ISSN:0975-9646

Secure Optimized Link State Routing Protocol for Ad-Hoc Networks

Priyanka A. Hajare[1#], Pritish A. Tijare[2#]

[1]ME Student, Dept of CE, SIPNA's College of Engineering, Amravati (MS) INDIA

[2]Assistant Professor, Dept of CSE, SIPNA's College of Engineering, Amravati (MS) INDIA

Abstract

The Optimized Link State Routing protocol (OLSR) has valuable features for mobile ad hoc networks such as no route discovery delay and ease of integration into existing systems, which makes it well-suited for time critical and emergency rescue applications. In OLSR, link state information is generated only by nodes elected as MPRs. Thus, optimization is achieved by minimizing the number of control messages flooded in the network. However, security, trust, and robustness are still a sizable challenge for OLSR. In this paper, we first highlight potential attacks, vulnerabilities, and key countermeasure points of OLSR in terms of security. Based on this analysis, we propose a new robust OLSR protocol for ad hoc network. We demonstrate that the proposed protocol can defend against various sophisticated attacks. We will evaluate and compared our proposed protocol to the original OLSR

1. Introduction

OLSR is a proactive routing protocol for mobile ad-hoc networks(MANETs). Mobile Ad hoc Network (MANET) is composed by a series of fast moving wireless nodes. Without the constraints of infrastructure, MANETs can adjust their topology on the basis of current situation flexibly. OLSR (Optimized Link State Routing Protocol), as a widely used and well tested protocol, is one of the main two Internet standards for wireless networks. However, MANET is involved in some othe r issues, such as instability. It is well suited to large and dense mobile Networks. OLSR uses hop-by-hop routing, i.e., each node uses its local information to route packets. The Optimized Link State Routing Protocol (OLSR) is a proactive link state routing protocol i.e., exchanges topology information with other nodes of the network regularly. Each node selects a set of its neighbor nodes as "multipoint relays" (MPR). In OLSR, only nodes, selected as such MPRs, are responsible for forwarding control traffic, intended for diffusion into the entire network. MPRs provide an efficient mechanism for flooding control traffic by reducing the number of transmissions required. Nodes, selected as MPRs, also have a special responsibility when declaring link state information in the network. Indeed, the only requirement for OLSR to provide shortest path routes to all destinations is that MPR nodes declare link-state information for their MPR selectors. Nodes which have been selected as multipoint relays by some neighbor node(s) announce this information periodically in their control messages. Thereby a node announces to the network, that it has reachability to the nodes which have selected it as an MPR. A node selects MPRs from among its one hop neighbors with "symmetric", i.e., bi-directional, linkages. OLSR is developed to work independently from other protocols. OLSR is well suited for networks, where the traffic is random and sporadic between a larger set of nodes rather than being almost exclusively between a small specific set of nodes. As a proactive protocol, OLSR is also suitable for scenarios where the communicating pairs change over time: no additional control traffic is generated in this situation since routes are maintained for all known destinations at all times.

The protocol inherits the stability of a link state algorithm and has the advantage of having routes immediately available when needed due to its proactive nature. OLSR is designed to work in a completely distributed manner and does not depend on any central entity. The protocol does NOT REQUIRE reliable transmission of control messages: each node sends control messages periodically, and can therefore sustain a reasonable loss of some such messages. Such losses occur frequently in radio networks due to collisions or other transmission problems. Also, OLSR does not require sequenced delivery of messages. Each control message contains a sequence number which is incremented for each message. Thus the recipient of a control message can, if required, easily identify which information is more recent - even if messages have been re-ordered while in transmission.

1.1 Types of messages

The Optimized Link State Routing Protocol (OLSR) is a proactive link state routing protocol for mobile ad hoc networks (MANETs), which uses HELLO and Topology Control (TC) messages to discover and disseminate link state information throughout the network.

1.1.1 HELLO Message

This involves transmitting the Link Set, the Neighbor Set and the MPR Set. In principle,a HELLO message serves three independent tasks:

- link sensing

- neighbor detection
- MPR selection signaling

Three tasks are based on periodic information exchange within a nodes neighborhood, and serve the common purpose of "local topology discovery". A HELLO message is therefore generated based on the information stored in the Local Link Set, the Neighbor Set and the MPR Set from the local link information base.

