Certificate Revocation in Mobile Ad Hoc Networks

Mrs. Priti Rathi[1], **Mr. Parikshit Mahalle**[2]

[1,2] Department of Computer Engineering, Smt. Kashibai Navle College of Engineering,
Off Sinhgad Road, Vadgoan (Bk), Pune-411041, India

ABSTRACT

In Mobile Ad hoc Networks (MANETs), certification systems play an important role to achieve network security. Handling the issue of certificate revocation in wired network is somewhat easy compared to the MANETs. In wired network when the certificate of a malicious node get revoked then the certificate authorities add the information about the revoked node in to certificate revocation lists (CRLs) otherwise broadcast the CRLs 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 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 detect 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 also the problem of window of opportunity where revoked certificates get assigned as a valid to new nodes.

Keywords: MANETs, Certificate Authority (CA), Certificate Revocation and Digital Certificate (DC).

1. INTRODUCTION

Mobile ad hoc networks (MANETs) are autonomous collection of mobile nodes which communicate over relatively bandwidth constrained wireless links [5]. MANETs differ from conventional wireless networks, such as cellular networks and IEEE 802.11 (infrastructure mode) networks, in that they are self-containing: the network nodes can communicate directly with each other without reliance on centralized infrastructures such as base stations. Additionally, MANETs are self organizing and adaptive [3]; they can therefore form and de-form on-the-fly without the need for any system administration.

These unique features make MANETs very attractive for scenarios which will require rapid network deployment, such as search and rescue operations. The decentralized nature of MANETs, particularly the absence of centralized entities, and hence the avoidance of single point of failures, makes these network paradigms also ideal for military and commercial applications that require high degree of robustness. There are however some challenging security issues which need to be addressed before MANETs are ready for widespread commercial or military deployment.

One of the core security issues 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 trust management security issue challenging task. The unavailability of trusted authorities also creates problem to perform necessary functions such as the revocation of DC. Another interesting MANET security problem is the issue of false accusation in the presence of malicious nodes, which will try to prove the legitimate node as malicious node due to which legitimate node get removed from the network. The malicious nodes can cause various communication problems such as window of opportunity problem.

The principal objective of this paper is to address 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 [1].

The wireless technology makes MANETs more vulnerable to security attacks and due to this the traditional security methods does not provide a novel solution to MANETs [5, 13]. A new protocol need to be developed to overcome the drawback in the traditional security methods such as DC, Symmetric key cryptography method which will require trusted third party and central repositories to maintain information about node whose certificate is get revoked but these traditional security methods are yet fail in providing the desired security in the case of wireless networks such as MANET's. In other words, the scope of the traditional security methods is only limited to the wired networks and to some extent in the wireless networks because the number of security threats is greater in wireless networks compared to wired networks.

An ultimate solution to such scenario is the threshold cryptography. This (k, n) threshold cryptography scheme was introduced by Shamir in [4]. This scheme distributes trust and functionality of CA [5] that provides efficient security measures to the wireless networks by distributing functionality of CA such as certificate validation, certificate revocation, managing certificate except issuing of certificate to all the nodes present in the network compared to the traditional cryptographic measures.

2. Existing Scheme

For conventional networks, CA issue CRLs [11] which contains information about revoked certificates at regular intervals. The CRLs are either placed in online repositories where they are readily available, or they may be broadcast to the individual nodes. Alternatively, different certificate validation protocols are used for conventional network that are online certificate status protocol (OCSP), CRLs. OCSP [12] can be used to ascertain information about the status of certificate. To achieve security in MANETs these certificate validation protocols are not suitable due to absence of centralized repositories, unavailability of CA in MANETs. The following are the different challenges associated with adapting this certificate validation protocol to MANETs.

<u>Disadvantages of Existing Scheme</u>

- In any ad hoc networks, there may neither be network connection to centralized CAs nor central repositories where CRLs can be retrieved, or centralized servers running certificate validation protocol. Thus, ascertaining whether certificate of the node is revoked or not is a challenging task in ad hoc networks environments.
- To-date, the security schemes utilizing digital certificates, proposed for ad hoc networks, either do not explicitly address the issue of certificate revocation.
- 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 because the certificates of good, uncompromised nodes to be revoked [2].
- The absence of centralized entities for performing critical key management tasks such as certificate revocation.

