Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks

Wei Liu, *Student Member*, *IEEE*, Hiroki Nishiyama, *Member*, *IEEE*, Nirwan Ansari, *Fellow*, *IEEE*, Jie Yang, and Nei Kato, *Senior Member*, *IEEE*

Abstract—Mobile ad hoc networks (MANETs) have attracted much attention due to their mobility and ease of deployment. However, the wireless and dynamic natures render them more vulnerable to various types of security attacks than the wired networks. The major challenge is to guarantee secure network services. To meet this challenge, certificate revocation is an important integral component to secure network communications. In this paper, we focus on the issue of certificate revocation to isolate attackers from further participating in network activities. 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.

Index Terms—Mobile ad hoc networks (MANETs), certificate revocation, security, threshold

1 Introduction

Mobile ad hoc networks (MANETs) 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, cellphones, and Personal Digital Assistants (PDAs), which can freely move in the network. In addition to mobility, mobile devices cooperate and forward packets for each other to extend the limited wireless transmission range of each node by multihop relaying, which is used for various applications, e.g., disaster relief, military operation, and emergency communications.

Security is one crucial requirement for these network services. Implementing security [1], [2] is therefore of prime importance in such networks. Provisioning protected communications between mobile nodes in a hostile environment, in which a malicious attacker can launch attacks to disrupt network security, is a primary concern. Owing to the absence of infrastructure, mobile nodes in a MANET have to implement all aspects of network functionality themselves; they act as both end users and routers, which relay packets for other nodes. Unlike the conventional network, another feature of MANETs is the open network environment where nodes can join and leave the network freely. Therefore, the wireless and dynamic natures of MANETs expose them more vulnerable to various types of security attacks than the wired networks.

Among all security issues in MANETs, certificate management is a widely used mechanism which serves as a means of conveying trust in a public key infrastructure [3], [4] to secure applications and network services. A complete security solution for certificate management should encompass three components: prevention, detection, and revocation. Tremendous amount of research effort has been made in these areas, such as certificate distribution [5], [6], attack detection [7], [8], [9], [10], and certificate revocation [11], [12], [13], [14], [15], [16], [17]. 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 who 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.

- *W. Liu, H. Nishiyama, and N. Kato are with the Graduate School of Information Sciences, Tohoku University, No. 3 Building of ECEI Aobayama 6-3-09, Sendai 980-8579, Japan. E-mail: {liuwei, bigtree, kato}@it.ecei.tohoku.ac.jp.*
- *N. Ansari is with the Advanced Networking Laboratory, Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102. E-mail: Nirwan.Ansari@njit.edu.*
- *J. Yang is with School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China. E-mail: janeyang@bupt.edu.cn.*

Manuscript received 9 Nov. 2011; revised 14 Feb. 2012; accepted 16 Feb. 2012; published online 2 Mar. 2012.
Recommended for acceptance by V. Misic.
For information on obtaining reprints of this article, please send e-mail to: tpds@computer.org, and reference IEEECS Log Number TPDS-2011-11-0824.
Digital Object Identifier no. 10.1109/TPDS.2012.85.

The reminder of this paper is organized as follows: In Section 2, we give a brief overview of related works on certificate revocation techniques in MANETs, and we analyze both advantages and disadvantages of voting-based and non-voting-based schemes, focusing our attention on their merits to improve certificate revocation. Section 3 describes the structure of the proposed cluster-based scheme and introduces the certificate revocation process. In Section 4, we present a new threshold-based method to enhance the reliability and accuracy of the scheme. We devote Section 5 to the performance evaluation of our scheme. Finally, we conclude the paper in Section 6.

2 Related Work and Motivation

Recently, researchers pay much attention to MANET security issues. It is difficult to secure mobile ad hoc networks, notably because of the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, and the lack of infrastructure. Various kinds of certificate revocation techniques have been proposed to enhance network security in the literature. In this section, we briefly introduce the existing approaches for certificate revocation, which are classified into two categories: voting-based mechanism and non-voting-based mechanism.

2.1 Voting-Based Mechanism

The so-called voting-based mechanism is defined as the means of revoking a malicious attacker's certificate through votes from valid neighboring nodes.

URSA [14] proposed by Luo et al. uses a voting-based mechanism to evict nodes. The certificates of newly joining nodes are issued by their neighbors. The certificate of an attacker is revoked on the basis of votes from its neighbors. In URSA, each node performs one-hop monitoring, and exchanges monitoring information with its neighboring nodes. When the number of negative votes exceeds a predetermined number, the certificate of the accused node will be revoked. Since nodes cannot communicate with others without valid certificates, revoking the certificate of a voted node implies isolation of that node from network activities. Determining the threshold, however, remains a challenge. If it is much larger than the network degree, nodes that launch attacks cannot be revoked, and can successively keep communicating with other nodes. Another critical issue is that URSA does not address false accusations from malicious nodes.

The scheme proposed by Arboit et al. [15] allows all nodes in the network to vote together. As with URSA, no Certification Authority (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 weights. The weight of a node is calculated in terms of the reliability and trustworthiness of the node that is derived from its past behaviors, like the number of accusations against other nodes and that against itself from others. The stronger its reliability, the greater the weight will be acquired. The certificate of an accused node is revoked when the weighted sum from voters against the node exceeds a predefined threshold. By doing so, the accuracy of certificate revocation can be improved. However, since all nodes are required to participate in each voting, the communications overhead used to exchange voting information is quite high, and it increases the revocation time as well.

2.2 Non-Voting-Based Mechanism

In the non-voting-based mechanism, a given node deemed as a malicious attacker will be decided by any node with a valid certificate.

Clulow et al. [16] proposed a fully distributed "suicide for the common good" strategy, where certificate revocation can be quickly completed by only one accusation. However, certificates of both the accused node and accusing node have to be revoked simultaneously. In other words, the accusing node has to sacrifice itself to remove an attacker from the network. Although this approach dramatically reduces both the time required to evict a node and communications overhead of the certificate revocation procedure due to its suicidal strategy, the application of this strategy is limited. Furthermore, this suicidal approach does not take into account of differentiating falsely accused nodes from genuine malicious attackers. As a consequence, the accuracy is degraded.

