IJETCR Open Access

ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 2; Issue 6; Page No. 124-129

A Study on Cluster Based Certificate Revocation Scheme for Mobile Ad hoc Networks

Mis. Megha Jarang [1], Prof. M.V.Nimbalkar [2], Prof. R.S.Sonar [3]

[1]Student, dept. of Information Technology, Sinhgad college of Engineering, Vadgaon, Pune 411041, India

jarangmegha@gmail.com

[2] Associate Professor, dept. of Information Technology, Sinhgad college of Engineering, Vadgaon, Pune 411041, India

mvnimbalkar.scoe@sinhgad.edu

[3] Associate Professor, dept. of Information Technology, Sinhgad college of Engineering, Vadgaon, Pune 411041, India

rssonar.scoe@sinhgad.edu

ABSTRACT

Mobile ad hoc networks (MANETs) have attracted more attention due to their mobility and simplicity of arrangement. However, the wireless and dynamic nature renders them more suspicious to various types of security attacks than the wired networks. To meet these challenges, certificate revocation is an important component for secure network communications. Certificate revocation is used to segregate attackers from participating in network activities in future. A Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme is the best scheme used to revoke the certificates of malicious node present in the network. It plays an important role in detecting the falsely accused nodes within the cluster and recovoke their certificates to address the issue of false accusation. To improve the reliability of this scheme, warned nodes are recovered to take part in the certificate revocation mechanism. To enhance accuracy, a threshold-based mechanism is proposed to evaluate and confirm warned nodes as legitimate nodes or not, before recovering their certificate[1].

Key Words: ad hoc networks (MANETs), security and certificate revocation

1. INTRODUCTION:

Recently mobile ad hoc networks (MANETs) have received increasing attention, due to their dynamic topology, mobility feature, and ease of deployment. MANET is a highly flexible network without infrastructure which is formed by a number of self-organized mobile devices like cell phones, laptops and Personal Digital Assistants (PDAs). Another problem with MANET is that open network environment where nodes can join and leave the network freely. This leads MANET more vulnerable to various types of security attacks than the wired network. Certificate management is a widely used mechanism in MANET which provides trust in a public key infrastructure [14],to secure the applications and network services. For certificate management, a complete security solution consists of three components, prevention, detection, and revocation. Many efforts have taken by researchers in some areas such as certificate attack detection, certificate distribution and certificate revocation. To secure many network communications and services, Certification is very essential. Using the digital signature of the issuer, public key is encrypted into an attribute. Which assure that a public key belongs to an individual and helps in preventing tampering and forging in mobile Ad hoc networks. Many research efforts are made to detect malicious attacks on the network. If any attack is identified, Certificate of attacker node is revoked which plays a major role in enlisting and removing the certificates of nodes which have been detected to launch attacks on the neighborhood. This helps in removing malicious nodes from the network and gets blocked from all its network activities. Certificate revocation's basically aimed at providing secure communications in MANETs. In Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme, [1] has ability to enhance the performance of MANET in which topology is constructed as clusters and each cluster consists of a Cluster Head and some Cluster Members (CMs) located within the transmission range of the cluster Head. Before joining the network, nodes have to acquire valid certificates from the Certification Authority (CA). CA is responsible for distribution and management of certificates [12] to all nodes present in the network. The CA maintains two list as warning list and black list which are used to hold

information of accusing nodes and accused nodes and updates these two lists regularly.

2. RELATED WORK

To enhance the network security a number of certificate revocation techniques have been discussed in the literature. There are mainly two existing approaches for certificate revocation, which are basically classified into two categories: voting-based mechanism and non-voting-based mechanism.

2.1 Voting-Based Mechanism

In voting-based mechanism, revocation of a malicious attacker's certificate is achieved through votes from valid neighboring nodes. "Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks" URSA [6], a voting-based mechanism proposed by H Luo uses to evict malicious nodes. The certificate of newly joining node is issued by its neighboring node. In this mechanism, each of the nodes performs one hop monitoring and exchanges their monitoring information with their neighbors. There is no third party like Certification Authority (CA) in this mechanism; the certificate of a infected node can be revoked when the number of votes against the node exceeds a certain threshold value. Where threshold detection remains challenge. If network degree is much smaller than its nodes that can launch attacks cannot be revoked and keep successfully communicating with other nodes. It does not deal with false accusation which is a critical issue.

