ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Certificate Revocation for Manet

Rajkumar L. Biradar
Dept. of Electronics & Telematics, G.Narayanamma Institute of Tech & Science, Hyderabad, India

Abstract
As the wireless network technology exploded, it has opened a new view to users and expanded the information and application sharing very conveniently and fast. Mobile ad hoc networks (MANETs) use wireless technology without a pre-existing infrastructure (access points). As the name states, MANETs consists of mobile nodes, which can vary from notebooks, PDAs to any electronic device that has the wireless RF transceiver and message handling capability. Mobility and no-infrastructure forms the basis of this network type. Certificate Revocation is a phase associated with Certificate Management which is a widely accepted method to provide trustworthy public key infrastructure for both application security and network service security. In the process of certificate management the three phases needed are: prevent, detect and revocation. Several works have been originated which suggests how to remove malicious attacks in the network. It is important that any attack should be identified as soon as possible.

Keywords
Adhoc, network, certificate, revocation, static, dynamic.

I. Introduction

Mobility gives maximum freedom to users, as they can be connected to the network, whether they are fixed or moving, unless they are in the range of the network. Also, it is highly dynamic, as the new nodes come, they can be connected to the network very easily.Unlike the fixed networks or traditional wireless networks, MANETs don't need any infrastructure to create and maintain communication between nodes. This property provides the ability to create a network in very unexpected and urgent situations very quickly, also without any extra cost.

A MANET is a decentralized network in which all network activities like the finding the topology and delivery of messages are handled by the nodes themselves, i.e., the mobile nodes are associated with the task of routing packets. MANETs are more sensitive to various types of security attacks due to their frequently varying wireless nature. To guarantee secure network services is a major challenge associated with any MANET. In order to have secure network communications, certificate revocation is an important task.

Certificate revocation is a major task where listing and removing the certificates of nodes that have been detected to launch attacks on the neighborhood, is done. A node should be removed from the network and cut off from all its activities immediately when it is found as misbehaved. This focuses on false accusation among nodes and limiting the entry to Black List (BL) with a threshold value. It is expected that the proposed work can handle all the delicate attacks for MANETs and develop a good application prototype. In Cluster-based certificate revocation scheme where nodes are self-organized to form clusters. There are number of cluster authorities (CAs) to efficiently perform the publication and revocation of certificates. A trusted certification authority is responsible to manage and maintain the control messages, consist of accuser and accused node in the warning list (WL) and blacklist (BL).

The certificate of the malicious node can be revoked by any single neighboring node. In addition, it can also handle 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 minimum time to complete the process of handling the certificate revocation. The significant advantage of the voting 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 slow. Also, it observes heavy communication overhead during the exchange of accusation information among each other. Cluster head detect the falsely accused nodes within its cluster and recovering their certificates to solve the issue of false accusation. Cluster based routing protocol is used in order to inherits the advantage of the voting based mechanism and to overcome the communication over head due to the exchange of the voting information.

All Nodes together form clusters and each cluster consists of a Cluster Head (CH) Along with several Cluster Members (CMs) that are located within the communication range of their CH. Each CM in the cluster belongs to two different clusters in order to provide robustness against changes in topology due to mobility. It should also be noted that because the clusters overlap, a node within the communication range of a CH is not necessary part of its cluster.

Clustering information is not used for routing purpose; it is only used for managing certificates. The aim of using clusters is to enable CHs to identify false accusations. Requests made to CA to recover the certificates of falsely accused nodes can only be made from CHs. A CH will send a Certificate Recovery Packet (CRP) to the CA to recover an accused node, only in the case where it is a CM in its cluster.

This is based on the fact that attacks can be detected by any node within the communication range of the attacker [1]. This implies that a CH will be able to detect any attack executed by one of its CMs, specifies that a CH can identify whether a CM is malicious or not. Since the CA regularly broadcasts certificate information on nodes which have been accused as malicious nodes, CHs will be able to detect false accusations against their CMs by comparing this information with their own local observations.

A. Path finding

The figure shows path is selected and the data is forwarded among the path to reach the destination quickly. Mostly data will be forwarded among cluster member within the same cluster region, or members belong to other cluster group.

