Novel Approach for reducing the effect of Wormhole attack by reactive routing Approach

ER. Hareesh Kumar
ECE Department
PCET,Punjab
harrymehta1@gmail.com

ER. MANASVI MANNAN
ECE Department
PCET,Punjab
MANASVI.MANNAN24@GMAIL.COM

Abstract
Most previous ad hoc networks research has focused on problems such as routing and Communication, assuming a trusted environment. In this study, this scheme is based on location information, it uses the location information by using a special hardware to detect the wormhole attack and after detection it chooses the path for routing. There are various network structures used to place the nodes in this research work reference point group mobility model and to prevent the wormhole.

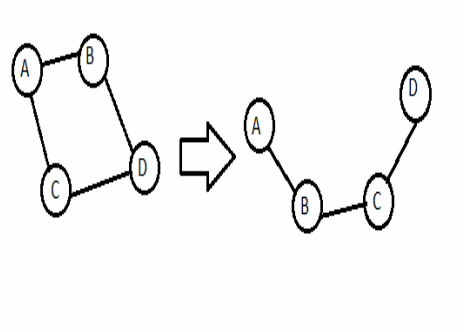
INTRODUCTION

A Mobile Ad Hoc Network (MANET) is the network having no infrastructure .These networks are self organizing ,all the mobile nodes plays the role of router by itself .These networks communicate via wireless links without any fixed infrastructure or fixed access point that maintains all routing activities of mobile nodes, in MANET term mobile nodes implies that the nodes are wireless devices like(Smart phones ,laptops and etc.),Ad-hoc implies that the network having no infrastructure for routing activities and wireless links shows that communication is done by dynamic topology.

Fig shows an example of an ad hoc network, where there are numerous combinations of transmission areas for different nodes. From the source node to the destination node, there can be different paths of connection at a given point of time. But each node usually has a limited area of transmission as shown in fig. 1 by an oval circle around each node. A source can only transmit data to node B but B can transmit data either to C or D.

Routing is the act of moving information from a source to a destination in a network. During this process, at least one intermediate node within the network is encountered. The routing concept basically involves two activities: firstly, determining optimal routing paths and secondly, transferring the information groups (called packets) through a network .Unlike wired network where data is transferred over the physical link which makes these networks more secure than the wireless networks .Wireless links makes easy way for attackers to attack because the communication medium is air(radio

communication channel).Due to this limitation various types of attacks active attacks and passive attacks .Active attacks drops the packets and also modify the data and Passive attacks only listen to the packets but does not modify In MANET topology changes very frequently as shown in the Figure 2.2.



2 Applications of MANET

Ad Hoc network gives various applications to many fields. As in day to day life emails and files are transferred over the network by using mobile nodes with in an ad hoc environment. The wide range of applications is available in the military area such as battlefield in an unknown territory, where an infrastructure is not possible .In that type of situations ad hoc network are capable to serve applications are:

a. Tactical Networks - Tactical networks are used for communicate in battlefield and other military applications.

b. Crises management Operations **–** Ad hoc networks are used in emergency rescue operations and in disaster fixed network replaced by ad hoc network to maintain communication.

c. Commercial environment – On commercial front these networks are used in electronic payments, mobile offices .dynamic database access and etc.

d. Education **–** Ad hoc communication during meetings and maintain virtual classrooms.

e. Personal area networking **–** Ad hoc network used as personal like cell phones, wrist watch and laptops.

2.3 **Characteristics of MANET**

Various characteristics of MANET are following:

Autonomous infrastructure

All nodes in MANET's are autonomous; they play the role of both host and router. There is no need for central administration.

Dynamic Topology

In mobile ad hoc network nodes are free to move randomly .Topology changes very frequently and have no margins. Nodes move arbitrarily so as the result topology changes in a irregular manner and nodes free to establish the links dynamically

Multiple hop Routing

In mobile ad hoc networks communication is done through multi hops .There are multiple nodes in the network and all nodes having limited range to transmit the packets .As all nodes are not in range of each other, so they use multi hops in between to communicate with each other.

