Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks

Kyul Park †, Hiroki Nishiyama †, Nirwan Ansari ††, and Nei Kato †
†*Graduate School of Information Sciences, Tohoku University, Japan*
††*Advanced Networking Laboratory, ECE Department, NJIT, USA*
pk1313@it.ecei.tohoku.ac.jp

***Abstract*— In Mobile Ad hoc NETworks (MANETs), certification systems play an important role in maintaining network security because attackers can freely move and repeatedly launch attacks against different nodes. By adopting certification systems, it becomes possible to exclude identified attackers from the network permanently by revoking the certifications of the attackers. A simple way to identify attackers is to collect information on attackers from nodes in the network. However, in this approach, it is difficult to differentiate valid accusations made by legitimate nodes from false accusations made by malicious nodes. In addition, the amount of traffic in order to exchange information on attackers and the necessary time to gather the information increases as the network size becomes larger. In this paper, we propose a certificate revocation scheme which can revoke the certification of attackers in a short time with a small amount of operating traffic. By clustering nodes and introducing multi-level node reliability, the proposed scheme can mitigate the improper certificate revocation due to false accusations by malicious users.**

I. Introduction

Owing to the advances in wireless communications technologies, Mobile Ad hoc NETwork (MANET) has attracted much attention. MANET is a highly flexible network where nodes can freely move and join, with no fixed infrastructure, and thus it is vulnerable to attacks by malicious users. Therefore, ensuring network security is one of the most important issues in MANET.

Although a large number of methods to detect various kinds of attacks have been developed for MANETs, only detecting and blocking attacks in each node is not enough to maintain network security because attackers can freely move and repeatedly launch attacks against different nodes. To reduce the damage from attacks, attackers must be immediately removed from the network after detection of the first attack; this can be achieved by using a certification system. In networks employing a certification system, nodes cannot communicate with each other without a valid certification. In other words, any attacker cannot exist in the network once its malicious behavior has been detected by others and its certification has been revoked accordingly by the system.

The performance of a certification system largely depends on its deployed certification revocation strategy. Accurate revocation, quick revocation, and small network overhead remain the challenging issues to be addressed in a certificate system, particularly, to be applicable in MANET. In particular, ensuring the accuracy of certificate revocation is a significant challenge because malicious users may abuse the certification system. For instance, in the system which identifies attackers based on the information on the occurrence of attacks provided by nodes belonging to the network, the certificate of a legitimate user might be revoked by the false accusation from malicious nodes. Therefore, certificate revocation methods must be able to distinguish false accusations from valid ones. Also, malicious nodes must be immediately removed from accessing the network with a small operating overhead.

In this paper, we propose a certificate revocation scheme which takes into account of false accusations from malicious users. The performance of the proposed scheme is evaluated in terms of promptness of revocation, operating overhead, and accuracy of revocation. The reminder of the paper is organized as follows. In Section II, existing certificate revocation methods are reviewed, and their advantages and drawbacks are briefly described. Section III presents the detailed mechanism of our proposed revocation scheme. The performance of the proposed scheme is evaluated and analyzed in Section IV, and Section V concludes the paper.

II. Related works

In this section, we briefly review several certificate revocation methods. In URSA [1], two neighboring nodes receive their certificates from each other and also exchange certificate information about other nodes that they know. Nodes sharing the same certificate information are regarded as belonging to the same network. In these networks, the certificate of a suspected node can be revoked when the number of accusations against the node exceeds a certain threshold. While URSA does not require any special equipment such as Certificate Authorities (CA), the operational cost is still high.

In contrast to URSA, DICTATE [2] employs a number of CAs to efficiently perform the publication and revocation of certificates. CAs monitor node behavior in order to detect attacks and share the certificate information with each other. If a CA identifies a malicious node, the certificate of the node is revoked by the CA and its information is shared among other CAs, thus resulting in the complete exclusion of the node from the network. However, the deployment of a sufficient number of CAs is not an easy task in MANETs.

