e-ISSN : 2349-9745
p-ISSN : 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

A HEURISTIC APPROACH FOR SECURE COMMUNICATION IN MOBILE AD HOC NETWORK

Elakkiya.E[1], Sakthivel.S2
[1]*Dept of ECE, Vivekananda college of engineering for women.*
[2]*Assistant professor, Dept of ECE, Vivekananda college of engineering for women.*

Abstract-- Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor. in which MANET does not require a fixed network infrastructure. Mobile ad hoc networks (MANETs) have attracted much attention due to their mobility and ease of deployment. However, the wireless and dynamic natures render them more vulnerable to various types of security attacks than the wired networks. The major challenge is to guarantee secure network services. To meet this challenge, certificate revocation is an important integral component to secure network communications. In this paper, we focus quick and accurate certificate revocation, we propose the Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme. In particular, to improve the reliability of the scheme, The performances of our scheme are evaluated by both numerical and simulation analysis. Extensive results demonstrate that the proposed certificate revocation scheme is effective and efficient to guarantee secure communications in mobile ad hoc networks.

I. INTRODUCTION

MOBILE ad hoc networks (MANETs) have received increasing attention in recent years due to their mobility feature, dynamic topology, A mobile ad hoc network is a self-organized 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 multichip 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.

II. EXISTING METHOD

2.1 VOTING BASED MECHANISM:

The mechanism is defined as the means of revoking a malicious attacker's certificate through votes from valid neighboring nodes. The certificates of newly joining nodes are issued by their neighbors. The certificate of an attacker is revoked on the basis of votes from its neighbors. In URSA, each node performs one-hop monitoring, and exchanges monitoring information with its neighboring nodes. When

the number of negative votes exceeds a predetermined number, the certificate of the accused node will be revoked.

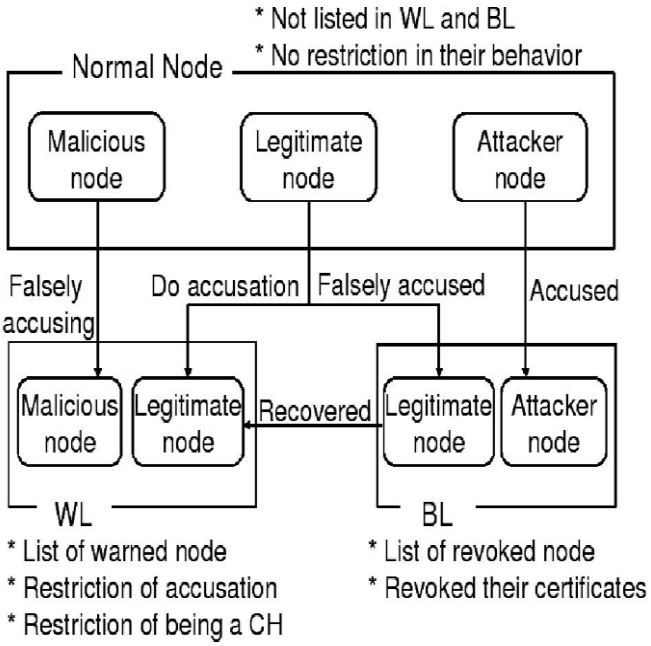
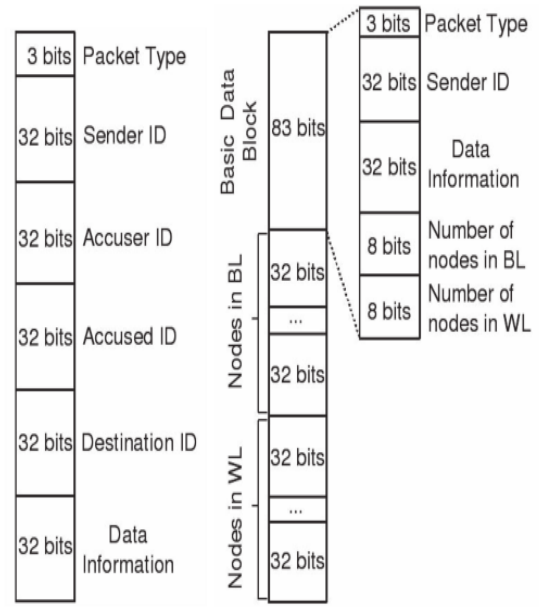


Fig. 1. The classification of nodes in our scheme

2.2 NON VOTING BASED MECHANISM:

In the non-voting-based mechanism, a given node deemed as a malicious attacker will be decided by any node with a valid certificate. The certificates of both the accused node and accusing node have to be revoked simultaneously. In other words, the accusing node has to sacrifice itself to remove an attacker from the network. Although this approach dramatically reduces both the time required to evict a node and communications overhead of the certificate revocation procedure due to its suicidal strategy, the application of his strategy is limited.



