The Study of Wormhole Attack in Mobile Ad Hoc Network

Ruchita Tailor
Department of Computer Science and Engineering,
Parul Institute of Engineering and Technology,
Vadodara, Gujarat

Jwalant Baria
Department of Computer Science and Engineering
Parul Institute of Engineering and Technology,
Vadodara, Gujarat

ABSTRACT
In MANET is a collection of autonomous system of mobile nodes connected with each other using wireless link and each node communicates with each other using wireless link that are within its transmission range. The network is unbounded by any fixed infrastructure or any central authority. The dynamic topology and open nature makes the Mobile Ad Hoc Network more vulnerable to security threats. The success rate of MANET highly depends on the confidence in the security shown by the users. Wormhole attack is one such security threat at network layer which causes routing disruption. The attacker at one point in the network records the packet and forwards it through a high speed tunnel to the other attacker present at distant location giving an false impression to nodes in both the network that they are immediate neighbors. This paper presents a study on wormhole attack and various existing techniques to detect and prevent wormhole attack in MANET.

General Terms
Security, Attack, Network

Keywords
Mobile Ad Hoc Network (MANET), Network Layer, Wormhole attack

1. INTRODUCTION
The field of wireless communication is experiencing an exponential growth since past decades due to advances in network infrastructure, mobile portable computing devices such as personal digital assistants, laptops and cell phones. With this rapid development of wireless technology, Mobile ad-hoc Network (MANET) has emerged as a new type of wireless network. A MANET is a self-configuring network of mobile devices connected by a wireless links, the union of which form an arbitrary topology as shown in Figure 1.

The network can be deployed easily at low cost without any centralized administration. It is an infrastructure less wireless network as it performs network operations without any need of a base station or access point. Each node not only acts as an end system, but also store and forwards the routing packets to other nodes in the network. Hence it is also known as multi hop routing. These nodes may have different capabilities and are resource constraints, that is, limited battery power and limited bandwidth. The routers are free to move randomly and organize themselves arbitrarily; thus the network's wireless topology may change rapidly and unpredictably. Each node will be able to communicate directly with other nodes that reside within its transmission range. For communicating with nodes that resides beyond this communication range, the node needs to use intermediate nodes that replay messages hop by hop. Thus, highly collaboration between mobile nodes leads to a successful communication between mobile nodes.

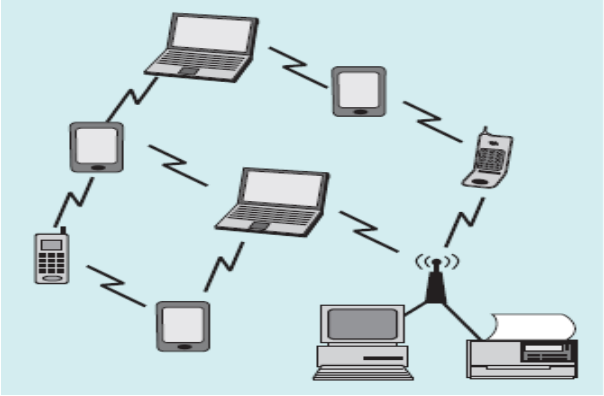

Fig. 1 Mobile Ad Hoc Network[1]

The network unlike traditional wired network is less reliable and has limited physical security, higher loss rates and many other design constraints. Despite these constraints the network is highly suitable and widely employed in case of rescue operations, where fixed network cannot be established or is setting up a network is too expensive, emergency operations, military operations, personal networking, commercial environment etc. To accommodate the changing topology special routing algorithms are needed. If the exact specifications of the routing protocols are not followed, an attacker can mount routing attacks which can disrupt the overall network communication during the routing phase. The security attack in MANET can be classified into two types, Active attack and Passive attack. In active attack, the attacker disrupts the normal functionality of the network while in passive attack, the attacker does not disrupt the network operation, but it attempts to analyze the network traffic. Thus, security plays a vital role in order to provide protected communication among the mobile nodes in the network.

Wormhole attack is one of the major security threats that can cause major disruption in network communication where a malicious node captures packet from one location in the network, tunnels it to another malicious node at distant point, when then replays it locally. The route via tunnel provides less number of hops and less latency than normal multi-hop routes and hence is generally more attractive to the legitimate nodes. Once the wormhole link is established the malicious nodes can either drop the packet, perform eavesdropping or any of Denial of Service attacks.

