to destination are then rated and the most trusted ones are selected for further communication. Reducing the delay and delay variance by predicting the nodes behavior. It reduces the effect of periodic dropping and worm hole problem by ignoring the tunnel path.



V CONCLUSION AND FUTUREWORK

In this proposed system, a fixed threshold is used to identify the faults. Instead of fixed threshold, varying threshold considering dynamic changing networks can be setas well as the periodic dropping of packets by calculating the ration of total packets sent with the total packet received can also be used to identify the malicious nodes The system can be compared with any of the multipath routing protocols like that given in . The additional delay due to probing might be reduced if the location of nodes after mobility especially destination node and adversaries can be predicted. This knowledge about nodes future location and behavior will be helpful in military applications and also in pervasive computing where mobile ad hoc networks plays a major role. Also this work with little variations along with service oriented architecture can be adapted for providing privacy and trust in pervasive computing.

REFERNCES

[1] K.Mohanaprakash[1], N.Dhanaraj[2], K.Dinakaran[3], T.Mani[4]
Implementation of Routing Protocols in MANET based on Energy Consumption and Security Volume-6, Issue-1, January-February-2016

[2] Pooja Chahal, Gaurav Kumar Tak, Anurag Singh Tomar Comparative Analysis of Various Attacks on MANET International Journal of Computer Applications (0975 – 8887) Volume 111 – No 12, February 2015

[3] Mai Abdelhakim1, Leonard E. Lightfoot2, Jian Ren3, An Overview of MANET: Applications, Attacks and ChallengesIJCSMC, Vol. 3, Issue. 1

[4]MR.HEPIKUMARR.KHIRASARIYA
SIMULATION STUDY OF JELLYFISH ATTACK IN MANET (mobile ad hoc network) USIND AODV ROUTING PROTOCOL VOLUME – 02, ISSUE – 02

[5] Shweta Shah1, Madhu Sharma2 and Ashish Jain3 “Mitigation for Jelly Fish Attack on MANET” Vol. 2 Issue 4 Year: 2016

[6] Ruohan Cao, Tan F. Wong, Tiejun Lv, *Senior Member, IEEE*, Hui Gao, *Senior Member, IEEE*,
and Shaoshi Yang, *Member, IEEE* “Detecting Byzantine Attacks Without Clean Reference”PUBLISHED IN IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 12, DECEMBER 2016

[7]LINYUAN ZHANG1, GUORU DING1,2,Defending Against Byzantine Attack inCooperative Spectrum Sensing: DefenseReference and Performance Analysis” Received June 9, 2016, accepted July 15, 2016, date of publication August 8, 2016, date of current version August 26, 2016.*Digital bject Identifier 10.1109/ACCESS.2016.2593952.*

[8] Parvinder Kaur1• Dalveer Kaur2• Rajiv ahajan3 "Simulation Based Comparative Study of Routing Protocols Under Wormhole Attack in Manet" Wireless Pers Commun (2017) 96:47–63DOI 10.1007/s11277-017-4150-2

Mr.Jitendra Soni is presently serving as Assistant Professor in IET-DAVV Indore His key research areas are Wireless Network Security ,Data Mining and Warehousing . He has published various papers in journals and conferences of international and national repute

Mr. Ashish Soni is presently serving as Research Scholar in IET-DAVV Indore His key research areas are MANET, Wireless Network Security ,Data Mining and Warehousing . He has published various papers in journals and conferences of international and national repute

Ms. Shweta Shah is presently serving as Research Scholar in IET-DAVV Indore Her key research areas are MANET, Wireless Network Security ,Data Mining and Warehousing . She has published various papers in journals and conferences of international and national repute

Dr. Kirti Mathur is presently serving as Associate Professor in DAVV Indore. Her key research areas are Data Mining and Warehousing , Wireless Network Security. She has published various papers in journals and conferences of international and national repute