Once the path has been found by using the cluster based routing protocol, data can be transmitted through the path and finally data reaches the destination. Data passed through the path may or may not reach the destination. Once data reaches the destination then there is no attacker available in the path. If the data does not reach the destination then there is an attacker available in the path. In this way we select the minimum path depending on the network

functionality and we finally transmit the data.

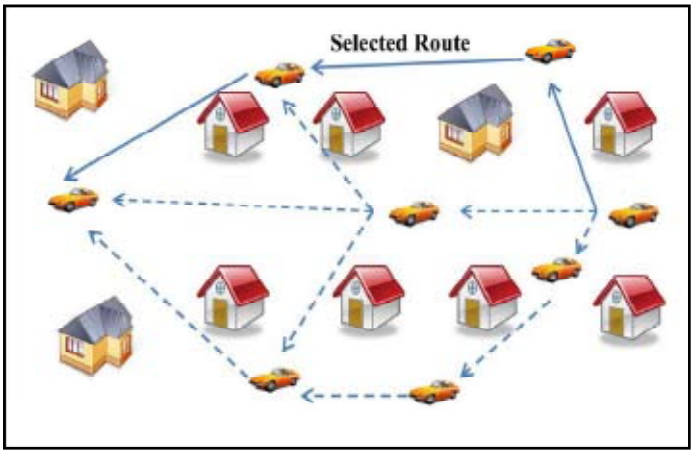


Fig. 1: Path Selection

After the path selection we consider the mechanism of the attacker node in our Mobile Adhoc Networks.

B. Attacker Node

In MANET, malicious node can easily disrupt network operations by violating routing. The attacker node will send the unrelated message continuously to the other node and make an attack to authorized node. This will make the authorized node not to perform its function properly. The attacker node can be detected by using the attacker detection methodology. The data will be transmitted from the sender node to the receiver node.

If the receiver node is an attacker node, then the receiver node will send continuously acknowledgement to the sender node and affect the sender node. These are referred as replay attack and can be detected by using the attack detection method.

The issue of certificate revocation in mobile ad hoc networks (MANETs) where there are no on-line access to trusted authorities is a challenging problem. In wired network environments, when certificates are to be revoked, certificate authorities (CAs) add the information regarding the certificates in question to certificate revocation lists (CRLs) and post the CRLs on accessible repositories or distribute them to relevant entities.

II. Different Trust Models

Certificates issued via non-threshold cryptographic schemes [2] require the utilization of some sort of trust model. These two different types of trust models play a crucial role. Depending on these two different trust models the certificates are issued. The most commonly used trust models are as follows.

A. Hierarchical Trust Model

The hierarchical trust model [3] is the more structured approach and the most widely used. In the hierarchical trust model, a root certificate authority issues certificates to delegated CAs or end users, the CAs in turn issue certificates to end users or to other

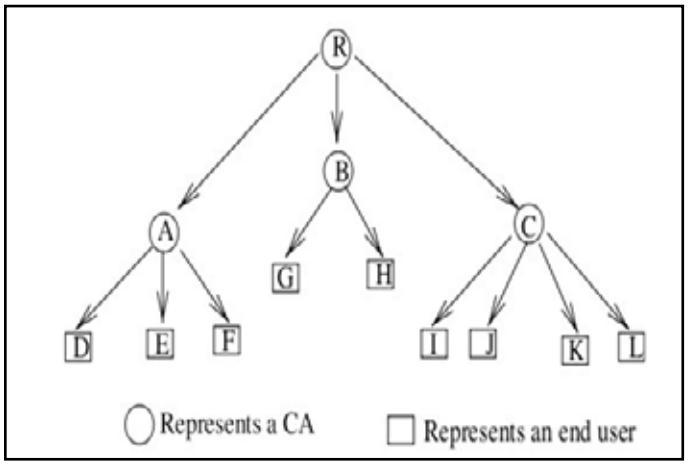


Fig. 2 : Hierarchical Trust Model

CAs. The circular shape one represents CA and the square one represents an end user. Depending on the functionality or the network we can also consider more number of nodes. The above figure illustrates the hierarchical trust model.

