Degradation of Ad-hoc Network Performance under Wormhole Attack

Vishal Pahal[1*]
Department of Computer Science and Engineering
Jind Institute of Engineering & technology.
Jind, Haryana, India.

Susheel Kumar[2]
Associate Professor
Department of Computer Science and Engineering
Jind Institute of Engineering & technology.
Jind, Haryana, India.

ABSTRACT

An ad-hoc network is self-organizing and adaptive. Networks are formed on-the-fly; devices can leave and join the network during its lifetime, devices can be mobile within the network, the network as a whole may be mobile and the network can be deformed on the-fly. In wireless ad hoc networks, nodes depend upon other node to forward packets for each other to communicate beyond their transmission range. Ad-hoc network are very useful in war , accidental , military services, flood , earthquake situations and also in normal conditions..In multihop wireless Ad-hoc networks, cooperation between nodes to route each other's packets exposes these nodes to a wide range of security attacks. Therefore, networks are vulnerable to various attacks launched through compromised nodes because malicious nodes can easily participate in the networks. . One of such type of attack is Wormhole Attack. It is a tunnel based attack in which a pair of nodes forms a tunnel with false identification [1]. In wormhole attacks, one malicious node tunnels packets from its location to the other malicious node.. If source node chooses this fake route, malicious nodes have the option of delivering the packets or dropping them. In this paper we have simulated the wormhole attack in wireless Ad-hoc networks & Manet's. And then we evaluated & discussed the impact on the network by comparing the results with secure network without wormhole attack and unsecure network with wormhole attack. In this way, the impact of the wormhole attack on the network performance is analyzed. Impact of wormhole attack on the network is shown using tool Ns-2.34. The implementation is done with the DYMO routing protocol .

General Terms

Security, Performance , Attack, Comparison .

Keywords

Wormhole Tunnel, Wireless, Cryptography, Impact on network performance, Network throughput.

1. INTRODUCTION

Ad-hoc networks are wireless networks where nodes communicate with each other using multi-hop links. There is no stationary infrastructure or base station for communication. Each node itself acts as a router for forwarding and receiving packets to/ from other nodes. Routing in ad-networks has been a challenging task ever since the wireless networks came into existence. The major reason for this is the constant change in network topology because of high degree of node mobility. 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 neighbor closer to the destination node. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still. Security in an Ad-hoc network is extremely important in scenarios such as a battlefield. The five goals of security – availability, confidentiality, integrity authenticity and non-repudiation are difficult to achieve in MANET, mainly because every node in the network participates equally in routing packets. Wormhole attack is also an important security threat for consideration, it badly effect network performance.

1.1.Problem of attack

In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive sooner than other packets transmitted over a normal multichip route, for example through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to itself, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole. If the attacker performs this tunneling honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently. However, the wormhole puts the attacker in a very powerful position relative to other nodes in the network, and the attacker could exploit this position in a variety of ways. The attack can also still be performed even if the network communication provides confidentiality and authenticity, and even if the attacker has no cryptographic keys. Furthermore, the attacker is invisible at higher layers; unlike a malicious node in a routing protocol, which can often easily be named, the presence of the wormhole and the two colluding attackers at either endpoint of the wormhole are not visible in the route. As such, the effect of the wormhole on legitimate nodes may even change as nodes move; two legitimate nodes previously connected only by routes through the wormhole and thus possibly unable to communicate, will be able to communicate normally if they come within direct wireless transmission range of each other updating frequency might be very low for ad-hoc networks.

1.2.Significance of Wormhole Attack

While wormhole could be a useful networking service as this simply presents a long network link to the link layer and up,it can provide a better path for routing , and fast link , but because of the bad intention of the attacker ,this link can create problem , because it has high tendency to attract the network traffic to send their packet through this route , the attacker may use this link to its advantage, attacker depend upon intension attacker do spy and damage of packet receiving through this network , in this way it is declared as attack on network ,which can highly degrades the performance of the network.

1.3.Classfication of wormhole attack

It is broadly classified into two categories
1.3.1.) Exposed attack 1.3.2) Hidden attack

1.3.1.Exposed attack

In exposed [2] attacks, wormhole nodes do not modify the content of packets but they include their identities in the packet header as legitimate nodes do Therefore, other nodes are aware of wormhole nodes' existence but they do not know wormhole nodes are malicious .

