ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Efficient Cluster Based CCRVC Scheme in Manet

Mrs.U.Devisree[1], Mrs.M.santhi[2]

M.E II Year, Department of CSE, Sri Subramanya College of Engineering &Technology, Palani-624 615, India[1]

Assistant professor, Department of CSE, Sri Subramanya College of Engineering &Technology, Palani-624 615, India[2]

ABSTRACT—Mobile ad hoc networks (MANETs) have attracted much care due to their mobility and ease of deployment. The wireless networks face the many various types of security attacks than the wired networks. The major dispute is to guarantee secure network services. In Existing the voting based and non-voting based mechanisms to guarantee the service. The certificate revocation is an important integral component to secure network communications. The issue of certificate revocation to isolate attackers in network activities. For quickly and exact certificate revocation, the Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme. To improve the reliability of the scheme, the warned nodes to participate in the certificate revocation process are revoked to enhance the accuracy. The threshold-based mechanism to evaluate and vindicate (justify) warned nodes as legitimate nodes or not, before recovering them. It is effective and efficient to guarantee secure communications in mobile ad hoc networks. The Efficient network should have the high quality of Service and also the high security. With the help of CCRVC method, the high security will be increased. With the help of Quality of service path first (QOSPF) routing protocol, the QOS will be increased. QOS contains throughput, delay, lifetime, Overhead, Packet delivery ratio and Packet Loss Ratio.

KEYWORDS: Mobile ad hoc networks (MANETs), certificate revocation, security, threshold, vindicate.

I. INTRODUCTION

Mobile ad hoc networks have received increasing attention in recent years due to their mobility feature, dynamic topology, and ease of deployment. A mobile ad hoc network is a self-organized wireless network which consists of mobile devices, such as laptops, cell phones, and Personal Digital Assistants (PDAs), which can freely move in the network. E.g., disaster relief, military operation, and emergency communications. A mobile ad hoc network (MANET) is a self-configuring infrastructureless network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

They act as both end users and routers, which relay packets for other nodes. Unlike the conventional network, another feature of MANETs is the most open network. Environment where nodes can join and leave the network freely.Certification is a prerequisite to secure network communications. It is embodied as a data structure in which the public key is bound to an attribute by the digital signature of the issuer, and can be used to verify that a public key belongs to an individual and to prevent tampering and forging in mobile ad hoc networks. Many research efforts have been dedicated to mitigate malicious attacks on the network. Any attack should be identified as soon as possible.

Certificate revocation is an important task of enlisting and removing the certificates of nodes that have been detected to launch attacks on the neighborhood. In other words, if a node is compromised or misbehaved, it should be removed from the network and cut off from all its activities immediately. In our research, we focus on the fundamental security problem of certificate revocation to provide secure communications in MANETs.

II. RELATED WORK

A novel solution to ubiquitous and robust access control in mobile ad-hoc networks. In URSA, only well-behaving nodes are granted access to routing and packet forwarding via valid tickets issued collectively by multiple local nodes. Our design has been motivated by the principle that the access control decision has to be fully *distributed* and *localized* in order to operate in a large-scale, moral force mobile ad-hoc network. We seek to maximize the service availability in each network locality, which is also crucial to supporting mobile users. Our experiences in both implementation and simulations have shown the effectiveness of our design [1].

This paper presented work suicide for the common good, an effective and efficient credential revocation strategy for self organizing systems. Suicide for the common good compares favourably to existing voting-based revocation mechanisms in terms of speed, communications overhead and storage requirements. Furthermore, to the best of our knowledge, it is the first fully decentralized revocation strategy that works even when nodes are highly mobile [2]. We hope that future work will identify more applications and present formal specifications of secure protocols to realize these ideas. In this presented research work [3] a decentralized certificate revocation scheme which utilizes certificates that are based on the hierarchical trust model. Our scheme assigns all key management tasks except the issuing of certificates to the nodes in a MANET; and it does not require any access to on-line certificate authorities (CAs).Our certificate revocation scheme is based on weighted accusations; whereby a quantitative value is assigned to an accusation to determine its weight. The weights of the accusations from nodes that are considered to be trustworthy are higher than those from less trustworthy nodes. A certificate of a node is revoked when the sum of the weighted accusations against the node is equal to or greater than assemble threshold (RT). The scheme mainly uses hash chains for providing data origin and Integrity checks and it does not require time synchronization. Communication complexity analysis which shows that order N2 accusation info messages are sufficient to cause the revocation of a malicious node certificate.

