ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Effective Cluster Based Certificate Revocation with Vindication Capability in MANETS Project Report

Mandadapu Sravya
M.Tech,
Department of CSE,
G. Narayanamma Institute of Technology and Science.

Ch.Mandakini
Assistant Professor,
Department of CSE,
G. Narayanamma Institute of Technology and Science.

ABSTRACT:

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 on the issue of certificate revocation to isolate attackers from further participating in network activities. For 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, we recover the warned nodes to take part in the certificate revocation process; to enhance the accuracy, we propose the threshold-based mechanism to assess and vindicate warned nodes as legitimate nodes or not, before recovering them. 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.

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 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 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.

EXISTING SYSTEM:

Recently, researchers pay much attention to MANET security issues. It is difficult to secure mobile ad hoc networks, notably because of the vulnerability of wireless links, the limited physical protection of nodes, the dynamically changing topology, and the lack of infrastructure. Various kinds of certificate revocation techniques have been proposed to enhance network security in the literature. In this section, we briefly introduce the existing approaches for certificate revocation, which are classified into two categories: voting based mechanism and non-voting-based mechanism.

DISADVANTAGES OF EXISTING SYSTEM:

Voting-Based Mechanism

- ⇨ 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.
- ⇨ When the number of negative votes exceeds a predetermined number, the certificate of the accused node will be revoked. Since nodes cannot communicate with others without valid certificates, revoking the certificate of a voted node implies isolation of that node from network activities.

Non-Voting-Based Mechanism

=> However certificates of both the accused node and accusing node have to be revoked simultaneously.

=> 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 this strategy is limited.

PROPOSED SYSTEM:

In the proposed system, the Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme. In particular, to improve the reliability of the scheme, we recover the warned nodes to take part in the certificate revocation process; to enhance the accuracy, we propose the threshold-based mechanism to assess and vindicate warned nodes as legitimate nodes or not, before recovering them. 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 intermediate Nodes.

ADVANTAGES OF PROPOSED SYSTEM:

Cluster Construction

- ⇨ A trusted third party, certification authority, is deployed in the cluster-based scheme to enable each mobile node to preload the certificate.
- ⇨ The CA is also in charge of updating two lists, WL and Blacklist, which are used to hold the accusing and accused nodes' information, respectively. Concretely, the BL is responsible for holding the node accused as an attacker, while the WL is used to hold the corresponding accusing node.

Reliability-Based Node Classification

- 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 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.
- 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 or a CM. Moreover, we should note that normal nodes consist of legitimate nodes and potential malicious nodes.

IMPLEMENTATION

Cluster Construction

We present the cluster based architecture to construct the topology. Nodes cooperate to form clusters, and each cluster consists of a CH along with some Cluster Members (CMs) located within the transmission range of their CH. Before nodes can join the network, they have to acquire valid certificates from the CA, which is responsible for distributing and managing certificates of all nodes, so that nodes can communicate with each other unrestrainedly in a MANET. While a node takes part in the network, it is allowed to declare itself as a CH with a probability of R. Note that neighbor sensing protocols, such as periodical broadcast of hello messages, are effective approaches used in routing protocols to check the availability of links between neighboring nodes. A new link is detected if a node receives a new hello message. Otherwise, the link is considered disconnected if none of the hello messages is received from the neighboring node during a time period.

Reliability-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 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.

Normal Nodes Depreciation

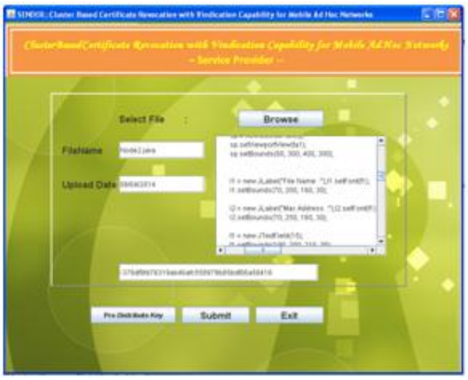
Nodes enlisted in the WL by certificate revocation lose the function of accusation since the CA does not accept accusation packets from nodes enlisted in the WL in order to prevent further damage from malicious nodes. Thus, as the number of malicious nodes increases, an increasing number of normal nodes are listed in the WL; subsequently, there will not be enough normal nodes to accuse the attacker nodes over time. Such scenario will affect the reliability of the scheme.

Node Releasing

As a solution to release nodes from the WL, we should first consider the two cases for nodes to be listed in the WL. the first case is that a legitimate node correctly accuses an attacker node, thus resulting in the accusing node and accused node being listed in the WL and BL, respectively; the other case is the enlisting of a malicious node in the WL because it sends false accusation against a legitimate node.