1.1.2 TC Message Generation

In order to build the topology information base, each node, which has been selected as MPR, broadcasts Topology Control (TC) messages. TC messages are flooded to all nodes in the network and take advantage of MPRs. MPRs enable a better scalability in the distribution of topology information.

OLSR minimizes the overhead from flooding of control traffic by using only selected nodes, called MPRs, to retransmit control messages. This technique significantly reduces the number of retransmissions required to flood a message to all nodes in the network. Secondly, OLSR requires only partial link state to be flooded in order to provide shortest path routes. The minimal set of link state information required is, that all nodes, selected as MPRs, MUST declare the links to their MPR selectors.

1.2 Multipoint Relays

The idea of multipoint relays is to minimize the overhead of flooding messages in the network by reducing redundant retransmissions in the same region. Each node in the network selects a set of nodes in its symmetric 1-hop neighborhood which may retransmit its messages. This set of selected neighbor nodes is called the "Multipoint Relay" (MPR) set of that node.

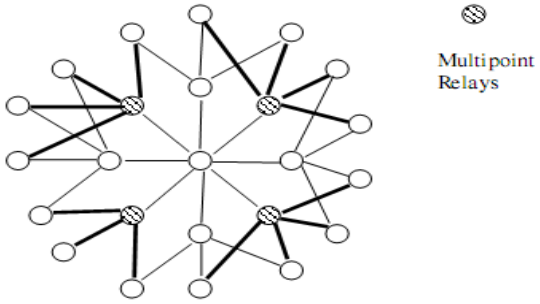

Figure: MPR election in OLSR protocol.

Each node maintains information about the set of neighbors that have selected it as MPR. This set is called the "Multipoint Relay Selector set" (MPR selector set) of a node. A node obtains this information from periodic HELLO messages received from the neighbors.

1.3 MPR Selection Algorithm

MPR set, as a key concept of OLSR protocol to reduce nodes to retransmit, is a subset of node's symmetric neighbors, which enables a node to reach any node in the symmetrical strict 2-hop neighborhood through relaying by one MPR node. In OLSR, MPR algorithm doesn't consider the link quality, and therefore, it is likely to select some neighbor as a MPR node, which is not suitable for packet forwarding. MPR set selection process describes as follows:

N(n): The set of node *n*'s symmetric 1-hop neighbors.
N_2(n): The set of node *n*'s symmetric 2-hop neighbors.
M(n): The set of node *n*'s 1-hop neighbors which is selected as MPR.
d(x): The count of links which one end is node *x* in N(n) and the other end is in N_2(n).

Original MPR Algorithm.

Initialize $M(s) = \phi$
FOR (y in N_2(s)) {
 IF (y has only one reachable 2-hop path from s,
 which passes node x, $x \in N(s)$) {
 $M(s) += \{x\}$; $N(s) -= \{x\}$;
 $N_2(s) -= \{$ neighbor list of x $\}$
 }
}
WHILE ($N_2(s) \neq \phi$) {
 Calculate d(x), $x \in N(s)$.
 IF ($i \in N(s)$ and $d(i) = \max\{d(x), x \in N(s)\}$) {
 $M(s) += \{x\}$; $N(s) -= \{x\}$;
 $N_2(s) -= \{$ neighbor list of x $\}$
 }
}

In addition, most proposals use authentication mechanisms for creating neighborhood trust, which is not enough to build a robust network, since a node under a wormhole attack can go through authentication by appearing as a legitimate neighbor of a node. In addition, an authenticated neighbor might perform improperly for many reasons, for example, limited physical resource, or bad conditions, or as the result of various attacks. A comprehensive neighborhood trust is needed for a robust OLSR to mitigate these problems.

2. Literature Review / Related works:

A number of secure extensions have been examined for OLSR[1-2] in order to improve its security, in which proposals such as secure OLSR [3] and An Advanced Signature System for OLSR [4] protect HELLO and TC messages with digital signature mechanisms against external attacks such as identity spoofing, routing disruption, and message tampering. The secure extension uses a symmetric cryptographic system to protect Hello and TC messages hop-by-hop against external attacks. Security aware OLSR protects the protocol with acknowledgement messages, sent by 2-hop neighbors, against link spoofing attack. Unfortunately these solutions still suffer shortcomings in terms of security, trust, robustness, and scalability. For instance, the secure extension, security enhancement mechanism [5], and advanced signature system [6] do not protect against wormhole attacks. The secure OLSR, security aware OLSR, and packet leashes[7] use time-based mechanisms to detect and prevent wormhole attacks, which requires tight time synchronization or nodes having clocks with outstanding precision, making it impractical in certain situations [8]. The secure extension also suffers scalability issues since it uses shared keys for signature which means that each node must prepare and send different messages to

different neighbors for each broadcast control message. Other research on wormhole attacks can be found in [11-15]. In addition, most proposals use authentication mechanisms for creating neighborhood trust, which is not enough to build a robust network, for that comprehensive neighborhood trust is needed for a robust OLSR to resolve these problems.