Energy Constraint

As in mobile ad hoc network all nodes has limited energy due to restricted battery life. Extra load decrease the battery level at higher rate. Therefore energy conservation is an important issue.

Low Bandwidth

All nodes in ad hoc network communicate in wireless environment. Wireless links are weaker than infrastructure networks .The links are affected by noise, interference, fading and multiple accesses.

Limited Security

Mobile ad hoc networks are distributed in nature and having no central administrator to maintain all network. Nodes are free to move in distributed manner which makes these networks more vulnerable to various threats .Attacker can easily attack on these type of networks due to random nature.

Literature Review

Abdesselam et al [1] presented an effective method for detecting and preventing wormhole attacks in OLSR.To find wormhole tunnels a simple four-way handshaking message exchange method is used. The proposed solution is easy to deploy: it does not need the time synchronization or any location information .It does not require any complex computation or special hardware requirement. The performance of this approach shows a high detection rate under various scenarios. This method first attempt to pinpoint links that may potentially be part of a wormhole tunnel, then a proper wormhole detection mechanism is applied to suspicious links by means of an exchange of encrypted probing packets between the two supposed neighbors (end points of the wormhole).

Mary et al [2] analyzed the performance of reactive multicast routing protocol On Demand Multicast Routing Protocol (ODMRP) under the influence of worm hole nodes under different scenarios and design a Worm Hole Secure ODMRP (WHS-ODMRP) by applying certificate based authentication mechanism in the route discovery process. The proposed protocol reduces the packet loss due to malicious nodes to a considerable extent thereby enhancing the performance.

Zhou et al [3] proposed a new algorithm called Neighbor-Probe-Acknowledge (NPA) for detection of wormhole attacks. NPA does not require time synchronization or any other hardware. Moreover, it accomplishes higher detection rate and lower false alarm rate than the methods using RTT under different background traffic load conditions. By theoretical analysis and comprehensive experiments, wormhole attacks links are easy to detect, standard deviation of *RTT* (*stdev* (*RTT*)) is a more effective metric than per-hop *RTT* to detect wormhole attacks.

Lazos et al [4] proposed the use of geometric random graphs induced by the communication range constraint of the nodes; we present the necessary and sufficient conditions for detecting and defending against wormholes. Using our theory, we also present a defense mechanism based on local broadcast keys. We believe our work is the first one to present analytical calculation of the probabilities of detection

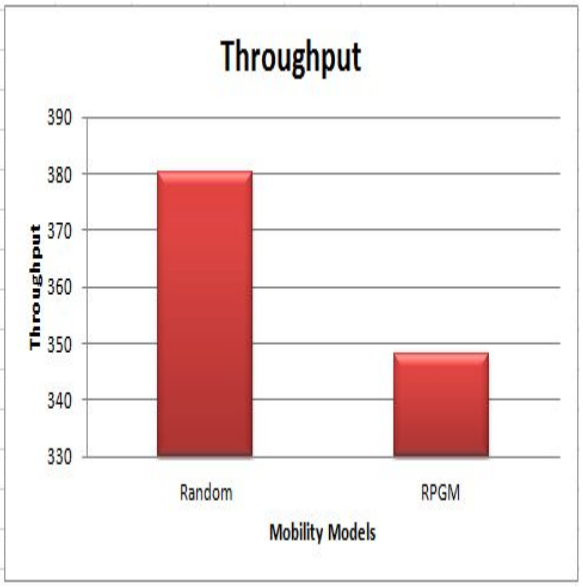
Dhurandher et al [5] proposed an energy efficient scheme to detect the wormhole attack called Energy efficient scheme to immune the wormhole attack (E2IW). This protocol usage the location information of the mobile nodes to find the presence of a wormhole, and in case a wormhole exists in the path, it discovers another routes involving the nodes of the selected path so as to get a more secure route to terminus. The protocol is capable of detecting wormhole attacks employing either hidden or participating malicious nodes. Simulations are conducted, showing that E2SIW can find wormholes with a high detection rate, less overhead, and can consume less energy in less time. This protocol keep down the overhead related with the control packets.