G. Arboit et al proposes the scheme which allows all nodes present in the network to vote together. In URSA, there is no certificate authority exists in the network, instead of which each node plays role in monitoring the behaviour of its neighboring nodes. The primary difference from URSA is that nodes in the network, vote with different weights. The variable weight of a node is calculated on the basis of reliability and trust-worthiness of that node from its previous behavior. If the weighted sum of votes exceeds a predefined threshold, certificate of the accused node will be revoked. This improves the accuracy of certificate revocation. But the communication overhead used to exchange voting information rises which increases the revocation time.

2.2 Non-Voting-Based Mechanism

In non-voting-based mechanism, a node as a malicious attacker will be decided by a node with a valid certificate to revoke its certificate.

J. clulow et al proposed another decentralized approach "suicide for the common good strategy" [7], in which certificate of accused node is revoked by only one accusation from its neighbor. Certificates of both the accused node and accusing node will be simultaneously revoked; the accusing node has to sacrifice itself to remove an attacker from the network. This approach reduces both the time required to evict a node and overhead of the communication. This approach does not differentiate falsely accused nodes from genuine malicious attackers.

Park et al. proposed a cluster-based certificate revocation scheme [8], in which nodes organizes themselves to form clusters All the accuser and accused node are held in the warning list (WL) and blacklist (BL) to manages control messages by a trusted certification authority (CA). Further, also it handles the issue of false accusation. Certificate of the malicious attacker node can be revoked by any single neighboring node with short time for certificate revocation process [4].

3. PROBLEMS in EXISTING SYSTEM

A Cluster based Certificate Revocation is the combination of voting and non-voting based mechanism. This system contains unique certification authority, which is responsible for the performance of cluster head with its cluster member and for the classification of nodes within the cluster. CA verifies the certificate of each node and put the accusing and accused nodes into the WL and BL respectively. Since WL contains the accusing nodes and BL contain the accused node which is deemed as a malicious attacker. If the node in the BL is considered as false accusation then it will be recovered and placed in the WL maintained by CA. In future the accusing nodes, which are placed in the WL, can be used as a cluster member. The nodes in the BL cannot be used directly for the communication process, once it is known as legitimate node. Which leads to the problem of false accusation of the legitimate node as a malicious attacker within the network [3].

4. CLUSTER-BASED CERTIFICATE REVOCATION SCHEME

This paper presents a Cluster-based Certificate Revocation scheme with Vindication Capability (CCRVC) [9]. CCRVC has ability to enhance the performance of MANET. In this scheme, topology is constructed as clusters. A cluster consists of a Cluster Head (CH) and Cluster Member (CM) nodes within its transmission range. There is a central Certification Authority (CA) which issues the valid certificate to each node. Nodes having a valid certificate are allowed to join the network. Nodes are arranged in the form of clusters that ensures preloading of certificate for secure communication among all the nodes within the network. The CA maintains and updates two lists regularly, one as Warned list and another as Black lists that holds information of

accusing and accused nodes respectively; where BL is composed of fully revoked nodes within the cluster, such nodes cannot be recovered in any conditions. Initially the WL contains both the accusing and accused node of the cluster, where as the nodes in the WL are analysed to detect the attacker node in cluster and revoked completely from the network and stored in the BL.

4.1 Steps in the Cluster-Based Certificate Revocation Scheme

The CCRVC scheme can be studied in three different steps as follows.

4.1.1 Cluster Construction

4.1.2 Certification Authority Function

4.1.3 Certificate Revocation

4.1.1 Cluster Construction

Nodes arrange themselves to form the clusters, along with a CH and some of the cluster members. Before joining the network, nodes have to acquire valid certificates from the CA, which is responsible for managing and distributing certificates to all nodes so that nodes can kept communicating with each other in the network. Using various clustering algorithms [11], [12], CH can be selected. Fig.1 shows an example of how clusters are constructed in the system.

