A Study on Certificate Revocation in Mobile Ad Hoc Networks

Citation:

Wei Liu, Hiroki Nishiyama, Nirwan Ansari, and Nei Kato, "A Study on Certificate Revocation in Mobile Ad Hoc Networks," IEEE International Conference on Communications (ICC 2011), Kyoto, Japan, Jun. 2011.

URL:

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5962925

A Study on Certificate Revocation in Mobile Ad Hoc Networks

Wei Liu
Tohoku University
Sendai, Japan
liuwei@it.ecei.tohoku.ac.jp

Hiroki Nishiyama
Tohoku University
Sendai, Japan
bigtree@it.ecei.tohoku.ac.jp

Nirwan Ansari
New Jersey Institute of Technology
New Jersey, USA
nirwan.ansari@njit.edu

Nei Kato
Tohoku University
Sendai, Japan
kato@it.ecei.tohoku.ac.jp

***Abstract*—Certificate revocation is an important security component in mobile ad hoc networks (MANETs). Owing to their wireless and dynamic nature, MANETs are vulnerable to security attacks from malicious nodes. Certificate revocation mechanisms play an important role in securing a network. When the certificate of a malicious node is revoked, it is denied from all activities and isolated from the network. The main challenge for certificate revocation is to revoke the certificates of malicious nodes promptly and accurately. In this paper, we build upon our previously proposed scheme, a clustering-based certificate revocation scheme, which outperforms other techniques in terms of being able to quickly revoke attackers' certificates and recover falsely accused certificates. However, owing to a limitation in the scheme's certificate accusation and recovery mechanism, the number of nodes capable of accusing malicious nodes decreases over time. This can eventually lead to the case where malicious nodes can no longer be revoked in a timely manner. To solve this problem, we propose a new method to enhance the effectiveness and efficiency of the scheme by employing a threshold based approach to restore a node's accusation ability and to ensure sufficient normal nodes to accuse malicious nodes in MANETs. Extensive simulations show that the new method can effectively improve the performance of certificate revocation.**

Keywords-mobile ad hoc networks; certificate revocation; recovery; clustering;

I. INTRODUCTION

With the increased focus on wireless communications, mobile ad hoc networks (MANETs) are attracting much attention in recent years. MANET is an infrastructureless mobile network formed by a number of self-organized mobile nodes; it is different from traditional networks that require fixed infrastructure. Owing to the absence of infrastructure support, nodes in MANET must be equipped with all aspects of networking functionalities, such as routing and relaying packets, in addition to playing the role of end users.

In MANET, nodes are free to join and leave the network at any time in addition to being independently mobile. Consequently, a mobile ad hoc network is vulnerable to many kinds of malicious attacks, and it is thus difficult to ensure secure communications [1]. Malicious nodes directly threaten the robustness of the network as well as the availability of nodes. Protecting legitimate nodes from malicious attacks must be considered in MANETs. This is achievable through the use of a key management scheme which serves as a means of conveying trust in a public key infrastructure. These certificates are signed by the Certificate Authority (CA) of the network, which is a trusted third party that is responsible for issuing and revoking certificates.

The mechanism performed by the CA [2]-[5] plays an important role in enhancing network security. It digitally signs a valid certificate for each node to ensure that nodes can communicate with each other in the network. In such networks, a certificate revocation scheme which invalidates attackers' certificates is essential in keeping the network secured. An attacker's certificate can be successfully revoked by the CA if there are enough accusations showing that it is an attacker. However, it is difficult for the CA to determine if an accusation is trustable because malicious nodes can potentially make false accusations. A malicious node will try to remove legitimate nodes from the network by falsely accusing them as attackers. Therefore, the issue of false accusation must be taken into account in designing certificate revocation mechanisms. Our previous scheme [6], which is based on a clustering approach, outperforms other techniques in terms of being able to quickly revoke certificates of accused nodes and also to explicitly distinguish false accusations. However, it has a shortcoming in that its performance degrades as the number of detected attackers increases. To tackle this issue, in this paper, we propose an enhancement to our original scheme.

The remainder of this paper is organized as follows. In Section II, we survey the related work in certificate revocation techniques for MANETs. Section III presents the advanced aspects of our previous clustering-based certificate revocation scheme. In Section IV, we point out the drawback of the previous scheme and propose a solution to fix the issue. Section V demonstrates the effectiveness of our proposed technique via extensive simulation results. Finally, Section VI concludes this paper.