Park et al. [17] proposed a cluster-based certificate revocation scheme, where nodes are self-organized to form clusters. In this scheme, a trusted certification authority is responsible to manage control messages, holding the accuser and accused node in the warning list (WL) and blacklist (BL), respectively. The certificate of the malicious attacker node can be revoked by any single neighboring node. In addition, it can also deal with the issue of false accusation that enables the falsely accused node to be removed from the blacklist by its cluster head (CH). It takes a short time to complete the process of handling the certificate revocation.

2.3 Motivation

As discussed above, we compare the advantages and disadvantages between voting-based and non-voting-based mechanisms. The significant advantage of the voting-based mechanism is the high accuracy in confirming the given accused node as a real malicious attacker or not. The decision process to satisfy the condition of certificate revocation is, however, slow. Also, it incurs heavy communications overhead to exchange the accusation information for each other. On the contrary, the non-voting-based method can revoke a suspicious misbehaved node by only one accusation from any single node with valid certification in the network. It is able to drastically simplify the decision-making process for rapid certificate revocation as well as reduce the communications overhead. However, the accuracy of determining an accused node as a malicious attacker and the reliability of certificate revocation will be degraded as compared with the voting-based method. We emphasize the significant performance difference between voting-based and non-voting-based methods: the former achieves higher accuracy in judging a suspicious node, but takes a longer time; the latter can significantly expedite the revocation process.

In this paper, we propose a Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme. Like our previously proposed cluster-based schemes [17],

[18], clustering is incorporated in our proposed scheme, where the cluster head plays an important role in detecting the falsely accused nodes within its cluster and recovering their certificates to solve the issue of false accusation. On the other hand, CCRVC inherits the merits of both the voting-based and non-voting-based schemes, in achieving prompt revocation and lowering overhead as compared to the voting-based scheme, improving the reliability and accuracy as compared to the non-voting-based scheme. Our scheme can quickly revoke the malicious device's certficate, stop the device access to the network, and enhance network security.

3 Model of the Cluster-Based Scheme

In this section, we introduce the model of the proposed cluster-based revocation scheme, which can quickly revoke attacker nodes upon receiving only one accusation from a neighboring node. The scheme maintains two different lists, warning list and blacklist, in order to guard against malicious nodes from further framing other legitimate nodes. Moreover, by adopting the clustering architecture, the cluster head can address false accusation to revive the falsely revoked nodes.

Owing to addressing only the issue of certificate revocation, not certificate distribution, the scheme assumes that all nodes have already received certificates before joining the network. On the other hand, we focus on the procedure of certificate revocation once a malicious attacker has been identified, rather than the attack detection mechanism itself. Each node is able to detect its neighboring attack nodes which are within one-hop away [8], [19].

3.1 Cluster Construction

We present the cluster-based [20] architecture to construct the topology. 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. While a node takes part in the network, it is allowed to declare itself as a CH with a probability of R. Note that neighbor sensing protocols, such as periodical broadcast of hello messages, are effective approaches used in routing protocols to check the availability of links between neighboring nodes. A new link is detected if a node receives a new hello message. Otherwise, the link is considered disconnected if none of the hello messages is received from the neighboring node during a time period.

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 T_u.

We note that each CM is assumed to belong to two different clusters in order to provide robustness against changes in topology. In case a CM moves out of the transmission range of its CH, it has to search for other CHP to participate in a new cluster. Especially, if the node does not receive any CHP for a certain period of time $2T_u$, namely, there is no CH within its one-hop range, it will declare itself as a CH and propagate CHP to form a new cluster. On the other hand, in case a CH has no CM in its neighborhood range, but if there are other CHs in its neighborhood, this node assigns itself as a CM to communicate with two of the CHs.

3.2 Function of Certification Authority

A trusted third party, certification authority, is deployed in the cluster-based scheme to enable each mobile node to preload the certificate. The CA is also in charge of updating two lists, WL and Blacklist, which are used to hold the accusing and accused nodes' information, respectively. Concretely, 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. This will be detailed in the threshold mechanism described in Section 4. Furthermore, the CA broadcasts the information of the WL and BL to the entire network in order to revoke the certificates of nodes listed in the BL and isolate them from the network.

3.3 Reliability-Based Node Classification

According to the behavior of nodes in the network, three types of nodes are classified according to their behaviors: legitimate, malicious, and attacker nodes. A **legitimate node** 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** does not execute protocols to identify misbehavior, vote honestly, and revoke malicious attackers. In particular, it is able to falsely accuse a legitimate node to revoke its certificate successfully. The so-called **attacker node** is defined as a special malicious node which can launch attacks on its neighbors to disrupt secure communications in the network.

In our scheme, these nodes can be further classified into three categories based on their reliability: **normal node**, **warned node**, and **revoked node**. When a node joins the network and does not launch attacks, it is regarded as a normal node 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 deemed as warned nodes with low reliability. Warned nodes are considered suspicious because the warning list contains a mixture of legitimate nodes and a few malicious nodes (see Section 3.4.2). 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

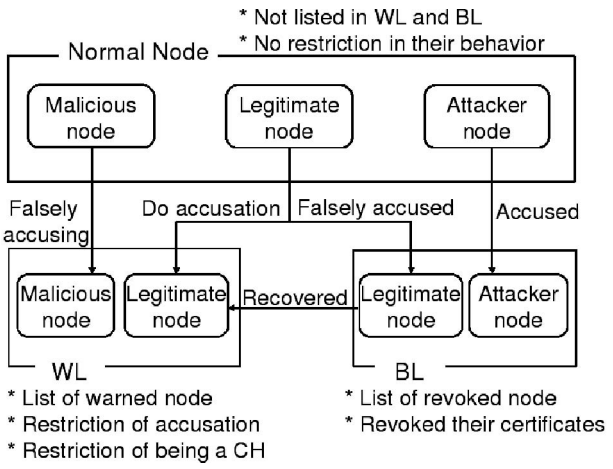


Fig. 1. The classification of nodes in our scheme.

blacklist are regarded as revoked nodes with little reliability. Revoked nodes are considered as malicious attackers deprived of their certificates and evicted from the network. The classification of these kinds of nodes is summarized in Fig. 1.