III. PROBLEM DEFINITION

A. Existing System

Certificate revocation to insulate attackers from further participating in network activities. Using voting based and nonvoting based mechanism for maintain the secure network. But its creates communication overhead, poor performance and reliability. Avoid the communication overhead, for quick and accurate certificate revocation, we propose the Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme.

In particular, to improve the reliability of the scheme, we recover the warned nodes to take part in the certificate revocation process; to enhance the accuracy, we propose the threshold-based mechanism to assess and vindicate warned nodes as legitimate nodes or not, before recovering them. The performances of our scheme are evaluated by both numerical and simulation analysis. Extensive results demonstrate that the proposed certificate revocation scheme is effective and efficient to guarantee secure communications in mobile ad hoc networks.

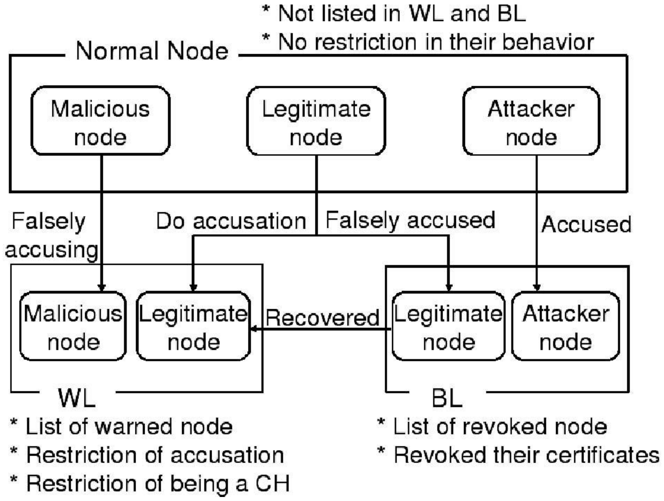


Fig. 1. The classification of nodes in our scheme.

In our scheme, these nodes can be further classified into three categories based on their reliability: normal mode, warned node, and revoked node. When a node joins the network and does not launch attacks, it is regarded as a normal mode with high reliability that has the ability to accuse other nodes and to declare itself as a CH or a CM. Moreover, we should note that normal nodes consist of legitimate nodes and potential malicious nodes. Nodes that are listed in the warning list are viewed as warned nodes with low reliability.

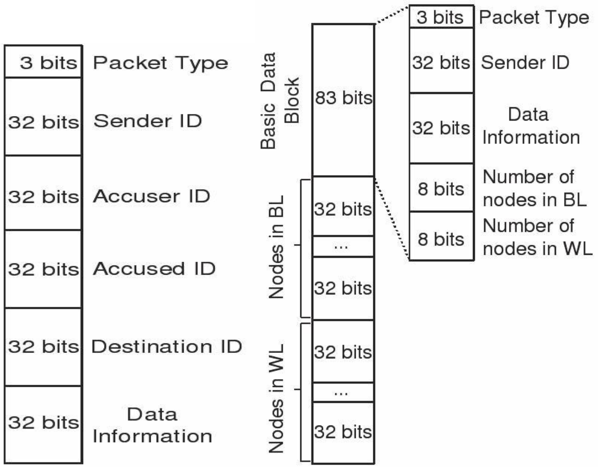


Fig. 2. Control packets

Warned nodes are considered suspicious because the warning list contains a mixture of legitimate nodes and a few malicious nodes Warned nodes are permitted to communicate with their neighbors with some restrictions, e.g., they are unable to accuse neighbors any more, in order to avoid further abuse of accusation by malicious nodes. The accused nodes that are held in the blacklist are regarded as revoked nodes with little reliability. Revoked nodes are considered as malicious attacker's disadvantage of their certificates and evicted from the network. It will be extracted in graph constructed based on interaction between cluster head and cluster authority. These features involving the number of nodes presented in network and the number of data transformed between nodes.