1.3.2.Hidden Attacks

Before a node forwards a packet, it must update the packet by putting their identity (MAC address) into the packet's header to allow receivers know where the packet directly comes from. However, in hidden attacks, wormhole nodes do not update packets' headers as they should so other nodes do not realize the existence of them.

1.4.Routing

It generally works by broadcasting the information and used air as medium .It's broadcasting nature and transmission medium also help attacker, whose intention is to spy or disrupt the network. Many type of attack can be done on such Mobile Ad-hoc network. To study wormhole attack, some detection methods and different techniques to prevent network from these attacks, Because of the fact that it may be necessary to hop several hops (multi-hop) before a packet reaches the destination, a routing protocol is needed. The routing protocol has two main functions, selection of routes for various source-destination pairs and the delivery of messages to their correct destination. The second function is conceptually straightforward using a variety of protocols and data structures (routing tables). This report is focused on selecting and finding routes.

2.LITERATURE SURVEY

In this section we will give a short overview of existing work and entry points to the literature. Many different types of attacks have been proposed The SECTOR protocol [3] presents a countermeasure against wormhole attacks by allowing nodes to prove their encounters with other nodes. However, several hypotheses are needed for this protocol to work correctly. Among these are, the necessity of coarse synchronization [4], the ability of nodes to measure their local timing with a nanosecond precision, the pre-establishment of security associations between each pair of nodes, and the presence of a central authority that controls the network membership. The so-called disjoint path based approaches have been adopted recently. A work on worm hole prevention is performed in [5]. The scheme relies on the idea that usually the wormhole nodes participate in the routing in a repeated way as they attract most of the traffic. Therefore, each node will be assigned a cost depending in its participation in routing. Besides preventing the network from the wormhole attack, the scheme provides a load balance among nodes to avoid exhausting nodes that are always cooperative in routing. In [6] a method of worm holed detection and avoidance is defined. In proposed solution, if sender wants to send the data to destination, firstly it creates a secure path between sender and receiver with the help of verification of digital signature. If there is presence of any malicious node in between the path then it is identified because malicious node does not have its own legal digital signature.

Wormhole attacks, in [7] which adversaries tunnel network data from one end of the network to another using an off-channel link, are a severe routing security concern in mobile wireless ad hoc networks. Wormhole attacks can not be prevented by cryptographic measures as in a wormhole attack they attackers do not create any packets themselves, but simply forward the packets they hear coming from valid network nodes. Several method use distance-bounding techniques to detect network packets that travel distances beyond radio range, thus preventing packets that have gone through the wormhole from being accepted. However, majority of these techniques rely on specialized hardware, and may not be practical. Of distance-bounding techniques, GPS-based ones are particularly interesting, as, of the specialized hardware proposed to combat wormhole attacks, GPS is perhaps the most general in purpose, most available currently, and overall most promising. The effectiveness of GPS-based wormhole attack solution is intuitively solid: a packet cannot travel to another end of the network undetected if all nodes know precisely where they are located and where their neighbors are Unfortunately, GPS-based wormhole combating techniques inherit the limitations of GPS technology. They cannot be used where GPS does not work (underwater, inside buildings, caves, etc.), or in small sensor networks (due to the resolution of GPS devices).Nonetheless, GPS-based techniques are interesting, particularly for military or emergency situations, where GPS devices could be used for location awareness purposes, and could be added to network routing without any additional costs. Network visualization technique presented in for dense sensor networks does not require special hardware, and appears to be very interesting. In this technique, each node reports its perceived distance to its neighbors to a centralized controller. Based on the data collected from network nodes, the controller calculates the estimation of network's physical topology, to which a wormhole, in certain scenarios, introduces impossibilities. It would be very interesting to study how this technique performs on networks that are mobile and not dense. Most likely, the technique will still work, but perhaps with reduces accuracy and higher false alarm rate. If that is the case, with the use of mobile agents for network visualization instead of the central controller this technique could be applied to general MANETs rather than to sensor networks only [8] propose a timing-based countermeasure that avoids the deficiencies of existing timing-based solutions. Using the proposed countermeasure, the nodes do not need synchronized clocks, nor are they required to predict the sending time or to be capable of fast switching between the receive and send modes. Moreover, the nodes do not need one-to-one communication with all their neighbors and do not require to compute a signature while having to timestamp the message with its transmission time.

