ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Improving Attack Detection and Reducing Communication Overhead For Mobile Adhoc Networks

B.Lakshmi Priya, D.Prabakar, Dr.S.Karthik

PG Scholar, Department of CSE, SNS College of technology, Coimbatore, India

Assistant Professor, Department of CSE, SNS College of technology, Coimbatore, India

Dean & Professor, Department of CSE, SNS College of technology, Coimbatore, India

ABSTRACT: In Mobile Ad hoc NETworks (MANETs), certification systems play an important role in maintaining network security because attackers can freely move and repeatedly launch attacks against different nodes. 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 certification systems is difficult to differentiate valid accusations made by legitimate nodes from false accusations made by malicious nodes and also the amount of traffic in order to exchange information on attackers and the necessary time to gather the information increases as the network size becomes larger.A certificate revocation scheme which can revoke the certification of attackers in a short time with a small amount of operating traffic. By clustering nodes and introducing multi-level node reliability, the Certificate scheme can mitigate the improper certificate revocation due to false accusations by malicious users.

1.INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless.Each device in a MANET is free to move independently in any direction, and therefore change its links to other devices frequently. Each node must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. The growths of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

1.1 MANETS FEATURES AND THEIR IMPACT ON SECURITY

The features of MANETs make them more vulnerable to attacks and misbehavior than traditional networks, and imposes the security solution to be different from those used in other networks.These features are:

- INFRASTRUCTURELESS:Central servers, specialized hardware, and fixed infrastructures are necessarily absent. The lack of infrastructure precludes the deployment of hierarchical host relationships; instead, nodes uphold egalitarian relationships.
- WIRELESS LINKS USE: The use of wireless links renders a wireless ad hoc network susceptible to attacks.
- MULTI-HOP: Because the lack of central routers and gateways, hosts are themselves routers, then

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

packets follow multi-hop routes and pass through different mobile nodes before arriving to the destination.

- AMORPHOUS: Nodes mobility and wireless connectivity allow nodes to enter and leave the network spontaneously.
- POWER LIMITATION: Adhoc enabled mobile nodes are small and lightweight, therefore, nodes are often supplied with limited power resources, small batteries, to ensure portability which causes vulnerability.
- MEMORY AND COMPUTATION POWER LIMITATION: Adhoc enabled mobile nodes have limited storage devices and weak computational capabilities. High complexity security solutions employed, as cryptography, should take these constraints into consideration.

1.2 CHARACTERISTICS OF MANETS.

A MANET consists of mobile platforms simply referred to as "nodes", which are free to move about arbitrarily. A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network. In the latter operational mode, it is typically envisioned to operate as a "stub" network connecting to a fixed internetwork. Stub networks carry traffic originating at and/or destined for internal nodes, but do not permit exogenous traffic to "transit" through the stub network.

MANET nodes are equipped with wireless transmitters and receivers using antennas which may be Omni directional (broadcast), highly- directional (point-to-point), possibly steerable. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multihop graph or "ad hoc" network exists between the nodes. The adhoc topology may change with time as the nodes move or adjust their transmission and reception parameters.

MANETs have several salient characteristics:

- DYNAMIC TOPOLOGIES: Nodes are free to move arbitrarily. The network topology which is typically multihop may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.
- BANDWIDTH-CONSTRAINED: Wireless links used to have significantly lower capacity than their hardwired counterparts.
- ENERGY-CONSTRAINED OPERATION: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.
- LIMITED PHYSICAL SECURITY: Mobile wireless networks are generally more prone to physical security threats than are fixed cable nets. The increased possibility of eavesdropping,spoofing, and denial-of-service attacks should be carefully considered.

2. MECHANISMS

2.1 VOTING-BASED MECHANISM

Voting-Based Mechanism is defined as the means of revoking a malicious attacker's certificate through votes from valid neighboring nodes.

2.2NON-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.

2.3RELIABILITY-BASED NODE CLASSIFICATION

According to the behavior of nodes in the network, three types of nodes are classified according to their behaviors: legitimate, malicious, and attacker nodes. A legitimate node is deemed to secure communications with other nodes. It is able to correctly detect attacks from malicious attacker nodes and accuse them positively, and to revoke their certificates in order to guarantee network security.

