Cluster Based Mobile Adhoc Network

Shweta M Nirmanik[1], Bhagyavati U[2], Preeti M[3], Sushma S K[4], Vaidehi T[5]

[1]Professor, Department of CSE, REC, Hulkoti

[2, 3, 4, 5]Department of CSE, REC, Hulkoti

Abstract: ***Mobile unintended networks (MANETs) have attracted abundant attention because of their quality and simple readying. However, the wireless and dynamic natures render them a lot of prone to numerous sorts of security attacks than the wired networks. the main challenge is to ensure secure network services. to fulfill this challenge, certificate revocation is a crucial integral element to secure network communications. during this paper, we tend to concentrate on the difficulty of certificate revocation to isolate attackers from additional taking part in network activities. For fast and correct certificate revocation, we tend to propose the Cluster-based Certificate Revocation with Vindication Capability (CCRVC) theme. specifically, to boost the dependableness of the theme, we tend to recover the warned nodes to require half within the certificate revocation process; to boost the accuracy, we tend to propose the threshold-based mechanism to assess and vindicate warned nodes as legitimate nodes or not, before sick them. The performances of our theme are evaluated by each numerical and simulation analysis. intensive results demonstrate that the projected certificate revocation theme is effective and economical to ensure secure communications in mobile unintended networks.***

1. Introduction

MOBILE ad hoc networks (MANETs) have received increasing attention in recent years due to their mobility feature, dynamic topology, and ease of deployment. A mobile ad hoc network is a selforganized wireless network which consists of mobile devices, such as laptops, cell phones, and Personal Digital Assistants (PDAs), which can freely move in the network. In addition to mobility, mobile devices cooperate and forward packets for each other to extend the limited wireless transmission range of each node by multi hop relaying, which is used for various applications, e.g., disaster relief, military operation, and emergency communications. Security is one crucial requirement for these network services. Implementing security is therefore of prime importance in such networks.

Provisioning protected communications between mobile nodes in a hostile environment, in which a malicious attacker can launch attacks to disrupt network security, is a primary concern. Owing to the absence of infrastructure, mobile nodes in a MANET have to implement all aspects of network functionality themselves; they act as both end users and routers, which relay packets for other nodes. Unlike the conventional network, another feature of MANETs is the open network environment where nodes can join and leave the network freely.

Therefore, the wireless and dynamic natures of MANETs expose them more vulnerable to various types of security attacks than the wired networks. Among all security issues in MANETs, certificate management is a widely used mechanism which serves as a means of conveying trust in a public key infrastructure, to secure applications and network services. A complete security solution for certificate management should encompass three components: prevention, detection, and revocation. Tremendous amount of research effort has been made in these areas, such as certificate distribution, attack detection, and certificate revocation. Certification is a prerequisite to secure network communications. It is embodied as a data structure in which the public key is bound to an attribute by the digital signature of the issuer, and can be used to verify that a public key belongs to an individual and to prevent tampering and forging in mobile ad hoc networks. Many research efforts have been dedicated to mitigate malicious attacks on the network. Any attack should be identified as soon as possible. Certificate revocation is an important task of enlisting and removing the certificates of nodes who have been detected to launch attacks on the neighborhood. In other words, if a node is compromised or misbehaved, it should be removed from the network and cut off from all its activities immediately. In our research, we focus on the fundamental security problem of certificate revocation to provide secure communications in MANETs.

