WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Survey of Routing Attacks in Mobile Ad-Hoc Networks

Shashi Ranjan Kumar[1], Dr. Narendra Sharma[2], Dr. Harsh lohiya[3]

[1]Research Scholar, Department of CSE, SSSUTMS, Sehore, Madhya Pradesh, India,
[2]Assistant professor, Department of CSE, SSSUTMS, Sehore, Madhya Pradesh, India
[3]Assistant professor, Department of CSE, SSSUTMS, Sehore, Madhya Pradesh, India

ABSTRACT

Last few years, mobile ad hoc networks have become a hot research topic for researchers due to their simplicity and independence from network connections such as mobile station base. Routing in MANETs is a particularly difficult task compared to traditional networks due to the unique features of dynamic network topologies, limited bandwidth and limited battery life. Early work in MANET research focused on the design of efficient routing protocols in highly dynamic and capacity constrained networks. Various effective methods have now been proposed for MANETs. Most of these processes assume an environment of trust and cooperation. However, in the presence of malicious nodes, the network is vulnerable to various attacks. Attacks are especially common with MANETs. In this article, we explore recent security issues in MANETs. In particular, we examine attacks such as link spoofing and collusion misrelay attacks and prevent these attacks in MANET protocols.

Keywords: Spoofing, Blackhole, Wormhole, MANET, OLSR.

1. Introduction

A mobile ad hoc network (MANET) is a collection of mobile devices that can communicate with each other without the use of a predefined infrastructure or centralized administration. In addition to freedom of mobility, a MANET can be constructed quickly at a low cost, as it does not rely on existing network infrastructure. Due to this flexibility, a MANET is attractive for applications such as disaster relief, emergency operations, military service, maritime communications, vehicle networks, casual meetings, campus networks, robot networks, and so on.

Unlike the conventional network, a MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes [1]. This feature makes it difficult to perform routing in a MANET compared with a conventional wired network.

Another characteristic of a MANET is its resource constraints, that is, limited bandwidth and limited battery power. This characteristic makes routing in a MANET an even more challenging task. Therefore, early work in MANET research focused on providing routing service with minimum cost in terms of bandwidth and battery power.

Currently, several efficient routing protocols have been proposed. These protocols can be classified into two categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol [2], nodes find routes only when required. In proactive routing protocols, such as the Optimized Link State Routing (OLSR) protocol [3], nodes obtain routes by periodic exchange of topology information.

Most of these routing protocols rely on cooperation between nodes due to the lack of a centralized administration and assume that all nodes are trustworthy and well-behaved. However, in a hostile environment, a malicious node can launch routing attacks to disrupt routing operations or denial-of-service (DoS) attacks [4] to deny services to legitimate nodes.

Recently, several research efforts were launched to counter against these malicious attacks. Most of the previous work focused mainly on providing preventive schemes to protect the routing protocol in a MANET. Most of these schemes are based on key management or encryption techniques to prevent unauthorized nodes from joining the network. In general, the main drawback of these approaches is that they introduce a heavy traffic load to exchange and verify keys, which is very expensive in terms of the bandwidth-constraint for MANET nodes with limited battery and limited computational capabilities. In [5], Hu et al. discuss these preventive schemes (e.g., authenticated routing for ad hoc net- works (ARAN) [6], Ariadne [7], secure AODV (SAODV) [8]) in detail. Therefore, we will not discuss these approaches further in this article.

In [9], the authors survey attacks and their countermeasures in mobile ad hoc network for five layers: application, transport, network, data link, and physical. For attacks against the network layer, the authors survey countermeasures for impersonation attacks, modification attacks, wormhole attacks, and blackhole attacks. How- ever, new attacks and countermeasures against a network layer attack, such as link spoofing and withholding of routing traffic have not been discussed in the literature.

In this article, we survey the current state of the art of attacks on the network layer, that is, routing attacks such as link spoofing, wormhole attacks, and colluding misrelay attacks, as well as countermeasures in a MANET. Then, we provide an overview of countermeasures for each attack.