3. Title, Authors, Body Paragraphs, Sections Headings and References

The proposed certificate revocation protocol for ad hoc networks provides a measure protection against false accusation attacks. It solves the issue of certificate revocation without taking any input from external entities. In this 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 are used to decide whether the certificate of node should be revoked or not, that information is 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 certificates of the peers with which they are communicating. So the certificate status information gets readily available towards each node; which will help to remove the window of opportunity problem.

In this proposed protocol, the nodes which are having valid certificate only those nodes 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, and simultaneously sends a request that the nodes send their profile tables. Table 1 shows the fields of profile table [2, 9]. The information in the profile tables is used to determine whether the certificate of a given node should be revoked or not. Each node is required to compile and maintain a profile table. A profile table can be represented in the form of a packet of varied length.

3.1 Goals and objectives

Designing certificate revocation scheme for MANETs which provides measure protection against false accusation attack and achieve better security. Information that are used to decide whether or not a certificate of node should be revoked is shared by all the nodes. The responsibility is given to individual nodes to revoke certificates of nodes as well as to maintain the information about the certificates status of the peers with which they are communicating. Certificate status information is thus readily available to each node consequently, enabling the elimination of the window of opportunity whereby revoked certificates can be accepted as valid.

3.2 Scope of Proposed Scheme

The scope of this proposed scheme is to make the use of threshold cryptography, and create a decentralized CA, using which the duty of certificate authority is get distributed among several nodes present in the network thus the challenge related with key management service in MANETs can get resolved. The development of this new decentralized CA making use of threshold cryptography also leads to a significant reduction in the time needed to revoke the certificate of malicious node and removes problem of false accusation and window of opportunity.

3.3 Advantages of Proposed Scheme

- The proposed certificate revocation scheme for ad hoc networks provide some measure protection against false accusation attack succeeding in causing the revocation of certificates of trustworthy, legitimate nodes.
- This proposed scheme also effectively eliminates the window of opportunity whereby a revoked certificate can be accepted as valid.
- In contrast to DICTATE [13], 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 get present in the network, whereas the URSA [8] protocol has not solved this issue.
- Proposed scheme, try to remove the malicious node from the network as soon as it have detected the first misbehavior of node so the time required to revoke the certificate of malicious node is get reduced compare to the time which is required to revoke the certificate of malicious node in Voting Based Scheme [9]

4. Title, Authors, Body Paragraphs, Sections Headings and References

In this proposed certificate revocation protocol scheme, two main tables are get maintained by each and every node present in the network that are profile table (PT) shown on Table 1 and status table (ST) respectively.

Profile Table: The PT gives information about the adversary node. It also maintains information about the behavior profile of each node in the network. Information in this table is used to determine whether the certificate of node is revoked or not.

Status Table: The ST is used to find out the status of a certificate. In addition to PT, each node in the network is required to compile and maintain a ST. Initially, it is compiled from the data present in the PT, and updated simultaneously when a new accusation message is broadcasted by any node.

4.1 Fields and contents of PT

Owner's ID: First 32-bits of the PT represents this field. It gives certificate serial number of the node that compiled the profile table.

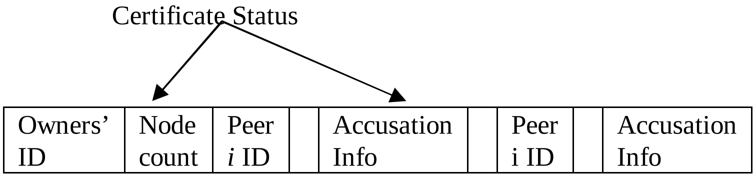
Node count: This is 16-bit field. It contains a short integer which indicates the owner's point of view regarding the current number of nodes (N) present in the network.

Peer *i* ID: This is 32-bit field. It gives the certificate serial number of misbehaving node *i*. This field also used for the purpose of a marker where if it contains zero, then it indicates the end of the profile table.

