A Novel Approach for Wormhole Detection in MANET

Nidhi Nigam
Dept. of Computer Science & Engg.
JIT, Borawan/Khargone
RGPV, Bhopal

Vishal Sharma
Dept. of Computer Science & Engg.
JIT, Borawan/ Khargone
RGPV, Bhopal

Mahesh Malviya
Dept. of Computer Science & Engg.
JIT, Borawan/Khargone
RGPV, Bhopal

ABSTRACT

The active operational environment of Mobile Ad hoc NETwork (MANET) makes it exposed to a variety of 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, relative approach, based on Reference Broadcast System (RBS). To improve network scalability and throughput, we propose the concept of the relative velocity between sender & the receiver node of the 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.

General Terms

Wireless networks, threshold, ACK, routing, relative velocity

Keywords

AODV, MANET, wormhole attack, relative velocity, RBS

1. INTRODUCTION

In this universe Wireless networks have become a primary component of the digital society due to the easiness in accomplishment and, in for the most part, the minor charge as compared to the wired networks. Furthermore due to its simplicity in utilizing and convenience, it is extremely popular with users and it is being paid even extra hence it exists in more and more places. Wireless networks have also been deployed in places that were deemed infeasible for the operation of wired networks and have been the preferred way in new areas. Wireless networks stay alive in all different sectors, specifically government and private sectors, across the globe and for different types of usage. On top of that, the outburst of devices and applications that were deliberate to work in wireless networks are just unbelievable. There are, in general, three varieties of wireless networks that are mainly common: ad-hoc networks, mesh networks and sensor networks. Mobile ad hoc networks (MANET) are the one category which consist a number of auto-configuring nodes that are movable in nature, freely moves and make use of wireless equipment to communicate with one another. This sort of network does not require a concentrated entity and are infrastructure-less [2]. The second division is a wireless mesh network (WMN) in which every node communicates with the other nodes through radio waves. Finally, a wireless sensor network (WSN), consists of a gateway or base station and communicate with other wireless sensors by a radio link. The collected data by means of the wireless sensor node, compressed, and transmitted to the gateway (sink) directly [3].

1.1 Overview of MANET

Mobile Ad-hoc network is a set of wireless devices known as wireless nodes, which dynamically connect and convey information. These nodes may be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices as shown in figure 1. In general, a wireless node can be any computing apparatus that employs the air as the transmission medium. In a 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 nearer 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 mobile ad-hoc network have many advantages [1] as fast & low cost of deployment, dynamic configuration etc.

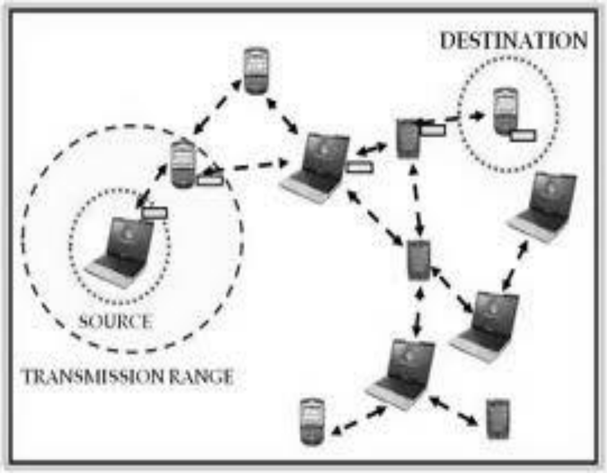

Fig 1: Mobile Ad hoc Network consists several of mobile nodes

MANET has several potential applications. Some classic examples comprise emergency search-rescue operations, meeting events, dealings, conferences, and battlefield communication between moving vehicles and/or soldiers. With the abilities to meet up the new demand of mobile computation, the MANET has a very bright future. Even though security has long been an active research issue in wired networks, the uniqueness of Ad Hoc networks presents a new set of nontrivial challenges in the direction of security design. These challenges include open network architecture, mutual wireless medium, stringent resource constraints, and highly dynamic topology. Some of the main security attributes [1] [2], which are used to examine the security status of the mobile ad-hoc network, are: Availability, Integrity, Confidentiality, Authenticity, Non repudiation, Authorization, Anonymity.