The rest of this article is organized as follows. We provide an overview of routing protocols in a MANET. We survey routing attacks against MANETs. We provide a brief overview of countermeasures against routing attacks. Then we summarize the article.

2. Routing protocols in a MANET

The goal of routing in a MANET is to discover the most recent topology of a continuously changing network to find a correct route to a specific node. Routing protocols in a MANET can be classified into two categories: reactive routing protocols (e.g., AODV) and proactive routing protocols (e.g., OLSR). In reactive routing protocols, nodes find routes only when they must send data to the destination node whose route is unknown. On the other hand, in proactive protocols, nodes periodically exchange topology information, and hence nodes can obtain route information any time they must send data. In this section, we describe two standard routing protocols that currently are being researched actively, that is, AODV and OLSR.

AODV [2] is a reactive routing protocol designed for a mobile ad hoc network. In AODV, when a source node S wants to send a data packet to a destination node D and does not have a route to D, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. The immediate neighbors who receive this RREQ rebroadcast the same RREQ to their neighbors. This process is repeated until the RREQ reaches the destination node.

Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. The same RREQ that arrives later will be ignored by the destination node.

In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node.

2.1 OLSR protocol

OLSR [3] is a proactive routing protocol, that is, it is based on periodic exchange of topology information. The key concept of OLSR is the use of multipoint relay (MPR) to provide an efficient flooding mechanism by reducing the number of transmissions required. In OLSR, each node selects its own MPR from its neighbors. Each MPR node maintains the list of nodes that were selected as an MPR; this list is called an MPR selector list. Only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs.

Routing Message in OLSR —Generally, in the OLSR protocol, two types of routing messages are used, namely, a HELLO message and a topology control (TC) message.

A HELLO message is the message that is used for neighbor sensing and MPR selection. In OLSR, each node generates a HELLO message periodically. A node's HELLO message contains its own address and the list of its one-hop neighbors. By exchanging HELLO messages, each node can learn a complete topology up to two hops. HELLO messages are exchanged locally by neighbor nodes and are not forwarded further to other nodes.

A TC message is the message that is used for route calculation. In OLSR, each MPR node advertises TC messages periodically. A TC message contains the list of the sender's MPR selector. In OLSR, only MPR nodes are responsible for forwarding TC messages. Upon receiving TC messages from all of the MPR nodes, each node can learn the partial network topology and can build a route to every node in the network.

MPR Selection — For MPR selection, each node selects a set of its MPR nodes that can forward its routing messages. In OLSR, a node selects its MPR set that can reach all its two-hop neighbors. In case there are multiple choices, the minimum set is selected as an MPR set that can reach all its two-hop neighbors. In case there are multiple choices, the minimum set is selected as an MPR set.

3. Routing attacks against MANET protocols flooding attack

The aim of the flooding attack [11] is to exhaust the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the rout- ing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a desti- nation node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service. In [12], the authors show that a flooding attack can decrease throughput by 84 percent.

3.1 Blackhole attack

In a blackhole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a suffi ciently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic.

Figure 1 shows an example of a blackhole attack, where attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A.

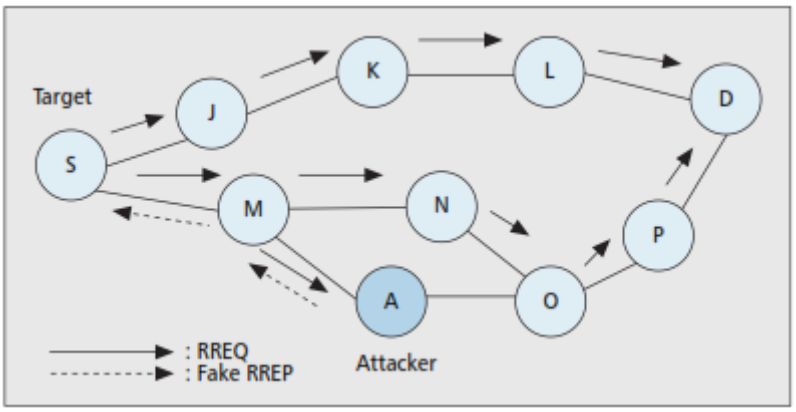

Figure1. Example of a blackhole attack on AODV.

