

Proposed Threshold Based Certificate Revocation in Mobile Ad Hoc Networks

Priti Swapnil Rathi and Parikshit N. Mahalle

Abstract Certification system plays an important role in mobile ad hoc networks (MANETs) to achieve network security. Handling the issue of certificate revocation in wired network is somewhat easy to compare the MANETs. In wired network, when the certificate of a malicious node get revoked, the certificate authorities add the information about the revoked node into certificate revocation lists (CRLs) or broadcast the CRL to each and every node present in the network or either store them on accessible repositories. Whereas the certificate revocation is a challenging task in MANETs and also this conventional method of certificate revocation is not useful for MANETs due to the absence of centralized repositories and trusted authorities. In this paper, we propose a threshold-based certificate revocation scheme for MANETs, which will revoke the certificate of malicious nodes as soon as it detects the first misbehavior of nodes. The proposed scheme also solves the improper certificate revocation, which can occur due to false accusations made by malicious node and also the problem of window of opportunity where revoked certificates are get assigned as a valid to new nodes.

Keywords MANET · Certificate authority (CA) · Certificate revocation · Digital certificate (DC)

P. S. Rathi (✉) · P. N. Mahalle
Department of Computer Engineering, STES's Smt. Kashibai Navle College of Engineering,
Pune, Maharashtra, India
e-mail: pritrathi2@gmail.com

P. N. Mahalle
e-mail: aalborg.pnm@gmail.com

1 Introduction

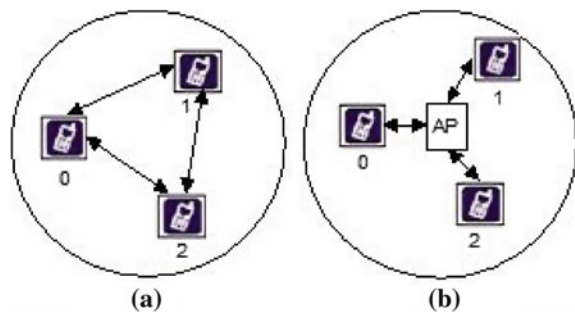
Mobile ad hoc networks (MANETs) are the collection of two or more mobile nodes where the communication between two nodes presents in ad hoc network done directly if they are within each other's radio range otherwise the communication can proceed in multihop fashion [1]. Each node can function as a sender, a receiver, or a router. Wireless network can operate in infrastructure or in ad hoc wireless network mode as shown in Fig. 1. Mobile image in Fig. 1 shows mobile nodes and the number below it indicates nodes number.

Infrastructure mode requires a wireless access point (WAP) to connect wireless node, whereas ad hoc mode does not require a WAP to connect wireless node as shown in Fig. 1. Every network has their own and unique characteristics; similarly, MANETs also have several unique characteristics such as infrastructure less network, dynamic topology, self-organizing, and self-configuring. These unique characteristics of MANETs will create different challenges, different attacks and opportunities to achieve security goal [1, 2].

One of the core security issues in MANETs is trust management. Trust is generally established and managed in wired and other wireless networks via centralized entities, such as CAs or key distribution center (KDC). The absence of centralized entities in MANETs makes it challenging task. It also creates problem to perform necessary functions such as revocation of DC, issue of false accusation. In this false accusation problem, the malicious node will try to prove the legitimate node as malicious node due to which legitimate node gets removed from the network [3]. The malicious nodes can cause various communication problems such as window of opportunity problem where revoked certificates get assigned as a valid.

Certification system plays an important role in MANETs to achieve security as well as to remove the attackers from the network [4]. The networks that make use of certification system to achieve security, and the nodes in that network are able to communicate with each other if and only if they are having valid, not expired certificate otherwise not. The node whose certificate is revoked does not receive any data from other valid nodes. Certificate revocation scheme plays an important

Fig. 1 Wireless network types



role in network, which makes use of certification system. This scheme helps to revoke the certificate of malicious node.

The main aim of this paper is to make use of threshold cryptography scheme and solve the above-mentioned MANETs security issues such as implementing better trust management, revoking certificate of malicious nodes only, solving false accusation and window of opportunity problem.

2 Related Work

For conventional networks, CA issues CRLs [5]. The CRLs give information about the nodes whose certificate has been revoked at regular intervals. The CRLs placed in online repositories where either they are readily available to nodes or they may be broadcast to the individual nodes. Alternatively, different certificate validation protocols are used for conventional networks that are online certificate status protocol (OCSP), CRLs but these certificate validation protocols used in conventional network are not suitable for MANETs to achieve security due to the absence of centralized repositories and unavailability of CA. Following are the different challenges associated with adapting this certificate validation protocol to MANETs.

