CCRVC- Cluster Based Certificate Revocation with Vindication Capability for Mobile ADHOC Networks

[1]Ruchita H. Bajaj*, [2]P. L. Ramteke
[1]M.E. in CS-IT from SGBAU, [2]M.E. in CSE from SGBAU
India, Amravati

***Abstract*—** Certificate revocation is an important security component in mobile ad hoc networks (MANET). Securing network from various kinds of Attacks (MANET) plays an important role. Certificate revocation mechanisms play an important role in securing a network. The main challenge of certificate revocation is to revoke certificates of malicious nodes promptly and accurately. In this paper we use Cluster based certificate Revocation with vindication capability (CCRVC) scheme. It's possible to identify attackers from the network and permanently revoke the Certificate of Attacker node. And it revokes the accused node based on a single node's accusation. However the certificate accusation and recovery mechanisms have some limitations. The number of nodes capable of accusing malicious nodes decreased over time. It eventually lead to case malicious nodes can no longer be revoked in timely manner. To overcome this problem we propose Threshold based mechanism approach to vindicate warned nodes as legitimate nodes or not. And it enhances effectiveness and efficiency. By this scheme we improve the reliability and accuracy.

***Index Terms*— Mobile ad hoc network, certificate revocation, clustering and security.**

I. INTRODUCTION

Owing to the advances in wireless communications technologies, Mobile Ad hoc NETwork (MANET) has attracted much attention. MANET is a highly flexible network where nodes can freely move and join, with no fixed infrastructure, and thus it is vulnerable to attacks by malicious users. Therefore, ensuring network security is one of the most important issues in MANET. Although a large number of methods to detect various kinds of attacks have been developed for MANETs, only detecting and blocking attacks in each node is not enough to maintain network security because attackers can freely move and repeatedly launch attacks against different nodes. To reduce the damage from attacks, attackers must be immediately removed from the network after detection of the first attack; this can be achieved by using a certification system. 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.

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. In particular, ensuring the accuracy of certificate revocation is a significant challenge because malicious users may abuse the certification system. For instance, in the system which identifies attackers based on the information on the occurrence of attacks provided by nodes belonging to the network, the certificate of a legitimate user might be revoked by the false accusation from malicious nodes. Therefore, certificate revocation methods must be able to distinguish false accusations from valid ones. Also, malicious nodes must be immediately removed from accessing the network with a small operating overhead. In this paper, we propose a certificate revocation scheme which takes into account of false accusations from malicious users. The performance of the proposed scheme is evaluated in terms of promptness of revocation, operating overhead, and accuracy of revocation. The reminder of the paper is organized as follows. In Section II, existing certificate revocation methods are reviewed, and their advantages and drawbacks are briefly described. Section III presents the detailed mechanism of our proposed revocation scheme. The performance of the proposed scheme is evaluated and analyzed in Section IV, and Section V concludes the paper.his document is a template. An electronic copy can be downloaded from the Journal website. For questions on paper guidelines, please contact the journal publications committee as indicated on the journal website. Information about final paper submission is available from the conference website.

II. LITERATURE REVIEW AND RELATED WORK

The Manet is a tremendous research area. Know researchers started pay attention to MANET Security problems. Securing the Mobile Ad ho Network is quite difficult. The topology keeps on changing and Manet is Infrastructure less environment. The different approaches of certificate revocation which enhance proposed literature scheme. In this section we are going to see the existing methods: voting based mechanism and non-voting based mechanisms.

The voting based mechanism which looks for valid votes and certificate is revoked for the malicious nodes. Here first comes URSA (14) is a Voting based mechanism. It protects the mobile ad hoc network each node should have ticket to verify the network. A ticket is considered valid if it is certified and unexpired. When a new node joins a network and existing node which joins new location, it should exchange tickets with its one-hop neighboring nodes to establish a mutual trust relationship. Misbehaving nodes with invalid ticket will be removed from the network. URSA ticket services ensure that ideally only well-behaving nodes receive tickets. The implementation of ticket renewal and revocation services is fully distributed into each well-behaving node Through an initialization process during the bootstrapping phase of the network [14]. For nodes that join or rejoin the network, they can be