2. ROUTING APPROACHES AND EFFECT OF WORMHOLE ATTACK IN MANET

Commonly ad hoc routing protocols are of two categories: proactive routing protocol, which based on the periodic broadcast of routing packet updates, and on-demand routing protocols that look for routes whenever required. A wormhole attack is uniformly worse for both proactive and on-demand routing protocols [4][7][8]. When a proactive routing protocol [9] are in use, ad hoc network nodes send periodic HELLO messages to others signify their participation in the network. In Figure 2, when node S sends a HELLO message, intruder M1 forwards it to the other end of the network, and node H listens to this HELLO message. Since H can take notice of a HELLO message from S, it assumes itself and node S to be direct neighbors. Therefore, if node H needs to forward something to S, it may accomplish so innocently in the course of the wormhole link. This effectively permits the wormhole attackers for full power during communication.

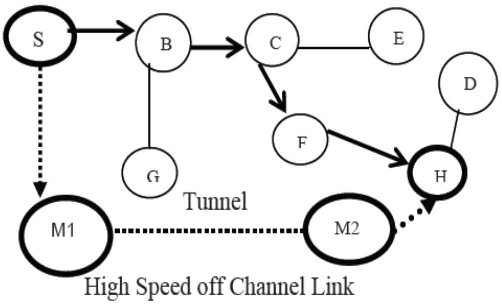

Fig 2: MANET with a wormhole attack

In case of on-demand routing protocols, for instance AODV [10], when a node wishes to communicate with another node, it floods requests to its neighbors, trying to determine a path to the destination. In above figure 2, if node S wants to communicate with H, it sends a request. A wormhole node, once more, forwards these requests without change to the other end of the network, may be directly to destination node H.A request moreover travels along the network in a systematic way; as a result H goes ahead to believe that it has a feasible route towards node S through the wormhole attacker node. If this route is selected in route discovery, once again wormhole attackers get full control of the traffic among nodes S and H. Once the wormhole attackers obtain control over a link, attackers can drop the entire packets, a random fraction of packets, or particularly some specific packets. Attackers can also forward packets out of order or ‘switch’ their link on and off [4].

In this paper, we have proposed an approach where wormhole attacker has been detected effectively using concepts of reference node and relative velocity. The AODV routing protocol is used as the underlying network topology.

3. RELATED WORK

Hu and Evans developed a protocol using directional antennas for prevention of wormhole attacks [6]. These directional antennas are capable to detect the angle of arrival of a signal. In this protocol, two nodes communicate with each other, knowing that one node should be receiving messages from one angle and the other should be receiving it at the opposite angle (i.e. one from the west and the other at the east). This protocol fails only if the attacker intentionally place wormholes between two directional antennas.

Rouba El Kaissi et.al [16] obstacles impede the successful deployment of sensor networks. In addition to the limited resources issue, security is a foremost concern especially for applications such as home security monitoring, military, and battlefield applications. This paper presents a defense mechanism against wormhole attacks in mobile ad hoc networks. Specifically, a simple routing tree protocol is used, which is modified furthermore.

Y. C. Hu et.al [14] has considered two types of packet leashes – geographic and temporal. In geographic leashes, node location information is used to connect the distance, from which a packet can traverse. Since wormhole attacks can affect localization, the information of location must be obtained using an out-of-band mechanism such as GPS. Further, the “legal” distance by which a packet can pass through is complicated to conclude. In temporal leashes, extremely accurate synchronized clocks are used to tie the propagation time of packets that could be inflexible to acquire for the most part in low-cost sensor hardware. Still when available, such timing analysis may not be able to detect such wormhole attacks.

In **S. Capkun et.al** [15], an authenticated distance bounding technique called MAD is used. This approach is related to packet leashes at a high level, but does not require location information or clock synchronization. But it still suffers from other limits of the packet leashes technique. In the Echo protocol, ultrasound signals are used to bind the distance for secure location verification. Use of ultrasound instead of RF signals as before helps in comforting the timing necessities; but requires an additional hardware. In a recent work [4], the authors have focused on practical methods of detecting wormholes. This technique uses timing constraints and authentication to confirm whether a node is a true neighbor or not. The authors developed a protocol that can be implemented in 802.11, capable hardware with minor modifications. Still it remains unclear that how practically such timing analysis possible with low-cost sensor hardware.