2.1 Evaluation of Related Work

- In any ad hoc networks, there is no network connection to centralized CAs or to central repositories where CRLs get stored and retrieved when there is need to find out the status of certificate.
- Certificate revocation is too important and challenging issue in MANET, so if adequate safeguards are not built into the process of determining when a certificate should be revoked, then malicious nodes can wrongfully accuse other nodes of misbehavior and due to this certificate of good and uncompromised nodes to be revoked [6].
- Due to unavailability of centralized entities, it is difficult to perform the critical key management tasks such as certificate revocation.

3 Proposed Scheme

In this proposed certificate revocation protocol, all trust management and key management tasks such as storage of certificate, validation of certificate, and certificate revocation are performed on the individual nodes, which are present within network except issuing of certificate. Information that is used to decide

whether the certificate of node should be revoked or not, get shared by all the nodes. This will indicate that, the responsibility is given to individual node for certificate revocation and also for maintaining information about the status of the peer's certificates with which they are communicating thus, certificate status information gets readily available toward each node, which will help to remove the window of opportunity problem. In this proposed protocol, the nodes having valid certificate are allowed to enter into a network. Initially, the number of nodes ' N ' using which user wants to create network that all ' N ' nodes are considered as valid and thus certificate get generated for all ' N ' nodes initially. After entering into a network, the first duty of a node is to broadcast its certificate to all the ' N ' nodes present in network as well as node need to send a request to obtain information about PT of all other nodes. Refer request for PT Module 3 for detail description of these certificate broadcast process and sending the request to obtain PT.

3.1 Advantages of Proposed Scheme

- This proposed certificate revocation scheme provides some measure protection against false accusation attack.
- It also effectively eliminates the window of opportunity problem.
- In contrast to DICTATE [7], the proposed scheme revokes certificate of accused node only, not the certificate of accuser.
- Proposed scheme is able to solve false accusation attack in the environment when there are multiple malicious nodes are present in the network, whereas the URSA [8] protocol has not solved this issue.
- In this proposed scheme, no node need to sacrifice itself to remove malicious node from the network, whereas in the decentralized suicide-based approach [9], at least one node need to sacrifice itself to remove malicious node from the network.

4 System Design

Proposed certificate revocation protocol maintains four main tables that are profile table (PT), status table (ST), certificate information table (CIT), and certificate repository table (CRT) toward each and every node present in the network.

PT	It gives information about the adversary node. Information in this table is used to determine whether the certificate of node is revoked or not.
ST	It is used to find out the status of a certificate.
CIT	It gives certificate information which is assigned to node.
CRT	It gives information about legitimate nodes.

4.1 Description of the Fields in PT

Table 1 shows the information about the fields present in PT and the size of each field in terms of bits.

Owner's ID	This field gives certificate serial number of the node that compiled the profile table.
Node count	It indicates the owner's point of view regarding the current number of nodes (N) present in the network.
Peer i ID	It gives the certificate serial number of misbehaving node i .
Certificate status C_i	This field gives information about the status of peer i certificate. Flag get set if the certificate of peer i is revoked otherwise unset.
Accusation info	It gives the information about the date when the accusation was made.

4.2 Fields and Contents of ST

Following are the different fields of ST and the notations used to represent them.

A_i Gives the information about the total number of accusations made against node i .

α_i Gives the information about the number of accusation messages made by node i .

β_i It is used to calculate the honesty of node i . The value of β_i is a number between $0 < \beta_i \leq 1$. The greater value of β_i will indicate that the node i is more trusted. β_i is calculated as shown in below Eq. (1).

$$\beta_i = 1 - \lambda A_i \text{ and } \lambda = \frac{1}{2N - 3} \quad (1)$$

ω_i It is numbered value, which is assigned to the accusation made by node i . The value of ω_i is a number between $0 \leq \omega_i \leq 1$. The value of ω_i is calculated as shown in below Eq. (2):

$$\omega_i = \beta_i - \lambda \alpha_i \text{ and } \lambda = \frac{1}{2N - 3} \quad (2)$$

Table 1 Fields of profile table

Fields	Owners' ID	Node count	Peer i ID	Certificate status	Accusation info
Number of bits	32 bits	16 bits	32 bits	1-bit flag	64 bits (32 + 32 bits)

R_j It is used to find out whether the certificate of node j should revoke or not. Certificate of node j is revoked if $R_j \geq R_r$. The value of R_j is calculated as shown in below Eq. (3):

$$R_j = \sum_{i=1}^N \sigma_{ij\omega_i} \tag{3}$$

4.3 System Architecture

Figure 2 shows the architecture of the proposed system, which includes interrelated functionalities. The description of each layer is given in Sect. 5.