B. Web of Trust Model

The next non-threshold cryptographic schemes of the trust model are the web-of-trust model. In this we will have more distributed approach. In this model, there is no distinction between CAs and end users. End users are responsible for all certificate management tasks, such as issuing, storage and revocation of certificates. The following figure illustrates the web-of-trust model.

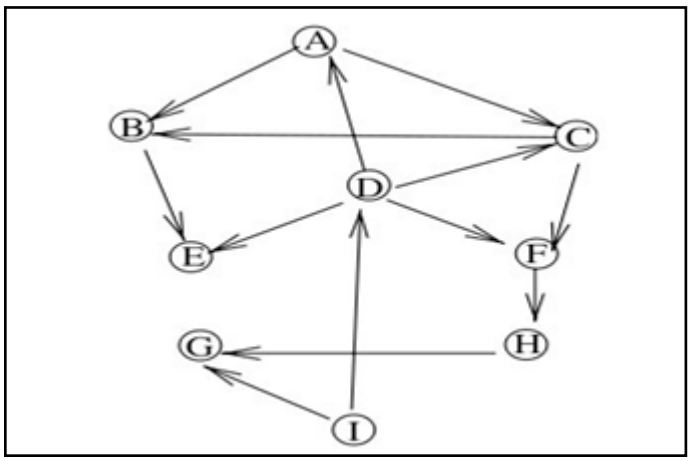


Fig. 3: Web-of-Trust Model

In purely ad hoc networks, there is typically no access to centralized repositories or trusted authorities; therefore the conventional method of certificate revocation is not applicable. Decentralized systems are more fitting for MANET applications. The majority of proposed decentralized reputation systems are transactional based; that is, they require inputs, such as size of upload or down files, quality, price and upload/download experiences, relating to interactions of providers of services and users of the services.

There are some notable challenges however in utilizing certificates that are based on the more reliable hierarchical trust model in MANETs, owing to the decentralized nature of these networks. One particular challenging problem is the issue of certificate revocation. For various reasons such as the compromisation of private keys certificates will need to be revoked periodically, and network peers need to be informed about the revoked certificates

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

in a timely manner.

In we have a decentralized certificate revocation scheme that allows the nodes within a MANET to revoke the certificates of malicious entities. The scheme is fully contained and it does not rely on inputs from centralized or external entities. This certificate revocation scheme requires each participating node to compile and maintain data based on broadcast accusation information about all the nodes in the network. The collected data is used to assign a quantitative value [4] for the trustworthiness of a node. Accusations from any given node are weighted based on the trustworthiness of the accuser: the higher the trustworthiness of a node, the greater the weight of its accusations, and vice versa. A node's certificate is revoked if the value of the sum of accusation weights against the given node is greater than a configurable threshold.

The protocol aims at providing similar data to each node for computing the trust ratings of the network peers; the end goal being that the nodes have consistent info regarding the status of the certificates of their network [5] peers. For efficiency considerations, rather than relying on digital signatures for message origin authentication and content integrity checks we mainly use one-way hash chains. One-way hash chains are based on one-way hash functions.

There are some assumptions which we should mainly consider. The following assumptions are made regarding to the MANETs and the nodes that constitute the networks:

- The number of malicious or selfish nodes is less than the number of well-behaving nodes.
- The network interfaces of the nodes are capable of operating in promiscuous reception mode.
- Each node has only one valid certificate.

The first duty of a node when it enters a MANET is to compute a series of hash chain values using an agreed upon hash function, if they have not been computed a priori; sign and broadcast it along with its certificate to the nodes in the network. Upon receiving a signed value and the corresponding certificate, the nodes verify that the certificate is valid. If it is valid and it is not revoked, and the signature on the value is valid, the nodes store both the certificate and sign in their profile tables and their values, and unicast them to the sender of the certificate. Note that if a node has already used any of its values to secure messages, it will sign and send the last value it utilized as its value to new entrants to the network. A profile table contains information about the behavior profile of the nodes in the MANET. Upon receiving the profile tables with valid sig- natures from its network peers, a node is required to compile its own profile table which is initially based on the information contained in the profile tables it received. Transmission of profile tables to new entrants to the network is necessary in order to ensure that the newcomers have up-to-date information regarding the behavior profile of its network peers.