II. RELATED WORK

Several different types of certificate revocation techniques have been developed for mobile ad hoc networks. The most popular method is a simple certificate control approach by using a Certificate Revocation List (CRL) [7] which is managed by a single CA or shared among multiple CAs. A digital certificate which is valid for a certain time period is assigned to each node by the CA. The CA revokes the certificates of suspicious nodes and adds them to the CRL.

Nodes can be accused by any node with a valid certificate and the updated CRL is broadcasted throughout the entire network.

URSA proposed by H. Luo *et al*. [8] uses certified tickets which are locally managed in the network to evict nodes. URSA does not use a third-party trust system such as a CA. The tickets of the newly joining nodes are issued by their neighbors. Since there is no centralized authority, the ticket of a malicious node is revoked by the vote of its neighbors. In URSA, each node performs one-hop monitoring, and exchanges monitoring information with its neighbors which allow for malicious nodes to be identified. When the number of votes exceeds a certain threshold, the ticket of the accused node will be successfully revoked. Since nodes cannot communicate with other nodes without valid tickets, revoking a node's ticket implies the isolation of that node. Although URSA is robust for false accusation attacks, there is still a remaining issue in coping with collusion attacks by multiple malicious attackers.

The scheme proposed by G. Arboit *et al.* [9], referred to as the voting-based scheme, allows all nodes in the network to vote. As with URSA, no CA exists in the network, and instead each node monitors the behavior of its neighbors. The primary difference from URSA is that nodes vote with variable weight. The weight is calculated from a node's reliability which is derived from its past behavior. The higher its reliability is, the greater its weight will be. The certificate of a suspicious node can be revoked when the sum of the weights of the votes against the node reaches or exceeds a predefined threshold. By doing so, the accuracy of certificate revocation can be improved. However, since all nodes are required to participate during every vote, the communication overhead required to exchange voting information is quite high, thus increasing the time needed to revoke the certificate.

J. Clulow *et al.* [10] proposed the decentralized suicide-based approach. In this approach, while the certificate revocation can be quickly completed with just an accusation, not only the certificate of the accused node but also accuser's certificate is revoked. In other words, at least one node has to sacrifice itself to remove an attacker from the network. This strategy dramatically reduces both the time required to evict a node and the communication overhead of the certificate revocation procedures. However, owing to its suicide-based strategy, the application of this approach is limited. Also, the scheme does not provide a mechanism to differentiate falsely accused legitimate nodes from properly accused malicious nodes.

III. CLUSTERING-BASED CERTIFICATE REVOCATION SCHEME

In this section, we briefly describe our clustering-based certificate revocation scheme which was originally proposed in [6]. Although a centralized CA manages certificates for all the nodes in the network, cluster construction is decentralized and performed autonomously. Nodes cooperate to form clusters and each cluster consists of a Cluster Head (CH) along with several Cluster Members (CMs) that are located within the communication range of their CH. Each CM belongs to two different clusters in order to provide robustness against changes in topology due to mobility. It should be noted that because the clusters overlap, a node within the communication range of a CH is not necessary part of its cluster. Clustering information is never used for routing; it is only used for managing certificates in the certification system. This provides a clear advantage as it enables the scheme to be used along with any type of routing technology.

The aim of using clusters is to enable CHs to detect false accusations. Requests for the CA to recover the certificates of falsely accused nodes can only be made from CHs. A CH will send a Certificate Recovery Packet (CRP) to the CA to recover an accused node, only in the case where it is a CM in its cluster. This is based on the fact that most types of attacks, such as flooding attack [11], black hole attack [12], wormhole attack [13] and sybil attack [14], can be detected by any node within the communication range of the attacker. In other words, a CH will be able to detect any attack executed by one of its CMs, implying that a CH can identify whether a CM is malicious or not. Since the CA regularly broadcasts certificate information on nodes which have been accused as malicious nodes, CHs will be able to detect false accusations against their CMs by comparing this information with their own local observations.

In order for clustering-based certificate revocation to work, CHs must be legitimate. Nodes can be classified into three different categories, normal nodes which are highly trusted, warned nodes with questionable trust, and attacker nodes which cannot be trusted. Only normal nodes are allowed to become CHs and accuse attackers by sending Attack Detection Packets (ADPs) to the CA. Nodes in the Warning List (WL) cannot become CHs or accuse attackers, but they can still join the network as CMs and communicate without any restrictions. Nodes classified as attackers are considered malicious and completely cut off from the network. The reliability of each node is determined by the CA as follows.