4.4 System Flowchart and Module of the Proposed System

Figure 3 shows the flow chart of the proposed system. It gets divided into 5 different modules that are as follows (Figs. 4, 5, 6, 7).

Module 1: Network Creation Module

This module is used to build the network according to user requirement regarding the number of nodes N , where $N > 0$. If user has specified $N = 5$, then it creates MANETs with 5 nodes, and if $N = 3$ then with 3 nodes as shown in Fig. 8. The position of nodes will not be the same every time due to the mobility feature of the MANETs. This module will not work in 3 that are as follows: if user has not

Fig. 2 Proposed architecture

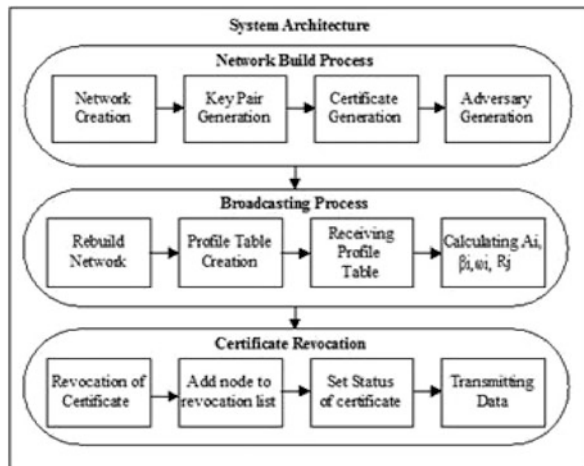


Fig. 3 System flowchart

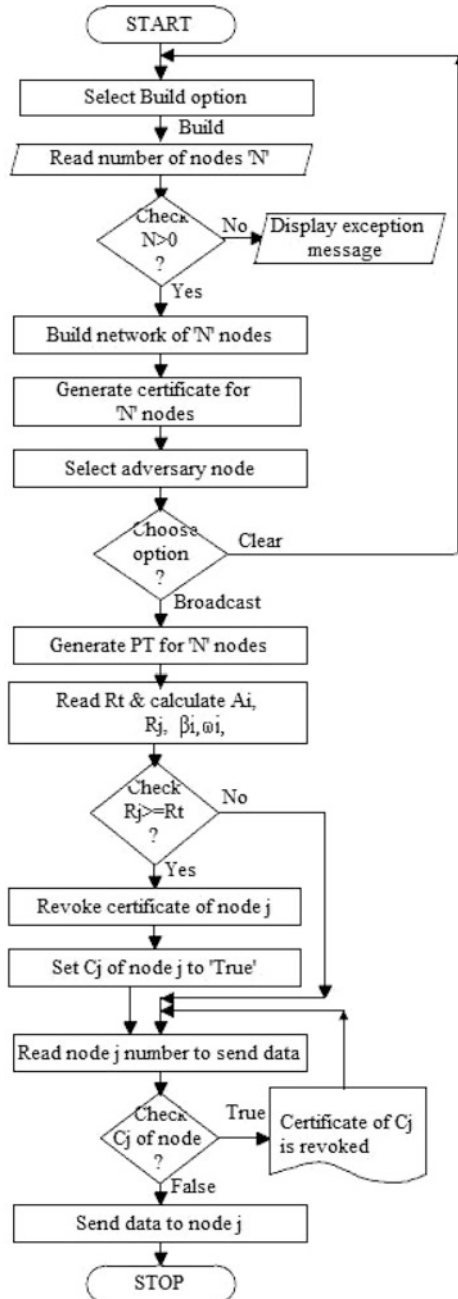


Fig. 4 Direct neighbors

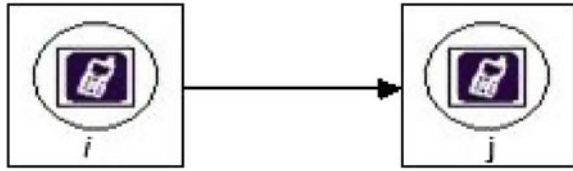


Fig. 5 Not direct neighbors

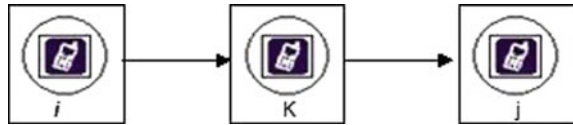


Fig. 6 Not direct neighbors with revoked node

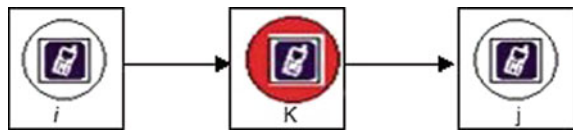


Fig. 7 Revoked destination

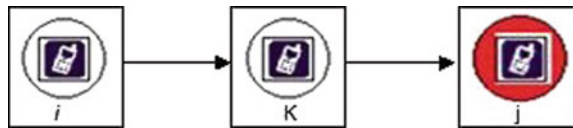
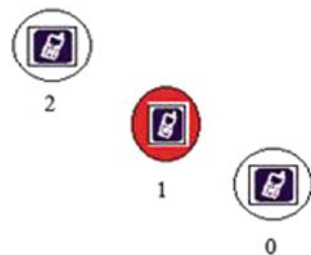


Fig. 8 MANETs with 3 nodes



provided value for N , if user has specified the negative value for the N , and if user has given the floating value for the N .

Module 2: Certificate Acquisition and Certificate Storing

This module is used to issue the certificate to the nodes as well as to store the certificate information about all the nodes as shown in Table 3. In the proposed scheme, the individual nodes within a network are responsible for all tasks such as certificate storing, assigning key pair to nodes, revoking certificate, except issuing of certificate due to the absence of central repositories and infrastructure support. A node is required to have a valid certificate issued by a CA before entering into a network [10]. All the nodes present in network have valid certificate initially

because after some period of time if it get detected as an adversary node then certificate of that node get revoked to protect the network.

Module 3: Requests for PT

When any new node gets entered into the network then that node required to perform two things that are, Broadcast its certificate to all the nodes which are present in the network so that the nodes already present in network obtain the information about it and also need to simultaneously send request to all the nodes present in the network to send their PT to obtain information about the nodes that has been detected as adversary before this new node has entered into the network. Using this information, the newly entered node is able to send and receive data only form non-adversary node, and thus, the network get protected from adversary node. Table 1 shows the fields of the PT.