A theoretical analyses of simple wormhole routing algorithms, showing them to be nearly optimal for butterfly and mesh connected networks. In year 2006, Yih-Chun Hu has defined a work on worm hole attack in sensor network. According to his work In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively)to another location, and retransmits them there into the network [9]. This paper present a general mechanism, called packet leashes, for detecting and, thus defending against wormhole attacks, and we present a specific protocol, called TIK, that implements leashes. To defend against the wormhole attack, The priority adjustment scheme dynamically modifies the priority of a message as the timing property of the message changes [10].

Our analysis requires initial random delays in injecting messages to the network [11]. Since the wormhole network is a popular communication system used in the new generation of large-scale parallel multiprocessors, real-time communication support on wormhole networks becomes an important issue. This paper evaluates a priority mapping scheme, adjustment scheme and a message dropping method for large-scale, real-time wormhole networks. The priority mapping scheme embeds the timing property of a message into a priority for flow control decisions.

The security mechanisms used for wired network such as authentication and encryption are futile under hidden mode wormhole attack, as the nodes only forward the packets and do not modify their headers. The study here establishes the foundation for future work towards designing a mechanism to identify the nodes and the links which are actively involved in the wormhole attack [12].

To complement the existing secure routing protocols to resist the creation of these in-band wormholes, and thus reduce the incidence of in-band wormhole attacks. Their techniques are based on reducing request packet delays and statistical profiling. These techniques do not require network-wide synchronized clocks and do not impose [13] any additional control packet overhead. Their implemented our techniques in a widely studied secure routing protocol called Ariadne.Both in SaW and DaW [14] similar propositions are made. Only difference is in the selection of routing protocols. In reference [15] AODV protocol was followed while in [14] DSR routing protocol was used. In both of these papers, trust based security models have been proposed and used to detect intrusion. Statistical methods have been used to detect the attacks. If any link is found to be suspicious, then available trust information is used to detect whether the link is a wormhole. In the trust model used, nodes monitor neighbors based on their packet drop pattern and not on the measure of number of drops. Karl Pearson’s formula for correlation coefficient is used in identifying the pattern of the drops. In [14] another algorithm for detecting the presence of wormhole in the network has been proposed. Here, after sending the RREQ, the source waits for the RREP. The source receives many RREP coming through different routes. The link with very high frequency is checked using the following expression

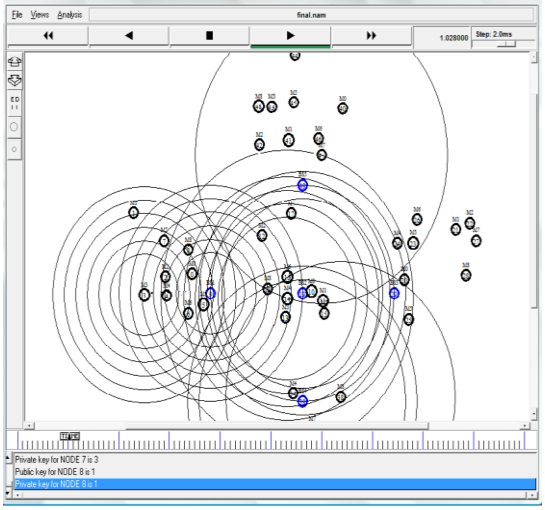
$Pi= ni /N$, for all Ii
$Pmax = max (Pi)$,

where *R* is the set of all obtained routes, *Ii* is the *i*th link, *ni* is the number of times that Ii appears in *R*, *N* is the total number of links in *R*, and *Pi* is the relative frequency that *Ii* appears in *R*. If *Pmax* > *Pthreshold*, check the trust information available in the RREP of that route. If the value of correlation coefficient for packets dropped to that sent is greater than the pre-set threshold *t*, then the node is malicious, inform the operator else continue with routing process.

In [16] a new protocol called Multi-path Hop-count Analysis (MHA) is introduced based on hop-count analysis to avoid wormhole attack. It is assumed that too low or too high hop-count is not healthy for the network. The novelty of the hop-count analysis in detecting wormholes is however questionable. Similar works have also been reported earlier. As an example, Djenouri et al. [17] may be considered.