initialized by a certain number of neighbours in order to serve other nodes for ticket renewal and revocation. Neighbouring nodes also monitor each other during the normal operations with certain misbehavior detection mechanisms of their choice. When its ticket is about to expire, a node solicits its neighbouring nodes to collectively renew its ticket. URSA act as a passport for networking node. It has simple mechanisms for controlling misbehaving node and well behaving node. A localized certificate revocation scheme for Mobile ad hoc networks scheme [15] nodes in network vote together each node in Mane monitors other neighbouring nodes. The malicious node is identified by weight of the node. Like its past behaviour of nodes related to the term trustworthiness and reliability the weight of the node is calculated, no of accusations against itself from other node and accusation against other nodes. The stronger its reliability, the greater the weight will be acquired. If weight of the votes exceeds certain threshold level certificate is revoked for particular node. Doing so accuracy is increased however, all nodes are required to participate in voting, exchanging of communication voting information is high. So revocation time is high. In Non-voting mechanism the node is considered as malicious node by its valid certificate. Suicide for the Common Good [16]. In this approach single node can decide. . If another node is misbehaved it carry's the punishment to that node. The malicious node falsely accuse legitimate node to overcome is problem is to act punishment is costly. So we propose a new Method: A suicide for the common good. Suicide note which includes the both A and M. and detecting a node m have some illegal activity. The other node verify the signature and revoke both A and m. the both nodes send to block list and delete all keys which they shared than convincing way to let neighbours is sincerity to transmit a signed self-revocation certificate. Finally it sends to WL and remove from the network both accuser and accused nodes. The A, M sig_k is a suicide note in fig.4 its consists of public key or symmetric key cryptography [16]. The latter case arises whenever a node presents itself in several locations, either re-using identities (node replication) or presenting different ones (Sybil). We can assume that orthogonal mechanisms exist for detecting and preventing Sybil attacks. The main advantage in this scheme has: Less communication, fully decentralization and very fast removable of malicious node. The main drawback is certificate is revoked along with accused node with the accuser node. Certificate Revocation to Cope with False Accusations in Manet [17]. The existing method URSA does not has CA. Which controls the node distribution to the network in this method has CA.

Reliability:

In this scheme, nodes are differentiated according to their reliability; 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 (WL) and Black List (BL). 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 as described later in detail CA which maintains and updates WL and BL.

Node clustering:

The clustering which is proposed scheme of Manet which consists of CH cluster head, it contains nodes as member in that network. As CM cluster member. It controls the nods which are in transmitting ion range. Some nodes act as a cluster member. Only normal nodes can able to become cluster head (CH). The false accusation by misbehaving nodes in the network is controlled by CH. It first check cluster member, it checks any misbehaving is done in recent times, if not it will send to the warned list (WL). And CA updates the WL and BL. The accused node will be free to the network.

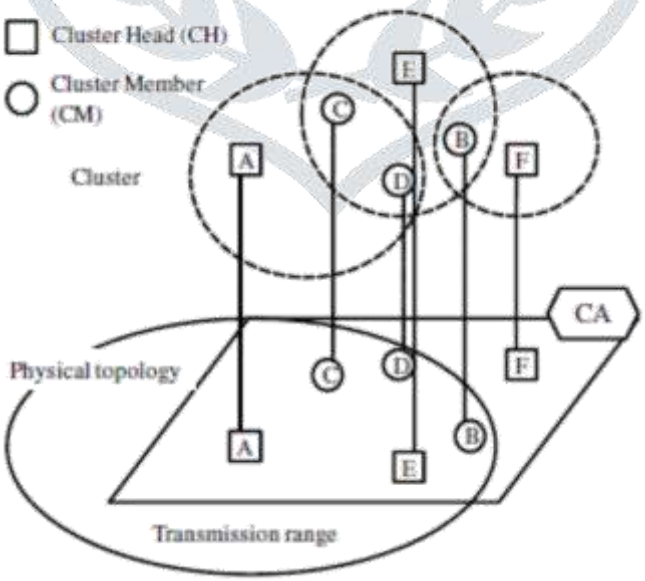

Fig1. Node Clustering

III. THE ENVISIONED SCHEME

Before delving into details of our envisioned scheme, it is worth noting a fundamental assumption. Nodes are assumed to be able to detect an attacker within their transmission range, e.g., in case of ad hoc flooding attacks [7], black hole attacks [8], worm hole attacks [9], and so forth.

Node reliability:

In the proposed 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 (WL) and Black List (BL), 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 as described later in detail. WL and BL are maintained by a CA which broadcasts all certificate information including WL and BL to the whole network upon the renewal of WL or BL.

Node clustering

By classifying nodes into clusters, the proposed scheme allows each Cluster Head (CH) to detect false accusation by a Cluster Member (CM) within the cluster. Node clustering provides a means to mitigate false accusations. CHs always monitors their CMs and watch for false accusations by means of the algorithm which will be discussed in Section 3.C.2). Fig. 1 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

