A comprehension on Wormhole Attack prevention technique using THREADS in MANET

Nidhi Nigam[1], Vishal Sharma[2]

[1] *Department of Computer Science, JIT Borawan/ RGPV, INDIA*
**e-mail: nigam.nidhi07@gmail.com*
[2] *Department of Computer Science, JIT Borawan/ RGPV, INDIA.*
**e-mail: vishalsharmakgn@gmail.com*

Abstract

*The open and dynamic operational environment of **M**obile **A**d hoc **NET**work (**MANET**) makes it vulnerable to various network attacks. Thus reducing the vulnerability is becoming a top priority. Wireless networks are susceptible to many attacks, including an attack known as the wormhole attack, has become a challenging work. The wormhole attack is very powerful and preventing this attack has proven to be very difficult. This paper addresses the aforementioned gap by introducing a new co-operative, clock synchronized technique based on Reference Broadcast System (RBS). To improve network scalability and throughput, we propose the concept of Thread for each & every node of MANET. So that our proposed scheme has three mechanisms namely, AODV (Ad hoc on demand distance vector protocol) for routing, Principle of RBS for threshold setting and ACK, for reliability of communication, are combined to detect wormhole attacks in ad hoc networks.*

Keywords – AODV**,** MANET, RBS, THREAD, Wormhole attacks.

1. Introduction

Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. In general, a wireless node can be any computing equipment that employs the air as the transmission medium. As shown, the wireless node may be physically attached to a person, a vehicle, or an airplane, to enable wireless communication among them.

In MANET, a wireless node can be the source, the destination, or an intermediate node of data transmission. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbour closer to the destination node. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still. Therefore the network topology changes from time to time.

Wireless ad-hoc network have many advantages [1]:

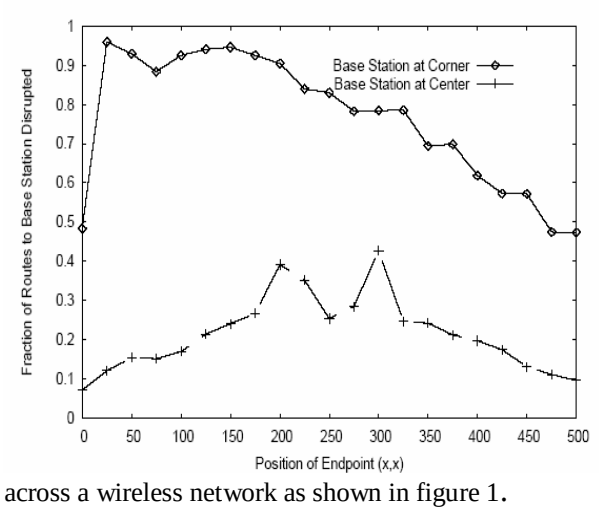
- *Low cost of deployment*: Ad hoc networks can be deployed on the fly; hence no expensive infrastructure such as copper wires or data cables is required.
- *Fast deployment*: Ad hoc networks are very convenient and easy to deploy since there are no cables involved. Deployment time is shortened.
- *Dynamic Configuration:* Ad hoc network configuration can change dynamically over time. When compared to configurability of LANs, it is very easy to change the network topology of a wireless network.

MANET has various potential applications. Some typical examples include emergency search-rescue operations, meeting events, conferences, and battlefield communication between moving vehicles and/or soldiers. With the abilities to meet the new demand of mobile computation, the MANET has a very bright future.

1.1 Significance of Wormhole attack

Ad-hoc or spontaneous wireless networks are threatened by a powerful attack known as the wormhole attack. A wormhole attack can be set up with

relative ease, but preventing one is difficult. To set up a wormhole attack, an attacker places two or more transceivers at different locations on a wireless network. This establishes a wormhole or tunnel through which data can transfer faster than it could on the original network. After setting up a wormhole, an attacker can disrupt routing to direct packets through the wormhole using a technique known as selective forwarding. A strategic placement of the wormhole can result in a significant breakdown in communicate on



across a wireless network as shown in figure 1.