Certificate status: This field gives information about the status of peer i certificate. It contains a 1-bit flag which is set if the certificate of peer i is revoked otherwise unset.

Accusation info: This is 64-bit field. First 32-bits indicate certificate serial number of a node who has detected the misbehavior of peer *i* and the remaining 32-bits contains the data when the accusation was made.

Table 1: Fields of Profile Table



Owners' ID	Node count	Peer *i* ID		Accusation Info		Peer i ID		Accusation Info

The information regarding the number of accusations, the identity of the accusers, the nodes being accused and the date the accusation was made, should be consistent in all PT. If the node requesting the PT, observe any inconsistency then the accusation message get generated against the nodes that sent the inconsistent data. PT data is assumed to be inconsistent if it differs from the data present in the majority of the other PT. The node compiles its own PT based on the data present in the majority of the PT. A node in the network is allowed to accuse a given node only once throughout its entire lifetime of a certificate. So, when any accusation message is broadcast, first the nodes are required to check the data present in their PT, if they found that this is new accusation then that node need to add this information about the new accusation such as certificate serial number of the accuser, the node being accused, and the date etc, only if there is no prior record of the accuser accusing that particular node.

4.2 Fields and contents of ST:

Number of accusations against node *i* (A*i*): This field gives the information about the total number of accusations made against node i.

Number of additional accusations made by node *i* (α_i): This field gives the information about the additional number of accusation messages that are made by node *i*.

Behavior index of node *i* (β_i): This field is used to calculate the honesty of node i. The value of β_i is a number between 0 and 1 such that 0< β_i<=1. The greater value of β_i will indicate that the node i is more trusted. The value of β_i is calculated as shown in below equation (1):

$$\beta_i = 1- \lambda A_i$$
$$\lambda = 1/2N-3 \qquad (1)$$

Where, N is the node count

Weight of node *i* accusation (ω_i): ω_i is a numbered value which is assigned to the accusation made by node *i*. It's depends on β_i and α_i. ω_i is a number between 0<= ω_i<=1. The value of ω_i is calculated as shown in below equation (2):

$$\omega_i = \beta_i - \lambda\alpha_i$$
$$\lambda = 1/2N-3 \qquad (2)$$

Where, N is the node count.

Revocation quotient (R_j): It is used to find out whether the certificate of node j should revoked or not. Certificate of node j is revoked if it satisfies the condition R_j>=R_t. The value of R_j is calculated as shown in below equation (3):

$$R_j = \sum_{i=1}^{N} \sigma_{ij}\, \omega_i \qquad (3)$$

Where σ_{ij} = 1 if node i made an accusation against node j otherwise it is zero. It is possible to construct an accusation graph using the data in the profile table, where the nodes of the graph represent the network nodes, and the edges represent accusations.

Certificate status (C_i): Indicates the status of the node i certificate.

Revocation quotient threshold (R_t): R_t is a configurable parameter whose value gets provided by the user. The value of R_t depends on the sensitivity of the security requirement. Typical values of R_t are 1/2, 1/3 or 1/4. Usually R_t could be equal to N/2, where N is the number of nodes in the network. The certificate of node get revoked if R_j value of a node j exceeds R_t and indicated in the C_i field of the ST. In this proposed scheme, the nodes are required to update their PT and ST immediately when any new accusation information is received. Hence, the window of opportunity get removed Nodes whose certificates are revoked are denied network access.