Module 4: Certificate Revocation



It is used to revoke the certificate of the node that has been detected as an adversary. It makes use of information present in the PT and constructs ST from it. ST helps to revoke the certificate of adversary node.

When any node in the network detects the misbehavior of other node at that time, the proposed system generates accusation message against that node. User need to provide the value of revocation quotient threshold R_t to revoke the certificate of adversary node. Its value depends on the sensitivity of the security requirement. Typical values of R_t are 1/2, 1/3, or 1/4. Generally, R_t could be equal to $N/2$, where N is the number of nodes in the network. After specifying R_t value, parameters in ST get calculated by making use of above Eqs. (1), (2), (3). This certificate revocation module revokes the certificate of node if $R_j \geq R_t$ and indicated in the C_i field of the PT. The node whose certificate has been revoked for that node this C_i field is set to ‘TRUE’ as shown in Table 5. Nodes whose certificates are revoked are denied network access. In this proposed scheme, the nodes are required to update their PT and ST immediately when any new accusation information is received. Hence, the windows of opportunity get removed.

Module 5: Send Data

Following are the different scenario that can occur while sending data from node i to node j . In MANETs, the data get send between two nodes directly if they are within each other radio range otherwise in multihop fashion. To send data between two nodes in multihop fashion, it makes use of intermediate node. Table 2

Table 2 Representation of nodes

Node description	Source node	Destination node	Intermediate node	Valid node	Adversary node
Representation of node	I	J	K		

shows the information about the variables and their description, which will be used to represent node.

Scenario 1: Node j is Direct neighbor of Node i .

The data sent by node i get received by node j successfully.

Scenario 2: Node j is not direct neighbor of Node i and intermediate node K is valid.

Data get sent from node i to node j successfully.

Scenario 3: Node j is not direct neighbor of Node i and intermediate node K is revoked node.

The data does not get sent to node j and error message such as ‘certificate of intermediate node is revoked, unsafe path’ get displayed to user.