S. Gupta et al [6] proposed an approach, called WHOP (Wormhole Attack Detection Protocol using Hound Packet), which is based on the AODV protocol and considered to detect wormhole attack with the help of hound packets. In this approach a hound packet is sent after the route discovery process, means after the route has been discovered. This hound packet is processed by all the nodes except that nodes which are involve in the path setup process. Basically the path discovery is done by the help of the two types of packet, called RREQ and RREP. When the sender gets the message, it creates a hound packet and computes its message digest and signed this message digest with its own private key and attached all this information with the hound packet. But processing delay of the packet becomes high.

Graphs:

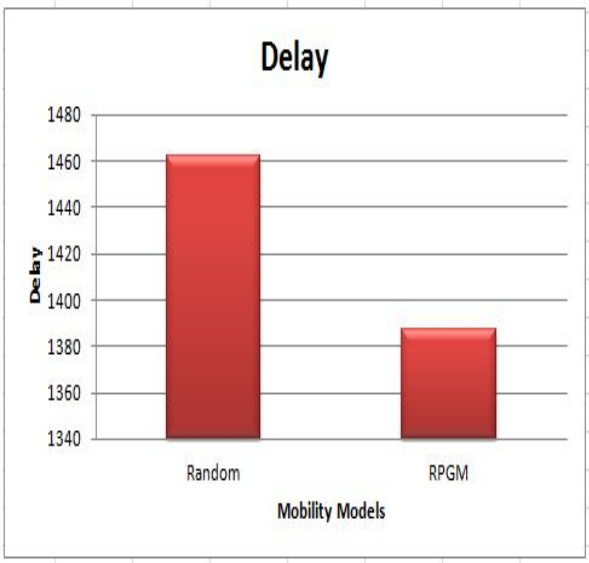
(a)Throughput:

It is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation i.e., information whether or not data packets correctly delivered to the destinations.

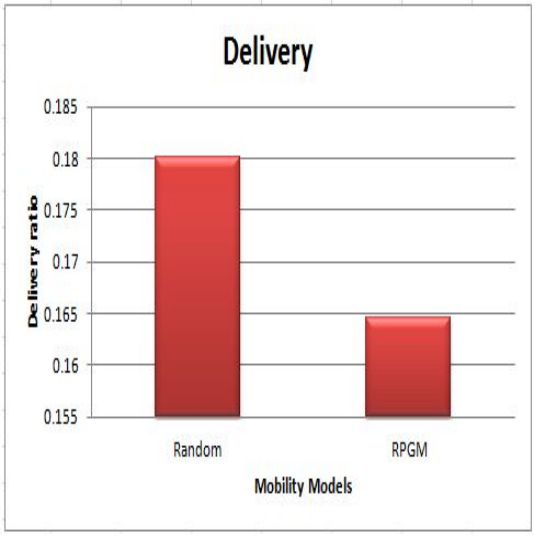


From graph it shows that RPGM take less time to deliver the packet on destination instead of Random model.

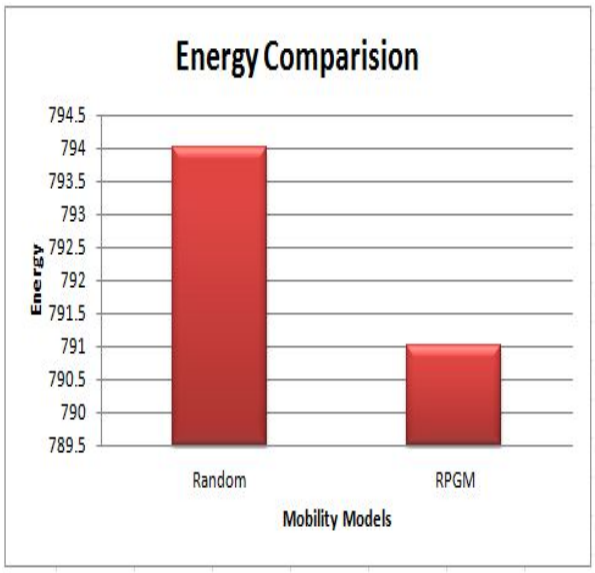
(b)End to end Delay: the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.