A profile table can be represented as a packet of varied length depending on the number of accusations launched against the nodes. The length ranges from a minimum of 80 bits when there are no accusations to a maximum of 97(N-2) + 145, where N is the number of nodes in the network. A profile table contains the following fields:

1. Owner's ID: This field is the first 32 bits of the profile table. It contains the certificate serial number of the node that compiled the profile table.
2. Node count: This 16-bit field contains a short integer indicating the node perspective regarding the number of nodes in the network.
3. Peer i ID: This is a 32-bit field containing the certificate serial number of a node that is accused of misbehavior. This field also serves the purpose of a marker: if it contains zero, it indicates the end of the profile table.
4. Certificate status: This field contains 1-bit flag. The bit is set if the certificate is revoked, and unset otherwise.
5. Accusation info: The first 32 bits of this 64-bit field contains the certificate serial number of a node that accused peer i of misbehavior. The remaining 32 bits contain the date that the accusation was made.

If field 3 does not contain zero, the profile table continues with the certificate status and accusation info fields; and if there are more than one accuser, it continues with 97-bit blocks containing information about the other accusers. The profile fields are shown.

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.

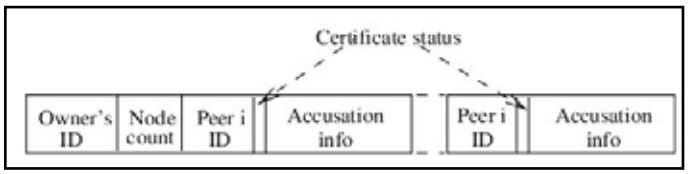


Fig. 4: Profile fields

After the initiation of transmission [6] the source node will identify whether the neighbor node is malicious or not. If it is a malicious node then it will await for certification revocation. Once the node is revoked then it should remove from the network.

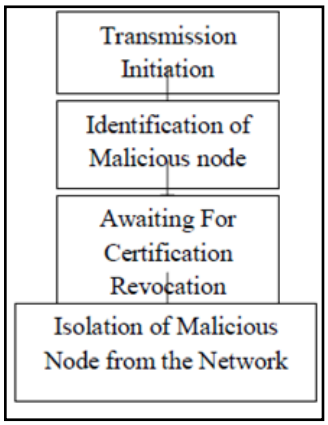


Fig. 5: Flow of certificate revocation

III. Certificate Revocation List

As clients leave the system, the certificates should be made as invalid even though the certificate lifetime has not expired. The Certificate revocation [7] processes use a Certificate Revocation List (CRL) that is periodically generated by the authority and distributed to all the participants via an overlay network with pull or push transfers.

The figure shows the Certificate Revocation List in a very detailed manner. In this we have server certificate, client certificate and the server revoked certificate. The CRL distribution overlay is established on the media data transmission network. This CRL

consist of index that stores the unique id of the certificate. The figure shows the certificate revocation list. We can see that there is a certificate authority which is a trusted third party, these authority will sign the certificate for the server, client. There is also certificate revocation list which contains the list of the members and their information. In certificate revocation process, any node in network is trying to do some malicious activity and if it is detected by some other node , then detector will intimate about the accused node to destination, claiming that nodes as accuser. Once trusted authority receives the complain, it forwards the accuser name to all cluster heads to know it is malicious or not. The entire cluster heads forwards that information to all nodes except to accuser and complained node. So now all nodes checks with their buffer whether this node previously performed malicious activity or not.

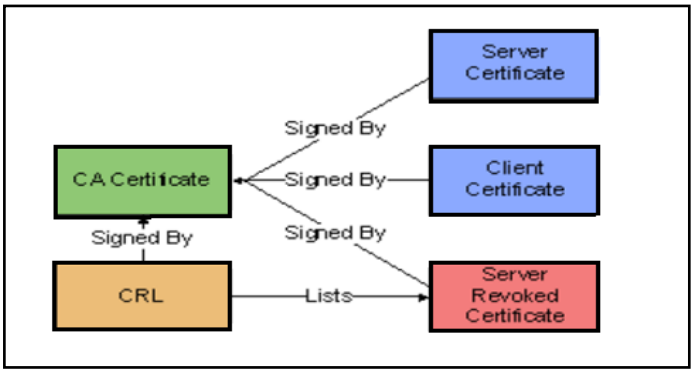


Fig. 6: Certificate revocation list

Once cluster heads receives all replays, it sends total number of attack counts and non attack counts to trusted authority. Now trusted authority will have all nodes replies about that accuser. If maximum number of nodes tells that, accused node is attacker, then that node is added to black list and intimated to all nodes through cluster heads. Else if none of the attackers count is more, the node in black list will be released and intimated node will be added to list.

