International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-4)

Research Article | **April 2014**

Worm-Hole Detection Mechanism for Reactive Routing of Mobile Ad-Hoc Network

Mr.Ashish M. Mishra
PG Scholar,
Dept. of CSE, SKSITS, Indore, India

Mr. Charan Singh
Assistant Professor & Head,
Dept. of CSE, SKSITS, Indore, India

Abstract-

Mobile ad-hoc network is an infrastructure less and self-organizing concept of network organization. Due to the ad-hoc nature of network there are various security issues arises in the network. These security issues decreases the network performance in terms of battery power consumption, throughput and other performance parameters. The security of network resources is breaches by the malicious nodes which may either internal or external. Malicious node influence network working via putting the several of kinds of attacks. Certain number of protocols and methods are advised to prevent network from malicious nodes. This work tries to detect wormhole attack which played by malicious node.

Keywords- Ad-hoc network, Vulnerabilities, Attack Types, Problem Domain, Solution Domain

I. INTRODUCTION

Wireless Mobile ad hoc network is an infrastructure less network & dynamic in nature. An infrastructure network does not have any fixed infrastructure for the communication. Each node in such type of network can communicate directly with other nodes in the network & there is no requirement of any centralized network access point. An important thing about these types of networks is that these networks do not have any routers but the wireless nodes work as a routers & a host. These networks don't have any fixed or static topology [1] [2].

A mobile ad hoc network consists of mobile nodes that use wireless transmission for communication. In these type of networks the nodes are movable (move from one place to another) and the motion of nodes may be random or periodical [3]. Due to node mobility nature of nodes, the nodes have limited battery power & limited bandwidth. In absence of centralized access point or administrator the source & destination communicate through multiple hops. The MANET is also called a multi hop wireless network. A MANET is an autonomous collection of mobile nodes or users [4].

II. MANET VULNERABILITIES

Weakness in security system is called vulnerability. An ad hoc system may be vulnerable to unauthorized access because the system does not verify a user's identity before allowing data access. Wireless MANET is more vulnerable than wired network. Some of the vulnerabilities are given below [5]:-

Absence of centralized management: Wireless MANET does not have any centralized monitor or management server or node. The absence of centralized management makes difficult to detect any type of attacks because it is not easy to monitor or manage the traffic in a highly dynamic and large scale MANET.

Scalability: Due to mobility of nodes, network topology of ad-hoc network changing all the time. So that in MANET scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

Cooperativeness: Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

III. ATTACKS ON MANET

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

External Attack: External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.

Internal Attack: Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities.

Denial of Service attack: This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.

Impersonation: If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.
Eavesdropping: This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.
Routing Attacks: The malicious nodes make routing services a target because it's an important service in MANETs. There are two flavors to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.
Black hole Attack:: In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it.[9] A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

IV. LITERATURE SURVEY

The aims of Ad hoc networks and particularly MANET have in recent years not only seen widespread use in commercial and domestic application areas but have also become the focus of intensive research. Applications of MANET's range from simple wireless home and office networking to sensor networks and similarly constrained tactical network environments. Security aspects play an important role in almost all of these application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the very fact that radio communication takes place. This dissertation contents various literature surveys, which cover all dimensions of study. We have reviewed many research papers which are published in various conference and International journals.

A. RELATED STUDY

Sunil Taneja, Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc networks" international Journal of Innovation Management and Technology , Volume.1 August 2010, ISSN 2010-0248. Mobile Ad Hoc Network (MANET) is collection of multi-hop wireless mobile nodes that communicate with each other without centralized control or established infrastructure [1]. The wireless links in this network are highly error prone and can go down frequently due to mobility of nodes, interference and less infrastructure. Therefore, routing in MANET is a critical task due to highly dynamic environment. In recent years, several routing protocols have been proposed for mobile ad hoc networks and prominent among them are DSR, AODV and TORA. This research paper provides an overview of these protocols by presenting their characteristics, functionality, benefits and limitations and then makes their comparative analysis so to analyze their performance. The objective is to make observations about how the performance of these protocols can be improved [9].

