International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 4: April 2015, pp 35-38. www.aetsjournal.com ISSN (Online) : 2394-6237

Huddle Based Certificate Revocation with Vindication Capabilty in Large Scale Wireless Networks

T.Archana Devi, K.Petchiappan, Dr.K.Balasubadra

Abstract— Certificate revocation is an important task of enlisting and removing the certificates of nodes that have been detected to launch attacks on the neighborhood. In this paper, we have addressed a major issue to ensure secure communications and file transferring for mobile ad hoc networks, namely, certificate revocation of attacker nodes. For this purpose, we propose a Cluster-based Certificate Revocation with Vindication Capability (CCRVC) 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. Our scheme can quickly revoke the malicious device's certificate, stop the device access to the network, and enhance network security. And also it performs the process of cryptographic puzzles technique for generating security for that file sharing. So sharing provides more security compared to the existing system. 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.
Key Word-

***Keywords*—** Certificate revocation, CCRCV, malicious certificate, accuracy etc.

I. INTRODUCTION

A A Mobile Ad hoc Network (MANET) is one that comes together as needed, not necessarily with any support from the existing Internet infrastructure or any other kind of fixed stations. We can formalize this statement by defining an ad hoc network as an autonomous system of mobile hosts connected by wireless links, the union of which forms a communication network modeled in the form of an arbitrary graph. This is in contrast to the well-known single hop cellular network model that supports the needs of wireless communication by installing base stations as access points. In these cellular networks, communications between two mobile nodes completely rely on the wired backbone and the fixed base stations. In a MANET, no such infrastructure exists and the network topology may dynamically change in an unpredictable manner since nodes are free to move.

Game theory can provide a useful tool to study the security problem in mobile ad hoc networks (MANETs). Most of existing works on applying game theories to security only consider two players in the security game model: an attacker and a defender. While this assumption may be valid for a network with centralized administration, it is not realistic in MANETs, where centralized administration is not available. Game theory is a useful tool to provide a mathematical framework for modeling and analyzing decision problems, since it can address problems where multiple players with contradictory goals or incentives compete with each other. In game theory, one player's outcome depends not only on his/her decisions, but also on those of others' decisions. Similarly, the success of a security scheme in MANETs depends not only on the actual defense strategies, but also on the actions taken by the attackers.

A complete security solution for certificate management should encompass three components: prevention, detection, and 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.

II. LITERATURE SURVEY

A. A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks

In this paper we have attempted to present an overview of the routing protocols, the known routing attacks and the proposed countermeasures to these attacks in various works. MANETs is an emerging technological field and hence is an active area of research. Because of ease of deployment and defined infrastructure less feature these networks find applications in a variety of scenarios ranging from emergency operations and disaster relief to military service and task forces. Providing security in such scenarios is critical. The primary limitation of the MANETs is the limited resource capability: bandwidth, power back up and computational capacity. Absence of infrastructure, changing topology makes

T.Archana Devi, P.G. Scholar, Department Of Computer Science & Engg, St. Michael College Of Engg. &Technology, Kalayarkoil, Sivaganga, India. (Email : archudevi92@gmail.com)

K.Petchiappan, Professor , Department Of Computer Science & Engg, St. Michael College Of Engg. &Technology, Kalayarkoil, Sivaganga, India. (Email : archudevi92@gmail.com)

Dr.K.Balasubadra, Professor & Head, Department of Information Technology, R.M.D College Of Engineering Kavaraipettai, Tiruvallur, India. (email : b a l a s u b a d r a @yahoo.com)

the security of MANETs particularly difficult. Also no centralized authority is present to monitor the networking operations. Therefore, existing security schemes for wire networks cannot be applied directly to a MANETs, which makes them much more vulnerable to security attacks.

B. Certificate-Based Encryption and the Certificate Revocation Problem Craig Gentry DoCoMo USA Lab cgentry@docomolabs-usa.com

We introduce the notion of certificate-based encryption. In this model, a certificate – or, more generally, a signature – acts not only as a certificate but also as a decryption key. To decrypt a message, a keyholder needs both its secret key and an up-to-date certificate from its CA (or a signature from an authorizer). Certificate-based encryption combines the best aspects of identity-based encryption (implicit certification) and public key encryption (no escrow). We demonstrate how certificate-based encryption can be used to construct an efficient PKI requiring fewer infrastructures than previous proposals, including Micali's Novomodo, Naor-Nissim and Aiello-Lodha-Ostrovsky.

C. Securing Ad Hoc Networks

This paper focuses on how to secure routing and how to establish a secure key management service in an ad hoc networking environment. These two issues are essential to achieving our security goals. Besides the standard security mechanisms, we take advantage of the redundancies in ad hoc network topology and use diversity coding on multiple routes to tolerate both benign and Byzantine failures. To build a highly available and highly secure key management service, we propose to use threshold cryptography to distribute trust among a set of servers. Furthermore, our key management service employs share refreshing to achieve proactive security and to adapt to changes in the network in a scalable way.

D.A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks.