The CA maintains both a Black List (BL) and a Warning List. When the CA receives an ADP from an accuser, the accused node is regarded as an attacker and is immediately registered in the BL. The BL includes nodes which are classified as attackers and have had their certificates revoked. The accuser of the attacker is then listed in the WL because the accuser might actually be making a false accusation. However, falsely accused nodes will be restored quickly by their CHs. We consider false accusation and false recovery as an act of misbehavior, and define nodes that do such act as misbehaving nodes. This is in contrast to more serious behavior such as conducting active attacks. When the CA receives a CRP sent by a CH to request a node to be recovered from the BL, the recovered node is removed from the BL and registered in the WL. At the same time, the CH which sent this packet is also placed in the WL. Since this will cause the CH to lose its credentials, the cluster topology will need to be reconstructed.

This conservative strategy is designed to cope with collusion attacks where a CH works to falsely recover other malicious nodes listed in the BL. Since all nodes are initially classified as normal nodes upon joining the network, nodes with malevolent intentions also have a chance to become CHs and run false recovery. However, by adopting this conservative strategy, we can minimize the damage caused by collusion

attacks. It should be noted that when the CA receives multiple ADPs or CRPs against the same target, the CA follows the procedure mentioned above when the first packet arrives.

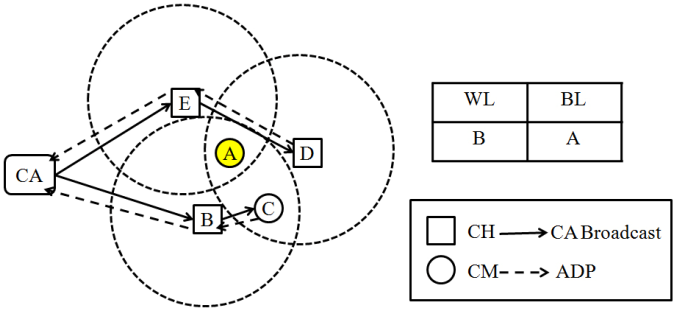

Figure 1. The procedure of certificate revocation

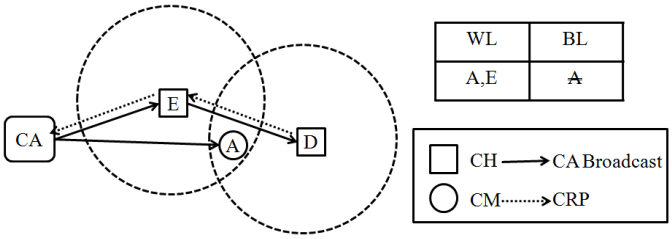

Figure 2. The procedure of certificate recovery

Fig. 1 and Fig. 2 show examples of certificate revocation and recovery procedures. As shown in Fig. 1, node A is a malicious node and launches attacks on its neighbors, i.e., nodes B, C, D and E. Its neighbors detect the attacks and send ADPs to the CA to accuse node A. Upon receiving the first ADP from node B, the CA puts it into the WL as an accuser and node A into the BL as an attacker. It then broadcasts the information contained in the WL and BL to the entire network. Fig. 2 shows the procedure of certificate recovery. When node E and D, which are the CHs of node A, are informed that node A is listed in the BL, if they have never detected any attacks coming from A, they will recognize this accusation as a false one. They will then send a CRP to the CA to recover node A's certificate. Upon receiving the first arrival CRP from node E, the CA removes the falsely accused node A from the BL, and enlists it into the WL along with node E. After the broadcast of the updated WL and BL, the certificate of node A will be recovered successfully.

Our clustering-based certificate revocation scheme provides the following advantages. The first benefit is quick revocation. As compared with the voting-based approaches in [8] [9], our scheme can immediately revoke the certificates of attackers once the first attack is detected because only one ADP is enough for the CA to decide that a node is an attacker. The second advantage is that the scheme incurs a small overhead. In contrast to other methods which require a large amount of messages to be exchanged in order to revoke a certificate, the communication overhead is limited to control traffic. Finally, our scheme resolves the problem of false accusations. By allowing only highly reliable nodes to contribute to the certification process, the chances of false accusations can be lowered and falsely accused nodes can be recovered quickly. It should be pointed out that the scheme also attempts to reduce the damage of collusion attacks by adopting a conservative strategy.