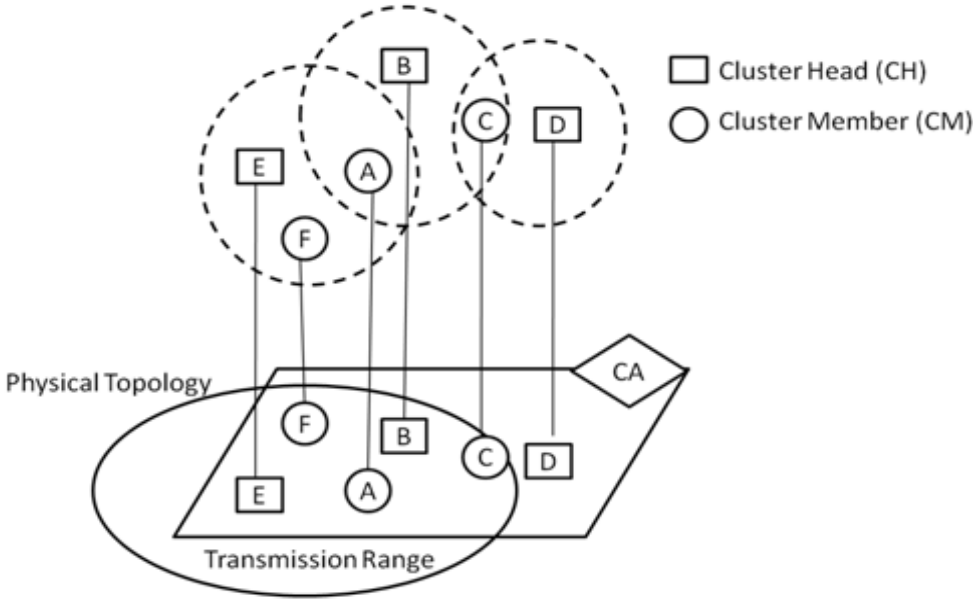

Figure 1: Clustering of Nodes

A Node except CH, which exist in the transmission range of two or more clusters can join different clusters of which CHs exist in them such nodes act as gateway nodes. By constructing such clusters, each CH can be aware of false accusation against any CM nodes.

To maintain clusters, CH and CM nodes continuously confirm their existence by exchanging messages among all the nodes within the network. CH periodically broadcasts CH Hello Packets to all the CM nodes within its transmission range and each CM replies to the CH with the CM Hello Packet [10].

4.1.2 Certification Authority Function

Certification Authority (CA), is deployed in the cluster-based scheme [13], to distribute certificates among all the nodes. The CA is also responsible for revocation of malicious nodes certificate and maintains WL and BL for accusing and accused node. The CA updates each list periodically according to the received control packets. In CCRVC scheme, nodes can be classified into three types as: legitimate nodes, malicious nodes, and attacker nodes.

- A legitimate node is a normal node in the network which is deemed to secure communication with other nodes and is able to correctly detect attacks from malicious attacker nodes and accuse them positively and for revoking their certificates.
- A malicious node does not execute misbehavior identifying protocols.
- An attacker node is a special malicious node which can launch attack in the network and disrupt the secure communication.

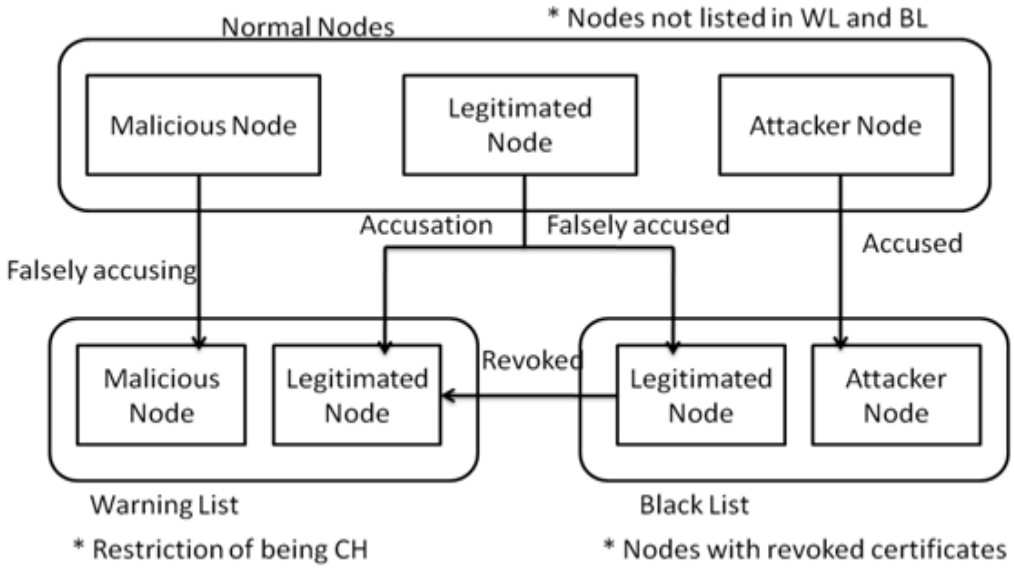

Figure 2: Classification of Nodes

Classification of the nodes is shown in fig. 2. Based on the reliability, nodes can be further classified into three categories as: normal nodes having a high reliability, warned nodes, suspected as potential attackers, and revoked nodes, accused by a normal node. Newly node joining the network is assumed to be normal node. Warned nodes and revoked nodes are listed in the Warning List (WL) and Black List (BL), respectively. Certificates of the nodes which are listed in the BL are revoked and removed from the network.