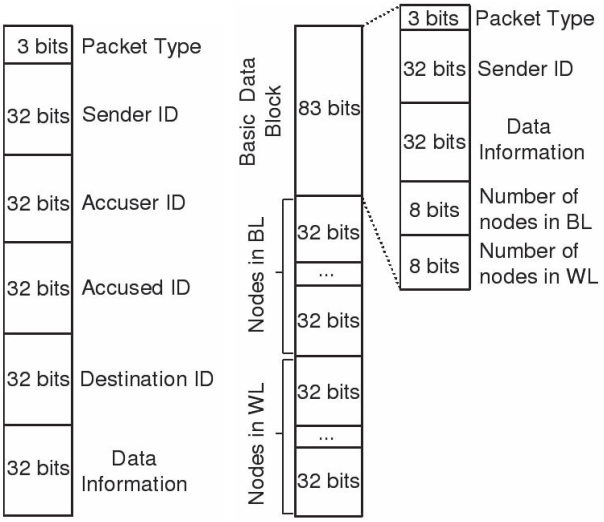
3.4 Certificate Revocation

3.4.1 Procedure of Revoking Malicious Certificates

We present the process of certificate revocation in this section. 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 is shown in Fig. 2a. 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 (see the format of broadcasting packet in Fig. 2b) including the WL and BL through the whole network by the CA, nodes that are in the BL are successfully revoked from the network.

For example, suppose that a malicious attacker M widely launches attacks within one-hop transmission range, as shown in Fig. 3, the procedure of revocation is described in the following:

- **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 M in 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.



(a) Format of accusation and recovery packets. (b) Format of broadcasting packet.

Fig. 2. Control packets.

3.4.2 Coping with False Accusation

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 in Fig. 2a) 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. Then, the CH sends a recovery packet to the CA in order to vindicate and revive this member from the network. When the CA accepts the recovery packet and verifies the validity of the sender, the falsely accused node will be released from the BL and held in the WL. Furthermore, the CA propagates this information to all the nodes through the network. Fig. 4 illustrates the process of addressing false accusation as follows:

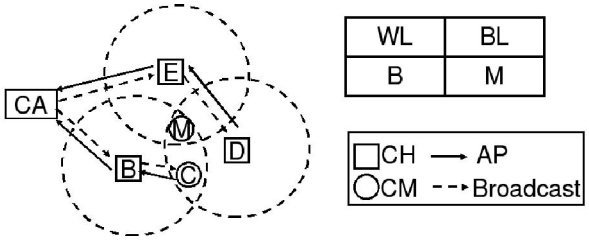


Fig. 3. Revoking a node's certificate.

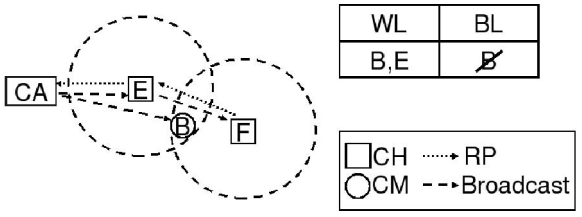


Fig. 4. Dealing with false accusation.

- **Step 1.** The CA disseminates the information of the WL and BL to all nodes in the network.
- **Step 2.** CH E and F update their WL and BL, and determine that node B was framed.
- **Step 3.** E and F send a recovery packet to the CA to revive the falsely accused node B.
- **Step 4.** Upon receiving the first recovery packet (e.g., from E), the CA removes B from the BL and holds B and E in the WL, and then disseminates the information to all the nodes.
- **Step 5.** The nodes update their WL and BL to recover node B.

4 WL Management

4.1 Normal Nodes Depreciation

Nodes enlisted in the WL by certificate revocation lose the function of accusation since the CA does not accept accusation packets from nodes enlisted in the WL in order to prevent further damage from malicious nodes. Thus, as the number of malicious nodes increases, an increasing number of normal nodes are listed in the WL; subsequently, there will not be enough normal nodes to accuse the attacker nodes over time. Such scenario will affect the reliability of the scheme.

Intuitively, if there are sufficient normal nodes around malicious attackers, the scheme is efficient in revoking attackers rapidly. On the contrary, if no normal node is available around an attacker node which is launching attacks to the neighborhood, the scheme cannot detect and revoke this attacker immediately until a normal node roams into the attacker's transmission range.

In a MANET, mobile nodes are assumed to be uniformly distributed over a coverage area so as to satisfy the binomial distribution $B(n, q)$ [21], which denotes the probability of a number of nodes existing in a special area. Herein, n denotes the total number of cells where a MANET is divided into; q is the probability that one cell is occupied by a single node. When n is very large and q is very small, the binomial distribution $B(n, q)$ is approaching the Poisson distribution with parameter λ, which is equal to the number of nodes, nq. Consequently, the probability that there are exactly m normal nodes (m being a nonnegative integer, $m = 0, 1, 2, \ldots$) within the transmission area S of an attacker node, is equal to

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

where ρ denotes the node density and θ means the proportion of normal nodes in the network.

As analyzed above, the number of normal nodes is decreasing over time. When $m = 0$, i.e., no normal nodes within an attacker's transmission range, the probability is

$$Pr(m = 0) = e^{-\theta\rho S}. \quad (2)$$

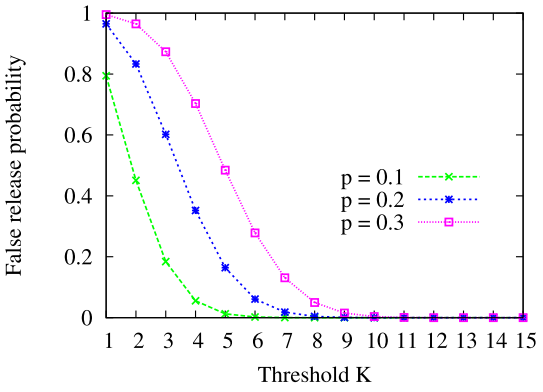
From (2), the probability $Pr(m = 0)$ greatly increases with the decrease of density ρ; the efficiency of detecting malicious attackers is significantly reduced. In other words, the probability $Pr(m = 0)$ must be reduced to guarantee a certain number of normal nodes in the network to revoke malicious attackers quickly. Consequently, the legitimate nodes should be released from the WL and be restored of their accusation function to increase the number of available normal nodes in order to enhance the robustness and reliability against the decreasing number of normal nodes over time.