2. WORMHOLE ATTACK

The Wormhole attack, a route disrupting attack is one of the most serious security issue in MANET. It is a kind of tunneling attack in which a malicious node receives packet at a one location in the network, tunnels them to another location in the network and then replays them into the network from that point.

Wormhole attack in reactive routing protocol is launched as shown in Figure 2[2].

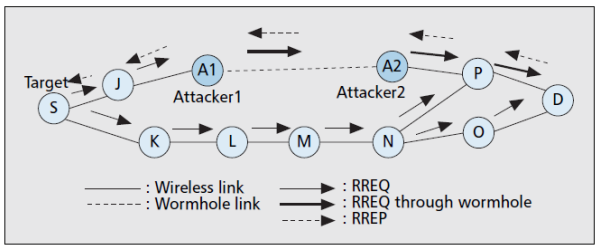

Fig. 2 Wormhole attack in reactive routing protocol

Node S, the source node wants to send packet to node D, the destination node. Node A1 and node A2 are two malicious nodes. The source node broadcasts an Route Request (RREQ) in order to find a route to destination node D. The neighbor node J and K receive and forwards the RREQ to its neighbors. The RREQ is then received by a malicious node A1 through node J. The malicious node A1 then records and tunnels the RREQ to another malicious node A2 through high speed tunnel. Malicious node A2 then rebroadcasts the RREQ which is later received by node P and then to the destination node D. As the RREQ through node P is received early at destination node D as compared to from node O, the destination node D choose the path from P i.e. D-P-J-S, to unicast the RREP to source S.

A single malicious node can launch this attack by broadcasting the route request at a high power level [7]. If multiple malicious nodes collude together to perform malicious acts, their activity of network disruption becomes even harder to detect. It creates an illusion that two remote nodes are immediate neighbors despite being located several hops away. It can significantly disrupt the network communication by dropping packets, eavesdropping, packet sniffing or can make any DoS (Denial of Service) attack. It can be launched easily without prior knowledge of routing protocols and without compromising any nodes in the network. It is easy to deploy but is hard to detect.

2.1 Wormhole Attack in Routing Protocol

Ad Hoc network routing protocol are classified into two categories: Proactive (Table-Driven) Protocol and Reactive (On-Demand) protocol.

(a.) Proactive (Table Driven) Routing Protocol: In Proactive type of protocols routes are established prior to requirement. Each node in the network maintains a routing table containing possible destination's routing cost in terms of the number of hops and the corresponding next hop information towards the destination. Whenever a change occurs or periodically, each node broadcasts its routing table and all nodes updates their routing table received from its neighbors. DSDV, OLSR are examples of Proactive type of routing protocol. The impact of wormhole attack on Proactive type of protocol in MANET is as shown in Figure 3. The tunnel is created between two malicious S2 and S9. In this type of protocol, when node S9 broadcasts its routing table, node S2 assumes that node S9 is one hop away and hence it updates the routing table for node S9 as one hop away and nodes S8, S11, S12, S10 to be two hop away and broadcasts its routing table. Similarly, other nodes updates its routing table and hence all the routes now pass through the malicious node S2.

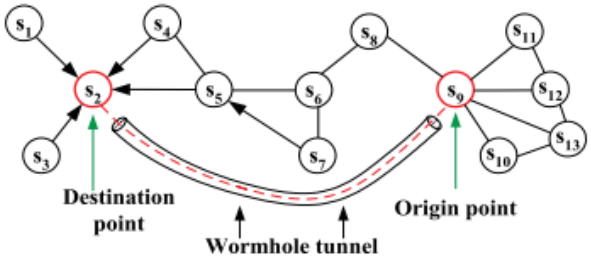

Fig. 3 Wormhole Attack in Routing Protocol

(b.) Reactive (On-Demand) Routing Protocol: In Reactive type of protocol, routes are discovered whenever a sender wants to send the packet to the destination. Thus route discovery occurs on demand basis. AODV, DSR are examples of Reactive type of protocol. The impact of reactive protocol on MANET is shown in Figure 3. When a node S9 wants to send data to node S2, it broadcasts RREQ in the network until it finds route to destination. When a route to destination is find RREP is sent to the sender. As node S2 is one hop away from S9, route gets established includes the wormhole link.