2. Architecture

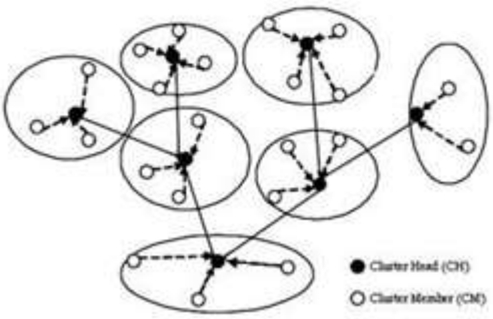

Figure 1: Cluster-Based Architecture

In MANETs, certificate management is the mechanism that is widely used since it helps in delivering trust in a public key infrastructure to protect applications and network services. For certificate management, a complete security solution has three components such as prevention, detection, and revocation. Many research efforts took place in some areas such as certificate distribution attack detection and certificate revocation. In order to secure network communications, Certification is essential. The public key is encrypted into an attribute using the digital signature of the issuer. It is used to assure that a public key belongs to an individual and helps in preventing tampering and forging in mobile Adhoc networks. Enormous research efforts are made to abate malicious attacks on the network. If any attack is identified, Certificate revocation plays a major task of enlisting and removing the certificates of nodes which have been detected to launch attacks on the neighborhood. This helps in removing misbehaving nodes from the network and gets blocked from all its activities suddenly. Certificate revocation's basic security problem is aimed at providing secure communications in MANETs. This paper proposes a Cluster-based Certificate Revocation with the scheme of Vindication Capability (CCRVC) which has ability to enhance the performance of MANET. Topology is constructed as clusters. A cluster consists of nodes within the transmission range and each cluster has Cluster Head (CH) and Cluster Member (CM). The nodes having a valid certificate alone are allowed to join the network. Certification Authority (CA) issues the valid certificates. Nodes are arranged as clusters that ensures preloading of certificate which is responsible for distributing and managing certificates of all nodes which in turn can communicate with each other without any constraints. The CA updates two lists such as Warned list and Black lists that holds information of accusing and accused nodes respectively

3. System Design

The system design involves the different steps involved in the proposed Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme. The entire process is summarized in the Fig.2 which gives a clear cut idea about the proposed method.

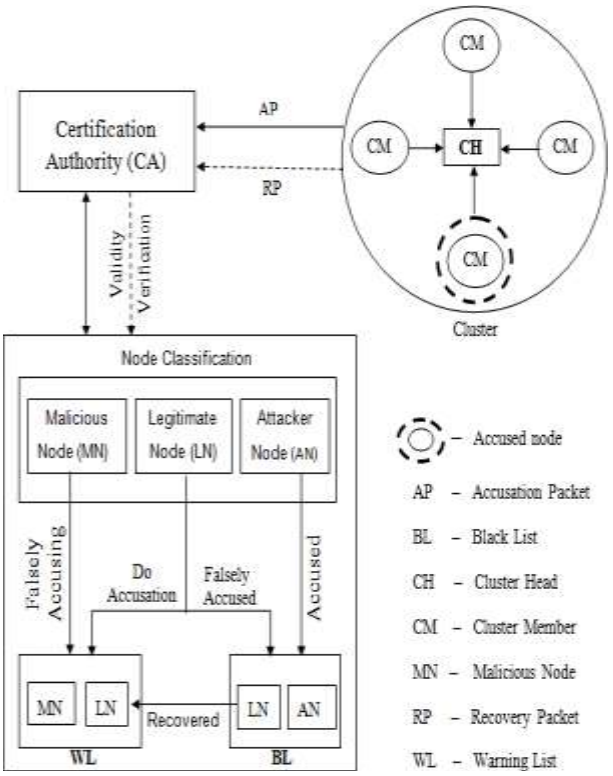

Figure 2: System Architecture for CCRVC Scheme

Process

When the neighboring nodes detect attacks from any one node then each of the nodes sends out an accusation packet to the certificate authority (CA) against attacker node. According to the first received packet, the CA holds neighboring node and attacker node in the Warning List (WL) and Black List (BL)., respectively, after verifying the validity of neighboring node the CA disseminates the revocation message to all nodes in the network. After receiving the revocation message nodes update their local WL and BL to revoke attacker's certificate. Meanwhile, CH update their WL and BL and determine that one of the node was framed. Then some of the nodes send recovery packet to CA to revive the falsely accused node. Upon receiving the first recovery packet, the CA removes the falsely accused node from the BL and holds both the falsely accused node and normal node in the WL and then disseminates the information to all the nodes. At last the nodes update their WL and BL to recover the falsely accused node.