4.2 Node Releasing

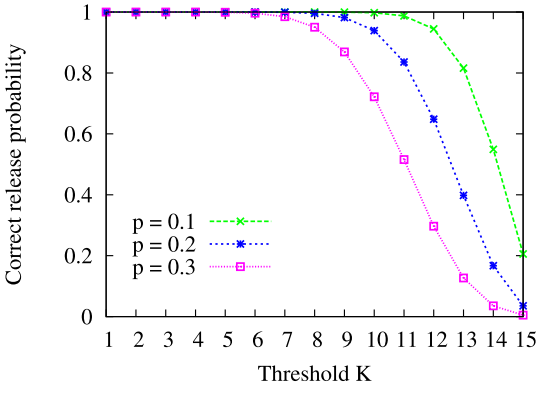
As a solution to release nodes from the WL, we should first consider the two cases for nodes to be listed in the WL. As shown in Fig. 1, the first case is that a legitimate node correctly accuses an attacker node, thus resulting in the accusing node and accused node being listed in the WL and BL, respectively; the other case is the enlisting of a malicious node in the WL because it sends false accusation against a legitimate node. Hence, nodes in the WL may be legitimate nodes as well as malicious nodes. Therefore, to improve the reliability and accuracy, nodes must be differentiated between legitimate nodes and malicious nodes so as to release legitimate nodes from the WL and withhold malicious nodes in the WL.

To distinguish legitimate nodes from malicious nodes, we propose a node releasing mechanism to evaluate and release legitimate nodes from the WL. First of all, we design a counter for the CA to record the number of accusations against each accused node. Moreover, the CA continues to receive accusations against the accused node following a voting period of time, T_v, which is used for collecting accusations and releasing legitimate nodes from the WL, and subsequently compare the number of received accusations with the threshold K. In this method, we consider the accused node as a real attacker if and only if the number of accusations reaches threshold K. In the mean time, we can finally vindicate the corresponding accusing node as a legitimate node so as to release it from the WL as well as restore its function as the normal node. Otherwise, if the number of accusations fails to reach threshold K, the related accusing node will be detained in the WL. Particularly, in a special case, if the time T_v is set to infinite, our scheme is similar to the non-voting-based scheme since the legitimate node in the WL cannot satisfy the release condition. As a consequence, determining the value of threshold K is essential for reliability and accuracy of our scheme.

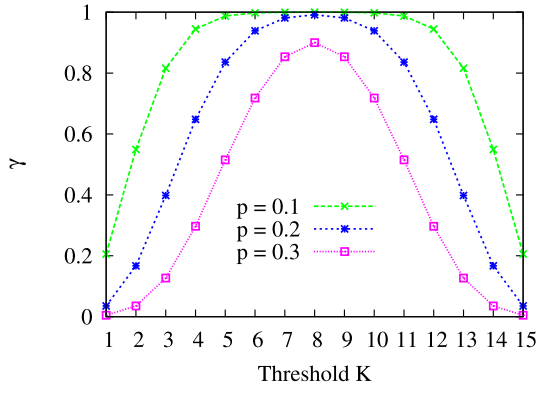
Conventional voting mechanisms set the threshold K as a constant value; for example, K is greater than the number of malicious nodes in the MANET. However, if the threshold is set too big, it will take a long time to determine whether a warned node is a legitimate node because the scheme has to wait for more accusations to reach the verdict; a malicious attacker may never be identified because of lack of adequate support from neighboring nodes. Conversely, if the



(a) The change of P_f.



(b) The change of P_c.



(c) The change of γ.

Fig. 5. Impact of threshold K on P_f, P_c, and γ for different values of p with $N = 15$.

predefined threshold is set too small, revoked malicious nodes can be released from the WL by other malicious nodes through collusion. To mitigate these extreme cases, we propose to determine the optimum threshold value K based on the number of neighboring nodes and the employed security policy.

4.3 Policies for Determining the Threshold

We first design a simplified mechanism to determine the number of neighboring nodes for any given node. Within time T_v, the given node crosses through an area and meets a number of neighbors N. Since mobile nodes are assumed uniformly distributed in the network, we may approximate N by

$$N = (\pi r^2 + 2rvT_v)\rho, \tag{3}$$

where r denotes the transmission range of nodes, v is the velocity, and ρ is the density of nodes in the network. Based on the obtained number of neighboring nodes N, we can confirm the value of threshold K. In the following, we detail three policies in determining the optimal value of threshold K.

4.3.1 Policy 1: Minimizing False Release Probability

In the first policy, we decide K in terms of the probability P_f that no less than K out of N neighbors falsely accuse the given node. In other words, P_f denotes the probability that a legitimate node is framed by at least K colluding nodes so that the malicious node is released erroneously. This probability is expressed as follows:

$$P_f(K) = \sum_{i=K}^{N} \binom{N}{i} p^i (1-p)^{N-i}. \tag{4}$$

Here, p denotes the probability of a node which participates in false accusation. For instance, Fig. 5a shows that (4) is a monotonically decreasing function where we set N as 15. From the figure, we can observe that the greater the threshold K is, the fewer the malicious node is falsely released, and thus the higher the accuracy is. Consequently, we expect to acquire the minimum value of P_f to reduce the probability of falsely releasing nodes from the WL. We can acquire the value K based on an acceptable range of P_f.

4.3.2 Policy 2: Maximizing Correct Release Probability

In the second policy, we determine the value of K on the basis of the probability P_c that no less than K out of N neighboring nodes can correctly accuse the attacker so that a legitimate node will be successfully released from the WL. We have the expression

$$P_c(K) = \sum_{i=K}^{N} \binom{N}{i} (1-p)^i p^{N-i}, \tag{5}$$

where $(1-p)$ means the probability of a node which participates in correct accusation. In order to achieve a high probability of successfully releasing legitimate nodes from the WL, the value of P_c should be large. As shown in Fig. 5b, P_c drops as the threshold K increases. It illustrates that the probability that a legitimate node is permanently held in the WL increases when K becomes large.