In order to provide a robust OLSR, for that potential attacks and vulnerabilities of the original OLSR protocol and analyze countermeasure points are summarize. Based on the analysis, we propose a new robust OLSR protocol (ROLSR), which can provide strong security protection against various attacks. The proposed robust OLSR protocol is based on a comprehensive neighborhood trust model (CNTM) and strong control message authentication. CNTM evaluates neighborhood trust with multiple characteristics such as authentication, link trust, and multi-point relay (MPR)[9-10] node behavior. In this model, a node chooses another node as a possible MPR neighbor, a non-MPR neighbor, or refuses it as a neighbor based on an universal trust evaluation. In CNTM, the authentication mechanism prevents unauthorized nodes from accessing the network and helps legacy nodes to establish a 1-hop broadcast key for protecting control messages against external attacks such as acquiring knowledge of the network topology and tampering with control messages. Link trust prevents invalid neighbor requests to protect against wormhole attacks, while the MPR node behavior monitor evaluates the performance of neighboring MPR node to prevent internal attacks such as link spoofing. A proposed strong control message authentication protects HELLO and TC messages from some sophisticated internal attacks.

2.1 Security Vulnerabilities of OLSR

OLSR is vulnerable to a variety of attacks which we summarize below.

2.1.1 Attacks on Control Message Generation

Identity Spoofing: A malicious node sends control messages while pretending to be another legitimate node. HELLO and TC messages with a spoofed originator address can result in conflicting routes to a node with possible loops or connectivity loss, or cause incorrect links to be advertised.

Link Spoofing: A malicious node advertises a false neighbor relationship in its HELLO or TC messages, such as a direct link with a distant node, to disrupt routing operation. By advertising non-existing links, the HELLO messages may cause inaccurate MPR selection and the resulting TC messages may contain conflicting routes and routing loops.

Message Forgery: A malicious node forges an incorrect control message that appears to originate from an authorized node with the aim of making the authorized node appear untrustworthy. With message forgery, a malicious node can also perform an identity spoofing attack.

2.1.2 Attacks on Control Message Relay

Message Tampering: A malicious node alters control messages originating from other nodes before relaying them in order to have a detrimental effect on routing operation. With message tampering, a malicious node can also perform an identity spoofing attack or a link spoofing attack.

Failure Relay: A malicious node relays TC messages improperly to cause a breakdown in network connectivity, leaving some nodes unreachable. For instance, dropping all or selected control messages. With failure relay, a malicious node can also create a sink hole, a black hole, etc.

Replay Attack: A malicious node re-sends previously valid control messages to make other nodes update their routing tables with stale routes.

Colluding Misrelay: Multiple internal malicious nodes collude together to perform a misrelay attack, such as dropping or altering control messages in order to avoid being detected by watchdog approaches.

Wormhole Attack: A pair of internal or external malicious colluding attackers record control messages at one location and relay them at another location through packet encapsulation or out-of-band channels[15-17]. The wormhole attack is one of the most sophisticated and severe attacks in MANETs. It can be launched even in a network where strong cryptographic mechanisms are preserved.

3. Analysis of Problem

3.1 Countermeasure Points

In order to build a comprehensive solution for a robust OLSR, we examine possible countermeasures for these attacks and summarize their countermeasures with the intention of considering them in our design.

3.1.1 Possible Countermeasures

Generally speaking, attacks on identity spoofing and message forgery can be prevented by identity authentication mechanisms with shared key or signature, where the signature can provide more security features such as non-repudiation. Message tampering can be prevented with message authentication and data integrity mechanisms such as a keyed hash function or signature. Replay attacks need to be prevented by combining data integrity with freshness mechanisms such as timestamps. Eavesdropping can be prevented by confidentiality mechanisms such as encryption. Unauthorized access can be avoided with authentication mechanisms such as passwords, tokens, certificates, etc. DoS attacks on control messages can be mitigated efficiently by setting up and enforcing proper control message intervals. While the above attacks can be prevented efficiently with active protection mechanisms such as authentication, integrity, confidentiality, and non-repudiation, other attacks such as link spoofing, failure relay, and colluding misrelay are difficult to prevent with only those mechanisms.