A. Procedure of Revoking Malicious Certificates

We present the process of certificate revocation. The procedure of revoking malicious certificates is done in a very detailed manner. Revoking a malicious certificate is a difficult process. To revoke a malicious attacker's certificate, we need to consider three stages: accusing, verifying, and notifying. The revocation [8] 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 the figure. 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. In the figure the format of the accusation packets and the recovery packets is shown. Meanwhile, the accusing node is held in the WL. Finally, by broadcasting the revocation message format including the WL and BL through the whole network by the CA, nodes that are in the BL are successfully revoked from the network. In this we have five kinds of control packets namely, CH Hello Packet (CHP), CM Hello Packet (CMP), Accusation Packet (AP), Recovery Packet (RP) and Broadcasting Packet in addition to the routing protocol control messages.

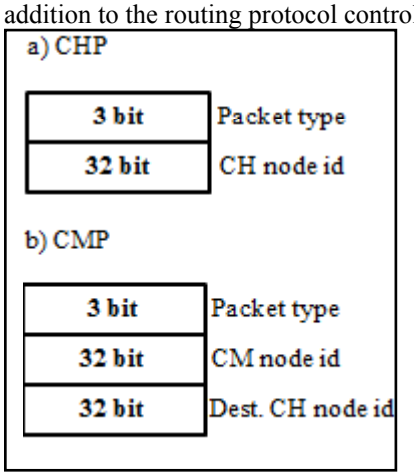
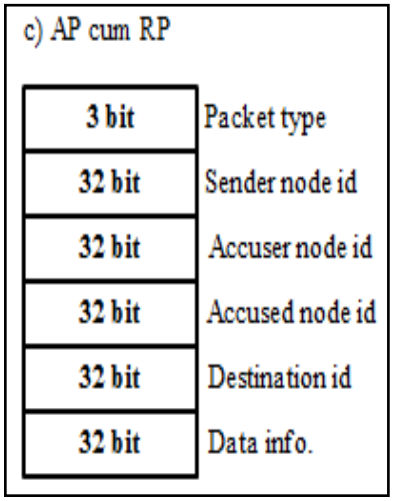
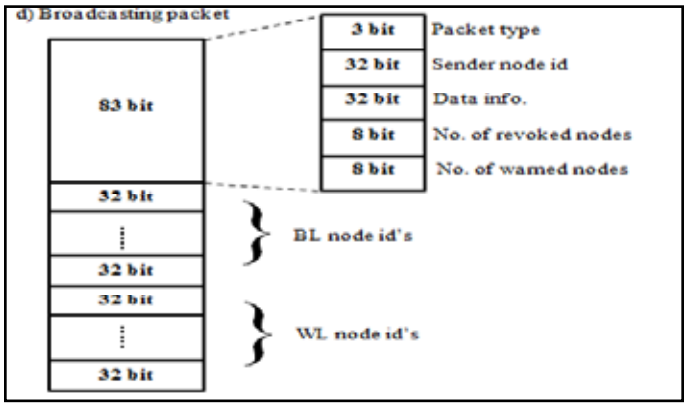


Fig. 7: Different Packets

The sizes of the prior four different control packets are fixed in contrast to the certificate information broadcasting [9] packet which has 83 + 32{n (BL) + n (WL)} bits where n (BL) represents the number of the nodes in the BL and the n (WL) is the number of nodes in the WL. Although, increase in the number of malicious and attacker nodes in the network slightly increase the amount of control traffic, it is not significant because most of the traffic consists of CHPs and CMPs of which their size and transmission frequency are independent from the number of suspicious nodes. The below figure shows the format of the broadcasting packet.