2.2 Classification of Wormhole Attack

Based on the packet forwarding behavior of malicious node participating in wormhole tunnel and their tendency to hide and show their identities, the wormhole attack can be classified in the following two classes.

(a.) *Hidden mode (HM):* In Hidden Mode (HM) the attackers while tunneling the packet from one point to another do not alter the content of the packet and packet header in the AODV advertisement packet and replays it to a another point in the network. As shown in Figure 4(a)[8], suppose sender S wants to establish a route to receiver R.

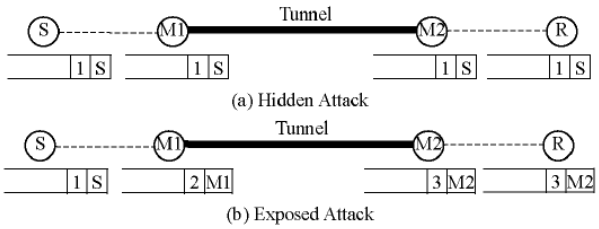

Fig. 4 Classes of Wormhole Attack

Sender node S broadcasts a RREQ message using AODV routing protocol. The node receiving RREQ checks if it a valid route to R. If it does not have a valid route to R, it should update the hop count information and add its identity in the packet header and then continue to broadcast RREQ. In case of HM wormhole attack, malicious node never updates the routing table. When a packet from S is received by a malicious node M1, it simply tunnels the packet to another malicious node M2 which replies to R without updating the

routing table. Hence when a packet is received by R, it finds the previous hop information of sender S. Malicious nodes are invisible from legitimate users and make the sender treat the receiver as its immediate neighbor.

(b.) *Participation/Exposed Mode (PM):* In the Exposed or Participation Mode (PM) mode attack, the attacker includes its identity in the packet header but do not modify the contents of the packet in AODV advertisement packet. As shown in Figure 4(b)[8] when a RREQ from Sender S is received by M1, M1 increases the hop count value and add its identity in packet header and tunnels the RREQ packet to malicious node M2. M2 performs the same setup procedure and broadcasts RREQ packet to R. R finds its previous node as M2 with hop count 3. Thus in this type of attack mode, malicious node process as a legitimate node and appear in wormhole infected route.

The attacker can tunnel the packets to each other by either using in-band (I-B) communication link or out-of-band (O-B) communication link as shown in Figure 5.

(a.) *I-B channel*: I-B channel also known as packet encapsulation channel, tunnels packets between the malicious nodes through pre-built path via genuine network nodes and are easy to launch. As shown in Figure 4, when a sender S broadcasts a RREQ message, malicious node m1 receives the packet and after encapsulating the packet sends it via a pre-built path between m1 and m2. When packet reaches m2, it extracts the original packet and sends it to R. As a result the number of hop counts through this channel is less than that of the normal routes.

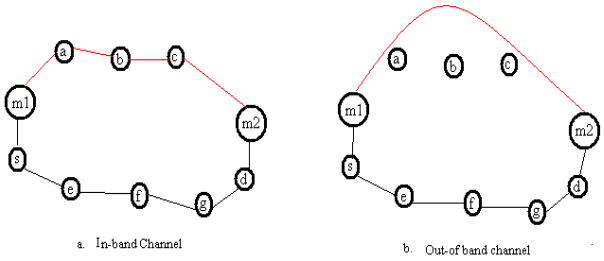

Fig. 5 Implementation of Tunnel

(b.) *O-B link:* O-B link is comparatively more complex than I-B link because it requires external communication links such as network cable or directional antennas to establish a direct communication between the wormhole nodes [1].

Wormholes are difficult to detect in MANET environment due to several reasons. The network is dynamic in terms of number of users, applications, their locations. Moreover devices are energy constrained with limited computing capability. The wormhole attack can be launched in different modes having different characteristics and challenges such as Participation mode, Hidden Mode, In-Band and Out-Band channels.