IV. Issues and Solutions

In this section, we examine the shortcomings in our previously proposed scheme, and propose a new method to enhance its effectiveness and efficiency.

A. Issues

Using our proposed scheme can effectively reduce the revocation time and communication overhead. However, there exists an issue which affects the performance of the scheme. The revocation and recovery operations described in Section III incur an increasing number of nodes to be held in the WL, thus leading to the reduction of the number of normal nodes over time.

Intuitively, if there are plenty of normal nodes around the malicious nodes, the scheme will be highly efficient in revoking malicious nodes' certificates as quickly as possible. In other words, the efficiency degrades when there are not enough normal nodes in the network. In this case, the attacker will not be detected until a normal node roams into the attacker's transmission range which may take a long time to occur.

In MANETs, we can associate a mobile node in a specified area with a probability. That is, we can use a binomial distribution $B(n, p)$ to represent the probability distribution that expresses the probability of a number of mobile nodes existing in a specified network area. (The network is divided into a large number of small cells, which are either empty or occupied by a single mobile node [15].) The binomial $B(n, p)$ is satisfied by the Possion Distribution, where n, the total number of cells in the network is very large, and p, the probability that a cell is occupied by a single node is very small.

Therefore, the probability that there are exactly k normal nodes (k being a non-negative integer, k = 0, 1, 2 ...) in a specific area in MANETs is equal to

$$\Pr(k) = \frac{(\theta\rho S)^k e^{-\theta\rho S}}{k!} \quad (1)$$

where ρ is the node density per unit area, which is dependent on the location in space; θ is the proportion of normal nodes in the network; S represents the transmission area of a malicious node.

As the number of accused malicious nodes increases, the number of normal nodes decreases in the network. If k = 0, it implies that there are no normal nodes within the transmission range of a malicious node. In this case, the probability becomes:

$$\Pr(k) = e^{-\theta\rho S} \quad (2)$$

In Eq. (2), the value of Pr is the probability that no normal nodes exist in the region of a malicious node. When the density of normal nodes decreases, the probability Pr increases significantly. Therefore, the performance of the scheme is dependent on the density of normal nodes. Efficiency is greatly reduced because the certificate revocation operation requires

normal nodes to accuse malicious nodes. Consequently, to improve the performance of the scheme, the probability that no normal nodes occur within the range of a malicious node should be reduced. This is necessary to guarantee that a certain number of normal nodes exist in the network. In other words, we need to release legitimate nodes from the WL and restore their accusation function to increase the number of normal nodes in the network.

B. Node release method

To solve the problem mentioned above, we propose a method to release nodes from the WL based on a threshold in order to increase the number of normal nodes in the network. Nodes in the WL are not only legitimate nodes but also misbehaving nodes. If misbehaving nodes are released, they may continue to falsely accuse other nodes. Therefore, we need to be able to distinguish between legitimate and misbehaving nodes to only release the legitimate nodes from the WL. In order to accomplish this, we define a threshold *K,* and assume that the number of misbehaving nodes in the network is less than *K*.

Unlike our previous method, where the CA only accepts the first ADP and ignores any additional accusations made against the same accused node, our new method assigns a counter to each accused node and the CA continues to receive accusations until the counter equals *K*. The accusers (except the first one which is put in the WL) are placed onto a temporal stack, so that each accusation made by the same accuser is counted only once. This will effectively prevent false accusations and collusion between misbehaving nodes. When the counter is less than *K*, we mark the accuser listed in the WL as a suspected node, in which it may either be a legitimate node or a misbehaving node. To prevent future damage by the misbehaving node, the accuser is not permitted to be released from the WL. Otherwise, if the counter equals *K*, the accused node is recognized as an attacker and its accuser is deemed as a legitimate node. This accuser is freed from the WL, so that its accusation ability can be restored. Consequently, the number of normal nodes will increase in the mobile network by using this method.

V. EVALUATION

In this section, we discuss the simulation results of our proposed method using the QualNet 4.0 [16] network simulator. The purpose of our simulations is to evaluate the performance of the scheme in terms of the efficiency in revoking the certificates of malicious nodes, and in particular to indicate the impact of mobility and threshold on the detection time of malicious nodes in the network.