In **Ning Song et.al** [17], showed that multi-path routing is vulnerable to wormhole attacks. A straightforward scheme based on statistical analysis (called SAM) is proposed for detection of such attacks and to identify malicious nodes. Compared to the earlier approaches (for example, using packet leash), no special requirements (such as time synchronization or GPS) are required in the proposed scheme. Simulation results demonstrate that SAM effectively detects wormhole attacks and locates the malicious nodes in networks with different topologies and with different node transmission range.

Khalil et al. [18] propose a protocol in favor of wormhole attack discovery in static networks called as LiteWorp. In LiteWorp, once deployed, nodes obtain fully two-hop routing information from their neighbors. Whereas in a standard ad hoc routing protocol, node usually keeps track of their neighbors. In LiteWorp they also know who the neighbors' neighbors are; they can take advantage of two-hop, rather than one-hop, neighbor information. This information can be exploited to detect wormhole attacks. Also, nodes monitor their neighbors' behavior to find out whether data packets are being properly forwarded by the neighbor.

Our proposed scheme makes use of the three approaches AODV for routing, RBS [5] theory for threshold setting and Ack of reliability of communication.

4. PROBLEM STATEMENT

The central research dilemma is how to provide security protection to the network topology and the routing process in a wireless network. The major challenges include dynamic topology, decentralized control, limited resources, and the lack of information dissemination control. We investigate the problem in mobile ad hoc network environment. As building blocks for securing wireless network topology and routing, are of special interest for researchers.

During a wormhole attack [4], 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 easy for the attacker to make the tunneled packet than a normal multihop route. 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 it, 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 compare to other nodes in the network, and the attacker could utilize this position in a variety of ways. 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.

The wormhole attack is principally dangerous against many ad hoc network routing protocols in which the nodes that listen a packet transmission directly from some node, consider themselves to be in the range of that node. For example, when used against an on-demand routing protocol such as AODV [10], a powerful application of the wormhole attack can be mounted by tunneling each ROUTE REQUEST packet directly to the destination target node of the REQUEST. When the destination neighbors hear this REQUEST packet, they will follow normal routing protocol processing to rebroadcast that copy of the REQUEST and then discard without processing all other ROUTE REQUEST packets originating from this same Route Discovery. This attack thus prevents any routes other than through the wormhole from being discovered, and if the attacker is near the initiator of the Route Discovery, this attack can even prevent routes more than two hops long from being discovered. Possible ways for the attacker to then exploit the wormhole include discarding rather than forwarding all data packets, thereby creating a permanent Denial-of-Service attack (no other route to the destination can be discovered as long as the attacker maintains the wormhole for ROUTE REQUEST packets), or selectively discarding or modifying certain data packets.

5. PROPOSED TECHNIQUE

We suggest a new method to detect the wormhole attack in on demand routing protocol. Before each node transfers data, it is necessary to check node authentication that is important feature of security, to its nearest neighbor. For this purpose two approaches are followed shortly, which come to know wormhole node:

(1) Calculate relative velocity between sender & receiver node by using RBS[5] concept, which will be further compare with threshold value already set between 0 & 1.Using RBS theory, relative velocity will compute through reference node and selection criteria for these reference node comprise any node nearer to sender node (other than a receiver node). According to this approach, the malicious node whose threshold value does not match with the defined threshold, cannot impersonate and use another node authentication. This approach is named as pre-processing level and is continued until the packet reaches to destination.

(2) When the packet is received by destination, the processing approach is started, in which it determined whether the node is trusted or not. As per nature of mobile ad-hoc network if node, who's taking part in data transmission, moves from its position then it has to inform respective nodes, taking part in data transmission. According to the theory of relative velocity, the relative velocity of nodes A & B with respect to the reference node P shown in following example in figure 3 as:

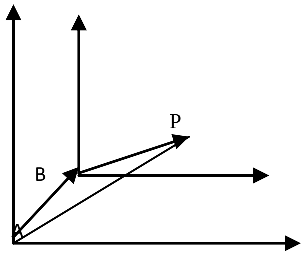

Fig 3:Concept of relative velocity using reference node

$V_{BA}=V_{PA}-V_{PB}$ (1)

Where V_{PA} is velocity of pt. P w.r.t A and so on …

Equation 1 depicts common equation for calculation of relative velocity with reference to one another.