Hence, nodes in the WL may be legitimate nodes as well as malicious nodes. Therefore, to improve the reliability and accuracy, nodes must be differentiated between legitimate nodes and malicious nodes so as to release legitimate nodes from the WL and withhold malicious nodes in the WL.

SCREEN SHOTS:


SENDER: Cluster Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks
Cluster Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks
-- Service Provider --
Select File :
Browse
Filename
Upload Date
Pre Distribute Key
Submit
Exit

Filename: Node2.java

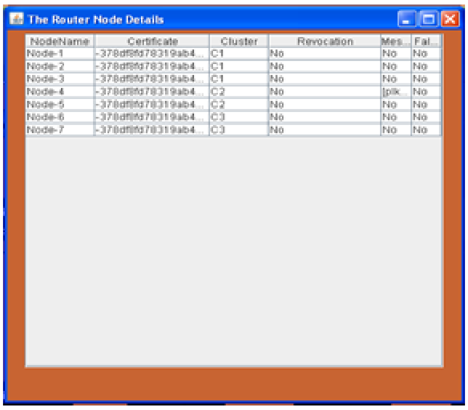
```
sp.setViewportView(ta1);
sp.setBounds(50, 300, 400, 300);

l1 = new JLabel("File Name :");l1.setFont(f1);
l1.setBounds(70, 200, 180, 30);

l2 = new JLabel("Mac Address :");l2.setFont(f1);
l2.setBounds(70, 250, 180, 30);

t1 = new JTextField(15);
```

Fig: Service Provider



NodeName	Certificate	Cluster	Revocation	Mes...	Fal...
Node-1	-378df8fd78319ab4...	C1	No	No	No
Node-2	-378df8fd78319ab4...	C1	No	No	No
Node-3	-378df8fd78319ab4...	C1	No	No	No
Node-4	-378df8fd78319ab4...	C2	No	jpik...	No
Node-5	-378df8fd78319ab4...	C2	No	No	No
Node-6	-378df8fd78319ab4...	C3	No	No	No
Node-7	-378df8fd78319ab4...	C3	No	No	No

Fig: Router Node Details

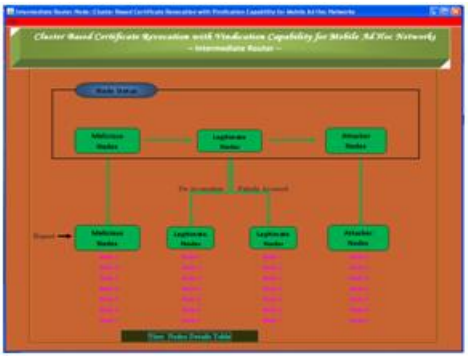

Cluster Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks
-- Intermediate Router --
Node Status
Malicious Nodes
Legitimate Nodes
Attacker Nodes
View Node Details Table

Fig: Intermediate Router

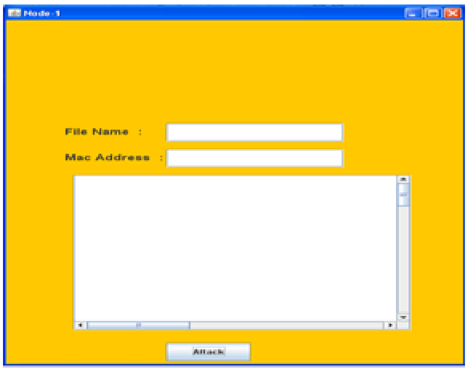
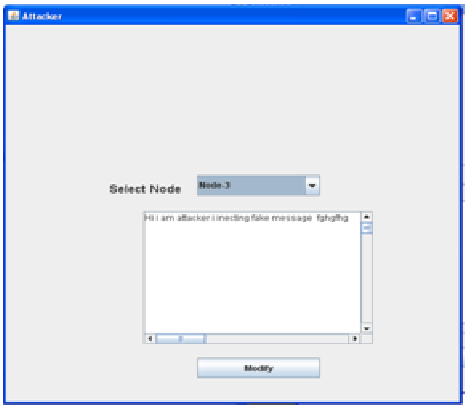


Fig: Node 1



Hi i am attacker i inecting fake message fghgfhg

Fig: Attacker

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] 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] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, “Resisting Flooding Attacks in Ad Hoc Networks,” Proc. Int’l Conf. Information Technology: Coding and Computing, vol. 2, pp. 657-662, Apr. 2005.

[8] 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.

[9] 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.

[10] 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.

[11] S. Micali, “Efficient Certificate Revocation,” Massachusetts Inst. Of Technology, Cambridge, MA, 1996.

[12] 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.

[13] H. Yang, J. Shu, X. Meng, and S. Lu, “SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks,” IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 261-273, Feb. 2006.