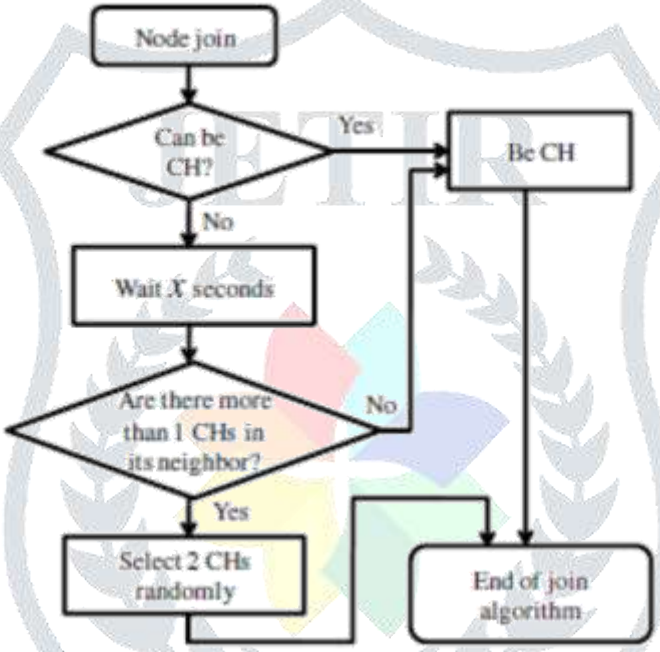

Fig2. Node join algorithm

CH might not be the member of the cluster and can be the CM of another cluster. For example, in Fig. 1, 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. Fig. 2 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. 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 above.

Two kinds of accusations

In the proposed scheme, two different kinds of accusation packets that induce update of the BL: *attack detection packets* that are used to register attackers in the BL, and *certificate recovery packets* that are used to eliminate legitimate nodes from the BL. While any normal node is allowed to send out attack detection packets upon detecting attackers around them, only CHs have permission to send certificate recovery packets. All nodes listed in BL or WL cannot accuse other nodes.

Attack detection packets:

Upon detecting attacks, normal nodes send out the attack detection packets to inform the CA of the attacker. Attack detection accusation can be done regardless of the clusters, i.e., any normal nodes detecting the attacks can accuse attackers. Attack detection packet includes not only the attacker's node ID but also the accuser's node ID. In the CA, if the accused attacker is not included in the BL, the attacker and the accuser are registered on the BL and WL, respectively. The reason behind registering the accuser in the WL is in the interest of conservation, to reduce the number of false accusations by malicious nodes. Even if the accuser is a malicious node, an additional false accusation can be prevented by registering the accuser in the WL because nodes listed in the WL are not allowed to make accusations. Fig. 3(a) shows the case where nodes A and C are lying in the transmission range of node B, and have detected an attack by node B at the same time. As the attack detection packet from node A arrives first at the CA, nodes B and A are registered on the BL and WL, respectively. After updating the lists, the CA broadcasts the certificate information packets including the latest list information to the whole network.

Since each node revokes the certificates of all nodes included in the BL according to the broadcasted information, node B is completely removed from the network. As described above, the attack detection packet allows nodes in the network to report attackers to the CA; the CA can then rapidly gather information about the attackers.

Certificate recovery packets:

In the proposed scheme, a legitimate node can be listed in the BL by a false attack detection packet sent from a malicious node. To cope with this issue, CHs are allowed to carry out the certificate recovery to correct the errors in the BL. Since all CMs are within the transmission range of their CH, the CH always detects any attacks by the CMs belonging to the cluster. In other words, if a CM is listed as an attacker in the BL without being detected by its CH, it implies that the CM was wrongly accused by malicious nodes. Errors in the BL can only be discovered by the CH. Therefore, CHs immediately carry out the certificate recovery to recover the certificate of the victim upon discovering the error in the BL. The certificate recovery packet includes the node IDs of the accuser and the exonerated victim. In the CA, if the victim has not been deleted from the BL yet, the BL can be appropriately corrected, both the victim and the accuser registered in the WL. Since the corrected information of the lists are broadcasted to all nodes in the network, the certificate of the victim can be recovered. Fig. 3(b) depicts the certificate recovery process in which node A's certificate has been revoked by the false attack detection packet by node B. While node D, which is one of the CHs of node A, receives the message from the CA that node A has been listed in the BL as an attacker, node D knows the information is inaccurate because node D has never detected any attacks from node A. Therefore, node D sends the accusation recovery packet to the CA in order to correct the error in the BL. When the certificate recovery packet from node D reaches the CA, the incorrect entry of node A in rather than on the BL is deleted while nodes A and D are registered in the WL. By broadcasting the updated lists, the certificate of node A is recovered throughout the network. As described above, the CA can grasp information about false accusations by using certificate recovery packets to mitigate the damage caused by false accusations.