In [3], the certificate of a node which has been accused by just one node will be revoked by every node. As a result, this scheme exhibits good performance in terms of promptness and low operating overhead. However, this scheme poses a controversial point that an accuser will be removed from

978-1-4244-2519-8/10/$26.00 ©2010 IEEE

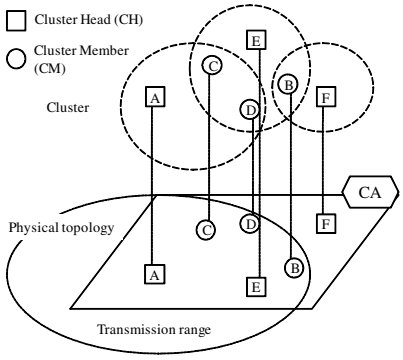


Fig. 1. Node clustering

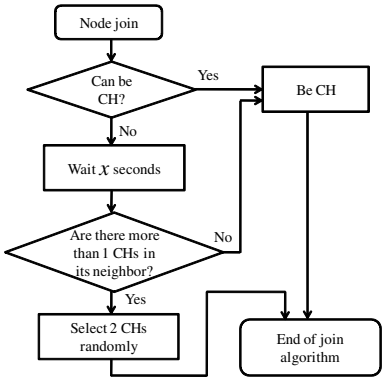


Fig. 2. Node join algorithm

the network along with the accused node. This approach is fundmentally flawed, and so this scheme cannot be commonly used.

The method proposed in [4] introduces a time session to refresh the certificate information of each node. The accusation count is reset at the end of each session. Therefore, while this scheme is able to mitigate the damage caused by false accusations, the performance can be largely degraded by the increase of malicious nodes.

In the voting based scheme [5], [6], if the number of nodes, which have accused a particular node, exceeds the predefined threshold, the accused node is removed from the network by having its certificate revoked. This scheme takes into account of the false accusations, i.e., each accusation has a different weight according to the accuser's reliability. However, this scheme has two problems, a large amount of operational traffic and a long revocation time, because the opinion of every node in the network is needed for each node to decide whether to revoke the certificate of the malicious node or not.

According to the above discussion, in this paper, we propose a certificate revocation scheme which can achieve prompt revocation, lower operational traffic, and mitigate damage from false accusations.

III. The Envisioned Scheme

Before delving into details of our envisioned scheme, it is worth noting a fundamental assumption. Nodes are assumed to be able to detect an attacker within their transmission range, e.g., in case of ad hoc flooding attacks [7], black hole attacks [8], worm hole attacks [9], and so forth.

A. Node reliability

In the proposed scheme, nodes are differentiated according to their reliability, i.e., *normal nodes* have a high reliability, *warned nodes* are suspected as potential attackers, and *attacker nodes* have been accused by a normal node. When nodes join the network, they are assumed to be normal nodes. Warned nodes and attacker nodes are listed in the Warning List (WL) and Black List (BL), respectively. The certificates of the nodes listed in BL are revoked whereby they are removed from the network. While the nodes included in WL can communicate with other nodes in the same way as normal nodes, there are a few restrictions placed on their behavior, i.e., unable to become a cluster head and not allowed to make any accusation as described later in detail. WL and BL are maintained by a CA which broadcasts all certificate information including WL and BL to the whole network upon the renewal of WL or BL.

B. Node clustering

By classifying nodes into clusters, the proposed scheme allows each Cluster Head (CH) to detect false accusation by a Cluster Member (CM) within the cluster. Node clustering provides a means to mitigate false accusations. CHs always moniters their CMs and watch for false accusations by means of the algorithm which will be discussed in Section 3.C.2). Fig. 1 shows an example of how clusters are constructed in the proposed scheme. While each cluster consists of one CH and CMs lying within the CH's transmission range, some nodes within the transmission area of the CH might not be the member of the cluster and can be the CM of another cluster. For example, in Fig. 1, node B does not belong to the cluster headed by node A while it is located within the transmission area of node A. Only normal nodes having high reliability are allowed to become a CH. Nodes except CHs join the two different clusters of which CHs exist in the transmission range of them. By constructing such clusters, each CH can be aware of false accusations against any CMs since each CH knows which CM executes attacks or not, because all of the attacks by a CM can be detected by any node, of course including the CH, within the transmission range of the CM. The reason why each node except CH belongs to two different clusters is to decrease the risk of having no CH due to dynamic node movement. To maintain clusters, CH and CMs frequently confirm their existence by exchanging messages, i.e., the CH periodically broadcasts CH Hello packets to the CMs within its transmission range, and each CM replies to the CH with the CM Hello packet.