3.2 Link withholding attack

In this attack, a malicious node ignores the requirement to advertise the link of specific nodes or a group of nodes, which can result in link loss to these nodes. This type of attack is particularly serious in the OLSR protocol.

3.3. Link spoofing attack

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks.

Figure 2 shows an example of the link spoofing attack in an OLSR MANET. In the figure, we assume that node A is the attacking node, and node T is the target to be attacked. Before the attack, both nodes A and B are MPRs for node T. During the link spoofing attack, node A advertises a fake link with node T's two-hop neighbour, that is, node D. According to the OLSR protocol, node T will select the malicious node A as its only MPR since node A is the minimum set that reaches node T's two-hop neighbours. By being node T's only MPR, node A can then drop or withhold the routing traffic generated by node T.

3.4 Replay attack

In a MANET, topology frequently changes due to node mobility. This means that current network topology might not exist in the future. In a replay attack [20], a node records another node's valid control messages and resends them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation in a MANET.

3.5 Wormhole attack

A wormhole attack [21] is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed net- work. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality.

Figure 3 shows an example of the wormhole attack against a reactive routing protocol. In the figure, we assume that nodes A1 and A2 are two colluding attackers and that node S is the target to be attacked. During the attack, when source node S broadcasts an RREQ to find a route to a destination node D, its neighbors J and K for- ward the RREQ as usual. However, node A1, which received the RREQ forwarded by node J, records and tunnels the RREQ to its colluding partner A 2 . Then, node A 2 rebroadcasts this RREQ to its neighbor P. Since this RREQ passed through a high-speed channel, this RREQ will reach node D first. Therefore, node D will choose route D-P-J-S to unicast an RREP to the source node S and ignore the same RREQ that arrived later. As a result, S will select route S-J- P-D that indeed passed through *A*1 and *A*2 to send its data.

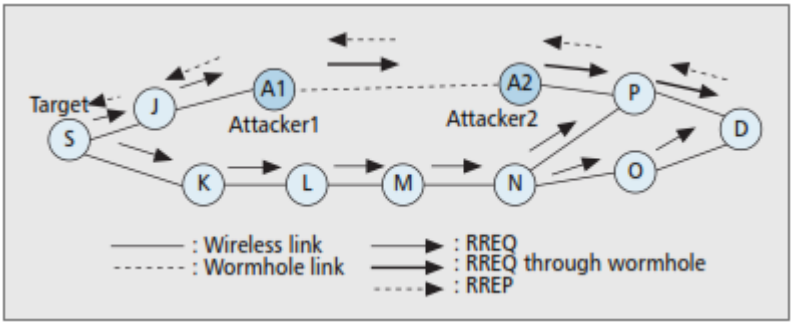

Figure 3. Example of a wormhole attack on reactive routing

3.6 Colluding misrelay attack

In this attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as watchdog and pathrater [10]. Figure 4 shows an example of this attack. Consider the case where node A1 forwards routing packets for node T. In the figure, the first attacker A1 forwards routing packets as usual to avoid being detected by node T. However, the second attacker A2 drops or modifies these routing packets. In [19] the authors discuss this type of attack in OLSR protocol and show that a pair of malicious nodes can disrupt up to 100 percent of data packets in the OLSR MANET.