(A) Format of the accusation packets and the recovery packets



(B) Format of broadcasting packet.

Fig. 8: Control packets

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Now we consider an example, suppose that a malicious attacker M widely launches attacks within one-hop transmission range, as shown in figure. The revoking of malicious nodes certificates occurs in totally five different steps.

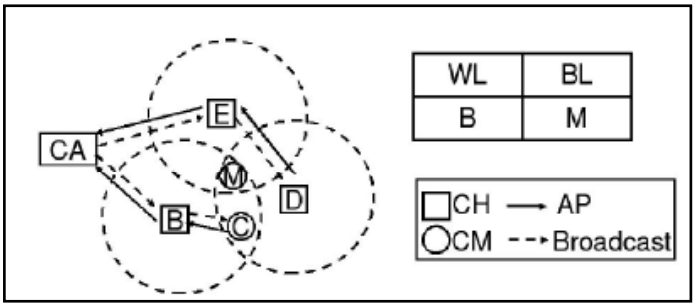


Fig. 9: Revocation

The above figure shows the certificate revocation mechanism, it has WL and BL lists. The step by step process of revoking a malicious nodes certificate is done. The procedure of revocation is described as follows.

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 holds Band 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.

In this way we finally revoke a malicious nodes certificate in our Mobile Adhoc Networks.

B. Coping with false accusation

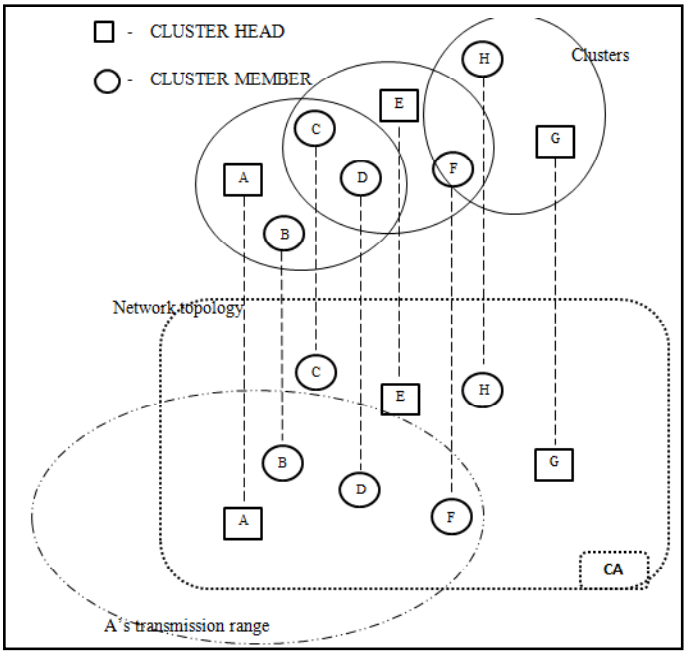


Fig. 10 : Cluster Architecture

In networks employing a certification system, nodes cannot communicate with each other without a valid certification. In other words, any attacker cannot exist in the network once its malicious behavior has been detected by others and its certification has been revoked accordingly by the system. By adopting certification systems, it becomes possible to exclude identified attackers from the network permanently by revoking the certifications of the attackers.

A simple way to identify attackers is to collect information on attackers from nodes in the network. The performance of a certification system largely depends on its deployed certification revocation strategy. Accurate revocation, quick revocation, and small network overhead remain the challenging issues to be addressed in a certificate system, particularly, to be applicable in MANET [10]. However, in this approach it is difficult to differentiate valid accusations made by legitimate nodes from false accusations made by malicious nodes.

In URSA, two neighboring nodes receive their certificates from each other and also exchange certificate information about other nodes that they know. Nodes sharing the same certificate information are regarded as belonging to the same network. In these networks, the certificate of a suspected node can be revoked when the number of accusations against the node exceeds a certain threshold. While, URSA does not require any special equipment such as Certificate Authorities (CA).

