Detection and Removal of Wormhole Attacks In Ad Hoc Wireless Networks for Secure Routing

kamal kumar[1],Mr. Sanjeev shrivastava[2], Dr. Mohit Gangwar[3], Mr. Suresh Gawande[4]

Abstract: *Wireless communication is the integral part of our today's life. Mobile phones, DTH services, internet services, are the few example of this technology. With the passes of time this wireless communication is becoming more and more advance. MANET is one of the recent developments of wireless technology. This provides new paradigm for wireless self organized networks. MANET is based on "on-demand" technology where routes are established only when it is required. This network is also termed as anywhere any time computing. Spontaneous formation of mobile networks takes place for a specified period of use.*

Practically, MANET suffers with lot security attacks due to its Dynamic nature. Lot of research work is going on towards this direction. So many protocols are also available but they do not provide proper security. Ad-Hoc network is accessible for both, intended user and malicious attackers if no security measures are considered. This is not desirable for any network. It is also found that different protocols needs different methodology for security. This dissertation provides overview of all the secured routing protocols, their advantages and disadvantages in terms of comparative study to analyze their performance.

Introduction

Communication is simply the process to establishing link between transmitter and receiver. Communication can be completed only when transmitter receiver and channel (medium) is present. Based upon types of channel, communication can be broadly classified into two major categories wired communication and wireless communication. Today is the era of wireless communication. Mobile phones, internet technologies, wacky talky, RADDAR technologies are the few example of wireless communication. With the passes of time this wireless communication is becoming more and more advance. Lot of research work is going on in this area. One of the latest developments in wireless technology is **Mobile Ad-Hoc Network (MANET).** MANET provides new paradigm for wireless self organized networks. The concept of Ad-Hoc networking is one of the advanced mechanisms that are used in wireless networking. Basically, Ad-Hoc networks consist of a collection of wireless nodes. These nodes are connected with each other to dynamically establish an Ad-Hoc or On-The-Fly network without any kind of support of ant centralized infrastructure. In fact, such a network supports anytime and anywhere mobile computing and thus, allowing the spontaneous formation of mobile networks for a period of usages. In this kind a network, each mobile host works as a router which enables peer-to-peer as well as peer-to-remote wireless communication. This Ad-Hoc network is a self-organized wireless network with no fixed infrastructure. In this network any node can act as transmitter, receiver or router. The few vital applications of MANET are listed below:-

1. Personal area networking formed with cell phones, laptops, notebooks, PDAs
2. Education sector such as Virtual classrooms, conferences, seminars.
3. Sensor networks for homes, environmental applications, wearable computing.
4. Civilian environments like meeting rooms, sports stadiums, hospitals.
5. Military environments in battlefields by soldier in tanks/planes.
6. Emergency operations such as search and rescue in case of natural disasters.

MANET is a collection of self organized mobile nodes connected through wireless nodes. Nodes within the range of each other is connected directly, if it is not so then they become bound to rely on intermediate node for communication. Few special characteristic of MANET are Dynamic Topology, Fast deployment and Robustness which makes this technology entirely different from other wireless technologies.

Communication in the MANET solely depends on trust on each other node. The step by step process of data transmission in MANET is follows:-

1) First of all transmitter node sends the signal to the adjacent node within the range.
2) Adjacent node communicates with the transmitter node.
3) Transmitter node sends the message to the receiver node.
4) If receiver node is within the range then message is received by the receiver else an intermediate node receives the message. It will act as router.
5) Restart the process of forwarding the message from step1 till the receiver node is reached.

With the logarithmic growth of wireless communication technologies some major challenges are also faced. These challenges are also considered while designing the new

type of network. Every user presumes that his/her message must be secured enough so that it could not be evaded. So, we can say information security is a major aspect of wireless technology. Some basic requirement of information security [1] is Confidentiality, Integrity. Availability, Non-repudiation and Authentication. Due to dynamic topology of MANET, it becomes highly vulnerable to attacks. It becomes difficult for attackers to estimate the behavior of network at particular instant. Secure routing protocols is also a challenge. Now a day researchers are offering lot of secure routing protocols meet their specific security requirements. Different protocols fulfill different security requirements and counter against certain attack patterns. Researchers evaluate their protocols on the basis of their resistivity in case of attacks. Performance of these protocols is tested during simulation. Simulation is basically the process of testing the proposed technology with respect to other available technologies. Also the performance is justified based upon different parameters like average Hop-Count, average time delay etc.