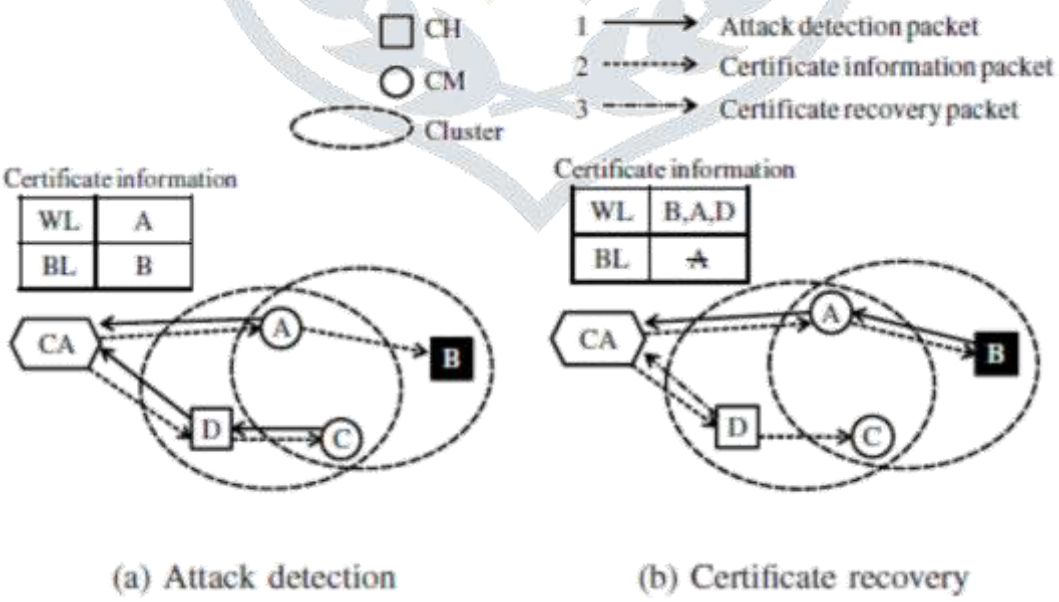

Fig3. Two kinds of Accusations

IV. APPLICATIONS

The original applications of ad-hoc networks were of a military kind. Vehicles on a battlefield are certainly mobile and move around in unpredictable manners. This is the original scene from where the very idea of ad-hoc networking was born. Other applications are in rescue operations where ad-hoc networks could be used by both police and firefighters. Search and rescue missions are also suitable applications. Possible commercial purposes could be for taxi communication, on boast, aircrafts and in sports stadiums. Personal uses are for laptops and notebook computers. Ad-hoc networking has even reached the entertainment business with Sony play station portable which uses this for multiplayer gaming.

V. CONCLUSION

Ad-hoc networking and clustering are very hot areas at the moment. There is a lot of research going on and not just in the military, where it all started. One can imagine how different, different ad-hoc networks can behave. There can be a generally high connectivity, that is many nodes in a small area, and there can be many aspects of the mobility. In a military application one can imagine a great deal of mobility of the nodes (vehicles of soldiers) in the middle of a battle. One can also expect certain nodes to stick together if the soldiers are organized in squads. In a non military scenario when nodes are people sitting with a laptop in a park for example one expects much less mobility. All these properties affect the choice of routing technique. Even if these different techniques are specialized in different areas some of them do have problems. Ad-hoc routing is a delicate problem and its not obvious how to do it, but because of the large number of applications and the bright future prospects, this is something I am sure we will see much more of in the future.

VI. ACKNOWLEDGEMENT

I heartly thank **Prof. P. L. Ramteke** for his valuable guidance during the preparation of the seminar. I am also grateful to our respected **Principal Dr. A. B. Marathe** .

Thanks and Regards,

REFERENCES

[1] 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.

[2] 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.

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

[4] H. Chan, V. D. Gligor, A. Perrig and G. Muralidharan, "On the distribution and revocation of cryptographic keys in sensor networks," IEEE Trans. Dependable and Secure Computing, vol. 2, no. 3, pp.233- 247. Oct.-Dec. 2005.

[5] C. Crepeau and C.R. Davis, "A Certificate Revocation Scheme for Wireless Ad Hoc Networks," Proc. of ACM Workshop Security of Ad Hoc and Sensor Networks, 2003.

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

[7] P. Yi, Z. Dai, Y. Zhong and S. Zhang, "Resisting flooding attacks in ad hoc networks," Int'l Conf. Information Technology: Coding and Computing, vol. 2, pp. 657-662, Apr. 2005.

[8] R.A. Raja Mahmood and A.I. Khan, "A survey on detecting black hole attack in AODV-based mobile ad hoc networks," Int'l Symp. High Capacity Optical Networks and Enabling Technologies, pp.18-20, Nov. 2007.

[9] F. Nait-Abdesselam, B. Bensaou and T. Taleb, "Detecting and avoiding wormhole attacks in wireless ad hoc networks," IEEE Commun. Mag., vol. 46, no. 4, pp.127-133, Apr. 2008.

[10] Scalable Network Technologies: "Qualnet," http://www.scalablenetworks.com/.