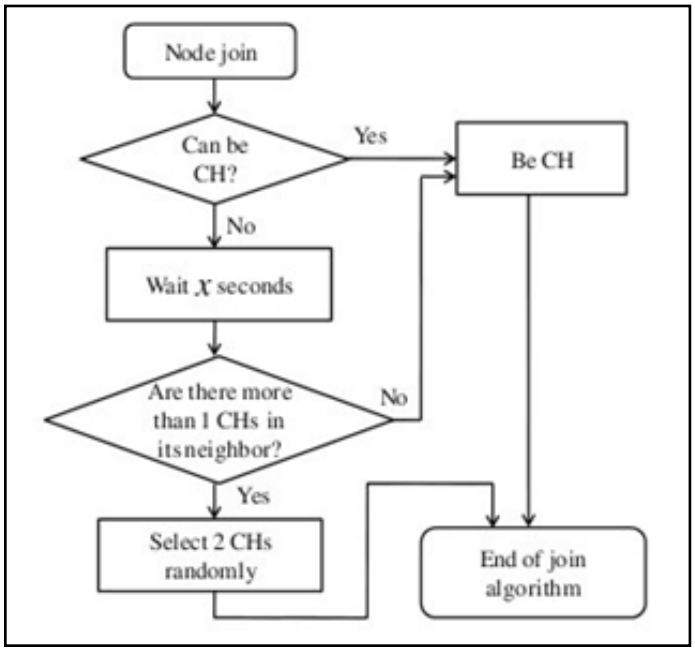


Fig. 11: Node join algorithm

In this scheme, nodes are differentiated according to their reliability, i.e., normal nodes have a high reliability, warned nodes are suspected as potential attackers, and attacker nodes have been accused by a normal node. When nodes join the network, they are assumed to be normal nodes. Warned nodes and attacker nodes are listed in the Warning List and Black List, respectively. The certificates of the nodes listed in BL are revoked whereby they are removed from the network. While the nodes included in WL can communicate with other nodes in the same way as normal nodes, there are a few restrictions placed on their behavior, i.e., unable to become a cluster head and not allowed to make any accusation.

By classifying nodes into clusters, the proposed scheme allows each Cluster Head to detect false accusation by a Cluster Member within the cluster. Node clustering provides a means to mitigate false accusations. CHs always monitor their CMs and watch for

false accusations by means of the algorithm. The figure shows an example of how clusters are constructed in the proposed scheme. While each cluster consists of one CH and CMs lying within the CH's transmission range, some nodes within the transmission area of the CH might not be the member of the cluster and can be the CM of another cluster.

For example, in figure, node B does not belong to the cluster headed by node A while it is located within the transmission area of node A. Only normal nodes having high reliability are allowed to become a CH. Nodes except CHs join the two different clusters of which CHs exist in the transmission range of them. By constructing such clusters, each CH can be aware of false accusations against any CMs since each CH knows which CM executes attacks or not, because all of the attacks by a CM can be detected by any node, of course including the CH, within the transmission range of the CM.

The reason why each node except CH belongs to two different clusters is to decrease the risk of having no CH due to dynamic node movement. To maintain clusters, CH and CMs frequently confirm their existence by exchanging messages, i.e., the CH periodically broadcasts CH Hello packets to the CMs within its transmission range, and each CM replies to the CH with the CM Hello packet. The above figure shows the node join algorithm which is carried out by newly joining nodes that enter the network. A newly joining node becomes CH at a constant rate.

A node, which has decided not to become a CH itself, will look for other CH nodes in the area. If there are more than two CHs near the node, it will attempt to join two of these clusters by randomly selecting two of their CHs and sending each of them a CM Hello packet. Otherwise, the joining node declares itself as a CH and broadcasts CH Hello packets. When a CM leaves the cluster, it needs to invoke a similar procedure to find out new CHs. If the CM receives no CH Hello packet from its CH for a certain period of time, the CM considers itself having departed from the cluster, and tries to find and join a new cluster.