A. Simulation Setup

We simulate a mobile ad hoc network with 50 normal nodes and a number of malicious nodes ranging from 10 to 60, which are distributed randomly in 1km^2 terrain. The node's transmission range is set to be 250m. We use AODV as an IP routing protocol. Nodes follow the Random-Waypoint mobility model [17], in which each node moves to a randomly selected location at a constant speed and then chooses another random position after 5 seconds of pause time. The specific parameters are shown in Table 1. In the simulations, we assume that the proportion of misbehavior nodes is actually quite small in the network. A malicious node periodically launches attacks every 5 seconds that can be detected by other nodes within its one-hop range. Each simulation was carried out 20 times.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Number of nodes	50 normal nodes and 10 - 60 malicious nodes
Mobility model	Random-Waypoint
Node placement	Random
Routing protocol	AODV
Pause time	5 sec
Transmission range	250 m
Terrain dimensions	1 km^2
Simulation Time	600 sec

B. Simulation Results

1)The detection performance

Here, we analyze the detection performance to verify the effectiveness of our method. The curve of the detection time described in Fig. 3 shows the trend in contrast to the previous method. The detection time represents the amount of time needed to detect all malicious nodes in the network.

By using the previous method, as expected in our analysis, when the number of malicious nodes is less than a specified value (40 in this simulation), the scheme works well and the detection time maintains only a slight escalation with the number of increasing malicious nodes. However, the curve suddenly increases drastically, implying a significant increase in the detection time required to detect the rest of malicious nodes. When the number of malicious nodes is more than 50, the CA is no longer able to detect any new attackers because all of the normal nodes in the network are now listed in the WL. In contrast, we can see from Fig. 3 that, by using the new method, even if the number of malicious nodes increases to 60, and exceeds the number of normal nodes, the scheme still continues to work steadily. It does not exhibit a significant impact on the detection performance and the curve continues to grow steadily, unlike the previous approach.

2)Impact of mobility on the detection performance

To evaluate the detection performance of the scheme, we study the impact of mobility on the detection time. Fig. 4 shows the detection time as the node mobility changes. In this simulation, the threshold is equal to 5. The mobility is set to be 1m/s, 2m/s, 5m/s and 10m/s, respectively. As expected from intuition, the results show that the detection time drops as the node mobility increases. This is because, in a MANET, as the mobility increases, the chance that normal nodes will roam into the region of a malicious node or an attacker moves into the range of a normal node increases.

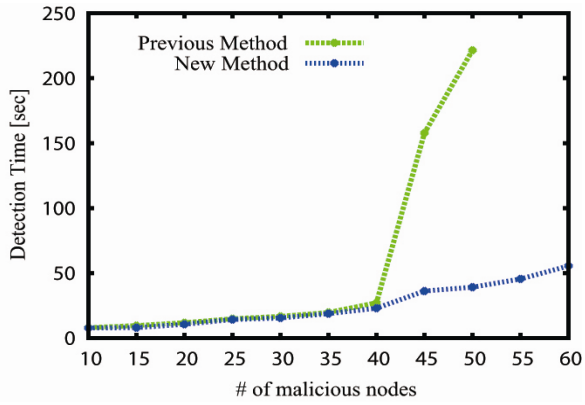

Figure 3. Previous method versus the new method.

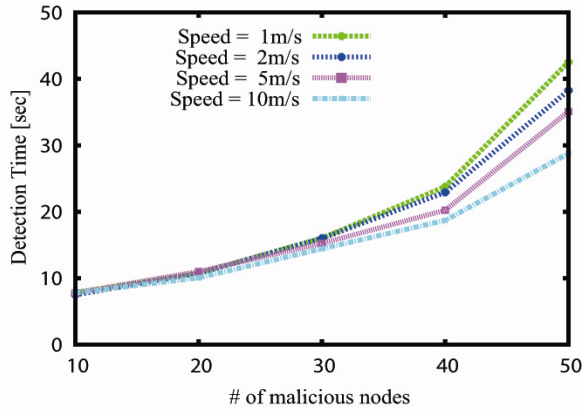

Figure 4. Impact of mobility.

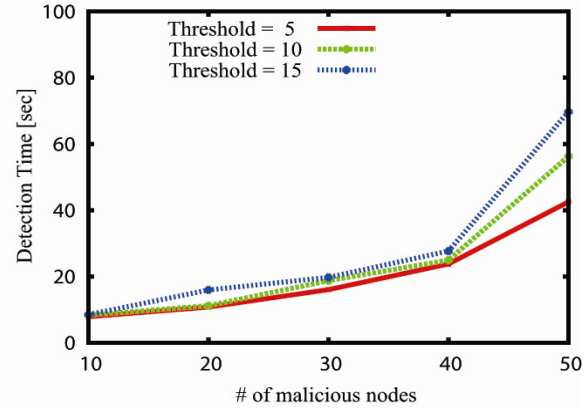

Figure 5. Impact of threshold.