4.1.3 Certificate Revocation

Certificate revocation procedure mainly focuses on revoking the certificate of malicious node and dealing with falsely accused node to recover them as normal node in the network, which is described below:

4.1.3.1 Revoking Certificate of Malicious node

The revocation procedure [1] [2] begins at detecting the presence of attacker node. When the neighbouring nodes in the network detect attacker node and each node sends out an accusation packet against the attacker node to the Certificate Authority (CA).

The procedure for certificate revocation is described below with the example, when a malicious attacker A launches attack within one-hop range as shown in following fig. 3.

• Node A is a malicious node and is responsible to launch attack on its neighbouring nodes B, C, D and E.

• Each of the neighboring nodes detects the attacks and sends an accusation packet to the CA against attacker node A. After receiving the first packet from node B, CA holds node B into WL as an accuser node and node A into the BL as an accused node. CH updates its WL and BL and determines that one of the node was framed.

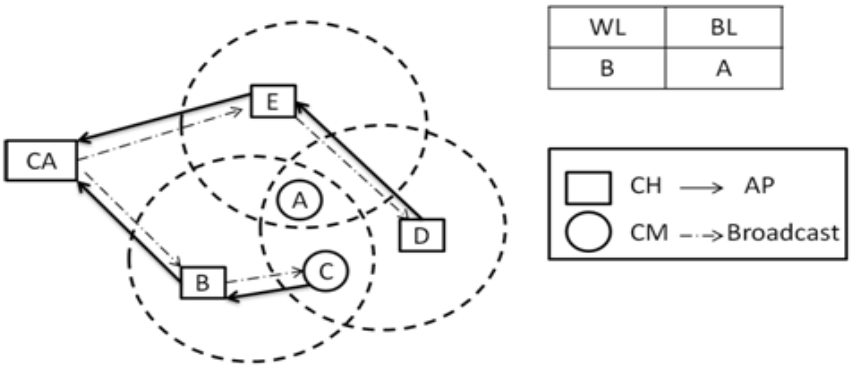

Figure 3: Revoking a node's certificate

4.1.3.2 False Accusation

If the CH does not detect any attacker node from the accused nodes enlisted in the BL from the CA, CH becomes aware of the occurrence of false accusation and sends a recovery packet to the CA in order to vindicate the node, which causes release of the falsely accused node from the BL and held it in the WL. This information is propagates to all the nodes through the network by CA [8]. Fig .4 shows the process of addressing false accusation as below.

• CA broadcasts the information of WL and BL throughout the network.

• Node E and D which are CH of node A update their WL and BL, and determine that node A was framed as accused node.

• E and D send a recovery packet to the CA to recover the certificate of falsely accused node A.

• After receiving the first recovery packet from node E, the CA removes the falsely accused node A from the BL, and held it into the WL along with node E.

• All the nodes will update their WL and BL and the certificate of node A will be recovered.

• CA broadcast the revocation message to all the nodes present in the network.

• Each Node in the cluster updates their local WL and BL to revokes certificate of node A.