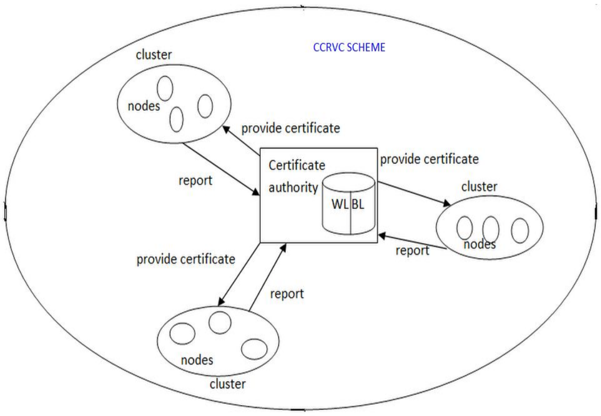


Fig 3 CCRVC architecture

B. Proposed System

Certificate revocation by CCRVC scheme for secure network, the predetermine value fixed by threshold based mechanism. the CCRVC scheme from voting based mechanism and non- voting based mechanism. The CCRVC scheme is effective and efficient. Improve QoS metrics could be defined in terms of one or a set of parameters with the help of QOS Path first Protocol, the QOS parameters such as throughput, delay, Packet delivery ratio, Lifetime are to be increased. The use of QoS-aware applications is evolving in the wireless environments. It is a challenging task to build QoS constrained with high performance, high success ratio, and low overhead and low system requirements.

IV. PERFORMANCE MEASURE

A. Cluster Construction

Nodes cooperate to form clusters, and each cluster consists of a CH along with some Cluster Members (CMs) located within the transmission range of their CH. Before nodes can join the network, they have to acquire valid certificates from the CA, which is responsible for distributing and managing certificates of all nodes, so that nodes can communicate with each other unrestrainedly in a MANET.

In this model, if a node proclaims itself as a CH, it propagates a CH Hello Packet (CHP) to notify neighboring nodes periodically. The nodes that are in this CH's transmission range can accept the packet to participate in this cluster as cluster members. On the other hand, when a node is deemed to be a CM, it has to wait for CHP. Upon receiving CHP, the CM replies with a CM Hello Packet (CMP) to set up connection with the CH. Afterward, the CM will join this cluster; meanwhile, CH and CM keep in touch with each other by sending CHP and CMP in the time period Tu.

B. Certification Authority (CA*)*

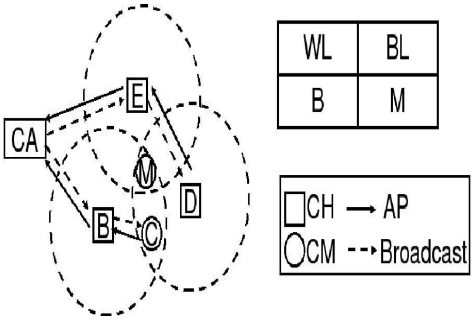
To enable each mobile node to preload the certificate. The CA is also in charge of updating two lists, WL and Blacklist, which is used to hold the accusing and accused nodes information**.** The BL is responsible for holding the node accused as an attacker, while the WL is used to hold the corresponding accusing node. The CA updates each list according to received control packets. Note that each neighbor is allowed to accuse a given node only once**.**