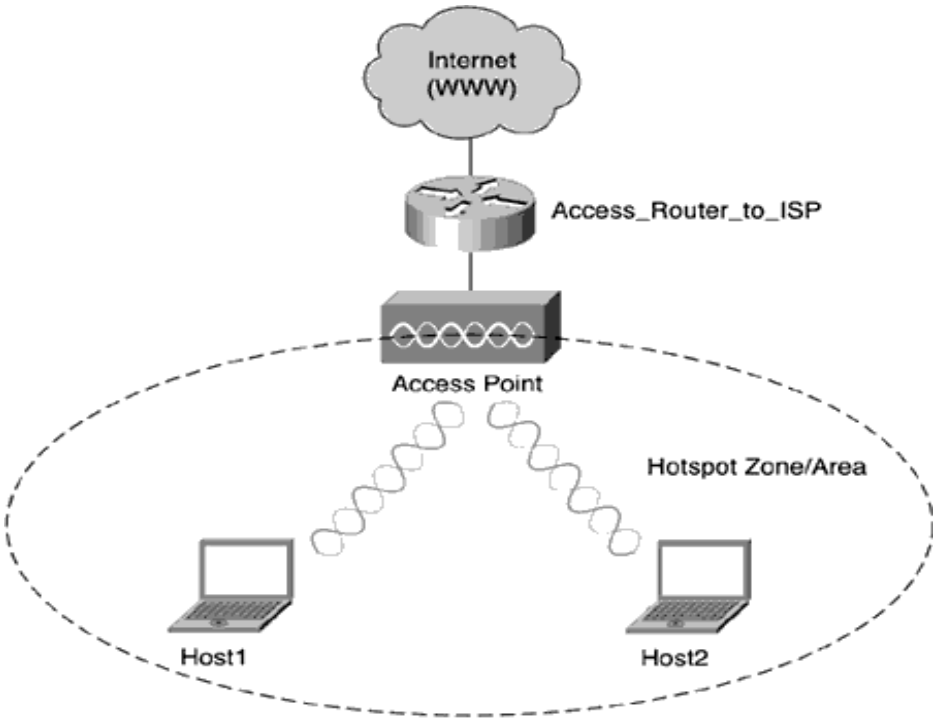

Figure.1 Infrastructure Wireless Network

The other type of network, Infrastructure less network, is known as Mobile Ad Hoc Network (MANET).

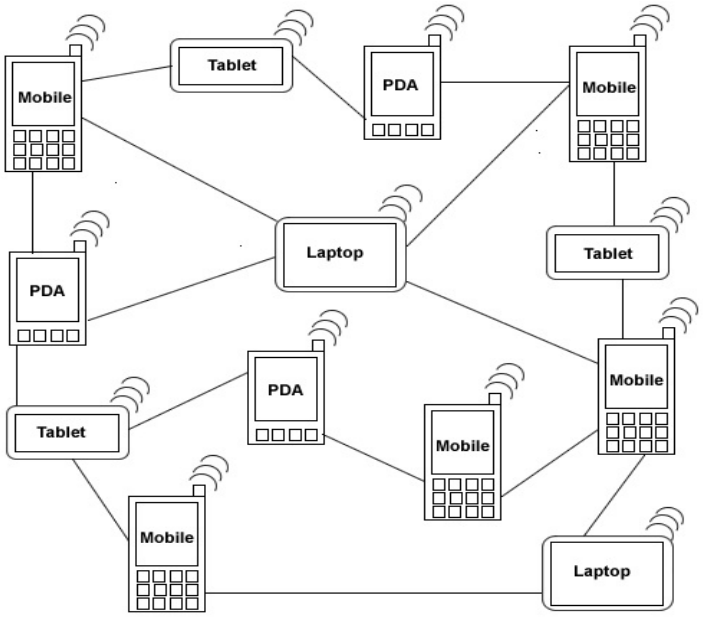

Figure 2 Infrastructure less Ad-hoc network (MANET)

In this research paper, an effort has been made to concentrate on the comparative study and performance analysis of various on demand/reactive routing protocols (DSR, AODV and TORA) on the basis of above mentioned performance metrics. The results after analysis have reflected in Table I and Table II. The first table is description of parameters selected with respect to low mobility and lower traffic. It has been observed that the performance of all protocols studied was almost stable in sparse medium with low traffic. TORA performs much better in packet delivery owing to selection of better routes using acyclic graph. Table II is evaluation of same parameters with increasing speed and providing more nodes. The results indicate that AODV keeps on improving with denser mediums and at faster speeds. Table III is description of other important parameters that make a protocol robust and steady in most cases. The evaluation predicts that in spite of slightly more overhead in some cases DSR and AODV outperforms TORA in all cases. AODV is still better in Route updating and maintenance process. It has been further concluded that due to the dynamically changing topology and infrastructure less, decentralized characteristics, security and power awareness is hard to achieve in mobile ad hoc networks. Hence, security and power awareness mechanisms should be built-in features for all sorts of applications based on ad hoc network. The focus of the study is on these issues in our future research work and effort will be made to propose a solution for routing in Ad Hoc networks by tackling these core issues of secure and power aware/energy efficient routing [9].

V. PROBLEM DOMAIN AND SOLUTION DOMAIN

A. Problem Domain -In Mobile Ad Hoc Network security plays an important role when data transmission is performed within un-trusted wireless environment. There are various kinds of attacks (attacks like Black Hole, White Hole, Gray Hole, Wormhole and many more) have been identified & corresponding solution have been proposed. All these attacks are caused by the malicious node hence ad wireless network is unprotected from the attacks of the malicious node. Out of all these attacks the wormhole attack is the most harmful attacks in which two or more malicious node create a virtual tunnel in the network. There are two types of wormhole attacks have been identified:

- Hidden attack
- Exposed attack

For both types of attacks many detection mechanisms or algorithms are proposed by the researchers. But the existing methods have some drawbacks.

The mechanisms DelPHI proposed by Hon Sun Chiu and King-Shan Lu "DelPHI Wormhole detection Mechanism for Ad Hoc Wireless Networks" 0-7803-9410-0/06, IEEE, in 2006. The mechanism able to tackle the both the wormhole attacks by calculating delay or hop value to serve as the indicator of detecting wormhole attacks.