Fig. 2 shows the node join algorithm which is carried out by newly joining nodes that enter the network. A newly joining node becomes CH at a constant rate. A node, which has decided not to become a CH itself, will look for other CH nodes in the area. If there are more than two CHs near the node, it will attempt to join two of these clusters by randomly selecting two of their CHs and sending each of them a CM Hello packet. Otherwise, the joining node declares itself as a CH and broadcasts CH Hello packets. When a CM leaves the cluster, it needs to invoke a similar procedure to find out new CHs. If the CM receives no CH Hello packet from its CH for a certain period of time, the CM considers itself having

departed from the cluster, and tries to find and join a new cluster. On the other hand, if the CH cannot receive any CM Hello packets for a while, this implies that no CM is in the cluster, it then inspects the number of neighboring CHs and becomes the CM for those clusters if at least two CHs are found. By implementing the above procedures, the proposed scheme is able to maintain clusters regardless of the node movements, thus enabling it to detect false accusations. Also, since nodes in the WL cannot become CHs, in the case where CMs lose their CH because the CH has been put into the WL, they can find and join a new cluster by executing the necessary procedures as described above.

C. Two kinds of accusations

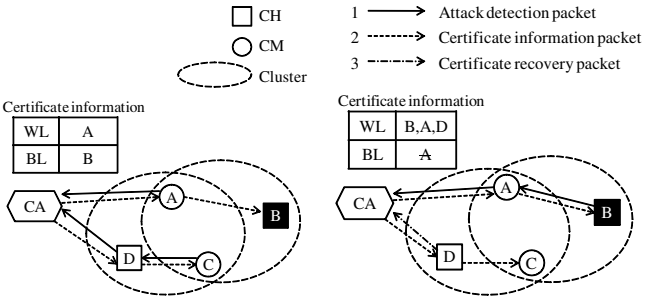
In the proposed scheme, two different kinds of accusation packets that induce update of the BL: *attack detection packets* that are used to register attackers in the BL, and *certificate recovery packets* that are used to eliminate legitimate nodes from the BL. While any normal node is allowed to send out attack detection packets upon detecting attackers around them, only CHs have permission to send certificate recovery packets. All nodes listed in BL or WL cannot accuse other nodes.

1) Attack detection packets: Upon detecting attacks, normal nodes send out the attack detection packets to inform the CA of the attacker. Attack detection accusation can be done regardless of the clusters, i.e., any normal nodes detecting the attacks can accuse attackers. Attack detection packet includes not only the attacker's node ID but also the accuser's node ID. In the CA, if the accused attacker is not included in the BL, the attacker and the accuser are registered on the BL and WL, respectively. The reason behind registering the accuser in the WL is in the interest of conservation, to reduce the number of false accusations by malicious nodes. Even if the accuser is a malicious node, an additional false accusation can be prevented by registering the accuser in the WL because nodes listed in the WL are not allowed to make accusations.

Fig. 3(a) shows the case where nodes A and C are lying in the transmission range of node B, and have detected an attack by node B at the same time. As the attack detection packet from node A arrives first at the CA, nodes B and A are registered on the BL and WL, respectively. After updating the lists, the CA broadcasts the certificate information packets including the latest list information to the whole network. Since each node revokes the certificates of all nodes included in the BL according to the broadcasted information, node B is completely removed from the network.

As described above, the attack detection packet allows nodes in the network to report attackers to the CA; the CA can then rapidly gather information about the attackers.