C. Communication between CH and CA

If a node is in warned list of certificate authority, it may move towards another cluster. At that time, Cluster Head must communicate with certification authority to request the history of the new node. If it was in Warned list, the CH eliminates that node. The false accusation of a malicious node against a legitimate node to the CA will degrade the accuracy and robustness of our scheme. To address this problem, one of the aims of constructing clusters is to enable the CH to detect false accusation and restore the falsely accused node within its cluster. Since each CH can detect all attacks from its CMs, requests for the CA to recover the certificate of the falsely accused node can be accomplished by its CHs by sending Recovery Packets (RPs) (see the format of recovery packet to the CA. Upon receiving the recovery packet from the CH, the CA can remove the falsely accused node from the BL to restore its legal identity. The sequence of handling false accusation is described hereafter.

First of all, the CA disseminates the information of the WL and BL to all the nodes in the network, and the nodes update their BL and WL from the CA even if there is a false accusation. Since the CH does not detect any attacks from a particular accused member enlisted in the BL from the CA, the CH becomes aware of the occurrence of false accusation against its CM. following steps for revoke node certificate.

Step 1. Neighboring nodes B, C, D, and E detect attacks from node M.
Step 2. Each of them sends out an accusation packet to the CA against M.
Step 3. According to the first received packet (e.g., from node B), the CA hold B and Min the WL and BL ,respectively, after verifying the validity of node B.
Step 4. The CA disseminates the revocation message to all nodes in the network.
Step 5. Nodes update their local WL and BL to revoke M's certificate.



WL	BL
B	M

Fig 4 Revoking a node's certificate

D. Node Classification

Three types of nodes are classified according to their behaviors**:**

A legitimate node

It is deemed to secure communications with other nodes. It is able to correctly detect attacks from malicious attacker nodes and accuse them positively, and to revoke their certificates in order to guarantee network security.

A malicious node

It does not execute protocols to identify misbehavior, vote honestly, and revoke malicious attackers.It is able to falsely accuse a legitimate node to revoke its certificate successfully.

A attacker node

It is defined as a special malicious node which can launch attacks on its neighbors to disrupt secure communications in the network.

E.CERTIFICATE REVOCATION

To revoke a malicious attacker's certificate, we need to consider three stages: accusing, verifying, and notifying. The revocation procedure begins at detecting the presence of attacks from the attacker node. Then, the neighboring node checks the local list BL to match whether this attacker has been found or not. If not, the neighboring node casts the Accusation Packet (AP) to the CA, which the format of accusation packet .Note that each legitimate neighbor promises to take part in the revocation process, providing revocation request against the detected node. After that, once receiving the first arrived accusation packet, the CA verifies the certificate validation of the accusing node: if valid, the accused node is deemed as a malicious attacker to be put into the BL. Meanwhile, the accusing node is held in the WL. Finally, by broadcasting the revocation message including theWLand BL through the whole network by the CA, nodes that are in the BL are successfully revoked from the network.

F.QOS

QoS: A set of service requirements that are met by the network while transferring a packet stream from a source to a destination.QoS metrics could be defined in terms of one or a set of parameters.With the help of quality of service path first routing Protocol(QOSPF), the QOS metrics such as throughput, delay, Packet delivery ratio, Lifetime are to be increased. These algorithms are based on the discovery of shortest path.QoS-aware routing protocol should find a path that satisfies the QoS requirements in the path from source to the destination .The use of QoS-aware applications are evolving in the wireless environments Other service models/parameters can/should be added Provides information for QoS routing calculation.solve issue of the false accusations certificate revocation. The end-to-end bandwidth can be calculated and allocated during the admission control phase.Using TDMA, time is divided into slots, which in turn are grouped into frames

Each frame contains two phases: control and data. During the control phase, each node takes turns to broadcast its information to all the neighbors in a predetermined slot.At the end of control phase, each node knows about the free slots between itself and its neighbors.Thus bandwidth calculation and allocation can be done in a distributed manner.