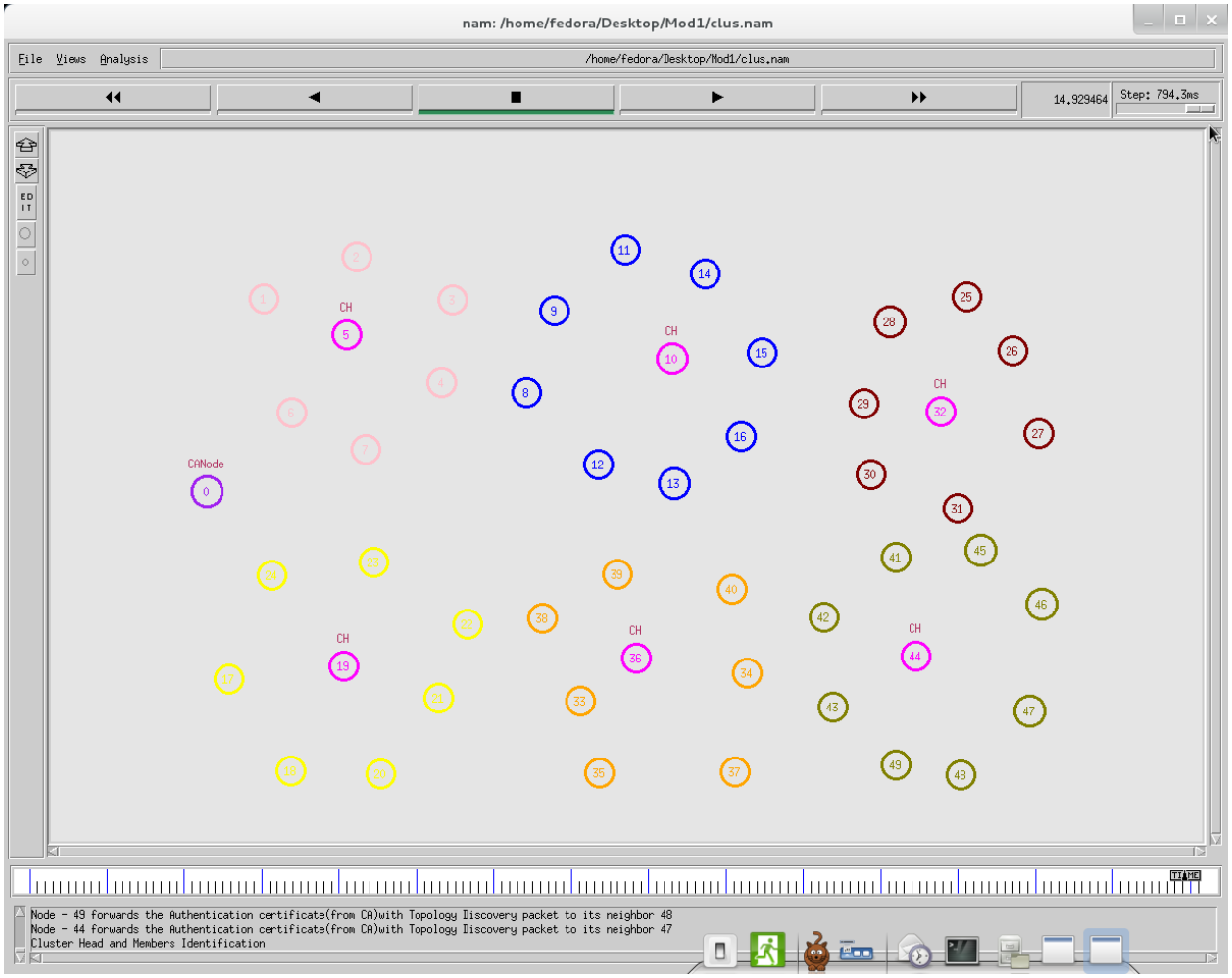
(a) Format of accusation and recovery packets. (b) Format of broadcasting packet.

Fig. 2. Control packets.

III. PROPOSED SYSTEM

We propose a Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme. Like our previously proposed cluster-based schemes clustering is incorporated in our proposed scheme, where the cluster head plays an important role in detecting the falsely accused nodes within its cluster and recovering their certificates to solve the issue of false accusation. On the other hand, CCRVC inherits the merits of both the voting- based and non-voting-based schemes, in achieving prompt revocation and lowering overhead as compared to the voting-based scheme, improving the reliability and accuracy as compared to the non-voting based scheme. Our scheme can quickly revoke the malicious device's certificate, stop the device access to the network, and enhance network security. 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, improving the accuracy as compared to the non-voting- based mechanism. The proposed scheme exhibits more reliable and higher efficiency as compared to the existing ones, because it guarantees sufficient normal nodes to revoke the certificates of the attackers and takes a short revocation time

IV. SIMULATION RESULT



V.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 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. 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] 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.
[2] 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.
[3] 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.
[4] 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
[5] 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.
[6] 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.