A malicious node does not execute protocols to identify misbehavior, vote honestly, and revoke malicious attackers. In particular, it is able to falsely accuse a legitimate node to revoke its certificate

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

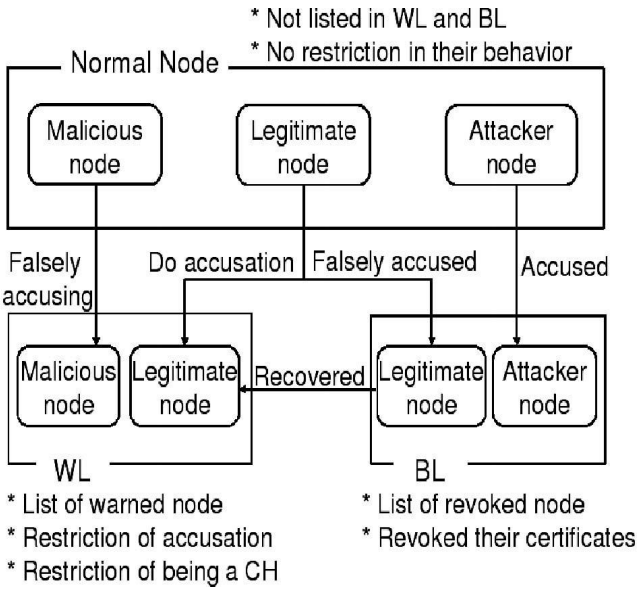
An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

successfully. The so-called attacker node is defined as a special malicious node which can launch attacks on its neighbors to disrupt secure communications in the network.



These nodes can be further classified into three categories based on their reliability: normal node, warned node, and revoked node. When a node joins the network and does not launch attacks, it is regarded as a normal node with high reliability that has the ability to accuse other nodes and to declare itself as a CH (Cluster Head) or a CM (Cluster Member).Normal nodes consist of legitimate nodes and potential malicious nodes.

Nodes that are listed in the warning list are deemed as warned nodes with low reliability. Warned nodes are permitted to communicate with their neighbors with some restrictions.

The accused nodes that are held in the blacklist are regarded as revoked nodes with little reliability. Revoked nodes are considered as malicious attackers deprived of their certificates and evicted from the network.

2.4 CERTIFICATE REVOCATION

2.4.1PROCEDURE OF REVOKING MALICIOUS CERTIFICATES

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. If not, the neighboring node casts the Accusation Packet (AP) to the CA, which the format of accusation packet.

2.4.2 COPING WITH FALSE ACCUSATION

The false accusation of a malicious node against a legitimate node to the CA will degrade the accuracy and robustness of our scheme.

To overcome this problem, our aim is to construct clusters. The clusters are to enable the CH to detect false accusation and it will restore the falsely accused nodes within its clusters.

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.

3. CONCLUSION

The concept addressed a major issue to ensure secure communications for mobile ad hoc networks, certificate revocation of attacker nodes. In contrast to existing algorithms, the proposed scheme combined with the Cluster-Based Certificate Revocation with Vindication Capability 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

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

revocation time as compared to the CCRVC mechanism. In addition, it have adopted the cluster-based model to restore falsely accused nodes by the CH, thus improving the accuracy as compared to the CCRVC mechanism.Particularly,a new incentive method is used to release and restore the legitimate nodes, and to improve the number of available normal nodes in the network and also produce sufficient nodes to ensure the efficiency of quick revocation.

REFERENCES

1.Bettstetter.C,Resta.G and Santi.P,(2003) "The Node Distribution of the Random Waypoint model for Adhoc Wireless Networks," IEEE Trans. Mobile Computing, vol. 2, no. 3, pp. 257-269, July-Sept. 2003.
2.Gentry.C,(2003)"Certificate-Based Encryption and the Certificate Revocation Problem," EUROCRYPT: Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques, pp. 272-293.
3.Hegland.A.M,Winjum.E,Rong.C,and Spilling.P,(2006)"A Survey of Key Management in Ad Hoc Networks," IEEE Comm. Surveys and Tutorials, vol. 8, no. 3, pp. 48-66.
4.Lian.J,Naik.K, and Agnew.G.B,(2007)"A Framework for Evaluating the Performance of Cluster Algorithms for Hierarchical Networks," IEEE/ACM Trans. Networking, vol. 15, no. 6, pp. 1478-1489.
5.Luo.H,Kong.J,Zerfos.P,Lu.S,and Zhang.L,(2004)"URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," IEEE/ACM Trans. Networking, vol. 12, no. 6, pp. 1049-1063.
6.Nakayama.H,Kurosawa.S,Jamalipour.A,Nemoto.Y, and Kato.N,(2009)"A Dynamic Anomaly Detection Scheme for Aodv-Based Mobile Ad Hoc Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 5, pp. 2471-2481.
7.Sakarindr.P and Ansari.N,(2007)"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.
8.Yang.H,Luo.H,Ye.F,Lu.S, and Zhang.L,(2004)"Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47.
9.Yang.H,Shu.J,Meng.X, and Lu.S,(2006) "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 261-273.
10.Yi.P,Dai.Z,Zhong.Y, and Zhang.S, (2005)"Resisting Flooding Attacks in Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, vol. 2, pp. 657-662.