4.3 System Flowchart:

Total system flow chart is given in following figure 1a

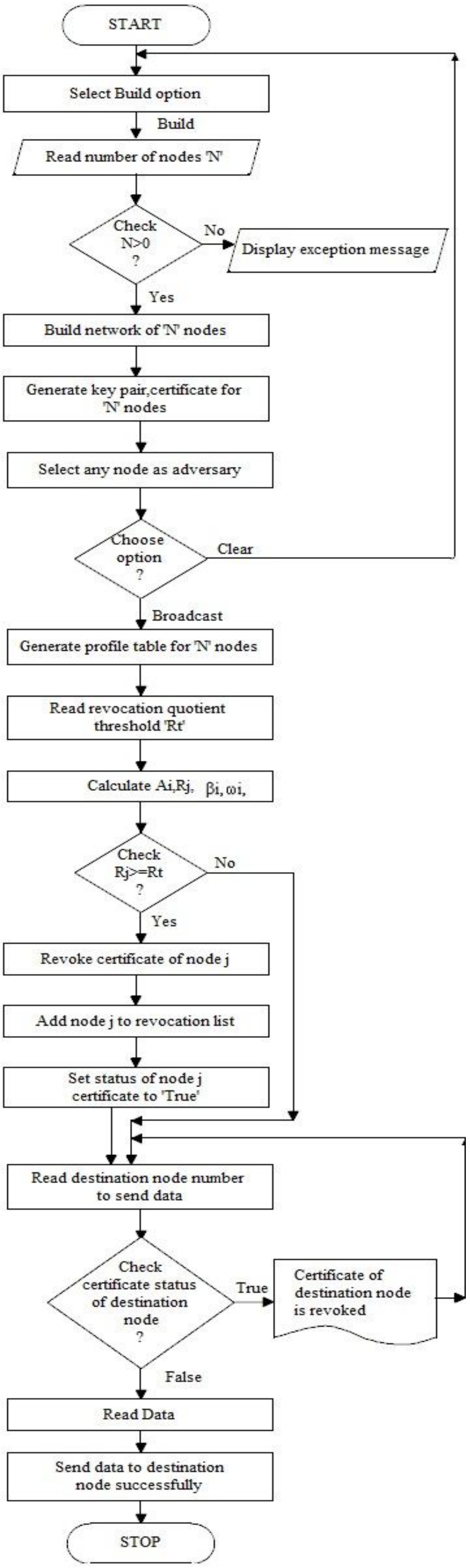

START
Select Build option
Build
Read number of nodes 'N'
Check N>0 ?
No
Display exception message
Yes
Build network of 'N' nodes
Generate key pair,certificate for 'N' nodes
Select any node as adversary
Choose option ?
Clear
Broadcast
Generate profile table for 'N' nodes
Read revocation quotient threshold 'Rt'
Calculate Ai,Rj, βi, ωi,
Check Rj>=Rt ?
No
Yes
Revoke certificate of node j
Add node j to revocation list
Set status of node j certificate to 'True'
Read destination node number to send data
Check certificate status of destination node ?
True
Certificate of destination node is revoked
False
Read Data
Send data to destination node successfully
STOP

Figure 1a: System Flowchart

4.4 System Architecture:

The total system architecture is given in the following Figure 1b.

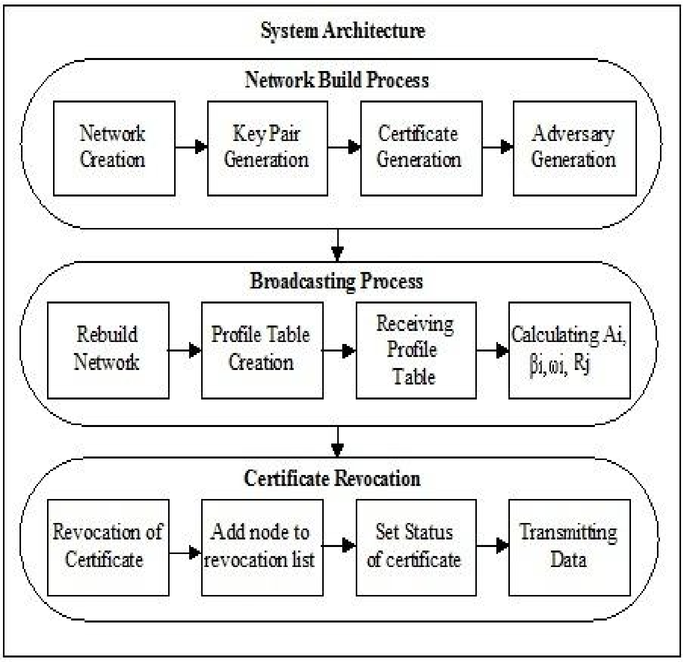


Figure 1b: System Architecture

5. Modules of the Proposed Scheme

5.1 Module 1- Network Creation

Network creation is the first module of the proposed scheme. The name itself will indicate that, it is used to create the network topology according to user requirement. To build the network, user needs to specify how many number of nodes ‘N’ needs to be present in the network so the network get created as per the user requirements. If user specifies N=5 then this module creates the network with 5 nodes. Following are some situations in which this module is not able to create network:

- If user has not provided the value of number of nodes N.
- If user has specified the negative value for the N.
- If user has given the floating value for the N.