(c) Packet delivery ratio: the ratio of the number of delivered data packet to the destination. The ratio of the number of delivered data packet to the destination.



(d)Energy Comparison:



Proposed Methodology

5.1 Simulation Platform:

5.1.1 Linux Operating System:

Linux operating system is a free software program. It is based on the Unix operating system. It is free to download and use. Linux is a multi-user, preemptive, multitasking operating system which provides a number of facilities including management of hardware resources, directories and file systems, and the loading and execution of programs. It is runs on a variety of platforms, especially personal computers with Intel 80386 or better processors. It supports a wide range of software, from TeX, to the X Window System,

to the GNU C/C++ compiler, to TCP/IP. It's a versatile, bona fide implementation of UNIX, freely distributed under the terms of the GNU General Public License.

Linux can turn any 80386 or better personal computer into a workstation that puts the full power of UNIX at your fingertips. Businesses install Linux on entire networks of machines, and use the operating system to manage financial and hospital records, distributed computing environments, and telecommunications. Universities worldwide use Linux to teach courses on operating system programming and design. Computing enthusiasts everywhere use Linux at home for programming, productivity, and all-around hacking.

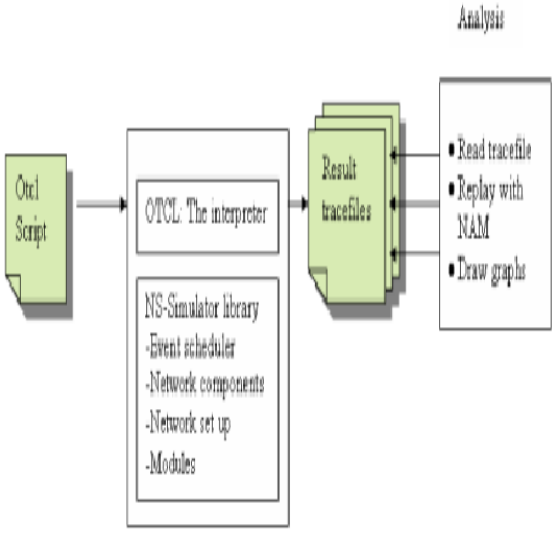
The two major components of Linux is the kernel and the shell. The kernel is the core of the Linux operating system which schedules processes and interfaces directly with the hardware. It manages system and user I/O, processes, devices, files, and memory. The shell is a command line interface to the kernel. Users input commands through the shell, and the kernel receives the tasks from the shell and performs them. The shell tends to do four jobs repeatedly: display a prompt, read a command, process the given command, then execute the command. After which it starts the process all over again.

5.1.2 NS-2 Simulator :

NS-2 is easily available and is free software. It can be installed in both Windows under Cygwin installation or under VMware and as well as in Linux. To Setup and run a simulation, Otcl scripts are written which is responsible for event scheduler, setting up the network topology and setting up the simulation time for sending transmitting packets through event scheduler. When the simulation is completed and environment for OTcl script is set i.e. when command ns filename.tcl is run, another file known as trace file is created that contain detailed simulation data and is a text based and is used to analyze directly or used in graphical user interface Network Animator (NAM).

Currently there are many tools available for simulation like NS-2, Omnetpp, Opnet, and GlomoSim. But none of them is effective for wireless sensor network simulation. Some functionalities are missing for sensor simulation so for those functionalities some external tools are available free to download and in Tools. For e.g. for Omnetpp, there is Castalia tool available for sensor simulation and for NS-2, MannaSim is available. These are the basically patch which is to be embedded during installation. These patch basic requirement is Linux environment.