II. RELATED WORK :

Since proposed Hybrid routing is used to detect and remove wormhole attack at physical layer using hop count [alternate route] and modification of AODV protocol using route reply decision and finally we using secure neighbor discovery using neighbor list method. These three methods are combined to obtain the command solution which is for better then individual methods. These hybrid routing is based on ON-Demand ad hoc routing protocol (AODV). Different methods used to detect and eliminate the wormhole attacks are briefly reviewed. The methods proposed in literature to defend against wormhole attacks can be divided into three categories. The first is to modify a well-known routing protocol, such as Ad hoc On demand Distance Vector (AODV)[4] or Dynamic Source Routing (DSR) [5], to avoid wormhole nodes during path discovery, such as [3,4,5,6,7].The second is to adopt extra hardware, such as a positioning system, a time synchronization mechanism or a directed antenna, in addition to modifying the routing protocol. Some of which are [8, 9, 11, 12, 13]. Finally, the third is to deploy an intrusion detection system (IDS) with or without hardware support, such as [14, 15, 10, and 16]. Since the proposed approach in this paper is a secure routing protocol without hardware support, only those researches belonging to the first category are introduced as follows. Wormhole attack detection in [3] proposed a modified DSR [2] protocol to defend against wormhole nodes by adopting a multi-path routing method.

A source node initiates route discovery, and the destination node, after receiving multiple paths, begins to calculate the proportion of each link between two nodes in the total paths. Due to wormhole node's great ability to grab routing paths, if the occurrence of one link exceeds the threshold value, the two ends of this link may be wormhole nodes. The destination would first send a test data packet to verify if this link is abnormal, such as the packet being dropped. If it is confirmed that the two ends of this link are wormhole nodes, the destination would send a warning message to the neighbors of the malicious nodes, informing them not to process any messages from the malicious nodes. In this way, the malicious nodes would be isolated, and then Quarantine. An AODV-based routing protocol proposed [4], named DelPHI, to defend against wormhole attacks. DelPHI also applied a multi-path approach, and recorded the delay and hop counts in transmitting RREQ and RREP (actually named DREQ and DREP in Delphi) through the paths. In this way, the average time taken by each hop can be calculated. In the case of a path subjected to wormhole attacks, the delay would be obviously longer than a normal path with the same hop count (i.e., the wormhole nodes may have a heavy load, and therefore, packet processing is slow).Hence, the path with longer delays would not be selected to transmit data packet and wormhole nodes could be avoided.

III. PROPSED ROUTING ALGORITHM

Due to nature of wireless transmission, MANET has more security issues compared to other wired networks. Without exploiting the nodes, wormhole directly alters the route establishment process. In this method, instead of detecting suspicious route we are going to detect and black list the wormhole attacker node, without considering any external environment and without modification of protocol too. Attacker node may be inside or outside of the network. Entire analysis is carried out based upon Hop Count and Time Delay. Simulation is going to be carried out with OPNET modeler 14.0.

Process model:

The process model is going to be recited below. This consists of transmitter, receiver and routers. Delay and data packet is also shown. Default routes are shown by the help of dotted lines. Solid lines represent the established routes.

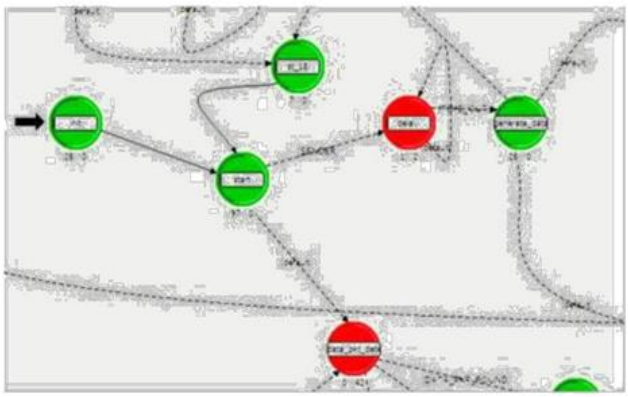

Figure 4.1 Part of Complete Process Model

It also shown that if time delay is too large then time out message appears and packet will not be transferred. First node is the initiator node. Means the process is going to be started here. After that start node is there where route discovery is actually started. After this one path is rejected due to access time delay and another path is accepted and data is transferred. Default path is also cited. Figure 4.1 is only the part of complete process model. Entire process model can be understood in the simulation scenario.