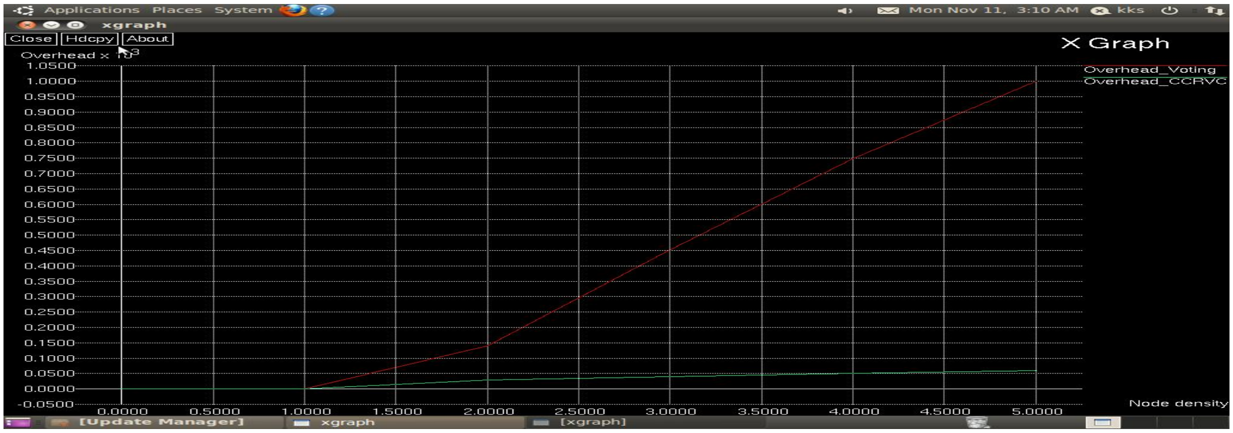


Fig 4a Communication overhead graph

Fig 4bWarned node graph

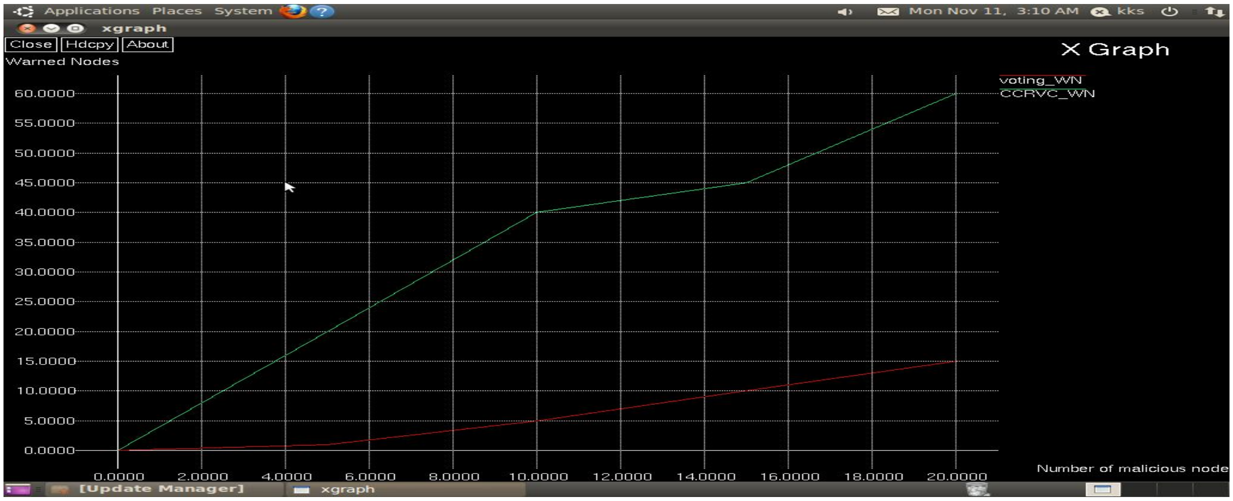
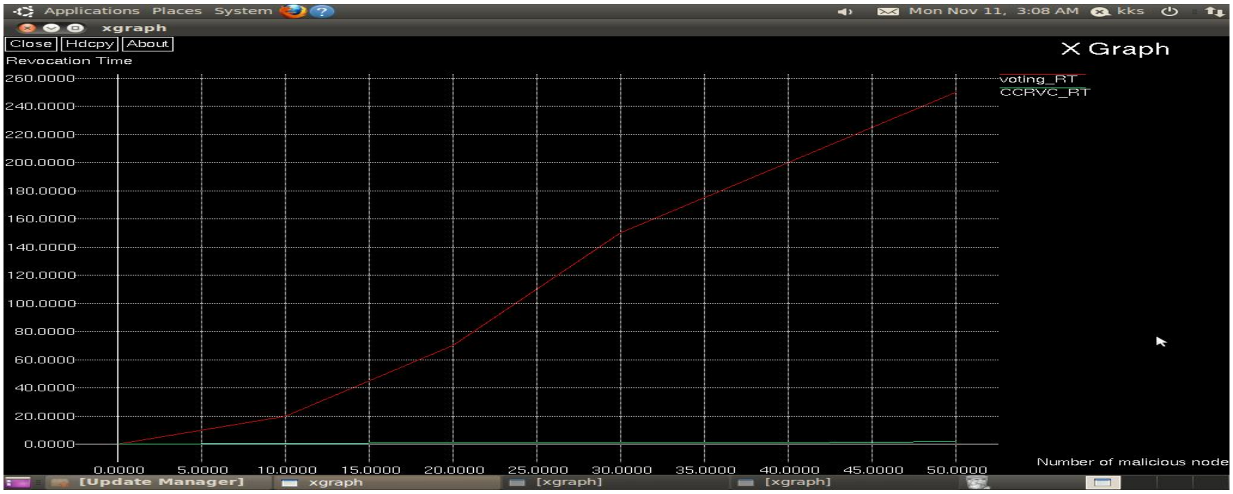