Fig 1: Strategic Placement of Wormhole. The routes to the base station are disrupted the closer the wormhole endpoints are to the base station.

Wireless networking is a young technology and thus, many wireless network devices have not been designed to defend against wormhole attacks.

2. Routing approaches in Mobile Ad hoc Network

Since the advent of Defense Advanced Research Projects Agency (DARPA) packet radio networks in the early 1970s, numerous routing protocols have been developed for ad hoc mobile networks. These are generally categorized as table-driven or proactive, on-demand or reactive and hybrid routing protocols [1].

Table-driven or Proactive Protocols: Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network by propagating, proactively, route updates at fixed intervals. As the resulting information is usually maintained in tables, the protocols are sometimes referred to as table-driven protocols. Representative proactive protocols include: Destination-Sequenced Distance-Vector (DSDV) routing, Clustered Gateway Switch Routing (CGSR), Wireless Routing Protocol (WRP), and Optimized Link State Routing (OLSR).

On-demand or Reactive Protocols: A different approach from table-driven routing is reactive or on-demand routing. These protocols depart from the legacy Internet approach. Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually initiated by the source node through discovery process within the network. Once a route has been established, it is maintained by the node until either the destination becomes inaccessible or until it becomes reachable.

In this paper, we present a set of mechanisms in defending against wormhole attack. First, the concept of Thread is proposed between mobile nodes. Then source node estimates the minimum path to the destination based on the Reference Broadcasting [3] during the route discovery. Wormhole node will create tunnel between any two of nodes in network, which will be detected by using some appropriate criteria as network traffic etc. Finally, those nodes will be detected and a normal route is selected for the data communication.

3. Related work

There have been some proposals recently to protect networks from wormhole attacks by detecting such attacks. There is much literature that addresses the issue of defending against wormholes. In this section, we give a brief overview of these methods' principles and their pros and cons.

The concept of leashes [4] is introduced to detect wormhole attacks. A leash is any information added to a packet in order to restrict the distance that the packet is allowed to travel. A leash is associated with each hop. Thus, each transmission of a packet requires a new leash. Two types of leashes are considered, namely geographical leashes and temporal leashes. A geographical leash is intended to limit the distance between the transmitter and the receiver of a packet. A temporal leash provides an upper bound on the lifetime of a packet. As a result, the packet can only travel a limited distance. A receiver of the packet can use these leashes to check if the packet has traveled farther than the leash allows and if so can drop the packet.

Another approach for detecting wormhole attacks [5] is deploying directional antennae. The approach here is based on the use of packet arrival direction to detect that packets are arriving from the proper neighbors. Such information is possible due to the use of directional antennae. This information about the direction of packet arrival is expected to lead to accurate information about the set of neighbors of a node. As a result, wormhole attacks can be detected since such attacks emanate from false neighbors.

The authors present a graph theoretic framework [6] for modeling the wormhole attack. They provide a necessary and sufficient condition that any solution to the wormhole problem needs to satisfy. In addition, the authors also propose the use of local broadcast keys whereby the keys in different geographic regions are different. As a result, an encrypted message replayed via the wormhole in a different location cannot be decrypted by the receivers in that region.

S. Capkun et.al**.** [12] presented, an authenticated distance bounding technique called MAD is used. The approach is similar to packet leashes at a high level, but does not require location information or clock synchronization. But it still suffers from other limitations of the packet leashes technique. In the Echo protocol, ultrasound is used to bind the distance for secure location verification. Use of ultrasound instead of RF signals as before helps in relaxing the timing requirements; but needs an additional hardware. In a recent work, authors have focused on practical methods of detecting wormholes. This technique uses timing constraints and authentication to verify whether a node is a true neighbor. The authors develop a protocol that can be implemented in 802.11 capable hardware with minor modifications. Still it remains unclear how realistic such timing analysis could be in low-cost sensor hardware.