Due to diverse applications, ad hoc networks are appealing for use in many domains. However, their features [18] of open medium, absence of infrastructure, dynamic changing network topology, cooperative algorithms, lack of centralized monitoring and management point, resource constraints and lack of a clear line of defense, they are vulnerable to many attacks. Therefore, there is a major concern about their security. Amongst attacks we are particularly interested in a severe attack called the wormhole attack. This scheme work for the wormhole attack detection and prevention. This scheme is based on a social science theory called the diffusion of innovations and serves all network nodes in detecting and preventing the attack even without prior interaction with malicious nodes. In order to implement this scheme, the routing protocol must be modified such as to allow the route selection based on nodes' opinions in each others. This is done by allowing each node to assign weights to other nodes in the network through different phases that will be explained in details. The scheme is totally decentralized and does not add an extra computational complexity to the nodes; which is one of the most important requirements for such networks.

3. IMPLEMENTATION SETUP



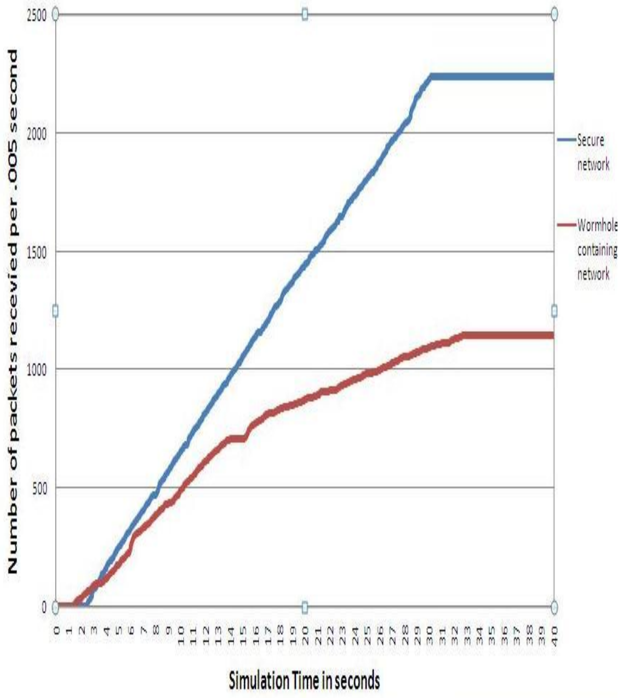
Private key for NODE 7 is 3
Public key for NODE 8 is 1
Private key for NODE 8 is 1

Figure 1 : NS2.34 Simulation

To show wormhole attack behavior, we have used the nodes that exhibit wormhole behavior, in wireless ad-hoc network that use DYMO routing protocol .It is successor to the popular AODV protocol .The simulation is done by using NS-2.34 network simulator. For running the simulation under DYMO routing protocol, a patch for DYMO is run for Ns-2.34. After that we can use DYMO protocol successfully .NS-2.34 gives output in two different forms i.e. NAM and trace files, we used both to analyses the results. We have setup the network architecture and strategically placed the wormhole link between two nodes. Then we have run simulation under a secure network. The output graph is generated for network parameter like number of packets. It shows the impact of wormhole link on the network.

4. RESULTS

It is revealed from figure 1 that the complete work is divided in 5 clusters. Each cluster is having 10 nodes. The simulated NAM output for the network is shown here.



Red color graph for →Existing Wormhole link in Network
Blue color graph for →Secure Network.

Figure 2: Graphic Result

The figure 1 is depicting the network structure , it is a showing the network communication at secure conditions after the implementation of some prevention scheme , but the graph in figure 2, shows the number of packets received on node in both secure and wormhole effected network. The graph is used to comparison of both the situation.

The final work is presented in the form of graph where the throughput is being compared using output graphs.. The results are here presented in Figure 2. In this figure 2 the comparison between the existing wormhole link network and secured network is defined. As we can see the number of packets received in network is decreased after the implementation of wormhole link in the network. It is comparison of number of packed packets received on node in a network. The red line graph is used to represent the number of packets received when there is attack on the network, on the other hand the blue color graph is used to show situation of number of packets in the absence of wormhole link. On analysis of graph, it is seen that blue color come above the red graph, which is due to impact of wormhole attack , hence the output clearly shows the impact of wormhole attack that performance get degrades in the wireless ad-hoc network under attack.