4.3.3 Policy 3: Maximizing Accuracy

We know that there is a tradeoff between the false release probability P_f and correct release probability P_c in determining the value of threshold K. From Figs. 5a and 5b, it can be seen that while both P_f and P_c decrease with the growth of K, P_f decreases in a much more rapid manner as compared to P_c. We would like to choose an appropriate value of K to achieve the maximum accuracy of releasing nodes that can increase correct release probability while simultaneously maintain low false release probability. To this end, we propose to use $\gamma(K)$ to determine the optimum threshold, where $\gamma(K)$ equals the difference between P_c and P_f,

TABLE 1
Numerical Results for K ($N = 15$)

p	Policy 1($P_f \leq \alpha$)		Policy 2($P_c \geq \beta$)		Policy 3
	$\alpha = 0.1$	$\alpha = 0.2$	$\beta = 0.9$	$\beta = 0.8$	
0.1	4	3	12	13	8
0.2	6	5	10	11	8
0.3	8	7	8	9	8

$$\begin{aligned}\gamma(K) &= P_c(K) - P_f(K) \\ &= \sum_{i=K}^{N} \binom{N}{i} \{(1-p)^i p^{N-i} - p^i (1-p)^{N-i}\}. \end{aligned} \quad (6)$$

Note that, in our scheme, the total number of malicious nodes and attacker nodes is supposed to be less than the number of legitimate nodes in MANETs. Namely, $(1-p)$ is greater than p. Taking $N = 15$, for example, Fig. 5c shows that the curve of $\gamma(K)$ is the maximum when K is equal to $\frac{N}{2}$, i.e., our desired optimal number.

Here, we prove that $\gamma(K)$ achieves the maximum when K equals to $\frac{N}{2}$. On the basis of (6), we only need to show that $\gamma(K)$ is monotonically increasing for K belongs $[0, \frac{N}{2}]$ and is monotonically decreasing for K belongs $[\frac{N}{2}, N]$. Let $K_1 < K_2$ and check whether the value of $(\gamma(K_2) - \gamma(K_1))$ is positive or not. When $0 \leq K1 < K2 \leq N$, we have

$$\begin{aligned}&\gamma(K_2) - \gamma(K_1) \\ &= -\sum_{K=K_1}^{K_2-1} \binom{N}{K} \{(1-p)^K p^{N-K} - p^K (1-p)^{N-K}\} \\ &= -\sum_{K=K_1}^{K_2-1} A\{p^{\frac{N}{2}-K} - (1-p)^{\frac{N}{2}-K}\}, \end{aligned} \quad (7)$$

where $A = \binom{N}{K}\{(1-p)^K p^{\frac{N}{2}} + (1-p)^{\frac{N}{2}} p^K\}$. Since $A > 0$ and $p < (1-p)$, we can conclude that $\gamma(K)$ is monotonically increasing in $K \in [0, \frac{N}{2}]$ $(\gamma(K_2) > \gamma(K_1))$ and monotonically decreasing in $K \in [\frac{N}{2}, N]$ $(\gamma(K_2) < \gamma(K_1))$. As a consequence, when K is equal to $\frac{N}{2}$, $\gamma(K)$ achieves the maximum.

4.3.4 Summary

In this section, we have introduced three policies to calculate the threshold value. By using Policies 1 or 2, we should first set the value of α or β to get the threshold K, respectively. We know that the less α is, the larger the threshold is. In other words, P_f decreases as α decreases. However, while P_f is decreasing, P_c is also decreasing, thus leading to decreased probability of releasing legitimate nodes from the WL, and vice versa. As shown in Table 1, according to different values of α and β, we can clearly observe that K varies with different settings. Consequently, to determine the optimal threshold K to keep balance between P_f and P_c, we adopt Policy 3 in our proposed scheme that can achieve maximum accuracy to judge the identity of nodes in the WL, thus enhancing the correct release probability while maintaining low false release probability simultaneously. In particular, the threshold K can be calculated independently of α and β. From Table 1, the results show that K is constant and equal to $\frac{N}{2}$ when γ obtains the maximum accuracy by using Policy 3, regardless of other parameters.

TABLE 2
Simulation Parameters

Parameter	Value
Node placement	Uniform distribution
Mobility model	Random waypoint
Terrain dimensions	1000m x 1000m
Trans. range	250m
Node speed	1m/s-10m/s
CH chosen probability, R	0.3
Cluster update interval, T_u	20s
Voting time period, T_v	10s
Simulation Time	600s

5 Performance Evaluation

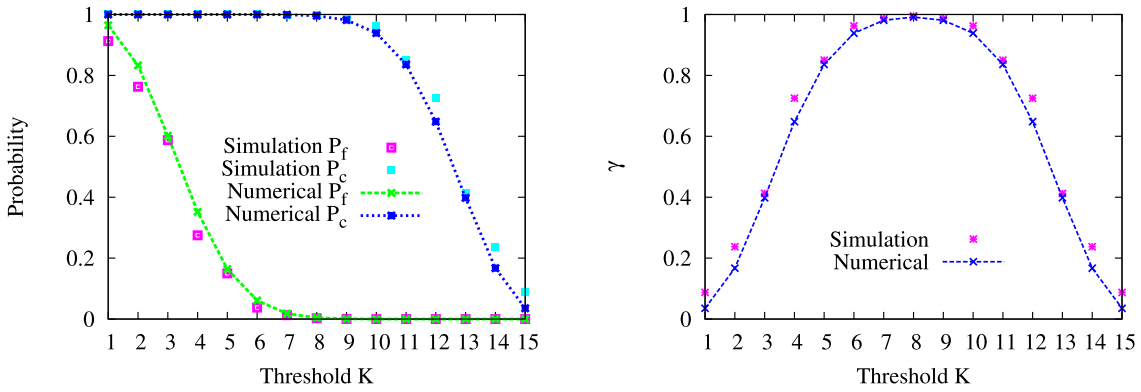
In this section, we present simulation results conducted in the network simulator, Qualnet 4.0 [22]. To demonstrate the optimal threshold K, we design the experiment to measure P_f and P_c in comparison with those of numerical results, and observe the impact of different threshold values on γ. To evaluate the performances of our proposed CCRVC scheme, we run simulations to verify its efficiency in releasing legitimate nodes from the WL and revoking attacker nodes' certificates, and compare them with the existing schemes. In particular, we are interested in the revocation time to evaluate the efficiency and reliability of certificate revocation in the presence of malicious attacks. Furthermore, we also estimate the accuracy of releasing legitimate nodes in our CCRVC scheme.