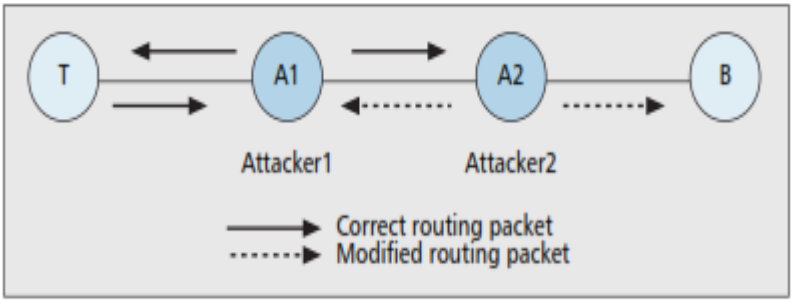

Figure 4. Example of a colluding misrelay attack

4. Countermeasures against attacks in a MANET

In this section, we discuss solutions that are proposed to counter against routing attacks described in the previous section.

4.1 Solutions to the flooding attack

In [11], the authors proposed a simple mechanism to prevent the flooding attack in the AODV protocol. In this approach, each node monitors and calculates the rate of its neighbors' RREQ. If the RREQ rate of any neighbor exceeds the predefined threshold, the node records the ID of this neighbor in a blacklist. Then, the node drops any future RREQs from nodes that are listed in the blacklist. One limitation of this approach is that it cannot prevent against the flooding attack in which the flooding rate is below the threshold. Another drawback of this approach is that if a malicious node impersonates the ID of a legitimate node and broadcasts a large number of RREQs, other nodes might put the ID of this legitimate node on the black- list by mistake.

In [12], the authors proposed an adaptive technique to mitigate the effect of a flooding attack in the AODV protocol. This technique is based on statistical analysis to detect malicious RREQ floods and avoid the forwarding of such packets. Similar to [11], in this approach, each node monitors the RREQ it receives and maintains a count of RREQs received from each sender during the present time period. The RREQs from a sender whose RREQ rate is above the threshold will be dropped without forwarding. Unlike the method proposed in [11], where the threshold is set to be fixed this approach determines the threshold based on a statistical analysis of RREQs. The key advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.

4.2 Solutions to the blackhole attack

In [13], the authors introduce the route confirmation request (CREQ) and route confirmation reply (CREP) to avoid the blackhole attack. In this approach, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has the route, it sends the CREP to the source. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges that the route is correct.

One drawback of this approach is that it can- not avoid the blackhole attack in which two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker send- ing CREPs that support the incorrect path.

In [14], the authors proposed a solution that requires a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node judges that the route is safe. The main drawback of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive.

In [15], the authors analyzed the blackhole attack and showed that a malicious node must increase the destination sequence number sufficiently to convince the source node that the route provided is sufficiently enough. Based on this analysis, the authors propose a statistical- based anomaly detection approach to detect the blackhole attack, based on differences between the destination sequence numbers of the received RREPs.

The key advantage of this approach is that it can detect the attack at low cost without introducing extra routing traffic, and it does not require modification of the existing protocol. However, false positives are the main drawback of this approach due to the nature of anomaly detection below the threshold.

4.3 Solutions to the message withholding attack

In [16], the authors show that by withholding a TC message in OLSR, a malicious node can isolate a specific node and prevent it from receiving data packets from other nodes. After analyzing and evaluating the impact of this kind of attack in detail, the authors proposed a detection technique based on observation of both a TC message and a HELLO message generated by the MPR nodes. If a node does not hear a TC message from its MPR node regularly but hears only a HELLO message, a node judges that the MPR node is suspicious and can avoid the attack by selecting one or more extra MPR nodes.

Similarly, in [17], the authors proposed an intrusion detection system to detect TC link and message withholding in the OLSR protocol. In this approach, each node observes whether an MPR node generates a TC message regularly or not. In case an MPR node generates a TC message regularly, the node checks whether or not the TC message actually contains itself to detect the attack.

The main drawback of these approaches are that they cannot detect the attack that is launched by two colluding consecutive nodes, where the first attacker pretends to advertise a TC message, but the second attacker drops this TC message.