Scenario 4: Node j is revoked and intermediate node K is valid.

Data does not get sent to destination node j and error message such as ‘destination node certificate is revoked’ get displayed.

5 Case Study

Let user has created MANETs with $N = 3$ nodes where node 1 is adversary as shown in Fig. 8.

The contents of PT, ST, CIT, CRT for MANET with 3 nodes are shown in below tables.

5.1 Certificate Information Table

The fields and content of certificate information table (CIT) are shown in Table 3.

5.2 Certificate Repository Table

The fields and content of certificate repository table (CRT) are shown in Table 4.

Table 3 Certificate information table

Certificate information table at node 1

Fields	Serial number	Issuer DN	Not before	Not after	Version
Value	1351511028573	CN = Node No: 1	DD/MM/YY	DD/MM/YY	1

Table 4 Certificate repository table

Certificate repository at node: 1				
Serial number	Issuer DN	Not before	Not after	Version
1351511028420	CN = Node No: 0	Mon Oct 29	Mon Oct 29	1
1351511028720	CN = Node No: 2	Mon Oct 29	Mon Oct 29	1

5.3 Profile Table

The fields and content of profile table (PT) where node 1 is adversary are shown in Table 5.

5.4 Status Table

The fields and content of status table (ST) where node 1 is adversary are shown in Table 6.

Here, for the MANETs with $N = 3$ nodes, the value of R_t becomes $N/2 = 3/2 = 1.5$ and the condition $R_j \geq R_t$ get satisfied for node 1, so the certificate of node 1 get revoked.

Table 5 Profile table

Profile table at node: 2			
Peer ID	Certificate signature	Certificate status	Accusation date
1	1351511028573	TRUE	Mon Oct 29

Table 6 Status table

Status table at node 2					
Peer ID	A_i	β_i	α_i	ω_i	R_j
0	0	1.0	1	0.667	0.0
1	2	0.33	0	0.333	1.5
2	0	1.0	1	0.667	0.0

6 Conclusion

In this paper, we have seen that ad hoc network security schemes utilizing threshold cryptography, potentially provide greater flexibility and security. However, the computational cost, particularly for low-powered wireless nodes, might be too prohibitive. In addition, these schemes require unselfish cooperation of the communicating peers, which cannot be guaranteed in certain networks environments. This paper proposed certificate revocation scheme for ad hoc networks, which provided some measures of protection against malicious accusation succeeding in causing the revocation of certificates of well-behaving nodes.

References

1. Zhou, L., Haas, Z.J.: Securing ad hoc networks. *IEEE Netw. Mag.* **13**(6), 24–30 (1999)
2. Yang, H., Luo, H., Ye, F., Lu, S., Zhang, L.: Security in mobile ad hoc networks: challenges and solutions. *IEEE Wirel. Commun.* **11**(1), 38–47 (2004)
3. Liu, W., Nishiyama, H., Ansari, N., Kato, N.: A study on certificate revocation in mobile ad hoc networks. *IEEE* (2011)
4. Park, K., Nishiyama, H., Ansari, N., Kato, N.: Certificate revocation to cope with false accusations in mobile ad hoc networks. In: *Proceedings of 2010 IEEE 71st Vehicular Technology Conference: VTC2010-Spring, Taipei, Taiwan, 16–19 May 2010*
5. Housley, R., Polk, W., Ford, W., Solo, D.: Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile, Internet Request for Comments (RFC 3280), April 2002
6. Crêpeau, C., Davis, C.R.: A certificate revocation scheme for wireless ad hoc networks. School of Computer Science, McGill University, Montreal, QC, Canada H3A 2A7 (2003)
7. Luo, J., Hubaux, J.P., Eugster, P.T.: DICTATE: Distributed certification authority with probabilistic freshness for ad hoc networks. *IEEE Trans. Dependable and Secure Comput.* **2**(4), 311–323 (2005)
8. Luo, H., Kong, J., Zerfos, P., Lu, S., Zhang, L.: URSA: ubiquitous and robust access control for mobile ad hoc networks. *IEEE/ACM Trans. Netw.* **12**(6), 1049–1063 (2004)
9. Clulow, J., Moore, T.: Suicide for the common good: A new strategy for credential revocation in self-organizing systems. *ACMSIGOPS Oper. Syst. Rev.* **40**(3), 18–21 (2006)
10. Conklin, A., White, G., Cothren, C., Williams, D., Davis, R.L.: Principles of computer security. (2004)