In these 3 situations this module is not able to create the network.

5.2 Module 2- Certificate Acquisition and Certificate Storing:

In the proposed scheme, the individual nodes within a network are responsible for all key management 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. The nodes in the MANETs need to be equipped with all aspect of network functionalities, such as routing, relaying packets etc thus the individual nodes in network is responsible for all key management task.

The certificate gets issued by a CA trusted by other network peers. A node is required to have a valid certificate issued by a CA before entering into a network [3]. 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. This module is used to issue the certificate to the nodes and store the certificate of all the nodes.

5.3 Module 3- Requests for PT:

When any new node gets entered into the network then that node required to perform 2 things that are first job which the newly entered node is required to perform is:

Broadcast its certificate to all the nodes which are present in the network: The newly entered node is required to broadcast its certificate to all other nodes which are already present in the network so that the nodes already present in network obtain the information about it.

Send Request to all the nodes present in the network to send their PT: The newly entered node also required to simultaneously send request to all the nodes 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 thus the network gets protected from adversary node.

5.4 Module 4-Certificate Revocation:

This module is used to revoke the certificate of the node that has been detected as an adversary. It makes use of the information present in the PT and constructs ST from it. The ST holds values of different parameters which will help to revoke the certificate of adversary node that are A_i , β_i,ω_i,R_j The value of β_i,ω_i,R_j parameters are get calculated from equation(1), equation(2) and equation(3). Users need to specify value of R_t and if R_j value of a node j exceeds R_t then this module revokes the certificate of the node j otherwise not. The status of the node j whose certificate gets revoked is set true.

6. Case Study

Suppose there is one network consisting 3 nodes as shown below Figure 2. It is not necessary that the every time when user creates network with N nodes at that time the position of N nodes will be the same as shown in below Figure 2 because in MANETs the position of the nodes does not fixed. In Figure2 nodes are represented by a mobile image and the number below the node indicate mobile node number.

Different tables are used to maintain information about the mobile nodes that are PT, ST, Certificate Repository table, Certificate Information table. The fields of these tables and their description are given below:

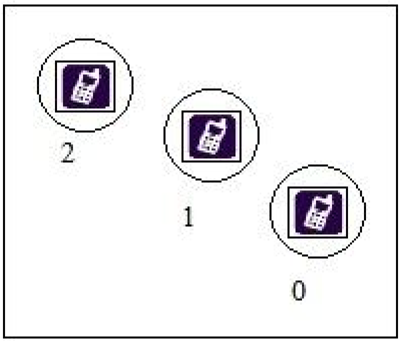


Figure 2: MANETs with 3 Nodes

6.1 Certificate Information Table:

Table 2: Certificate Information Table

Certificate Information Table At Node 1	
Fields	Value
Serial Number	1351511028573
Issuer DN	CN=Node No:1
Not Before	DD/MM/YY
Not After	DD/MM/YY
Version	1

Certificate information table get maintained by each and every node present in the network. The fields of certificate information table are shown in above Table2. It gives various information about certificate which is assigned to the node-1. It shows that, the certificate serial number of node-1 is 1351511028573 and other things.

The MANETs shown in Figure2 consisting of 3 nodes so the proposed scheme will maintain Table2 for node-0, node-1 and node-2 having information of node-0, node-1 and node-2 respectively. Suppose user has selected node-1 as an adversary node as shown in below Figure 3.