Kaissi et al.[9] came with DAWWSEN mechanism for defending against wormhole attacks in wireless sensor network. This is a detecting and defending mechanism for wireless sensor networks. Sensor nodes are usually resource constrained, like limited memory, lower power, etc. They also usually work with wireless communication to get data to base station. The wormhole attack is very dangerous to the routing protocol and can significantly disrupt nodes in the wireless sensor networks. To combat wormhole attacks, DAWWSEN recommends a proactive routing protocol that will have a hierarchical tree with base station as the root node and the sensor nodes as internal or leaf nodes. A mechanism is put in place for a sensor node to identify if a packet is from a wormhole attack. There are a lot of other researches done for sensor networks.

Song et al. [11] proposes a wormhole discovery mechanism based on statistical analysis of multipath routing. Song observes that a link created by a wormhole is very attractive in routing sense, and will be selected and requested with unnaturally high frequency as it only uses routing data already available to a node. These factors allow for easy integration of this method into intrusion detection systems only to routing protocols that are both on-demand and multipath.

Khalil et al. [10] propose a protocol for wormhole attack discovery in static networks they call LiteWorp. In LiteWorp, once deployed, nodes obtain full two-hop routing information from their neighbours. While in a standard ad hoc routing protocol nodes usually keep track of their neighbours are, in LiteWorp they also know who the neighbours' neighbours are, - they can take advantage of two-hop, rather than one-hop, neighbour information. This information can be exploited to detect wormhole attacks. Also, nodes observe their neighbours' behavior to determine whether data packets are being properly forwarder by the neighbour.

In DelPHI protocol [8] allows a sender to observe the delays associated with the different paths to a receiver. Therefore, a sender can check whether there are any malicious nodes sitting along its paths to a receiver and trying to launch wormhole attacks. The obtained delays and hop count information of some disjoint paths are used to decide whether a certain path, among these disjoint paths, is under a wormhole attack.

Mahajan et al. [7] proposed some proposals to detect wormhole attacks like:
1) The abrupt decrease in the path lengths can be used as a possible symptom of the wormhole attack.
2) With the available advertised path information, if the end-to-end path delay for a path cannot be explained by the sum of hop delays of the hops present on its advertised path, existence of wormhole can be suspected.
3) Some of the paths may not follow the advertised false link, yet they may use some nodes involved in the wormhole attack. This will lead to an increase in hop delay due to wormhole traffic and subsequently an increase in end-to-end delay on the path. An abrupt increase in the end-to-end delay and the hop queuing delay values that cannot be explained by the traffic supposedly flowing through these nodes can lead us to suspect the presence of wormhole.

4. Experimental Analysis

One common method to conduct research in the networking and security fields is to simulate and evaluate the protocol(s) in various scenarios. Fortunately, there are various computer simulation applications that are available for doing those tasks, such as NS-2 [13], OPNET [14], GLOMOSIM [15], etc. This will be heavily based on the implementation and experiments in the NS-2 simulation environment.

NS-2 [13] is chosen as a simulation environment because it is one of the leading environments for network modeling and simulation. ns is LBNL's Network Simulator [24]. The simulator is written in C++; it uses OTcl as a command and configuration interface. ns v2 has three substantial changes from ns v1: (1) the more complex objects in ns v1 have been decomposed into simpler components for greater flexibility and composability; (2) the configuration interface is now OTcl, an object oriented version of Tcl; and (3) the interface code to the OTcl interpreter is separate from the main simulator. It supports large number of built-in industry standard network protocols, devices, and applications. In addition, its programming library helps researchers to easily modify the network elements and measure their performance in the simulation environment. It also provides rich data analysis features.