The hardware used for implementing the proposed idea is Laptop with efficient memory for preceding the work. The operating system used is Ubuntu 11.10. The network simulator used is NS-2 (version 2 .34).



NS-2 is easily available and is free software. It can be installed in both Windows under Cygwin installation or under VMware and as well as in Linux. To Setup and run a simulation, OTcl scripts are written which is responsible for event scheduler, setting up the network topology and setting up the simulation time for sending transmitting packets through event scheduler. When the simulation is completed and environment for OTcl script is set i.e. when command ns filename.tcl is run, another file known as trace file is created that contain detailed simulation data and is a text based and is used to analyze directly or used in graphical user interface Network Animator (NAM).

References:

[1] Bo Sun, Yong Guan, Jian Chen and Udo W. Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Networks", In the Proceedings of European Personal and Mobile Communications Conference, pp. 490-495,2003.

[2] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks". In the Proceedings of the 42nd Annual Southeast Regional Conference, ACMSE , pp. 96-97, 2004.

[3] Pradeep Kyasanur, and Nitin H. Vaidya "Selfish MAC Layer Misbehavior in Wireless Networks", IEEE Transactions on Mobile Computing Journal, Vol. 4(5), pp. 502-516, 2005.

[4] Gao Xiaopeng, and Chen Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", In the Proceedings of IFIP International Conference on Network and Parallel Computing, pp. 209-214, 2007.

[5] R.A. Raja Mahmood and A.I. Khan, "A Survey on Detecting Black Hole Attack in AODV-Based Mobile Ad Hoc Networks", In the Proceedings of IEEE International Symposium on High Capacity Optical Networks and Enabling Technologies, pp. 1-6, 2007.

[6] Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto, and Nei Kato, " A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks", IEEE Transactions on Vehicular Technology, Vol. 58(5), pp.2471 –2481, 2009.

[8] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", In the Proceedings of the 42nd Annual Southeast Regional Conference. ACM, pp. 96-97, 2004.

[9] Onkar V. Chandure and V. T. Gaikwad, "A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV Routing Protocol in MANET", International Journal of Computer Science and Information Technologies, Vol. 2(6), pp. 2607-2613, 2011.

[10]Chetan S. Dhamande and H.R. Deshmukh ," A Efficient Way to Minimize the Impact of Gray Hole Attack in Ad-hoc Network", International Journal of Emerging Technology and Advanced Engineering, Vol. 2(2), pp. 106-110, 2012.

[11] Onkar V. Chandure, Aditya P. Bakshi, Saudamini P. Tidke and Priyanka M. Lokhande, " Simulation of Secure AODV in Gray Hole Attack for Mobile Ad-hoc Network" , International Journal of Advances in Engineering & Technology, Vol. 5(1), pp. 67-76 , 2012.

[12] Avenash Kumar and Meena Chawla, "Destination Based Group Gray Hole Attack Detection in MANET through AODV", International Journal of Computer Science Issues Vol. 9(4), pp. 292-295, 2012

[13] Sarita Chaudhary and Kriti Sachdeva, "Discovering a Secure Path in MANET by Avoiding Black/ Gray holes", International Journal of Recent Technology and Engineering, Vol. 1(3), pp. 88-93, 2012.

[14] Ashok M. Kanthe, Dina Simunic and Ramjee Prasad," A Mechanism for Gray Hole Attack Detection in Mobile Ad–hoc Networks", International Journal of Computer Applications ,Vol. 53(16), pp. 23-30, 2012.

[15] C.S. Dhamande and H.R. Deshmukh , "A Competent Way to Diminish the Brunt of Gray Hole Attack in MANET ", International Journal of Wireless Communication, Vol. 2(1), pp. 29-34, 2012

.