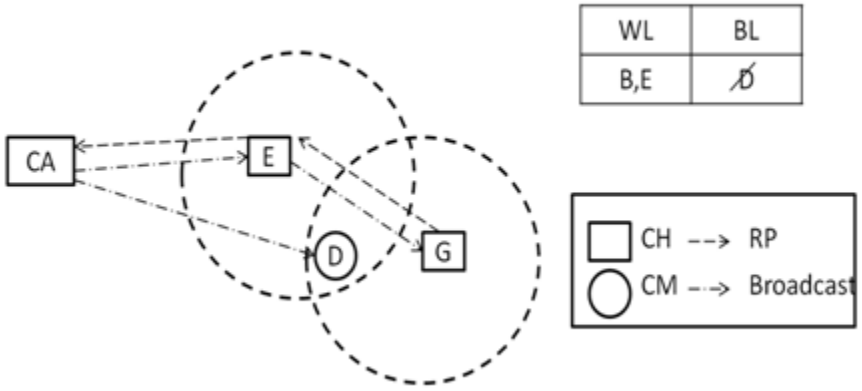

Figure 4: False accusation

5. COMPARISON OF SURVEYED REVOCATION SCHEMES

Some comparative parameters of surveyed certificate revocation schemes are given in Table 1. The proposed cluster-based Certificate Revocation with Vindication Capability scheme adapts the merits of both voting-based and non-voting-based schemes [1]. It achieves prompt revocation of certificate by lowering the communication overhead as compared with voting-based schemes. Also reliability and accuracy of the scheme is high as compared to both the non-voting-based scheme. But sometimes accuracy and robustness of cluster-based scheme can be reduce due to false accusation.

Table 1: Comparison of surveyed Revocation Schemes

Sr. No	Parameters	Voting-Based Mechanism	Non-Voting-Based Mechanism	cluster-based Certificate Revocation scheme
1	Accuracy	Very High	Low	High
2	Decision process	Slow	Rapid	Rapid
3	Communication overhead	Heavy	Less	Less
4	Reliability	Less	Less	High
5	Security	Less	Less	High

6. CONCLUSION AND FUTURE WORK

The CCRVC scheme presents the Revocation based on Clustering. CCRVC scheme addresses a major issue to ensure secure communications for mobile ad hoc networks by revoking the certificate of attacker node. A cluster-based certificate revocation with vindication capability scheme combines the merits of both voting-based and non-voting based mechanisms to revoke malicious certificate promptly and also solve the problem of false accusation. Certificate revocation of an accused node is based on a single node which reduces the revocation time in comparison with the voting-based mechanism. Also the cluster model restores the falsely accused node by the CH, which results in improving the accuracy as compared to the non-based mechanism.

The future work focus on CCRVC scheme to become more effective and efficient in revoking certificates of malicious attacker nodes, reducing revocation time, and improving the accuracy and reliability of certificate revocation scheme.

REFERENCES:

1. Wei Liu, Nei Kato, "Cluster-based Certificate Revocation with Vindication Capability for Mobile ad hoc Networks", IEEE Transactions on Parallel and Distributed systems, vol.24, no.2,doi: 10.1109/TPDS.2012.85. February 2013.
2. Jane Y.Yu, H. J. Chong, "A Survey of Clustering Schemes for Mobile Ad Hoc Networks", IEEE Communication Surveys, Volume 7, No 1, 2005.
3. K. Kiruthiga, B. Lakshmipathi, K. Prem, Preetha M. Kurup, "Cluster Based Certificate Authentication for Mobile Ad hoc Network", International Conference on Simulation in Computing Nexus (ICSCN), ISBN : 978-93-83060-45-0, 20-21 March, 2014.(1)
4. Nausheen Shamsi, Ranjana B Nagagoudar, Amareshwari Patil, "Efficient Certificate Revocation with Vindication Capability for Mobile Ad hoc Networks", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (3) , 4265-4271,2014. (2)
5. S.Herman Jeeva, D.Saravanan, RM.Chandrasekaran, "Enhancing Security in MANET using CCRVC Scheme", International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320-9801, Vol.2, Special Issue 1, March 2014. (3)
6. 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.
7. 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.
8. 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.
9. D.Jebastin Paul Christopher, "Cluster Based Certificate Revocation for Mobile Ad hoc Networks", International Journal of Science and Engineering Research (IJ0SER), Volume 1 issue 1 December 2013. (4)
10. M. Srividya, K. Radhika, D. Jamuna, "Review On Certificate Revocation Of Mobile Ad Hoc Networks", ISSN 2278-0181, Vol. 1 Issue 7, September – 2012.(5)
11. SoumyabharatSaha, SuparnaDasGupta, "Weight Based Hierarchical Clustering Algorithm for Mobile Ad Hoc Networks", doi:10.1016/j.proeng.2012.06. 137, Published by Elsevier, 2012.
12. Vincent Bricard Vieu, Nidal Nasser, "A Weighted Clustering Algorithm Using Local Cluster-heads Election for QoS in MANETs", Published in IEEE GLOBECOM, 2006.
13. Y. Dong, Ai-Fen Sui, "Providing distributed certificate authority service in cluster-based mobile ad-hoc networks", Elsevier, DOI: 10.1016, 2007.
14. Jayanta Biswas, S.K. Nandy, "Efficient Key Management and Distribution for MANET", Published in IEEE ICC, 1-4244-0355-3, 2006.