2.3 Impact of Wormhole Attack

Among various attacks, the wormhole is more dangerous as it does not exploit any node. The wormhole attack has significant impact on both type of routing protocols, i.e. proactive as well as reactive routing protocols. Once a wormhole is established, the attacker can get control of the routing traffic. The attacker can perform network disrupting operation such as packet dropping while results in low network throughput, eavesdropping and packet snooping. The wormhole attack can be possible even if authenticity and confidentiality i.e. any cryptographic techniques in communication is provided. Though no harm is done if the wormhole is used properly for efficient relaying of packets, it puts the attacker in a powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network.[7]

2.4 Metrics to detect wormhole attack

The capability of a node involved in wormhole attack can be measured by considering several metrics such as:

1. *Strength*: Strength is the number of end-to-end paths attracted by false link advertisements sent by the attacker. The effectiveness of the wormhole attack is the number of traffic attracted by a wormhole [3]. The more is the number of traffic passing through the wormhole tunnel, the more effective is the wormhole attack.
2. *Difference between the advertised path and the actual path length*: If the advertised path has a path length of smaller number of hops as compared to that of actual path, this difference in the path length can be a useful metric to detect wormhole attack. The irregularity can be more easily observed if there is larger difference between the advertised path and the actual path.
3. *Attraction:* Attraction refers to the decrease in path length offered by wormhole. If the attraction is small then, the small improvements in normal path may reduce the strength of wormhole attack as the nodes may choose an alternative route that does not pass through the wormhole tunnel.
4. *Robustness:* Robustness refers to the ability of wormhole attack to persist its effect without significant decrease in its strength even in the presence of minor topology change.
5. *Packet delivery ratio:* The Packet delivery ratio metrics refers to the ratio of total number of packets delivered to the total number of packed sent.

3. WORMHOLE DETETCION AND PREVENTION TECHNIQUES

Several works has been proposed to address the problem of wormhole attack by detecting, preventing or mitigating the wormhole attack in MANET. Various detection strategies proposed are classified broadly into: neighbour validation and end-to-end techniques. Packet leashes and statistical based detection based methods are types of neighbour validation schemes, while end-to-end detection schemes detect wormhole based on round trip time (RTT), Hop count analysis (HC), frequency of nodes appearance in the route or location of the nodes. The neighbourhood validation schemes are useful to detect Hidden mode wormhole attack while end-to-end scheme is useful to detect Participation mode wormhole attack. These techniques have number of limitations including, the inability to detect all wormhole variants, the requirement of dedicated hardware, reliance on certain MANET environment, high computational overheads and/ or bandwidth loads upon the network. [4]

A packet leash[5] is type of neighbour validation scheme. It is a mechanism to detect and defend the wormhole attack by restricting the time that packets can be transferred. There are two types of packets leashes: Temporal packet leash and geographic packet leash. In temporal leashes each node based on the speed of light calculates the packet expiration time and

appends it to the packet to restrict the packet from travelling further than a specific distance. The expiration of packet is checked by the receiver by comparing the current time and expiration time in the packet. In Geographic leashes, sender node appends its precise location and transmission time while sending a packet. When the receiving node receives the packet it compares its location and the time at which packet is received by the node with the information appended by the sender node. A temporal leash requires tight clock synchronization and does not rely on GPS technology, while in Geographic leashes the nodes need not be tightly synchronized and reply on accurate measurement of GPS technology. It is effective only for Hidden mode wormhole attack as in Participation mode wormhole attack, a legitimate node can save itself from being detected by avoiding the validity check.

Directional antennas is a hardware based approach where each nodes are equipped with directional antennas In order to communicate with each other, nodes use specific sectors of antennas and examine the direction of received signal. If the directions of both the pairs match, relation is set. This approach fails if an attacker strategically places the wormhole between the communicating nodes. It is less expensive and ensures efficient use of energy and better spatial use of bandwidth.

Statistical Analysis scheme is based on the concept of analysing the relative frequency of each link appearing in routes and identifying the highest frequency link. It is based on the idea that wormhole attack is present if there is less number of hops and the nodes encounter low transmission delay. It does not require any additional hardware. It works only with multipath on-demand routing protocol.

FEEPVR (First end-to-end protocol to secure Ad Hoc Networks with Variable range)[6] detects wormhole node based on the number of hops and location information. A path is suspected of wormhole if the number of hop count for a route is less than the minimum lower bound. It does not require tight synchronization and has low computation and storage overhead. It depends on GPS technology for wormhole detection.