5.1 Simulation Setup

We consider a realistic environment, where there are many devices (mobile phones, laptops, PDAs, etc.) to construct a mobile ad hoc network within a certain area (campus, station, etc.). These devices move randomly and communicate with their neighboring devices in the network. We simulate this MANET environment within 1,000 m by 1,000 m terrain in Qualnet simulator for 802.11b, running ad hoc on-demand distance vector (AODV) as the routing protocol. The devices are deployed in a random uniform distribution, and each device is seen as a node which has the fixed transmission range as 250 m. The random way-point mobility pattern [23], [24] is used to model node movements. Each node is assumed to move to a randomly selected location at different velocities from 1 to 10 m/s. The probability R that the newly joining node becomes a CH is 0.3. CH and CMs are sensing each other with Hello packets in every time interval T_u. The voting time T_v is set to 10 s. For each experiment, we get the average results from 50 simulation runs. Table 2 specifies the important parameters used in the simulation.

5.2 Deriving the Optimal Threshold K

In this simulation, we prove the optimum threshold value in comparison with the numerical result. We set 80 nodes in the network, which contains eight malicious nodes and eight attacker nodes. According to the aforementioned numerical results listed in Table 1, we run the simulation with the specific values of $N = 15$, where K is varied from 1 to N, to determine whether a warned node is a legitimate or a malicious node. Based on the number of accusations against each accused node, we can acquire the values of P_f



(a) Comparison of P_f and P_c. (b) Impact of threshold K on γ.

Fig. 6. Comparison of the numerical and simulation results on P_f, P_c, and γ where $N = 15$.

and P_c. In particular, we focus on the value of γ, obtained by using the policy 3.

As shown in Fig. 6a, the simulation results of P_f and P_c demonstrate that they are close to the mathematically analyzed results. Additionally, Fig. 6b shows the change of γ, which is related to the values of P_f and P_c. To determine the optimal value of K, which enables our scheme to achieve the maximum accuracy, the plot in Fig. 6b indicates that, the value of γ is the maximum when the threshold K is set to 8. As a consequence, the optimal threshold K is equal to $\frac{N}{2}$, which is indeed consistent with the mathematical analysis. In conclusion, the simulation results closely align with the numerical results.

5.3 Comparing the Effectiveness of Certificate Revocation

Since the threshold method is able to release nodes from the WL, to evaluate the effectiveness of our CCRVC scheme, we first observe the change of the number of nodes in the WL according to different number of malicious nodes, and compare it with our previously proposed scheme [17]. In this experiment, we deploy 100 nodes in the network, where both the number of malicious and attacker nodes are set to 5, 10, 15, and 20 for each simulation run, respectively. We examine the impact of different malicious nodes on the number of nodes in the WL. Fig. 7 clearly demonstrates that it can effectively reduce the number of nodes listed in the WL, i.e., the number of available nodes in the network has been improved by using the CCRVC scheme. We can see that the number of nodes listed in the WL is almost equal to the number of malicious nodes. Actually, almost all the malicious nodes are successfully kept in the WL.

Revocation time is an important factor for evaluating the performance of the revocation scheme. Revocation time is defined as the time from an attacker node's launching the attack until its certificate is revoked. To evaluate the impact of different numbers of attacker nodes on the revocation time, 50 legitimate nodes are considered in the network, while the number of attacker nodes is varied from 10 to 50. Fig. 8 presents how the revocation time changes with different numbers of attacker nodes between the existing schemes (i.e., voting-based scheme [14] and non-voting-based scheme [17]) and the CCRVC scheme. Note that as the number of attacker nodes is not larger than the number of legitimate nodes, the results always converge because there are enough legitimate nodes to revoke attackers' certificates within finite time in our simulation. Obviously, the voting-based scheme requires longer revocation time than that of our proposed scheme. This is because the voting-based scheme needs to wait for multiple votes to make a decision for revoking while the CCRVC scheme requires a single vote only. In addition, the results show that, even if the number of malicious attacker nodes is increased to 50, the revocation time tends to increase gracefully and slowly and does not exceed 50s by using our proposed scheme. The non-voting-based scheme has to take a long time to revoke the certificates of attacker nodes as the

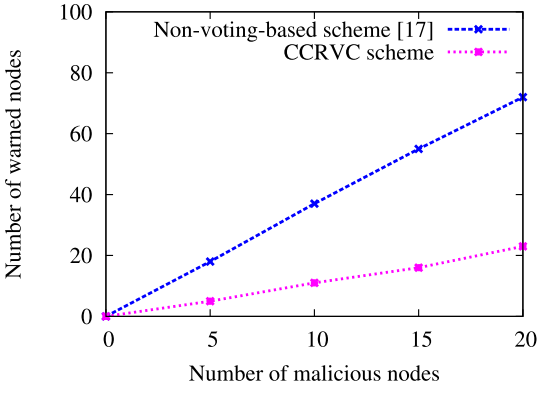


Fig. 7. The number of warned nodes in WL.

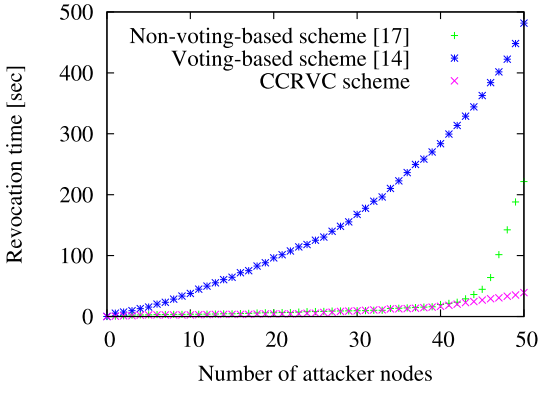


Fig. 8. Revocation time.

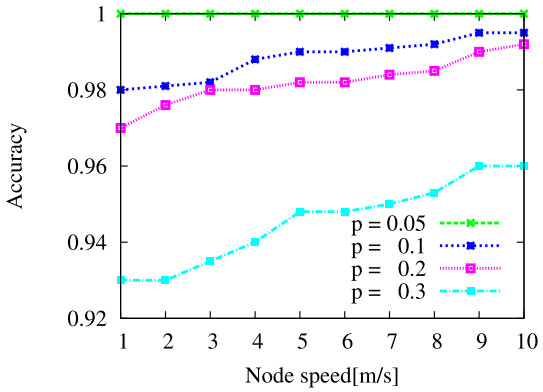


Fig. 9. Impact of node speed on accuracy.