2) Certificate recovery packets: In the proposed scheme, a legitimate node can be listed in the BL by a false attack detection packet sent from a malicious node. To cope with this issue, CHs are allowed to carry out the certificate recovery to correct the errors in the BL. Since all CMs are within the transmission range of their CH, the CH always detects any attacks by the CMs belonging to the cluster. In other words, if a CM is listed as an attacker in the BL without being detected by its CH, it implies that the CM was wrongly accused by malicious nodes. Errors in the BL can only be discovered by the CH. Therefore, CHs immediately carry out the certificate recovery to recover the certificate of the victim upon discovering the error in the BL.



(a) Attack detection (b) Certificate recovery

Fig. 3. Two kinds of accusations

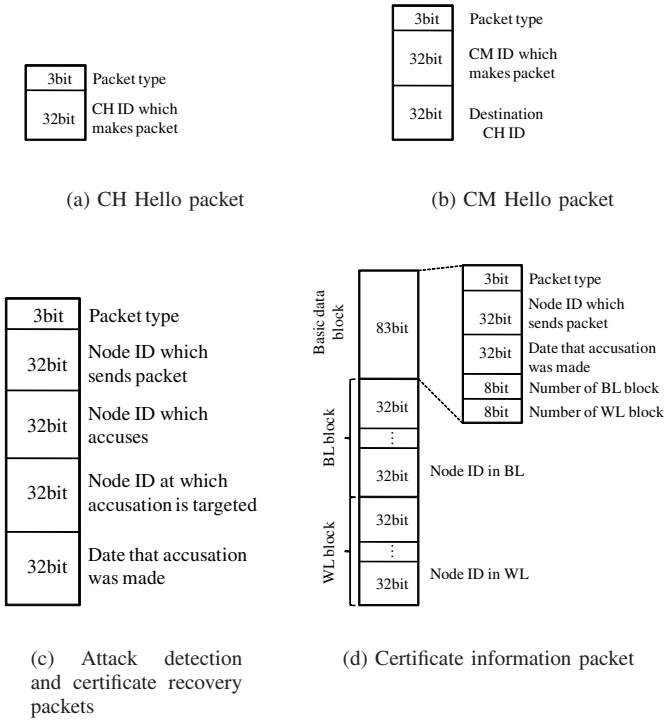
The certificate recovery packet includes the node IDs of the accuser and the exonerated victim. In the CA, if the victim has not been deleted from the BL yet, the BL can be appropriately corrected, both the victim and the accuser registered in the WL. Since the corrected information of the lists are broadcasted to all nodes in the network, the certificate of the victim can be recovered.

Fig. 3(b) depicts the certificate recovery process in which node A's certificate has been revoked by the false attack detection packet by node B. While node D, which is one of the CHs of node A, receives the message from the CA that node A has been listed in the BL as an attacker, node D knows the information is inaccurate because node D has never detected any attacks from node A. Therefore, node D sends the accusation recovery packet to the CA in order to correct the error in the BL. When the certificate recovery packet from node D reaches the CA, the incorrect entry of node A in rather than on the BL is deleted while nodes A and D are registered in the WL. By broadcasting the updated lists, the certificate of node A is recovered throughout the network.

As described above, the CA can grasp information about false accustions by using certificate recovery packets to mitigate the damage caused by false accusations.

D. Control packets

In the proposed scheme, five kinds of control packets are used, i.e., CH Hello packet, CM Hello packet, certificate information packet, and attack detection and certificate recovery packets. Fig. 4 shows the structure of each control packet. The size of CH Hello packet, CM Hello packet and both accusation packets are fixed, in contrast to the certificate information packet having $83 + 32(n_{BL} + n_{WL})$ bits where n_{BL} and n_{WL} represent the number of nodes listed in the BL and WL, respectively. Although an increase in the number of malicious nodes results in a slight increase in the amount of control traffic, it is not significant in the proposed scheme because most of the control traffic consists of CH Hello packets and



(a) CH Hello packet

(b) CM Hello packet

(c) Attack detection and certificate recovery packets

(d) Certificate information packet

Fig. 4. Control packets

CM Hello packets of which size and transmission frequency are independent from the number of malicious nodes.