5. Conclusion

Wormhole attacks are significant problems that need to be addressed in wireless network security. Security of ad hoc networks has recently gained momentum in the research community .Due to the open nature of ad hoc networks and their inherent lack of infrastructure, security exposures can be an impediment to basic network operation .Security solutions for MANET have to cope with a challenging environment including scarce energy and computational resources and lack of persistent structure MANETS, this approach will tackle the issue in an efficient manner by reducing a number of attacks. The scheme discusses a semantic security mechanism to handle attacks based on packet dropping and message tampering, which can accurately detect the malicious nodes in the network. The malicious nodes identified are isolated for future sessions. In the proposed scheme, scope of enhancements and improvements are enormous. An immediate enhancement is evaluation of more network parameters. Further, the scheme can be made more secure against other types of possible network layer attacks that threaten the network.

As security is major concern in MANETS, this approach will tackle the issue in an efficient manner. Reactive methods should be used instead of proactive methods since attacks on packet forwarding cannot be prevented. The core idea of this scheme is to detect malicious nodes launching attacks and misbehaving links to prevent them from communication network. A robust and a very simple idea are presented here which can be implemented and tested in future for more number of attacks by increasing number of nodes.

6. References

[1] C. Siva Ram Murthy and B. S Manoj, *Ad Hoc Wireless Networks, Architecture And Protocols*(Prentice Hall PTR, 2004).

[2] G.S. Mamatha ,S. C. Sharma, A New Secured Approach for MANETS against Network Layer Attacks, 2010 *First International Conference on Integrated Intelligent Computing, 978-0-7695-4152-5*

[3] J. Elson, L. Girod, and D. Estrin, Fine-Grained Network Time Synchronization Using Reference Broadcasts, *Proc. 5th Symp. Op. Sys. Design and Implementation, 2002, pp. 147–63.*

[4] Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2003 Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, *Twenty-Second Annual Joint Conference of IEEE Computer and Communications, Volume 3, pp. 1976-1986.*

[5] L. Hu, D. Evans, Using Directional Antennas to Prevent Wormhole Attacks, *Proceedings of the 11th Network and Distributed System Security Symposium, pp. 131-141, 2003*

[6] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach, *IEEE Communication Society, WCNC 2005*

[7] V. Mahajan, M. Natu, A. Sethi. ,Analysis of wormhole intrusion attacks in MANETS, *IEEE Military Communications Conference (MILCOM), pp. 1-7, 2008.*

[8]H.S.Chiu and K. Lui. ,DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks, *Proceedings of International Symposium on Wireless Pervasive Computing, pp. 6-11, 2006.*

[9] Kaissi, R. E., Kayssi, A., Chehab, A., & Dawy, Z. (2005). DAWWSEN: A defense mechanism

against wormhole attacks in wireless sensor networks. *The Second International Conference on Innovations in Information Technology* (IIT'05). American University of Beirut. Beirut, Lebanon.

[10]Khalil, I., Bagchi, S., & Shroff, N. B. (2007). Liteworp: detection and isolation of the wormhole attack in static multi-hop wireless networks. *Computer Networks. Vol 51(15)*

[11]N. Song, L. Qian, X. Li, Wormhole Attack Detection in Wireless Ad Hoc Networks: a Statistical Analysis Approach, *Parallel and Distributed Processing Symposium, 2005, Proceedings of, 19th IEEE International IPDPS'05, 04-08 April 2005, pp.*

[12] S. Capkun, M. Cagalj, and M. Srivastava, Secure localization with hidden and mobile base stations, *Proceedings of the 25th IEEE International Conference on Computer Communications Societies (INFOCOM '06), Barcelona, Spain, April 2006.*

[13] [online] Building ns-2 on Cygwin, http://www.isi.edu/nsnam/ns/ns-cygwin-old.html

[14] [online] OPNET Modeler 11.0. http://www.opnet.com/products/modeler/home.html

[15] [online] Glomosim – Global Mobile Information Systems Simulation Library. http://pcl.cs.ucla.edu/projects/glomosim