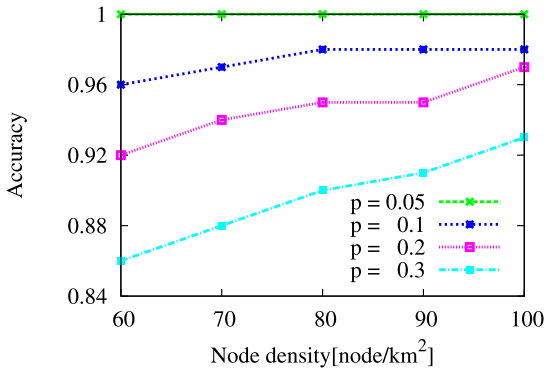


Fig. 10. Impact of node density on accuracy.

number of normal nodes decreases. Consequently, we can conclude that, by adopting CCRVC, revocation time is significantly reduced as compared to the voting-based scheme. Moreover, it is able to revoke a node's certificate as fast as the non-voting-based scheme does. Particularly, even if a large number of attacker nodes exist in a MANET, our scheme can substantially improve the reliability and reduce the revocation time as compared to the non-voting-based scheme since it ensures sufficient available nodes in the network.

5.4 Accuracy of Releasing Nodes

To study the accuracy of releasing nodes from the WL by using our proposed CCRVC scheme, we first define the accuracy as

$$Accuracy = 1 - R_{false} - R_{unreleased}, \tag{8}$$

where R_{false} denotes the probability of the falsely released nodes and $R_{unreleased}$ means the probability of the unreleased legitimate nodes (legitimate nodes enlisted in the WL have not been correctly released). We examine the change of the accuracy in terms of different values of speed and density of the nodes.

Fig. 9 demonstrates the impact of different node speeds on the accuracy of the revoked nodes. Here, we deploy 100 nodes in the network, in which both the numbers of malicious nodes and attacker nodes are set to 5, 10, and 15 for each simulation, respectively. In other words, the ratio of the malicious and attacker nodes to the total number of nodes, p, is equal to 0.1, 0.2, and 0.3, respectively. Node speed is fixed from 1 to 10 m/s, respectively. As noted from the figure, the accuracy is gradually improving with the increasing speed. This is because the faster the nodes move, the larger the number of neighboring nodes becomes, leading to a higher value of the threshold K. On the other hand, as p increases, the accuracy degrades.

Fig. 10 demonstrates the effect of node density on the accuracy, as the node density varies from 60 to 100 nodes/km^2. Both of the malicious nodes and attacker nodes are set to account for 5, 10, and 15 percent of the total number of nodes in the simulation, respectively. The accuracy continues to improve with the increase of the node density.

In particular, as the number of attackers and malicious nodes is above the threshold K in our simulations, the accuracy cannot reach 100 percent because of the situation that almost all these nodes located in the same place falsely accuse a legitimate node simultaneously. However, if the number of these nodes is below the threshold K, they cannot collude false accusations successfully. For example, with p set to 0.05 in these two experiments, the results shown in Figs. 9 and 10 indicate that the accuracy can reach 100 percent because there are not enough nodes to successfully falsely accuse a legitimate node.

Based on the above analysis, the results demonstrate that our scheme can maintain high accuracy in distinguishing legitimate nodes from malicious nodes and releasing legitimate nodes from the WL, especially the number of falsely accusing nodes is less than the threshold K.

5.5 Summary

In summary, the simulation results substantiate the performance of the CCRVC scheme: 1) the threshold $K = \frac{N}{2}$ is the optimum value to distinguish legitimate nodes from malicious nodes; 2) the proposed scheme exhibits more reliable and higher efficiency as compared to the existing ones, because it guarantees sufficient normal nodes to revoke the certificates of the attackers and takes a short revocation time; 3) it achieves high accuracy in releasing legitimate nodes.

6 Conclusion

In this paper, we have 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.

REFERENCES

[1] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," *IEEE Wireless Comm.,* vol. 11, no. 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 Comm.,* vol. 14, no. 5, pp. 8-20, Oct. 2007.

[3] A.M. Hegland, E. Winjum, C. Rong, and P. Spilling, "A Survey of Key Management in Ad Hoc Networks," *IEEE Comm. Surveys and Tutorials,* vol. 8, no. 3, pp. 48-66, Third Quarter 2006.

[4] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," *IEEE Network Magazine,* vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.

[5] L. Zhou, B. Cchneider, and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority," *ACM Trans. Computer Systems,* vol. 20, no. 4, pp. 329-368, Nov. 2002.

[6] H. Chan, V. 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, July 2005.

[7] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, "Resisting Flooding Attacks in Ad Hoc Networks," *Proc. Int'l Conf. Information Technology: Coding and Computing,* vol. 2, pp. 657-662, Apr. 2005.

[8] B. Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemoto, and N. Kato, "A Survey of Routing Attacks in MANET," *IEEE Wireless Comm. Magazine,* vol. 14, no. 5, pp. 85-91, Oct. 2007.

[9] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A Dynamic Anomaly Detection Scheme for Aodv-Based Mobile Ad Hoc Networks," *IEEE Trans. Vehicular Technology,* vol. 58, no. 5, pp. 2471-2481, June 2009.

[10] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Network: Analysis & Defenses," *Proc. Third Int'l Symp. Information Processing in Sensor Networks,* pp. 259-268, 2004.

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

[12] C. Gentry, "Certificate-Based Encryption and the Certificate Revocation Problem," *EUROCRYPT: Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques,* pp. 272-293, 2003.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] W. Liu, H. Nishiyama, N. Ansari, and N. Kato, "A Study on Certificate Revocation in Mobile Ad Hoc Network," *Proc. IEEE Int'l Conf. Comm. (ICC),* June 2011.

[19] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, "Resisting Flooding Attacks in Ad Hoc Networks," *Proc. Int'l Conf. Information Technology: Coding and Computing,* 2005.