If above two circumstances satisfy the network then the authentication of the node is confirmed, the packet is sent otherwise the next neighbor is selected for data transmission. In this paper, we present a set of mechanisms for detection of wormhole attacker. First, the concept of relative velocity is proposed between mobile nodes. Then source node estimates the minimum path to the destination based on the Reference Broadcasting [5] during the route discovery. Wormhole node will create tunnel between any two of nodes in the 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.

Above written Proposed scheme can be easily understand through the algorithm shown in below.

Algorithm Steps for detection of wormhole node

```
1) Begin
2) Route discovery using AODV protocol by Sender node.
3) Choose refernce node,who is nearer to the sender node.
4) Compute relative velocity via sender node.
5) Compare  the relative velocity with a threshold value,
        If(satisfies criteria)
            then go to step 6.
        Else
            go to step 2.
6) Then transmission starts.
7) As nature of mobile ad-hoc network, any node who is taking part in data transmission moves from its place and,
        If (it informs to other nodes who are involved in transmission)
            then Node behaves normal.
             go to step 1.
        Else
            Wormhole node is detected.
8) End
```

We used AODV routing protocol for performing such job. AODV [20] is a hop-by-hop routing protocol, which introduces a dynamic strategy to find out and repair route. It keeps only active routes to decrease overheads and control traffic. This protocol is appropriate for different levels of node density, mobility and loads and suitability in support of scenarios with moderate mobility and density networks. Efficient route establishment, resource reservations and less computational complexity since, the proposed approach uses a simple semantic security mechanism [21] because nobody can compute relative velocity other than reference node. It monitors misbehaving nodes correctly through the acknowledgement scheme. Thus, problems such as ambiguous collisions, receiver collisions, and the ability of a node to control its transmission power do not exist in the approach.

5.1 Advantages of proposed scheme

The proposed scheme leads general aspects like relative velocity; acknowledgement etc, hence there is no need for extra arrangements as compared to other existing methods. This method also provides better results after evaluation of simulation since proposed method is implemented through simulator. Some of the existing methods for detection of wormhole node such as Packet leashes, temporal [14], LiteWorp [18] are impractical. Some existing methods require additional resources like directional antennas in Directional antennas [6], for practically implementation. Our proposed technique does not require any extra equipment. The routing protocol selected for implementation is AODV that only requires dynamic routes so it reduces overhead and helps in traffic control. Since proposed scheme introduces concept of reference node means no other node is responsible for calculation of relative velocity which represents authentication feature of security.

6. EXPERIMENTAL ANALYSIS AND RESULTS

One common method to conduct research in the networking and security fields is to simulate and evaluate the protocol(s) and there are various computer simulation applications that take responsibility for performing those tasks, such as NS-2 [11], OPNET [12], GLOMOSIM [13], etc.

NS-2, LBNL's Network Simulator [11] [19] is preferred as a simulation environment since it is one of the leading environments for network modeling and simulation. This simulator is written in C++; uses OTcl as a command and configuration interface. It supports large number of built-in industry standard network protocols, devices, and applications. Furthermore, its programming library helps researchers to easily modify the network elements and determine their performance inside the simulation environment. It also provides rich data analysis features. We used NS 2.34 version for performance evaluation of proposed scheme and modified AODV routing protocol.

Parameters used for simulation are routing protocol, traffic type as constant bit rate, mobility model etc. The mobility scenarios are generated using a Random waypoint model. Random Way Point mobility model is the most frequently used form for research purpose. In this model all the nodes are randomly distributed with identical speed. It includes pause time between changes in destination and speed. Pause time indicates to overcome sudden end and start in random way point model. The simulation parameters are summarized in following Table 1.

Table 1. Simulation Parameter.

Parameter	**Value**
Simulation duration	100 sec
Simulation area	1000*1000
Number of mobile nodes	25
Traffic type	CBR (UDP)
Packet rate	4 packet/sec
Abnormal node	01
Routing Protocol used	AODV
Movement model	Random way point
Payload size	512 bytes

A MANET of 25 nodes was simulated. Simulation scenario is shown in following figure 4.One node was set as wormhole and rest nodes represent normal nodes in the network scenario. Following figure shows the simulation scenario of used scheme during pause time 20s. At this time our abnormal node involves in routing path.