For the wormhole attack, a number of mitigation techniques have been proposed. They can be categorized as time-based, GPS-based, graph-based, watchdog based, link rating-based, antennae-based, and statistical-based. Watchdog-based and link rating-based approaches can only detect wormhole attacks after traffic is dropped and network disruption is occurring. The frequency-based wormhole attack detection approach described in was designed to be a distributed method of detecting dormant wormholes and could be considered for use in designing a robust OLSR. In the case of a compromised node, there is little research addressing a solution. The best approach appears to be monitoring behavior to look for anomalies.

3.1.2 Countermeasure Points in OLSR

In order to make OLSR attack-resilient without compromising performance, we need a comprehensive neighborhood trust model which can authenticate nodes,

protect confidentiality, detect invalid 1-hop links, and evaluate performance of MPR nodes. The trust model should mitigate attacks such as unauthorized access and wormhole attacks, and select well performing nodes as MPRs for reliability and robustness. In addition, in order to provide a confidential ad hoc network which does not allow leakage of network topology information to eavesdroppers, an efficient broadcast key management system is needed during authentication to protect all broadcast HELLO and TC messages hop-by-hop. From the attack countermeasure analysis, we see that to protect HELLO and TC messages from external attacks, a hop-by-hop encryption mechanism combining with keyed hash is sufficient and efficient. However, to deal with some sophisticated internal attacks, HELLO and TC messages needs strong security protection such as digital signature, monitoring, detection, and prevention mechanisms, which can further mitigate compromised nodes by monitoring their behavior. In addition, to make OLSR more efficient, node behavior monitoring should be focused only on MPR nodes since if all MPR nodes perform well and accurately, each node will get all valid TC messages and correct information about the entire network topology.

4. Proposed work

Robust OLSR (ROLSR) provides a comprehensive neighborhood trust model against various external attacks and strong control message authentication combining with MPR node monitoring against various internal attacks.

4.1 Comprehensive Neighborhood Trust Model:

The goal of the comprehensive neighborhood trust model (CNTM) is to establish trust among neighbor nodes and protect control messages hop-by-hop against external attacks. The trust model enables improved MANET connectivity and provides secure services for the OLSR routing protocol. This is achieved by combining the master key, 1-hop broadcast key, neighborhood authentication, invalid 1-hop link detection, and MPR node performance evaluation.

4.1.1 Key Management:

There are four different keys in the proposed CNTM model– a master key, a node certificate, a neighbor node shared key, and a 1-hop broadcast key. A node must obtain the master key and a node certificate prior to accessing the network. In the proposed system, an offline certificate authority (CA) first creates a master key for all nodes and each node stores it to its secure memory. The CA then issues a node certificate for each node, which binds the MAC address and the identity of a node to protect against MAC and identity spoofing. A certificate may contain multiple MAC addresses for a node with multiple interfaces. When it first accesses the network or detects a new neighbor, a node establishes a shared key with each neighbor node using the following confidential neighborhood authentication protocol. Each node also generates and manages a 1-hop broadcast key shared with its neighbors for control message protection. In addition, the system chooses a keyed hash function ($H_K()$) for message integrity and uses the Diffie-Hellman key agreement protocol for shared secret key establishment between two neighbor nodes.

4.1.2 Confidential Neighborhood Authentication:

Confidential neighborhood authentication could be a valuable feature for military ad hoc networks since disclosing the real identity of a node or any information of the organization may lead to targeted attacks against specific nodes of import. When a node receives an HELLO message from a new neighbor node (e.g., B), the node (e.g., A) starts the three-way handshaking authentication protocol to establish a shared secret key and exchanges its 1-hop broadcast key with node B to gain access the network.

4.1.3 Efficient 1-hop Broadcast Key Management:

The 1-hop broadcast key provides data integrity and confidentiality for control messages hop-by-hop against external attacks. As mentioned, using a shared key (e.g., [2]) for this purpose is very inefficient since HELLO and TC messages are broadcast messages in OLSR. In order to improve scalability without reducing security, we use the following efficient 1-hop broadcast key management scheme.