3)Impact of threshold on the detection performance

This simulation measures the impact of the threshold value K on the detection performance, as shown in Fig. 5. We conduct a set of experiments for different values of K (5, 10 and 15). All nodes maintain constant movement at 1m/s in the mobile network. As shown in Fig. 5, when the threshold K becomes large, the detection time slightly increases since nodes are permitted to release from the WL until the threshold condition is satisfied. This is due to the fact that when the number of accusations against an attacker equals K, the CA restores the accuser's accusation ability. We can conclude that the lower the threshold, the faster the detection time.

VI. CONCLUSION

In this paper, we have enhanced our previously proposed clustering-based certificate revocation scheme which allows for fast certificate revocation. In order to address the issue of the number of normal nodes being gradually reduced, we have developed a threshold based mechanism to restore the accusation function of nodes in the WL. The effectiveness of our proposed certificate revocation scheme in mobile ad hoc networks has been demonstrated through extensive simulation results.

REFERENCES

[1] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," IEEE Wireless Communications, 11(1), pp. 38-47, Feb. 2004.

[2] P. Sakarindr and N. Ansari, "Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks," IEEE Wireless Communications, 14(5), pp. 8-20, 2007.

[3] L. Zhou, B. Cchneider and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Transactions on Computer Systems, Vol.20, No.4, pp.329-368, Nov. 2002.

[4] A.M. Hegland, E. Winjum, C. Rong, and P, Spilling, "A survey of key management in ad hoc networks", IEEE Communications Surveys and Tutorials, vol 8, no. 3, pp. 48-66, 2006.

[5] L. Zhou and Z.J. Haas, "Securing ad hoc networks," IEEE Network Magazine, 13 (6), pp. 24-30, 1999.

[6] K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate revocation to cope with false accusations in mobile ad hoc networks," *Proc. 2010 IEEE 71st Vehicular Technology Conference: VTC2010-Spring*, Taipei, Taiwan, May 16-19, 2010.

[7] S. Micali, "Efficient certificate revocation," Massachusetts institute of technology, Cambridge, MA, 1996.

[8] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: ubiquitous and robust access control for mobile ad hoc networks," IEEE/ACM Trans. Networking, vol. 12, no. 6, pp.1049-1063, Oct. 2004.

[9] G. Arboit, C. Crepeau, C. R. Davis, and M. Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks," Ad Hoc Network, vol. 6, no. 1, pp. 17-31, Jan. 2008.

[10] J. Clulow and T. Moore, "Suicide for the Common Good: A NewStrategy for Credential Revocation in Self-organizing Systems," ACMSIGOPS Operating Systems Reviews, vol. 40, no. 3, pp.18-21, Jul. 2006.

[11] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, "Resisting flooding attacks in ad hoc networks," Int'l Conf. Information Technology: Coding and Computing, vol. 2, pp. 657-662, Apr. 2005.

[12] R.A. Raja Mahmood and A.I. Khan, "A survey on detecting black hole attack in AODV-based mobile ad hoc networks," Int'l Symp. High Capacity Optical Networks and Enabling Technologies, pp.18-20, Nov. 2007.

[13] F. Nait-Abdesselam, B. Bensaou and T. Taleb, "Detecting and avoiding wormhole attacks in wireless ad hoc networks," IEEE Commun. Mag., vol. 46, no. 4, pp.127-133, Apr. 2008.

[14] J. Newsome, E. Shi, D, Song and A, Perrig, "The Sybil Attack in Sensor Network: Analysis & defenses," Information Processing in Sensor Networks, 2004, pp. 259-268.

[15] J. Kong, X. Hong, Y. Yi, J.-S. Park, J. Liu, and M. Gerla, "A secure ad-hoc routing approach using localized self-healing communities," Proceedings of the 6th ACM International Symposium on Mobile Ad hoc Networking and Computing, 2005, pp. 254-265.

[16] Scalable Network Technologies: "Qualnet" http://www.scalable-neworks.com

[17] T. Camp, J. Boleng, and V. Davies, "The survey of mobility models for ad hoc network research," Wireless Communication and Mobile Computing, vol.2, no. 5, pp. 483-502, Aug. 2002.