SEEEP (Simple and Efficient End –to –End protocol)[7] is a simple algorithm to secure ad hoc networks against wormhole attack based on the measurement of length of path between source and destination d and the communication range r. The packet from source to destination must travel at least [d/r] hops.[7] It does not require tight synchronization and has low computation and storage overhead. It also depends on GPS technology for wormhole detection.

DelPHI (Delay Per Hop Indication) is based on the calculation of (delay/hop) value of disjoint paths. It is based on the fact that under normal condition, the delay a packet experiences in propagating one hop should be similar along each hop path, while in case of wormhole attack, the delay for propagating across false neighbours are high as there are many hops between them. It does not need any extra hardware or tight time synchronization and has high power efficiency [8]. It works for both I-B and O-B mode.

TTM is a transmission time based approach based on the idea of calculating RTT (Round Trip Time) between two successive nodes in the network during route setup procedure. It is based on the fact that the transmission time between two malicious nodes is considerably higher than the normal nodes in the network which are within radio range of each other.[9] It has comparatively good performance, little overhead and requires no special hardware. It works only for O-B mode.

WARP (Wormhole Avoidance Routing Protocol)[10] is based on anomaly detection technique to detect wormhole. It takes into consideration multiple link-disjoint paths but use only one path to transmit data packet. It enables the neighbors of wormhole nodes to discover that the wormhole nodes have abnormal path attractions. The wormhole nodes would be gradually isolated by their neighboring nodes and finally be isolated by the whole network. As compared to other techniques, it achieves degradation in packet loss without any additional hardware support.[10]. It works for both I-B and O-B wormhole modes.

MHA (Multi- Hop Count Analysis) scheme is based on the hop count analysis to detect the wormhole attack. It examines the hop count values of all the routes and sets a set of safe route for data transmission. It has high efficiency as it has low computational overhead. It needs no specialized hardware and has good performance.

4. COMPARISON OF EXISTING METHODS

The comparison between existing methods used to detect wormhole attack in MANET is shown in the Table 1 along with the advantages and disadvantages of each of them.

Table 1 Comparison Between Existing Methods

Methods	Description	Advantages	Disadvantages
Geographical Leashes[5]	Neighbourhood validation mechanism: Ensures receiver must be within certain distance from the sender	Used when tight clock synchronization not needed.	Limitation of GPS technology, increase computation and network overhead
Temporal Leashes[5]	Neighbourhood validation mechanism: Time stamp is given to a packet and a comparison is made between locally maintained time and assumed transmission speed.	Do not rely on GPS information, highly efficient when used with TIK.	All nodes require tight synchronization

End to End Leashes	Neighbourhood validation mechanism: Each intermediate node appends time and location information and receiver authenticates time and location information of a packet using symmetric key	No need of clock synchronization, In absence of error in location, there are no false alarm.	Limitation of GPS technology, Computational complexity
Directional Antennas	Each pair of nodes determines the direction of received signals from neighbour if direction matches relation is set.	Less expensive, efficient use of energy and better spatial use of bandwidth	Need for directional antenna
Statistical Analysis	Identify highest frequency link through relative frequency measurement of each link appearing in obtained routes.	No additional hardware is needed.	Works only with multipath on demand protocols
FEEPVR[6]	Geographical based solution: A lower bound to minimum number of hops is assumed and any path having less number of hop counts is suspected to a be under wormhole attack	No tight clock synchronization needed. Effect or error is low, low storage and computational overhead	Limitation of GRS technology
SEEER[7]	Geographical based solution: It uses speed to detect wormholes	No tight clock synchronization needed. Effect or error is low, low storage and computational overhead	Limitation of GRS technology
WARP[10]	Neighbourhood validation method: Considers multiple link-disjoint paths but use only one path to transmit data packet.	No extra hardware support, no tight clock synchronization	Works for both I-B and O-B mode.
MHA[12]	Based on Hop count Analysis scheme: Examine the hop count value of all routes and sets a safe set of routes for data transmission.	Computational overhead is low, High efficiency, good performance, No need of specialized hardware	Only efficient in specific scenario-compromise HM wormhole detection
DelPHI[8]	Round Trip Time based solution: Sender and a receiver. Then, the Delay time and length of disjoint route between sender and receiver are calculated and the average delay time per hop along each route is computed.	No extra hardware and tight time synchronization needed, high power efficiency	Works for both I-B and O-B mode.
TTM[9]	Round Trip Time based solution: Transmission time between two fake neighbours created by wormhole is considerably higher than that between two real neighbours which are within radio range of each other.	Good performance, little overhead and no special hardware required	Works only in O-B mode