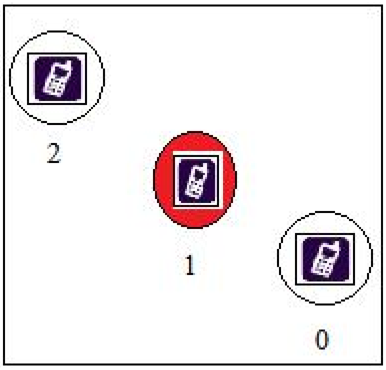


Figure 3: MANETs with node 1 as adversary

The adversary node indicated in red color.

6.2 Certificate Repository Table:

Each and every node in the network maintains this table. It gives information about legitimate nodes. Table3 shows the fields of certificate repository table. After doing comparison of the fields present in Table2 and Table3 user will found that both tables are having same fields but they represent different information.

After making node-1 as an adversary node as shown in Figure3, the certificate repository table at node-1 gives the information as shown in Table3. Table3 gives information about node-0 and node-2 because these are legitimate nodes whereas node-1 is adversary node so it will not gives any information about node-1.

Table 3: 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

Table3 shows that, the certificate serial number of node-0 and node-2 is 1351511028420 and 1351511028720 respectively.

6.3 Profile Table (PT):

It is also maintained by each and every node in the network. It gives information about adversary node whereas the PT at adversary node does not contain any information. Fields of the PT are shown in below Table4.

Table 4: Profile Table

Profile Table of Node: 2			
Peer Id	Cert Signature	Cert Status	Accusation Date
1	1351511028573	TRUE	Mon Oct 29

Table4 gives information about node-1 only because user has made only node-1 as an adversary node as shown in above Figure 3.

6.4 Status Table (ST):

ST is also maintained by each and every node in the network. It gives information about the status of certificate. It is initially compiled from PT and updated simultaneously when any new accusation gets received from any node. The fields ST are shown below Table5.

In Figure 3, user has made only node-1 as an adversary node whereas node-0 and node-2 remains legitimate nodes. In this situation, the ST shows following information:

Table 5: 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

Here, for the MANETs with N=3 nodes the value of revocation threshold R_t becomes N/2= 3/2=1.5. The certificate revocation Module-4 checks whether R_j>=R_t or not. If this condition gets satisfied then Module-4 revokes the certificate of node j. For this example, condition get satisfied for adversary node-1 so the certificate of node-1 get revoked whereas condition is not get satisfied for node-0 and node-2 so certificate of node-0 and node-2 are still valid.

7. 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.] Wei Liu, Hiroki Nishiyama, N. Ansari, N.Kato, "A study on Certificate Revocation in Mobile Ad Hoc Networks", IEEE 2011.

[2.] Claude Crêpeau and Carlton R. Davis," A Certificate Revocation Scheme for Wireless Ad Hoc Networks "School of Computer Science, McGill University, Montreal, QC, Canada H3A 2A7.

[3.] Arthur Conklin.W.M, Gregory B.Whit, Chuck Cothren, Dwayne Williams, Roger L .Davis, "Principles of computer security", 2004.

[4.] Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, November 1979.

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

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

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

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

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

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

[11.] R. Housley, W. Polk, W. Ford, D. Solo, Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile, Internet Request for Comments (RFC 3280), April 2002.

[12.] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, X.509 internet public key infrastructure online certificate status protocol – OCSP, Internet Request for Comments (RFC 2560), June 1999.

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

AUTHORS

Priti Rathi has completed her BE in Computer Science and Engineering from Swami Ramanand Teerth Marathwada University, Nanded in 2010 and achieved distinction throughout academic examination in BE. She has having six month of experience in teaching field at P. L. Government Polytechnic, Latur. She is pursuing post graduation in Computer Engineering at Smt. Kashibai Navale College of Engineering, Pune University.

Parikshit N. Mahalle received the post graduation degree in Computer Engineering from University of Pune in 2007 and pursing Ph.D in Wireless Communication from Aalborg University. He has 13 years of experience in teaching field, presently working as Assistant Professor and Head of Computer Engineering Department at Smt. Kashibai Navale College of Engineering, Pune. He has received best faculty award by Sinhgad Technical Education Society in association with Cognizant Technology solutions in 2009. He is having membership with ACM, IEEE, Life Member ISTE as well as member of Indian Science Congress Association. He has published many journals and conference papers as well as attended many International Courses.