Node distribution:

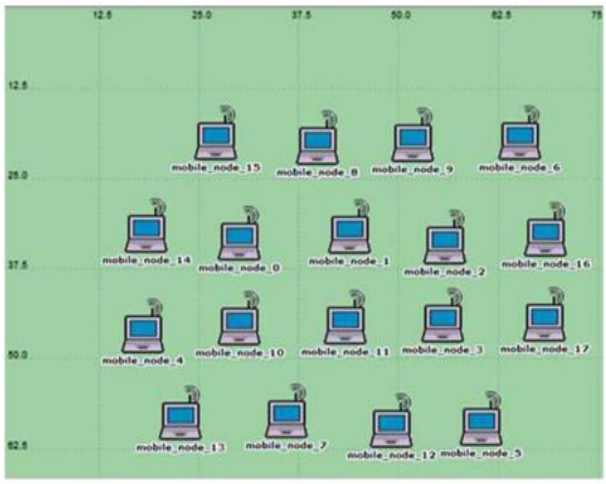

Figure 4.2 Node distribution

Node distribution for 17 nodes is shown in this figure. All are connected wirelessly with each other. Each node is capable to act as sender, receiver or router.

Typical Applications of Modeler

Models of wide range of systems are developed by the help of modelers. Some applications of modeler are explained below:-

Standards-based LAN and WAN performance modeling: Modelers provide number of protocols for Wide Area Network (WAN) and Local Area Network(LAN).

Internetwork planning: Scalable, deterministic and stochastic models can be used to generate network traffic. Hierarchical topologies are followed.

Research and development in communications architectures and protocols: Natural representations of protocols are obtained by Finite State Machine.Modeler provides full support for communication related applications.

Distributed sensor and control networks, on-board systems: Sophisticated, adaptive, application level models can be developed by modelers. Customized performance metric can be obtained.

Resource sizing: Demand of packets is not uniform always. So, at the source sizing is required. This must be accurate and detailed. Library models are provided for many standard resources.

Mobile packet radio networks: Modeler provides proper support for mobile nodes, including predefined trajectories and fully customizable radio link models.

Satellite networks: Modeler also provides utility program for orbit generation, orbit visualization and orbital-configuration.

C3I and tactical networks: Tactical networks support for diverse link technologies, modeling of adaptive protocols.

Simulation and results:

Simulation Environment and Parameters-In this section the effectiveness of proposed algorithm is going to be evaluated. The entire simulation is performed with OPNET modeler 14.0 to prove the practical efficiency of the model. The detail of parameters is noted below:-

Packet size	: 1024 bits constant
Data Rate	: 11 Mbps.
Area	: 10 square Km.
No. of Nodes	: 18
Routing Protocol	: AODV
Traffic Model	: CBR
MAC	: IEEE 802.11
Mobility	: Random
Packet inter arrival time	: 02 seconds. (Constant)