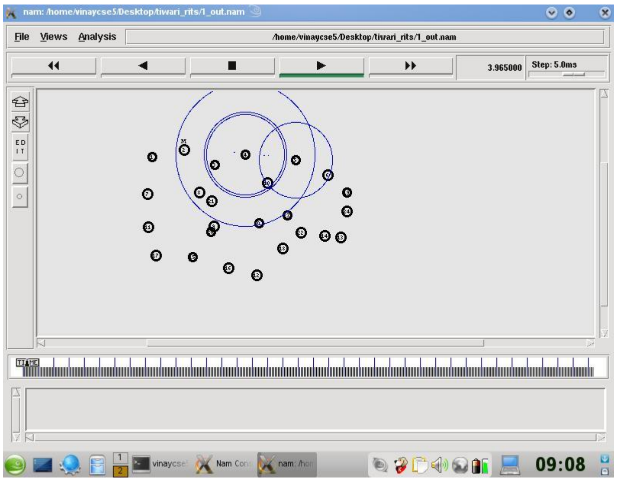
nam: /home/vinaycse5/Desktop/tiwari_rits/1_out.nam
File
Views
Analysis
/home/vinaycse5/Desktop/tiwari_rits/1_out.nam
3.965000
Step: 5.0ms
EDIT
vinaycse
Nam Con
nam: /ho
09:08

Fig 4: simulation scenario of NAM with wormhole node for detection of wormhole node.

We consider some network parameters as throughput, average end-to-end delay, jitter etc for estimation of results. We compared the results before and after the attack to observe the effect of the wormhole attack on the network. Few of them are defined as follows:

(1)Throughput: It gives the fraction of the channel capacity used for useful transmission (Data packets accurately delivered to the destination) and is defined as the total number of packets received by the destination. It is in fact an evaluation of the effectiveness of a routing protocol. Following figure 5 shows comparative xgraph result of throughput.

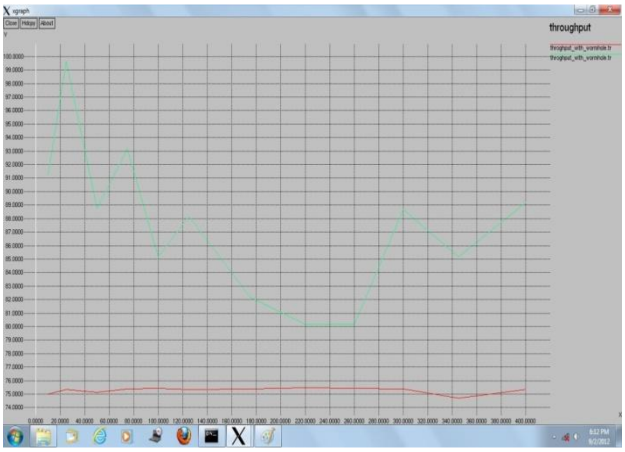

Fig 5: Xgraph result for average throughput

(2)Average end-to-end delay***:*** This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times. Figure 6 shown below represent average end-to-end delay with and without wormhole.

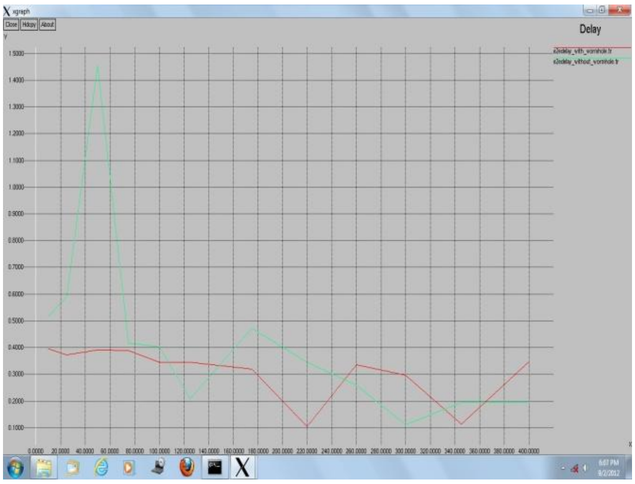

Fig 6: Xgraph result for average end-to-end delay

(3) Packet delivery fraction**:** The ratio of the data packets delivered to the destinations to those generated by the traffic sources.