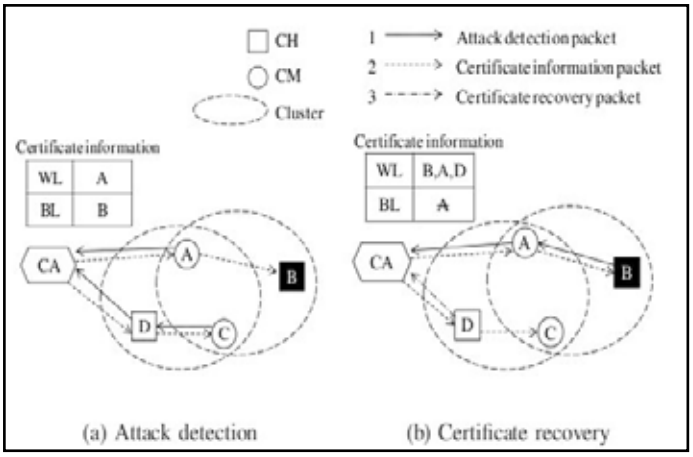


Fig. 12: Two kinds of accusation

On the other hand, if the CH cannot receive any CM Hello packets for a while, this implies that no CM is in the cluster, it then inspects the number of neighboring CHs and becomes the CM for those clusters if at least two CHs are found. By implementing the above procedures, the proposed scheme is able to maintain clusters regardless of the node movements, thus enabling it to detect false accusations.

Also, since nodes in the WL cannot become CHs, in the case where CMs lose their CH because the CH has been put into the WL; they can find and join a new cluster by executing the necessary procedures as described below.

The other example of certificate revocation to cope up with false accusation is as follows. The false accusation of a malicious node against a legitimate node [11] 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) 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. The following figure illustrates the process of addressing false accusation as follows:

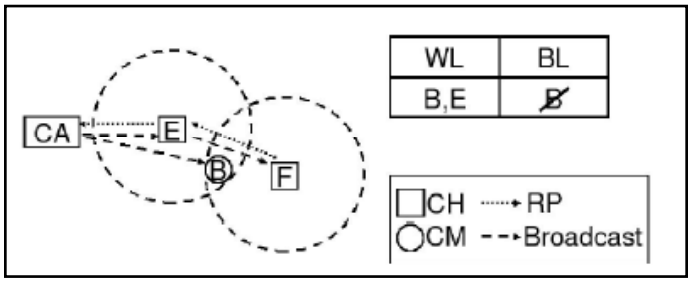


Fig.13: Dealing with false accusation

The false accusation of malicious nodes occurs in totally five different steps. The step by step process to cope up with the false accusation of malicious nodes is done. The procedure of false accusation is described as follows.

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. In this way we finally cope with the false accusation of a malicious nodes certificate in our Mobile Adhoc Networks.

IV. Conclusion

In this paper, the proposed cluster-based certificate revocation with vindication capability scheme combined with the merits of voting-based and non-voting- based mechanisms to revoke malicious certificate and solve the problem of false accusation. The scheme

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

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.

References

[1]. *Sahil Batra, Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks"., Wireless Comm. and Mobile Computing (WCMC) Special Issue on Mobile Ad Hoc Networking" Research, Trends, and Applications, vol. 3, no.5, pp.502-511, 2009.*

[2]. *RaihanaFerdous, Vallipuram Muthukkumarasamy, Elankayer Sithirasenan: "Trust-based Cluster head Selection Algorithm for Mobile Ad hoc Networks". IEEE Trans. Mobile Computing, vol. 3, no. 9, pp. 256-269, Sept-Oct. 2005.*

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

[4]. *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.*

[5]. *Scalable Network Technologies: Qualnet, http://www.scalablenetworks.com, 2012. (Visited on 21-03-14).*

[6]. *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.*

[7]. *Asokan-N, Ginzboorg-P: Key agreement in ad hoc networks, Computer Communications (Netherlands), vol.23, no.17, p.1627-37, 1 Nov. 2000.*

[8]. *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.*

[9]. *Jie Wu, Fei Dai, "Broadcasting in Ad Hoc Networks: Based on Self-Pruning", Twenty Second Annual Joint Conferences of IEEE Computer and Communication Societies, IEEE INFOCOM 2003*

[10]. *VintiParmar, Rahul Rishi3 "MANET: Vulnerabilities, Challenges, Attacks, Application", IEEE Trans. Mobile Computing, vol. 3, no. 6, pp. 263-284, July-Sept. 2009.*

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