[20] J. Lian, K. Naik, and G.B. Agnew, "A Framework for Evaluating the Performance of Cluster Algorithms for Hierarchical Networks," *IEEE/ACM Trans. Networking,* vol. 15, no. 6, pp. 1478-1489, Dec. 2007.

[21] 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," *Proc. Sixth ACM Int'l Symp. Mobile Ad hoc Networking and Computing,* pp. 254-265. 2005, Q1

[22] Scalable Network Technologies: Qualnet, http://www.scalable-networks.com, 2012.

[23] C. Bettstetter, G. Resta, and P. Santi, "The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Networks," *IEEE Trans. Mobile Computing,* vol. 2, no. 3, pp. 257-269, July-Sept. 2003.

[24] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," *Wireless Comm. and Mobile Computing (WCMC)* Special Issue on Mobile Ad Hoc Networking: Research, Trends, and Applications, vol. 2, no. 5, pp. 483-502, 2002.

Wei Liu received the BS and MS degrees in information engineering from Zhengzhou University, China, in 2003 and 2008, respectively. He is currently working toward the PhD degree at the Graduate School of Information Sciences at Tohoku University, Japan. His main research interests include Mobile Ad Hoc Networks, Security Network, and Key Management. He is a student member of the IEEE.

Hiroki Nishiyama received the MS and PhD degrees in information science from Tohoku University, Japan, in 2007 and 2008, respectively. He was a research fellow of the Japan Society for the Promotion of Science (JSPS) until finishing the PhD degree following which he went on to become an assistant professor at the Graduate School of Information Sciences at Tohoku University. He has received Best Paper Awards from the IEEE Global Communications Conference 2010 (GLOBECOM 2010) as well as the 2009 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC 2009). He was also a recipient of the 2009 FUNAI Foundation's Research Incentive Award for Information Technology. His active areas of research include, traffic engineering, congestion control, satellite communications, ad hoc and sensor networks, and network security. He is a member of the IEEE, Institute of Electronics, and Information and Communication Engineers (IEICE).

Nirwan Ansari (S'78-M'83-SM'94-F'09) received the BSEE (summa cum laude with a perfect GPA) degree from the New Jersey Institute of Technology (NJIT), Newark, in 1982, the MSEE degree from the University of Michigan, Ann Arbor, in 1983, and the PhD degree from Purdue University, West Lafayette, IN, in 1988. He joined the Department of Electrical and Computer Engineering, NJIT, as an assistant professor in 1988, tenured and promoted to an associate professor in 1993, and has been a full professor since 1997. He has also assumed various administrative positions with NJIT. He authored *Computational Intelligence for Optimization* (Berlin, Germany: Springer, 1997, translated into Chinese in 2000) with E.S.H. Hou, and edited *Neural Networks in Telecommunications* (Springer, 1994) with B. Yuhas. He has contributed more than 400 technical papers, over one third published in widely cited refereed journals/magazines. His current research interests include various aspects of broadband networks and multimedia communications. He guest-edited a number of special issues, covering various emerging topics in communications and networking. He was a visiting (chair) professor with several universities. He has served on the Editorial/Advisory Boards of eight journals, including as a senior technical editor of the IEEE Communications Magazine from 2006 to 2009. He has served the IEEE in various capacities such as the chair of the IEEE North Jersey COMSOC Chapter, the chair of the IEEE North Jersey Section, a member of the IEEE Region 1 Board of Governors, the chair of the IEEE COMSOC Networking TC Cluster, the chair of the IEEE COMSOC Technical Committee on Ad Hoc and Sensor Networks, and the chair/TPC chair of several conferences/symposia. He has been frequently invited to deliver keynote addresses, distinguished lectures, tutorials, and talks. Some of his recent recognitions include NJIT Excellence in Teaching in Outstanding Professional Development in 2008, the IEEE MGA Leadership Award in 2008, the NCE Excellence in Teaching Award in 2009, the Thomas Alva Edison Patent Award in 2010, a couple of best paper awards, and designation as an IEEE Communications Society Distinguished Lecturer from 2006 to 2009 (two terms). He was also awarded over 15 US patents. He is a fellow of the IEEE.

Jie Yang received the BE, ME, and PhD degrees from Beijing University of Posts and Telecommunications, shortly BUPT, China in 1993, 1999, and 2007, respectively. Currently she is an associate professor and deputy dean of School of Information and Communication Engineering, BUPT. Her research interests include broadband network technology, information theory in communication systems, network traffic monitoring, and P2P network technology.

Nei Kato received the MS and PhD degrees in information science from Tohoku University, Japan, in 1988 and 1991, respectively. He joined the Computer Center of Tohoku University in 1991, and has been a full professor at the Graduate School of Information Sciences since 2003. He has been engaged in research on computer networking, wireless mobile communications, image processing and neural networks, and has published more than 200 papers in journals and peer-reviewed conference proceedings. He currently serves as the chair of the IEEE Satellite and Space Communications Technical Community (TC), the secretary for the IEEE Ad Hoc & Sensor Networks TC, the vice chair of the IEICE Satellite Communications TC, a technical editor for *IEEE Wireless Communications* (since 2006), an editor of *IEEE Transactions on Wireless Communications* (since 2008), and as an associate editor of *IEEE Transactions on Vehicular Technology* (since 2009). He also served as a co-guest-editor for *IEEE Wireless Communications Magazine* SI on "Wireless Communications for E-healthcare," a symposium co-chair of GLOBECOM'07, ICC'10, ICC'11, ChinaCom'08, ChinaCom'09, and the WCNC2010-2011 TPC vice chair. His awards include the Minoru Ishida Foundation Research Encouragement Prize (2003), the Distinguished Contributions to Satellite Communications Award from the IEEE , Satellite and Space Communications Technical Committee (2005), the FUNAI information Science Award (2007), the TELCOM System Technology Award from the Foundation for Electrical Communications Diffusion (2008), the IEICE Network System Research Award (2009), and many best paper awards from prestigious international conferences such as IEEE GLOBECOM, IWCMC, and so on. Besides his academic activities, he also serves as a member on the Telecommunications Council expert committee, the special commissioner of the Telecommunications Business Dispute Settlement Commission, for the Ministry of Internal Affairs and Communications, in Japan, and as the chairperson of ITU-R SG4, in Japan. He is a senior member of the IEEE, member of the Institute of Electronics, Information and Communication Engineers (IEICE).