5. LIMITATIONS OF EXISTING WORMHOLE DETETCTION /PREVENTION TECHNIQUES

Most of the solutions proposed for wormhole detection need special assumptions such as tight time synchronization, location information, zero delay time on nodes or need for an additional specialized hardware. To some degree, they even incur a price in terms of their wormhole coverage capability, computational complexity, and network overhead to achieve improved detection rates. These constraints limit their applicability in dynamic environment where nodes change their positions and have limited processing power and capabilities. Moreover, several approaches restrict their application to certain wormhole variants and specific network condition.

6. CONCLUSION

Wormhole attack is one of the major security concern of Mobile Ad Hoc Network as it disrupts the routing protocols

by creating false routing paths during route discovery process by capturing and forwarding the packet from one location in the network to the other using high speed tunnel. The existing system on wormhole attack detection is either based on neighbor validation or end-to-end detection. But most of the existing techniques either has high computational complexity or need hardware or tight time synchronizations or is applicable only to specific wormhole detection modes. There is a need to develop a generic wormhole detection strategy for all types of wormhole variants.

7. ACKNOWLEDGMENTS

I am truly grateful to Mr. Jwalant Baria, Asst. Professor, Parul Institute of Engineering and Technology, for providing me his continuous support and guidance to realize this survey.

8. REFERENCES

[1] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, An Overview of Mobile Ad Hoc Networks: Applications and Challenges.

[2] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Tohoku University and Abbas Jamalipour, University of Sydney, "A Survey of Routing Attacks in Mobile Ad Hc Networks", Security in Wireless Mobile Ad Hoc Networks and Wireless Sensors, IEEE Wireless Communications, October 2007

[3] Viren Mahajan, Maitreya Natu, Adarshpal Sethi, "Analysis of Wromhole Intrusion Attacks in MANETS", University of Dealware, IEEE, 2008.

[4] Jonny Karlsson, Laurence S. Dooley and Göran Pulkkis, "Identifying Time Measurement Tampering in the Traversal Time and Hop Count Analysis (TTHCA) Wormhole Detection Algorithm ", Sensors 2013

[5] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad Hoc Networks", IEEE 2003.

[6] Khurana S., Gupta N.," FEEPVR: First End-to-End Protocol to Secure *Ad hoc*Networks with Variable Ranges Against Wormhole Attacks", Proceedings of the 2nd International Conference on Emerging Security Information; Cap Esterel, France. 25–31 August 2008; pp. 74–79.

[7] Gupta N., Khurana S., "SEEEP: Simple and Efficient End-to-End Protocol to Secure *Ad hoc*Networks Against Wormhole Attacks", Proceedings of the 4th International Conference on Wireless and Mobile Communications (ICWMC'08); Athens, Greece. 27 July–1 August 2008; pp. 13–18."

[8] Chiu H.S., Lui K.-S. "DelPHI: Wormhole Detection Mechanism for *Ad hoc*Wireless Networks.", Proceedings of the 1st International Symposium on Wireless Pervasive Computing; Phuket, Thailand. 16–18 January 2006.

[9] Phuong Van Tran1, Le Xuan Hung1, Young-Koo Lee1, Sung, Young Lee1, and Heejo Lee2, "TTM: An Efficient Mechansim to Detect Wormhole Attacks in Wireless Ad-Hoc Networks."

[10] Ming-Yang Su, "WARP:A Wormhole avoidance routing protocol by anamoly detetction mobile ad hoc networks", Miang Chuan Univeristy, Taiwan, Elsevier, 2009

[11] Karlsson, Jonny; Dooley, Laurence S. and Pulkkis, G¨oran (2011). "A new MANET wormhole detection algorithm based on traversal time and hop count analysis." Sensors, 2011(12), pp. 11122–11140.

[12] Shang-Ming Jen , Chi-Sung Laih and Wen-Chung Kuo, "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET", Sensors 2009

[13] Stefano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic, Mobile Ad Hoc Networking, A John Wiley & Sons, Inc., Publication, 2004

[14] Teerawat Issariyakul, Ekram Hossain, "Introduction to Network Simulator NS2",Springer 2009