4. Flow Chart

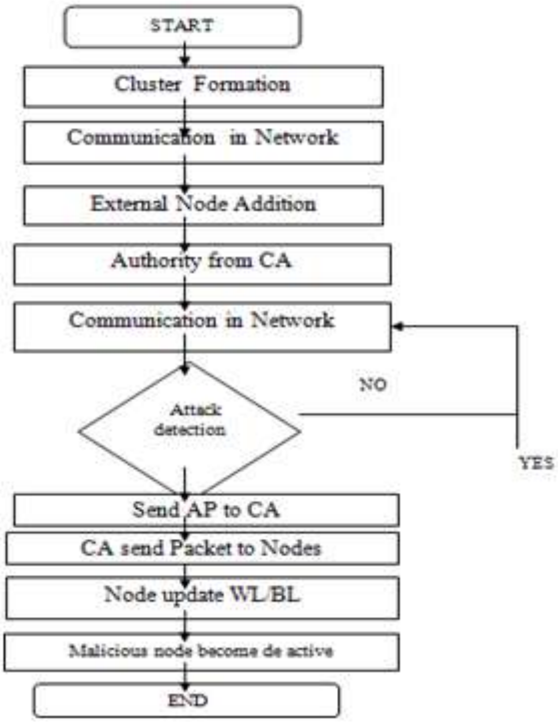

Figure 3: Certificate Revocation flowchart

Policies

- Topology Formation
- Detection and trace back of ATTACKS
- Certificate Revocation

1) Topology Formation

Constructing Project design in NS2 should takes place. Each node should send hello packets to its neighbor node which are in its communication range to update their topology.

2) Detection and trace back of ATTACKS

Neighboring nodes detect attacks of attacker node. Each of them sends out an accusation packet to the CA against attacker node. According to the first received packet (e.g., from node B), the CA hold B and M in the WL and BL, respectively, after verifying the validity of node B. The CA disseminates the revocation message to all nodes in the network.

3) Certificate revocation

To revoke a malicious attacker's certificate, we need to consider three stages: accusing, verifying, and notifying. The revocation 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. To revoke a malicious attacker's certificate, three techniques used: accusing, verifying, and notifying. The revocation 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. The accusing node is held in the WL. Finally, by broadcasting the revocation messages including the WL and BL through the whole network by the CA, nodes that are in the BL are in the BL are successfully revoked from the network.

5. Conclusion

In this paper, we have addressed a major issue to ensure secure communications for mobile ad hoc networks, namely, certificate revocation of attacker nodes. In contrast to existing algorithms, we propose a cluster-based certificate revocation with vindication capability scheme combined with the merits of both voting-based and non-voting based mechanisms to revoke malicious certificate and solve the problem of false accusation. The scheme 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 clusterbased 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. In doing so, we have sufficient nodes to ensure the efficiency of quick revocation. The extensive results have demonstrated that, in comparison with the existing methods, our proposed CCRVC scheme is more effective and efficient in revoking certificates of malicious attacker nodes, reducing revocation time, and improving the accuracy and reliability of certificate revocation.

References

[1] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[2] P. Sakarindr and N. Ansari, "Security Services in Group Communications Over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks," IEEE Wireless Comm., vol. 14, no. 5, pp. 8-20, Oct. 2007.

[3] A.M. Hegland, E. Winjum, C. Rong, and P. Spilling, "A Survey of Key Management in Ad Hoc Networks," IEEE Comm. Surveys and Tutorials, vol. 8, no. 3, pp. 48-66, Third Quarter 2006.

[4] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Nov./Dec. 1999.

[5] L. Zhou, B. Cchneider, and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.

[6] H. Chan, V. 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, July 2005.

[7] B. Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemoto, and N. Kato, "A Survey of Routing Attacks in MANET," IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.

[8] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A Dynamic Anomaly Detection Scheme for Aodv-Based Mobile Ad Hoc Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 5, pp. 2471-2481, June 2009.

[9] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Network: Analysis & Defenses," Proc. Third Int'l Symp. Information Processing in Sensor Networks, pp. 259-268, 2004.

[10] S. Micali, "Efficient Certificate Revocation," Massachusetts Inst. Of Technology, Cambridge, MA, 1996.