IV. Performance evaluation

A. Simulation setup

To evaluate the performance of the proposed scheme, we conducted simulations by using the network simulator, QualNet 4.0 [10]. We assume that attacks can be detected by any nodes within the transmission range of each attacker, and they periodically launch attacks every five seconds. Table 1 shows the set of simulation parameters. One CA is randomly located in the field. In the proposed scheme, the transmission interval of both CH Hello packets and CM Hello packets, and the waiting time, x as shown in Fig. 2, are set to 20 seconds. The probability that the newly joining node becomes a CH is equal to 0.3. The voting based scheme is used for comparison. The presented results show the averaged values over fifty trials if not otherwise specified.

B. Simulation results

First of all, we evaluate the promptness of the certificate revocation. Fig. 5 shows an instance of the time change in the ratio of attackers removed from the network by successfully revoking their certificates in the case that 10% of all 100 nodes are attackers. In Fig. 5, the results of the first few seconds before the attacks start are omitted. It can be seen that the proposed scheme succeeds in immediately removing attackers from the network as compared to the voting based scheme. This is because the proposed scheme does not require a large number of accusations from a lot of nodes in order to revoke certificates as in the voting based scheme. While we cannot present more results owing to the space limitation, similar results as shown in Fig. 5 are obtained for different node densities and different attacker ratios.

TABLE I

The List of Simulation Parameters

Parameter	Value
Field	1000m × 1000m
Node transmission range	250m
Number of nodes	50 − 100
Node placement	Random
Mobility model	Random-Waypoint
Node speed	1 m/s
Pause time	5 sec
Routing protocol	AODV
Simulation time	500 sec

Fig. 6 shows the attack success count with different attacker ratios when the number of nodes is 100. The attack success count is defined as the number of successful attacks during the entire simulation; we assume that attacks can succeed only against the nodes which have never been attacked before by the same attacker, and have not received any information on the attacker. From Fig. 6, it can be confirmed that the proposed scheme is able to reduce the damage from attacks by quickly removing the attackers from the network.

To evaluate the operating overhead, we investigate the amount of control traffic required by varying the node density. All kinds of packets as shown in Fig. 4 are counted as control traffic. The attacker to node ratio is set to 10%. Fig. 7 shows that the proposed scheme uses a small amount of control traffic in different node densities, and the difference between the proposed scheme and the voting based scheme becomes large as the node density increases. This is because most of the operating traffic in the proposed scheme corresponds to the amount of Hello packets which are not largely affected by the number of nodes, while the amount of control messages in the voting based scheme is significantly increased due to a large number of nodes because each node broadcasts the message to all the nodes in the network. It should be noted that the proposed scheme is able to achieve quick revocation of an attacker's certificate, while maintaining a small operating overhead, thus minimizing the damage from attacks.

C. Security analysis

In the proposed scheme, a CH can recover the certificate of a victim whose certificate has been revoked by false accusations by malicious nodes. In other words, if both CHs of the CM are malicious nodes, the CM can be removed from the network permanently because no CH carries out any certificate recovery for the CM. In the remainder of this section, we analyze the the probability of a node in selecting malicious nodes as its CHs, thus resulting in the success of false accusation because there are no CHs to carry out the certificate recovery. We assume that all malicious nodes declare themselves as a CH to be selected by the targets as the CH.

In each node, the number of nodes within its transmission range except itself, A, can be calculated by using the node density, n, and the transmission range, d, as follows:

$$A = n\pi d^2 - 1 \tag{1}$$

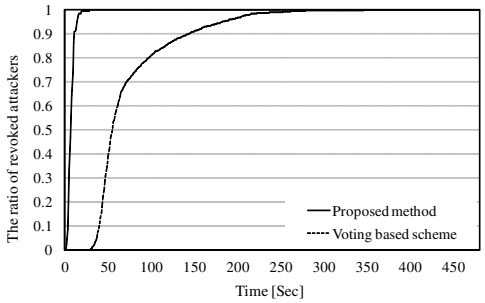


Fig. 5. The ratio of revoked attackers over time

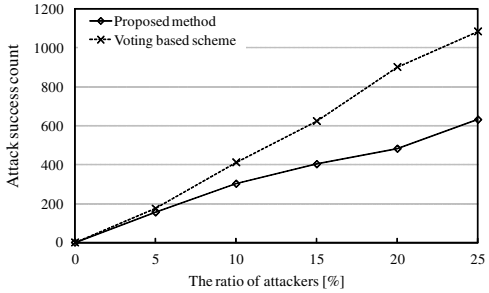


Fig. 6. Attack success count by ratio of attackers

The number of malicious nodes declaring themselves as CHs is equal to Am where m is the ratio of malicious nodes to the total population of nodes. On the other hand, the number of valid CHs is equal to $A(1-m)p$, where p indicates the probability that a legitimate node becomes a CH. Accordingly, the number of all CHs is equal to $A(p+(1-p)m)$. Therefore, the probability, P, that a normal node is removed from the network because of selecting two malicious nodes as its CHs can be represented as follows:

$$P = \frac{{}_{Am}\mathrm{C}_2}{{}_{A(p+(1-p)m)}\mathrm{C}_2} \tag{2}$$

P varies by changing the number of malicious nodes as shown in Fig. 8. The solid line in Fig. 8 shows the analytical results derived from Eq. (2) in which n and p are equal to 100 node/km^2 and 0.3, respectively, while the dashed line indicates the results obtained by simulations. The simulation results conform closely to the analysis, i.e., the revocation ratio increases as the number of malicious nodes increases. In the proposed scheme, once nodes carry out the accusation, they cannot make any accusations again because they have been listed in the WL, thus effectively mitigating the damage caused by false accusations.

V. Conclusion

In this paper, we have focused on the certificate revocation methods used in the certification system for MANETs. To cope with the wrong revocation of the certificate of legitimate users caused by false accusations by malicious nodes, we have proposed a certificate revocation scheme which takes into account of the reliability of each node, and accordingly constructs clusters to detect false accusations. Through computer simulations and analysis, it can be confirmed that the proposed scheme is able to promptly remove attackers from the network

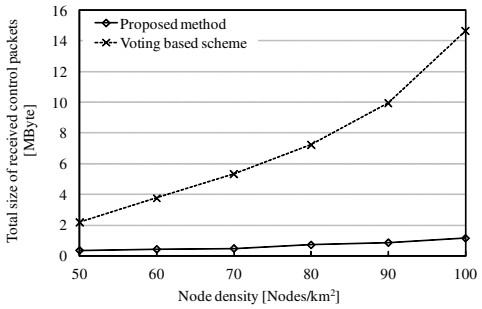


Fig. 7. Control packet traffic by node density

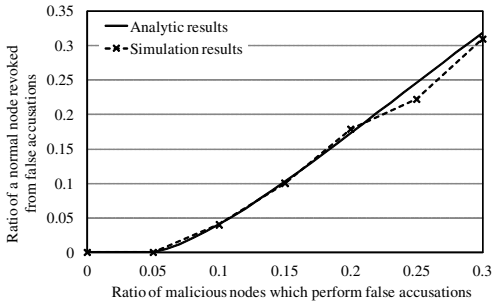


Fig. 8. Ratio of a normal node revoked from false accusations

with low operating traffic even in the existence of malicious nodes carrying out false accusations.

Acknowledgment

This work was supported through the Strategic International Cooperative Program, JST and NSF (under grant no. 0726549).

References

[1] 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.

[2] J. Luo, J. P. Hubaux and P. T. Eugster, "DICTATE: DIstributed CerTification Authority with probabilisTic frEshness for ad hoc networks," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 4, pp.311-323, Oct.-Dec. 2005.

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

[4] H. Chan, V. D. Gligor, A. Perrig and G. Muralidharan, "On the distribution and revocation of cryptographic keys in sensor networks," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 3, pp.233-247. Oct.-Dec. 2005.

[5] C. Crepeau and C.R. Davis, "A Certificate Revocation Scheme for Wireless Ad Hoc Networks," Proc. of ACM Workshop Security of Ad Hoc and Sensor Networks, 2003.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] Scalable Network Technologies: "Qualnet," http://www.scalable-networks.com/.