5. CONCLUSION

The analysis of the output graph shows the network performance in both situations. The presence of wormhole link in the network system degrades the performance of the network. The network lost its reliability. Attacker can spy the packets, discard packets or modify packets. So there is degradation of performance of network under the wormhole attack. A secure system provides better throughput and less packet loss over the network. Also the paper presents the overall measurement of the impact when a network is under the wormhole attack and helps in designing the topology which is more robust. The limitation of the simulation is that the measurement of the impact on MANETs becomes difficult when the mobility of the nodes increases too much.

5. REFERENCES

[1] A. Ephremides, J. E. Wieselthier and D. J. Baker, “A design concept for reliable mobile radio networks with frequency hopping signaling,” *Proc. IEEE*, vol. 75, no. 1, Jan. 1987, pp. 56-73.

[2] Phuong, T. V., N. T. Canh, and Young-Koo. Lee, S. Lee, and H. Lee, “Transmission Time-based Mechanism to Detect wormhole Attacks”, *IEEE Computer society*, 2007, pp. 172-178.

[3] S. Capkun, L. Buttyan, and J. Hubaux, *“*SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks*,” In Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks (ACM SASN), Fairfax, USA, Oct*. 2003

[4] Monis Akhlaq, “Addressing Security Concerns of Data Exchange in AODV Protocol”, *World Academy of Science, Engineering and Technology*, 2006, vol 16 , pp. 29-33.

[5] Mariannne. A. Azer, “Wormhole Attacks Mitigation*”, Sixth International Conference on Availability, Reliability and Security*, 2011

[6] Pallavi Sharma, Aditya Trivedi, “An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature”, *2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, May 27-29 2011, pp.307-311.

[7] Maria Alexandrovna Gorlatova “Review of Existing Wormhole Attack Discovery Techniques*” A Contractor Report at DRDC Ottawa* ,pp 1-23,August 2006.

[8] Majid Khabbazian,” Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks*”, IEEE Transactions On Wireless Communications*, vol. 56, no. 7, pp. 1536-1276 , 2009.

[9] Yih-Chun Hu, “Wormhole Attacks in Wireless Networks*”, IEEE Journal On Selected Areas In Communications*, VOL. 24, NO. 2, pp- 370-380, FEBRUARY 2006.

[10] Jong-Pyng Li,” Priority Based Real-Time Communication for Large Scale Wormhole Networks *Parallel Processing Symposium, 1994. Proceedings., Eighth International*.pp-433-438.

[11] *Sergio* A. *Felperin*, Prabhakar Raghavan, Eli Upfal*: “ A* Theory of Wormhole Routing in Parallel Computers”. *IEEE Trans. Computers* vol.45, no.6: 704-713 (1996)

[12] Reshmi Maulik1 and Nabendu Chaki2 **,”** A Study on Wormhole Attacks in MANET “,*International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988* vol. 3 ,pp. 271-279,2011

[13] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wireless Networks*, vol. 11, no. 1-2, pp. 21–38, 2005.

[14] Khin Sandar Win. "Analysis of Detecting Wormhole Attack in Wireless Networks*", World Academy of Science, Engineering and Technology 48 ,2008,* pp. 422-428.

[15] Shang-Ming Jen, Chi-Sung Laih, Wen-Chung Kuo . "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", Sensors**,** Vol. 9, Issue 6, Pages: 5022-5039, 2009

[16] D. Djenouri, O. Mahmoudi, D. Llewellyn-Jones, M. Merabti, "On Securing MANET Routing Protocol Against Control Packet Dropping". *In IEEEInternational Conference on Pervasive Services, 2007,* pp.100-108

[17] M.S. Sankaran, S. Poddar, P.S. Das, S. Selvakumar. "A Novel Security model SaW: Security against Wormhole attack in Wireless Sensor Networks*". In Proceedings of International Conference on PDCN*, (2009).

[18] Marianne Azer, Sherif El-Kassas, Magdy S. El-Soudani:"An innovative approach for the wormhole attack detection and prevention in wireless ad hoc networks"*. ICNSC,2010,* pp.: 366-371,.