4.4 Solutions to the link spoofing attack

To detect a link spoofing attack, the author of [18] proposed a location information-based detection method by using cryptography with a GPS and a time stamp. This approach requires each node to advertise its position obtained by the GPS and the time stamp to enable each node to obtain the location information of the other nodes. This approach detects the link spoofing by calculating the distance between two nodes that claim to be neighbors and checking the likelihood that the link is based on a maxi- mum transmission range.

The main drawback of this approach is that it might not work in a situation where all MANET nodes are not equipped with a GPS. Further- more, attackers can still advertise false information and make it hard for other nodes to detect the attack.

In [19], the authors show that a malicious node that advertises fake links with a target's two-hop neighbors can successfully make the target choose it as the only MPR. Through simulations, the authors show that link spoofing can have a devastating impact on the target node. Then, the authors present a technique to detect the link spoofing attack by adding two-hop information to a HELLO message. In particular, the proposed solution requires each node to advertise its two-hop neighbors to enable each node to learn complete topology up to three hops and detect the inconsistency when the link spoofing attack is launched.

The main advantage of this approach is that it can detect the link spoofing attack without using special hardware such as a GPS or requiring time synchronization. One limitation of this approach is that it might not detect link spoofing with nodes further away than three hops.

4.5 Solutions to the replay attack

In [20], the authors proposed a solution to pro- tect a MANET from a replay attack by using a time stamp with the use of an asymmetric key. This solution prevents the replay attack by com- paring the current time and time stamp contained in the received message. If the time stamp is too far from the current time, the message is judged to be suspicious and is rejected.

Although this solution works well against the replay attack, it is still vulnerable to a wormhole attack where two colluding attackers use a high- speed network to replay messages in a far-away location with almost no delay. This attack will be discussed in the next subsection.

4.5 Solutions to the wormhole attack

In [21], packet leashes are proposed to detect and defend against the wormhole attack. In particular, the authors proposed two types of leash- es: temporal leashes and geographical leashes. For the temporal leash approach, each node computes the packet expiration time, te, based on the speed of light c and includes the expiration time, te, in its packet to prevent the packet from traveling further than a specific distance, L. The receiver of the packet checks whether or not the packet expires by comparing its current time and the te in the packet. The authors also proposed TIK, which is used to

authenticate the expiration time that can otherwise be modified by the malicious node. The main drawback of the temporal leash is that it requires all nodes to have tightly synchronized clocks. For the geographical leash, each node must know its own position and have loosely synchronized clocks. In this approach, a sender of a packet includes its current position and the sending time. There- fore, a receiver can judge neighbor relations by computing distance between itself and the sender of the packet. The advantage of geographic leashes over temporal leashes is that the time synchronization need not to be highly tight.

In [18], the authors offer protection against a wormhole attack in the OLSR protocol. This approach is based on location information and requires the deployment of a public key infra- structure and a time-stamp synchronization between all nodes that is similar to the geographic leashes proposed in [21]. In this approach, a sender of a HELLO message includes its current position and current time in its HELLO message. Upon receiving a HELLO message from a neighbor, a node calculates the distance between itself and its neighbor, based on a position provided in the HELLO message. If the distance is more than the maximum trans- mission range, the node judges that the HELLO message is highly suspicious and might be tunnelled by a wormhole attack.

In [22], the authors propose a statistical analysis of multipath (SAM), which is an approach to detect the wormhole attack by using multi- path routing. This approach determines the attack by calculating the relative frequency of each link that appears in all of the obtained routes from one route discovery. In this solution, a link that has the highest relative frequency is identified as the wormhole link.

The advantage of this approach is that it introduces limited overhead when applied in multipath routing. However, it might not work in a non-multipath routing protocol, such as a pure AODV protocol.

4.6 Solutions to a colluding misrelay attack

A conventional acknowledgment-based approach might detect this type of attack in a MANET, especially in a proactive MANET, but because routing packets destined to all nodes in the net- work require all nodes to return an ACK, this could lead to a large overhead, which is considered to be inefficient.