1. Key Generation: Each node generates a 1-hop broadcast key when it first accesses the network;

2. Key Lifetime: Each 1-hop broadcast key has a limited lifetime, which should be set much longer than HELLO message interval;

3. Key Distribution: Each node sends its current 1-hop broadcast key to its new authenticated neighbors using the above neighborhood authentication protocol, and keeps the current 1-hop broadcast key to its expiry even if some neighbors have left. Multiple interfaces of a node can share only one 1-hop broadcast key for efficiency and simplicity.

4. Key Updating: A node generates a new 1-hop broadcast key before it expires, encrypts it with its pairwise secret keys, and sends them to the corresponding neighbors.

4.1.4 Invalid 1-hop Link Detection:

The invalid 1-hop link detection is used to detect whether a neighbor node is a real neighbor or a wormhole neighbor in order to prevent wormhole attacks. As we mentioned, using GPS is the most efficient and simple way for wormhole detection but GPS technology has limitations under certain environments. Another approach is the frequency-based wormhole attack detection technology (FWAD) but there may be some delay for detecting a wormhole since it needs to collect enough samples (approximately 30) for accurate analysis. ROLSR combines the following efficient GPS-based approach with the frequency-based technology to detect and mitigate the wormhole nodes for efficiency and robustness since GPS tools have become cheaper and smaller, and widely employed in military environments.

4.1.5 Efficient MPR Node Monitoring

As mentioned, in order to protect OLSR against attacks such as link spoofing, failure relay, and colluding misrelay, we need to employ watchdog techniques to monitor node behavior. However, monitoring all nodes is costly and may be unnecessary. ROLSR monitors only MPR nodes and reports attack detection to related nodes directly using unicast. MPR node monitoring is used to evaluate routing performance of MPR nodes based on the following policy:

1. Each node monitors whether received TC messages generated by its neighbor MPR nodes include its address. Otherwise, it will delete the node from its MPR list.

2. Each node monitors whether received TC messages generated by its non-neighbor MPR nodes include its address. If so, it will report a link spoofing attack to the neighbors of the MPR node using unicast.
3. Each MPR node monitors packet forwarding behavior of its neighbor MPR nodes by counting their packet drop rate. It sends a packet drop rate report to all neighbors of the MPR node if the drop rate of the MPR node reaches a threshold and updates the drop rate when the drop rate alteration reaches another threshold.
4. Each node calculates the packet drop rate μ of a neighbor MPR node based on all reports received from the neighbor MPR nodes of the MPR node.
5. Each node calculates the universal neighborhood trust value based on the packet drop rate μ and other trust parameters for further decision making.

4.2 Strong Control Message Authentication:
In order to prevent certain sophisticated internal attacks such as identity spoofing, message tampering, and message forgery, we need to add a Signature Message TLV to each HELLO Message and TC Message for strong control message authentication instead of using the Keyed Hash Message TLV.
For strong HELLO message authentication, the generator of an HELLO message signs the whole HELLO message, adds a Signature Message TLV at the end of the HELLO message, and adjusts the HELLO message header to include the size of the Signature Message TLV in the Message Size field. Each neighbor node can authenticate the received HELLO message to prevent counterfeiting or tampering.
For strong TC message authentication, the generator of a TC message signs the whole TC message, adds a Signature Message TLV at the end of the TC message, and adjusts the TC message header to include the size of the Signature Message TLV in the Message Size field. Each node receiving the TC message can then authenticate whether the message is counterfeit or tampered. Unlike keyed hash authentication, in which neighboring nodes having the same 1-hop broadcast key as the sender of a packet can do identify spoofing, message forgery, or message tampering attacks easily, digital signature authentication can prevent these attacks by cryptographically binding the sender to the packet.

5. Application
1. Robust OLSR is proactive link state routing protocol. The proactive characteristic of the protocol provides that the protocol has all the routing information to all participated hosts in the network. However, OLSR protocol needs that each host periodic sends the updated topology information throughout the entire network, this increase the protocols bandwidth usage. But the flooding is minimised by the MPRs, which are only allowed to forward the topological messages.

2. OLSR protocol is well suited for the application which does not allow the long delays in the transmission of the data packets. The best working environment for OLSR protocol is a dense network, where the most communication is concentrated between a large number of nodes.