Scenario 1:- Nodes Distribution without Wormhole Attack

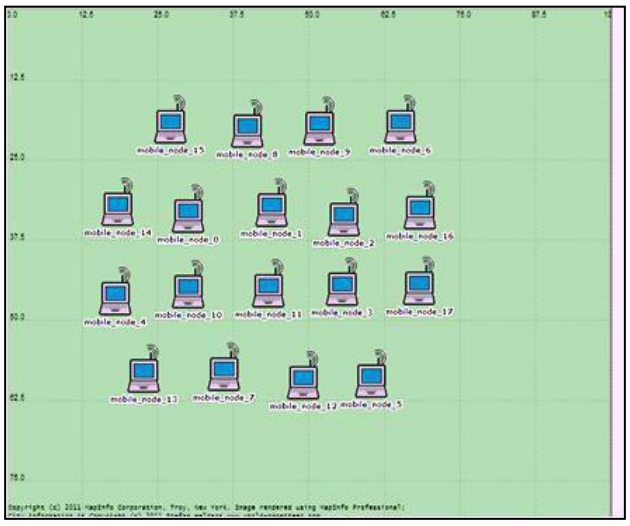

Figure 5.3 node distributions without wormhole attack

5.2.1.1 Average Hop count per route in scenario 1 without wormhole attack

Figure 5.4 Average Hop count per route in scenario 1 without wormhole attack

5.2.1.2 Average delays per route in scenario 1 without wormhole attack

Figure 5.5 Average delays per route in scenario 1 without wormhole attack

5.2.2 Scenario 2:- Node distribution with wormhole attack

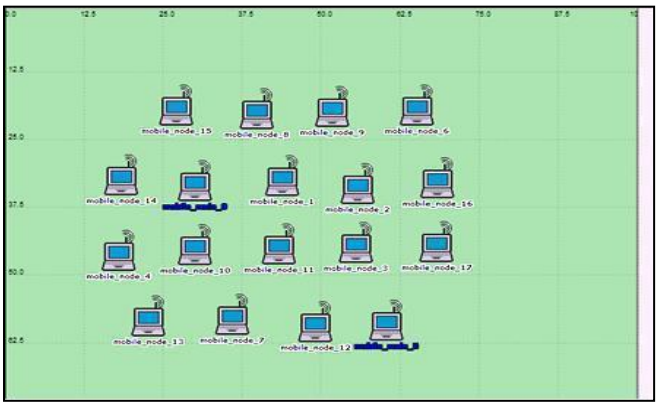

Figure 5.6 Scenario 2:- Node distribution with wormhole attack

5.2.2.1 Average Hop count per route in scenario 2 with wormhole attack

Figure 5.7 Average Hop count per route in scenario 2 with wormhole attack

5.2.2.2 Average delays per route in scenario 2 with wormhole attack

Figure 5.8 Average delays per route in scenario 2 with wormhole attack

Conclusion

With this dissertation, we presented an overview of various security goals, security threats and various secure routing protocols. From study, a comparison table is provided, which gives comparison of different protocols and their security capacity. From comparison, it is clear that no protocol accomplish all security goals.

References:

[1] Perkins CE, Royer EM, Das SR. Ad hoc on-demand distance vector (AODV) routing, IETF internet draft. MANET Working Group;

[2] Johnson DB, Maltz DA, Hu YC. The dynamic source routing protocol for mobile ad-hoc network (DSR), IETF internet draft (work in progress); July 2004.

[3] Ning Song, Lijun Qian, and Xiangfang Li. Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach. In the proceedings of the 19th IEEE international parallel and distributed processing symposium (IPDPS'05); 2005.

[4] Hon Sun Chiu, King-Shan Lui. DelPHI: wormhole detection mechanism for ad hoc wireless networks. In the proceedings of the 1st international symposium on wireless pervasive computing; 2006.

[5] Gunhee Lee, Dong-kyoo Kim, Jungtaek Seo, An approach to mitigate wormhole attack in wireless ad hoc networks. In the proceedings of the international conference on information security and assurance; 2008 pp. 220-5.

[6] Xu Su and Rajendra V. Boppana. On mitigating in-band wormhole attacks in mobile ad hoc networks. In the proceedings of the IEEE international conference on communications; 2007. pp. 1136–41.

[7] Farid Naıt-Abdesselam, Brahim Bensaou, Jinkyu Yoo. Detecting and avoiding wormhole attacks in optimized link state routing protocol. In the proceedings of the IEEE conference on wireless communications and networking; 2007. pp. 3117–22.

[8] Issa Khalil, Saurabh Bagchi, Ness B. Shroff. LITEWORP: a Lightweight countermeasure for the wormhole attack in multihop wireless networks. In the proceedings of the international conference on dependable systems and networks (DSN'05); 2005.

[9] Issa Khalil, Saurabh Bagchi, and Ness B. Shroff. MOBIWORP: mitigation of the wormhole attack in mobile multihop wireless networks. In the IEEE securecomm and workshops; 2006. pp. 1–12

[10] Xia Wang, Intrusion detection techniques in wireless ad hoc networks. In the proceedings of the IEEE international computer software and applications conference; 2006

[11] Xia Wang and Johnny Wong, An end-to-end detection of wormhole attack in wireless ad-hoc networks. In the proceedings of the 31st annual international computer software and applications conference (COMPSAC); 2007.

[12] Hu Yih-Chnu, Perrig Adrian, Jonhson David B. Wormhole attacks in wireless networks. IEEE Journal on Selected Areas in Communication 2006; 24(2):370–80.

[13] Lazos L, Poovendran R, Meadows C, Syverson P, Chang LW. Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach. In the proceedings of the IEEE conference on wireless communications and networking; 2005, vol. 2. pp. 1193–9.

[14] Gorlatova MA, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano. Detecting wormhole attacks in mobile ad hoc networks through protocol breaking and packet timing analysis. In the proceedings of the IEEE conference on military communications; 2006.

[15] Marianne A. Azer, Sherif M. El-Kassas, Abdel Wahab F, Magdy S. El-Soundani. Intrusion detection for wormhole attacks in ad hoc networks a survey and a proposed decentralized scheme. In the proceedings of the IEEE international conference on availability, reliability and security; 2008. pp. 636–41.

[16] Tran Van Phuong, Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, and Heejo Lee. Transmission time-based mechanism to detect wormhole attacks. In the proceedings of the IEEE Asia-Pacific service computing conference; 2007. pp. 172–8

[17] Hu YC, Perrig A, Davic B. Johnson. Ariadne: a secure on-demand routing protocol for ad hoc networks. In the proceedings of the ACM conference on mobile computing and networking (Mobicom); 2002. pp. 12–23

[18] Clausen T, Jacquet P. Optimized link state routing protocol (OLSR). 3626. IETF RFC; October 2003.