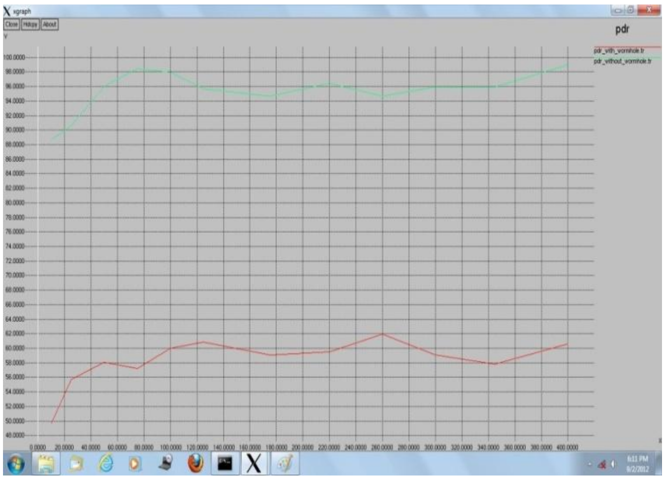

Fig 7: Xgraph result for Packet Delivery Ratio

The graphs showed above represent comparative evaluation in the network with and without wormhole and clearly shows the effect of wormhole in the network.

7. CONCLUSION

Wormhole attacks are major problems that need to be addressed in wireless network security. Security of ad-hoc networks has recently gained momentum in the research society .Due to the open nature of ad hoc networks and their intrinsic lack of infrastructure, security exposures can be an impediment to basic network operation .Security solutions for MANET have to survive with a challenging environment together with limited energy and computational resources and lack of persistent structure of MANETS. This approach will deal with the issue in a proficient manner by reducing a numeral attacks. The idea discusses a semantic security mechanism to handle attacks based upon packet dropping and message tampering, which is capable of accurately identify the malicious nodes in the network. The known malicious nodes are isolated for future sessions. In the proposed system, possibility of enhancements and improvements are enormous.

An instant enhancement is assessment of more network parameters. Further, the scheme can be made safer against other types of probable network layer attacks that threaten the network.

8. REFERENCES

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

[2] Nguyen, D. Q., & Lamont, L, “A Simple and Efficient Detection of Wormhole Attacks”. IEEE Conferences New Technologies, Mobility and Security (pp. 1-5). NTMS '08.

[3] Chris, T., & Steven,”Wireless Sensor Networks: Principles and Applications”. Retrieved 18 2, 2011, from MicroStrain: microstrain.com/white/Wilson-chapter-22.pdf

[4] Y.-C. Hu, A. Perrig, D. B. Johnson; “Wormhole Attacks in Wireless Networks”; IEEE Journal on Selected Areas of Communications, vol. 24, numb. 2, pp. 370-380, 2006.

[5] 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.

[6] L. Hu and D. Evans, “Using directional antennas to prevent wormhole attacks,” in Proceedings of the Network and Distributed System Security Symposium.

[7] Yang, H. and Luo, H. and Ye, F. and Lu, S. and Zhang, U.; “Security in Mobile Ad Hoc Networks: Challenges and Solutions”; Wireless Communications, IEEE, vol. 11, num. 1, pp. 38-47, 2004

[8] Y.-C. Hu, A. Perrig; “A Survey of Secure Wireless Ad Hoc Routing”; Security and Privacy Magazine, IEEE, vol. 2, issue 3, pp. 28-39, May 2004.

[9] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum, L. Viennot; “Optimized Link State Routing Protocol”; Proceedings of IEEE INMIC, Pakistan 2001.

[10] Charles E. Perkins and Elizabeth M. Royer. "Ad hoc On-Demand Distance Vector Routing." Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp. 90-100, 1999.

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

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

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

[14] Y. C. Hu, A. Perrig, and D. Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks,” in INFOCOM, 2003.

[15] S. Capkun, L. Buttyn, and J. P. Hubaux, “SECTOR: Secure tracking of node encounters in multi-hop wireless networks,” in 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), October 2003.

[16] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy,”Dawsen: a defense mechanism against wormhole attacks in wireless sensor networks“, IN Second International Conference on Innovations in Information Technology (IIT’05).

[17] 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.

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

[19] Mark Corner and Brian Noble. “Zero-Interaction Authentication”. In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), pages 1–11, September 2002.

[20] Charles E. Perkins and Elizabeth M. Royer. “Ad-Hoc On-Demand Distance Vector Routing”. In Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’99), pages 90–100, February 1999.

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