Fig 4c Revocation time graph



V. CONCLUSION

In this paper, addressed a major issue to ensure secure communications for mobile ad hoc networks, namely, certificate revocation of attacker nodes. In contrast to existing algorithms, we propose a cluster-based certificate revocation with vindication capability scheme combined with the merits of both voting-based and non-voting based mechanisms to revoke malicious certificate and solve the problem of false accusation. The scheme can revoke an accused node based on a single node's accusation, and reduce the revocation time as compared to the voting-based mechanism. In addition, we have adopted the cluster-based model to restore falsely accused nodes by the CH, thus improving the accuracy as compared to the non-voting based mechanism.

Particularly, we have proposed a new incentive method to release and restore the legitimate nodes, and to improve the number of available normal nodes in the network. In doing so, we have sufficient nodes to ensure the efficiency of quick revocation. The extensive results have demonstrated that, in comparison with the existing methods, our proposed CCRVC scheme is more effective and efficient in revoking certificates of malicious attacker nodes, reducing revocation time, and improving the accuracy and reliability of certificate revocation. Improve QOS metrics such as throughput, delay, Packet delivery ratio, Lifetime are to be increased.

REFERENCE

[1]. Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc NetworksWei Liu, Student Member, IEEE, Hiroki Nishiyama, Member,IEEE, Nirwan Ansari, Fellow, IEEE, Jie Yang, and Nei Kato, Senior Member, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 2, FEBRUARY 2013

[2]. 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.

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

[4].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.

[5].K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks," Proc IEEE 71st Vehicular Technology Conf. (VTC '10),May 16-19, 2010.

[6] S. Micali, "Efficient Certificate Revocation,"Massachusetts Inst.Of Technology, Cambridge, MA, 1996.

[7] C. Gentry, "Certificate-Based Encryption and the Certificate Revocation Problem," EUROCRYPT: Proc. 22nd Int'l Conf.ations of Cryptographic Techniques, 2003.

[8] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 261-273, Feb.2006.

[9] 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.

[10] 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

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