3. Robust OLSR protocol is use in military applications, as in military many types attack like wormhole attack, identity spoofing attack occure, to prevent confidential information from this attack robust OLSR protocol is use.

6. Conclusion
In this paper, we summarized security vulnerabilities of the original OLSR protocol and analyzed known countermeasure points for mitigating these attacks. Based on this analysis, we presented a robust OLSR protocol capable of functioning securely and efficiently within the threat model presented. This ROLSR uses a comprehensive neighborhood trust model to provide efficient and confidential ad hoc network environments for military applications. Among the advantages provided by ROLSR are the use of trust monitoring to mitigate internal attacks, the securing of control messages to prevent topology information leakage, confidential neighborhood authentication to protect anonymity and prevent leakage of command hierarchy, and control message authentication to defend various routing attacks.

References:

[1] T. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, October, 2003.
[2] Ronggong Song and Peter C. Mason, ROLSR: A Robust Optimized Link State Routing Protocol for Military Ad-Hoc Networks,IEEE Conference-Networking protocols and performance Track, 2010.
[3] A. Hafslund, A. Tonnesen, R. Bjorgum, J. Andersson, and O. Kure, Secure Extension to the OLSR Protocol, in Proceedings of the 2004 OLSR Interop and Workshop, San Diego, USA, August 6-7, 2004.
[4] F. Hong, L. Hong, and C. Fu, Secure OLSR, in Proceedings of the 19th IEEE International Conference on Advanced Information Networking and Applications, Taipei, Taiwan, March 28-30, 2005.
[5] B. Kannhavong, H. Nakayama, and A. Jamalipour, SA-OLSR: Security Aware Optimized Link State Routing for Mobile Ad Hoc Networks, in Proceedings of the 2008 IEEE International Conference on Communications, Beijing, China, May 19-23, 2008.
[6] D. Stinson, Cryptography - Theory and Practice, CRC Press, Inc. 2002.
[7] E. Cayirci and C. Rong, Security in Wireless Ad Hoc and Sensor Networks, United Kingdom: A John Wiley & Sons, Ltd, 2009.
[8] I. Doh, K. Chae, H. Kim, and K. Chung, Security Enhancement Mechanism for Ad-Hoc OLSR Protocol, in Proceedings of the 2006 International Conference on Information Networking, LNCS 3961, Sendai, Japan, January 16-19, 2006.

[9] D. Raffo, C, Adjih, T. Clausen, and P. Muhlethaler, An Advanced Signature System for OLSR, in Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks, Washington DC, USA, October 25, 2004.

[10] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, Analysis of the Node Isolation Attack against OLSR-based Mobile Ad Hoc Network, in Proceedings of the IEEE 7th International Symposium on Computer Networks, Istanbul, Turkey, June, 2006.

[11] D. Dhillon, J. Zhu, J. Richards, and T. Randhawa, Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs, in Proceedings of the 2006 International Wireless Communications and Mobile Computing Conference, Vancouver, Canada, July 3-6, 2006.

[12] R. Poovendran and L. Lazos, A Graph Theoretic Framework for Preventing the Wormhole Attack in Wireless Ad Hoc Networks, Journal of Wireless Networks, vol.13, no.1, pp.27-59, February, 2007.

[13] Y. C. Hu, A. Perrig, and D. Johnson, Packet Leashes: a Defense against Wormhole Attacks in Wireless Networks, in Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies, San Francisco, USA, March 30-April 3, 2003.

[14] I. Khalil, S. Bagchi, and N. B. Shroff, LiteWorp: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks, in Proceedings of the 2005 IEEE International Conference on Dependable Systems and Networks, Yokohama, Japan, June 28-July 1, 2005.

[15] R. Maheshwari, J. Gao, and S. R. Das, Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information, in Proceedings of the 26th IEEE International Conference on Computer Communications, Alaska, USA, May 6-12, 2007.

[16] D. Lynch, S. Knight, M. A. Gorlatova, L. Lamont, R. Liscano, and P. C. Mason, Providing Effective Security in Mobile Ad Hoc Networks without Affecting bandwidth or Interoperability, in Proceedings of the 26th Army Science Conference, Orlando, USA, December 1-4, 2008.

[17] W. Wang, B. Bhargava, Y. Lu, and X. Wu, Defending against Wormhole Attacks in Mobile Ad Hoc Networks, Journal of Wireless Communication and Mobile Computing, vol.6, no.4, pp.483-503, June, 2006.