In [23], the author proposes a method to detect an attack in which multiple malicious nodes attempt to drop packets by requiring each node to tune their transmission power when they forward packets. As an example, the author studies the case where two colluding attackers drop packets. The proposed solution requires each node to increase its transmission power twice to detect such an attack. However, this approach might not detect the attack in which three colluding attackers work in collusion. In general, the main drawback of this approach is that even if we require each node to increase transmission power to be K times, we still cannot detect the attack in which K + 1 attackers work in collusion to drop packets. Therefore, further work must be done to counter against this type of attack efficiently.

5. Future work

Future research should focus not only on improving the effectiveness of security schemes, but also on minimizing the cost of making them suitable for the MANET environment. Furthermore, any proposed solution only works for specific attacks and is still vulnerable to unexpected attacks. Therefore, MANET researchers should also focus on researching MANETs to make them secure and reliable networks and prevent all possible attacks.

REFERENCES

[1] S. Ci et al., “Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks,” IEEE Trans. Vehic. Tech., vol. 55, no. 4, July 2006 pp. 1302–10.

[2] C. Perkins, E. Belding-Royer, and S. Das, “Ad Hoc On- demand Distance Vector (AODV) Routing,” IETF RFC 3561, July 2003.

[3] Th. Clausen et al., “Optimized Link State Routing Proto- col,” IETF Internet draft, draft-ietf-manet-olsr-11.txt, July 2003.

[4] A. Shevtekar, K. Anantharam, and N. Ansari, “Low Rate TCP Denial-of-Service Attack Detection at Edge Routers,” IEEE Commun. Lett vol. 9, no. 4, Apr. 2005, pp. 363–65.

[5] Y-C Hu and A. Perrig, “A Survey of Secure Wireless Ad Hoc Routing,” IEEE Sec. and Privacy, May–June 2004.

[6] K. Sanzgiri et al., “A Secure Routing Protocol for Ad Hoc Networks,” Proc. 2002 IEEE Int’l. Conf. Network Protocols, Nov. 2002.

[7] Y-C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,” Proc. MobiCom ’02, Atlanta, GA, Sept. 23–28, 2002.

[8] M. G. Zapata and N. Asokan, “Securing Ad-Hoc Routing Protocols,” Proc. 2002 ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

[9] B. Wu et al., “A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,” Wireless/Mobile Network Security, Springer, vol. 17, 2006.

[10] S. Marti et al., “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” 6th MobiCom, Boston, MA, Aug. 2000.

[11] P. Yi et al., “A New Routing Attack in Mobile Ad Hoc Networks,” Int’l. J. Info. Tech., vol. 11, no. 2, 2005.

[12] S. Desilva, and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[13] S. Lee, B. Han, and M. Shin, "Robust Routing in Wire- less Ad Hoc Networks," 2002 Int'l. Conf. Parallel Pro- cessing Wksps., Vancouver, Canada, Aug. 18–21, 2002.

[14] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conf. 2004.

[15] S. Kurosawa et al., "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," Proc. Int'l. J. Network Sec., 2006.

[16] B. Kannhavong et al., "Analysis of the Node Isolation Attack against OLSR-Based Mobile Ad Hoc Network," 7th Int'l. Symp. Comp. Networks, 2006.

[17] D. Dhillon et al., "Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs," Proc. Int'l. Conf. Commun. and Mobile Comp., 2006.

[18] D. Raffo et al., "Securing OLSR Using Node Locations," Proc. 2005 Euro. Wireless, Nicosia, Cyprus, Apr. 10–13, 2005.

[19] B. Kannhavong et al., "A Collusion Attack Against OLSR-Based Mobile Ad Hoc Networks," IEEE GLOBE- COM '06.

[20] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks Against OLSR: Distributed Key Management for Security," 2nd OLSR Interop/Wksp., Palaiseau, France, July 28–29, 2005.

[21] Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[22] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multi-path," IEEE Wire- less Commun. and Networking Conf. '05.

[23] Z. Karakehayov, "Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks," Wksp. Real-World Wireless Sensor Networks, June 20–21,2005.