The DelPHI method avoids the need of synchronization & it does not require any special hardware there for it provides higher power efficiency but it has some drawbacks such as reliability & message overhead.

B. Solution Domain In our proposed solution, First of all we will find out the Time to Leave (TTL) values and the same time we will also find out the hop count values between source nodes to destination node of each and every route. After finding the values of TTL & Hop Count we will find out the Delay per Hop (DPH) values of each & every route by using the values of TTL & Hop Count. After finding the value of DPH we will check the energy of each and every node previous to destination node.

- **Calculating of TTL**: When source node calculates the value of TTL of every route from source node to destination node it generates RREQ packet marked with R flag, set Ts field (Sending Time of RREQ packet) & hop count is equal to zero initially & forward the RREQ packet to its all neighbors to establish a route. Neighbors node receives an RREQ packet, increases hop count value by one & forward RREQ packet to its neighbors. When the destination node receives RREQ packet it generates an RREP packet marked R flag to RREP flag, set hop count is equal to zero initially & forward the RREP packet to its all neighbors in reverse or backward route (route from destination node to source node).

  Neighbors node receives an RREP packet, increases hop count value by one & forward RREQ packet to its neighbors in reverse direction.

Source node receives two or more RREP packets from different routes & calculates the Time to Leave (TTL) value of each & every route.

$$TTL=Tr-Ts$$

Where Tr is receiving time of RREP packet & Ts is sending time of RREQ packet.

- **Hop Count:** When source node receives two or more RREP packets from different routes it gets the hop count value of every route.
- **Calculation of Delay per Hop(DPH):** When source node gets the value of TTL & Hop Count it calculates the DPH(Delay Per Hop) value of each & every route by given formula

  DPH=TTL/2*Total Hop Count
- **Energy checking of nodes previous to destination:** Now source node sends energy check packet through every route towards destination node & calculate the energy of every nodes previous to destination node.

VI. SIMULATOR TOOL

Network Simulator-2: The entire simulations were carried out using ns 2.31 network simulator which is a discrete event driven simulator developed at UC Berkeley as a part of the VINT project. The goal of NS2 is to support research and education in networking. It is suitable for designing new protocols, comparing different protocols and traffic evaluations. NS2 is developed as a collaborative environment. It is distributed as open source software. A large number of institutes and researchers use, maintain and develop NS2. NS2 Versions are available for Linux, Solaris, Windows and Mac OS X.

VII. CONCLUSION

In ad hoc network wormhole attacks can degrade network performance significantly and harms the network security. Wormhole attacks detection is quite complicated. Different types of security attacks described. After describing security attacks, the existing wormhole detection techniques discussed. Finally, by analyzing the advantages and disadvantages of all the existing techniques, an approach proposed to detect wormhole attack in ad hoc networks.

REFERENCES

[1] Pallavi Sharma, Aditya Trivedi, "An Approach to Defend Against Wormhole Attacks in Ad Hoc Network using Digital Signature". IEEE ISSN 978-1-61284-486-2/2011.
[2] Radhika Saini, Manju Khari, "Defining Malicious Behaviour of a Node and its Defensive Methods in Ad Hoc Network" International Journal of Computer Applications (0975-8887) Volume 20-No.4, April 2011.
[3] Rajbir Kaur, M.S. Gaur, V. Laxmi. " A Novel Attack Model Simulation in DSDV Routing" 978-1-4244-8704-2 IEEE 2011.
[4] Reshmi Maulik and Nabendu Chaki, "A Study on Wormhole Attacks in MANET" International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279.
[5] E.A. Mary Anita, V. Thulasi Bai, "Defending Against Wormhole Attacks in Multicast Roruting Protocols for Mobile Ad Hoc Networks" 978-1-4577-0787-2/2011 IEEE.
[6] Saurabh Gupta, Subrat Kar, S. Dharmaraja, "WHOP: Wormhole Attack Detection Protocol Using Hound Packet" 978-1-4577-0314-0/2011 IEEE.
[7] Xiaomeng Ban, Rik Sarkar, Jie Gao, "Local Connectivity Test to Identify Wormholes in Wireless Networks" ACM 978-1-4503-0722-2/11/05. May 2011.
[8] Pallavi Sharma, Aditya Trivedi, "Prevention of Wormhole Attack in Ad-Hoc Network" ISSN 0975-8887 ICEICE No.5, Dec 2010.
[9] Sunil Taneja, Ashwani Kush " A Survey of Routing Protocols in Mobile Ad Hoc networks" International Journal of Innovation Management and Technology, Vol.1 August 2010, ISSN 2010-0248.
[10] Priyanka Goyal, Sahil Batra Ajit Singh, "A Literature Review of Security Attack in Mobile Ad- Hoc Networks" International Journal of Computer Applications (0975-8887) Volume 9, No. 12 November 2010.
[11] Marianne Azer, Sherif EI-Kassas, Magdy EI-Soudani, "A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks In wireless Ad Hoc Networks" International journal of Computer Science and Information security, IJCSIS Vol. 1, No. 1 May 2009.