The issue of certificate revocation in mobile ad hoc networks (MANETs) where there are no on-line access to trusted authorities is a challenging problem. In wired network environments, when certificates are to be revoked, certificate authorities (CAs) add the information regarding the certificates in question to certificate revocation lists (CRLs) and post the CRLs on accessible repositories or distribute them to relevant entities. In purely ad hoc networks, there are typically no access to centralized repositories or trusted authorities; therefore the conventional method of certificate revocation is not applicable. In this paper, we present a decentralized certificate revocation scheme that allows the nodes within a MANET to revoke the certificates of malicious entities. The scheme is fully contained and it does not rely on inputs from centralized or external entities.

E. Throughput and delay in random wireless networks with restricted mobility.

This paper studies the delay scaling at throughput for a random network with restricted mobility. First, a variant of the scheme presented by Diggavi, Grossglauser and Tse is presented and it is shown to achieve throughput using different (and perhaps simpler) techniques. The exact order of delay scaling for this scheme is determined, somewhat surprisingly, to be of _(n log n), which is the same as that without the mobility restriction. Thus, this particular mobility restriction *does not* affect either the maximal throughput scaling or the corresponding delay scaling of the network. This happens because under this 1-D restriction, each node is in the proximity of every other node in essentially the same manner as without this restriction.

III. EXISTING SYSTEM

In existing system recent advances in mean field game theory that proposed a novel game theoretic approach with multiple players for security in MANETs. The mean field game theory provided a powerful mathematical tool for problems with a large number of players. The scheme can enable an individual node in MANETs to make strategic security defense decisions without centralized administration. In addition, since security defense mechanisms consume precious system resources (e.g., energy), and this scheme considered not only the security requirement of MANETs but also the system resources. Moreover, each node in the proposed scheme only needs to know its own state information and the aggregate effect of the other nodes in the MANET. Existing system proposed a dynamic mean field game theoretic approach to enable an individual node in MANETs to make strategic security defense decisions without centralized administration.

The security defense mechanisms in a wireless mobile node consume precious system resources (e.g., energy), the proposed scheme considers not only the security requirement of MANETs but also the system resources.

The algorithm used in the existing system is only concentrate on the process of cryptographic puzzles technique for generating security for that file sharing provides less security . The most of the algorithms are discussed about how to solve the well known clustering problem and defend against the new security threats.

IV. PROPOSED SYSTEM

Our proposed scheme is Cluster-based Certificate Revocation with Vindication Capability 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. And also it performs the process of cryptographic puzzles technique for generating security for

that file sharing. So sharing provides more security compared to the existing system.

1) Cluster Construction
2) Certificate Authority
3) Node Classification
4) Revocation
   - Certificate Revocation
   - False Accusation Revocation.

Module Descriptions

Cluster Construction:

In this process first we create the node for the system. In this process, we form the fifteen nodes for the single cluster. Totally process contains the forty five nodes and three clusters. In this process, cluster contains the process of both the malicious and normal node. So First it need to select the header node for each cluster. Header node sends the request (hello packets) to the node in its cluster. Accepted node or properly response node is said to the normal. Other nodes are considered as the attacker node or malicious node. So we need to provide the certificate authority.

1) Issuing of certificates
2) Storage of certificates
3) Certificate validation
4) Revocation of certificates.

A. Issuing of Certificate

In this process, certificate authority need to provides the certificate to the each node. This certificate needs the certificate parameters like node name, IP address, Private Key, Public Key, Creation Time and Expiry Time.

B. Storage of Certificate

In this process, details of nodes and certification details is stored into the cluster authority database.

C. Certificate Validation

This validate the each node's certificate in each cluster.

D. Revocation of Certificate

This revocation process is for revocate the false accusation nodes and malicious node.

V. Implementation and Results

A method and system are provided for authenticating a user of a computer over a computer network. In one embodiment of the invention, the method includes transmitting an applet having a challenge string and a first encryption key, receiving a login packet having the challenge string and a password that is encrypted using the first encryption key, decrypting the password, receiving information from an authentication provider, and authenticating the password by using the information provided by the authentication provider. The challenge string can be either a sequence number or a session identifier. The login packet can further include a user name, wherein the session identification, the user name, and the password are encrypted. Additionally, the login packet can include a hash of the session identification, the user name, and the password. Authenticating the password by using an authentication provider can include receiving from an authentication provider a second encryption key; encrypting using the second encryption key and transmitting to the authentication provider the password, receiving from the authentication provider a second hash of the password and a character string; and determining from the character string if the password is correct. The authentication provider can be a software program or an authentication server. An advantage of embodiments of the present invention is that a computer can provide secure Internet communications using a web browser that does not support SSL and can provide secure integration with third party security systems.

The security-related issues in a single broadcast LAN (local area network) such as Ethernet. The authors formalize various possible network attacks. Their basic strategy is to develop profiles of usage of network resources and then compare current usage patterns with the historical profile to determine possible security violations. Thus, the work is similar to the host-based intrusion-detection systems. Different from such systems, however, is the use of a hierarchical model to refine the focus of the intrusion-detection mechanism. The authors also report on the development of an experimental LAN monitor currently under implementation. Several network attacks have been simulated, and results on how the monitor has been able to detect these attacks are analyzed. Initial results demonstrate that many network attacks are detectable with the authors' monitor, although it can be defeated.

An integrated network security system is provided which permits log-on to a normally locked client on the network in response to at least one coded non-public input to the client by a user. At least a selected portion of the coded input is encrypted and sent to a network server where the user is authenticated. After authentication, the server preferably returns a decryption key, an encryption key for future use and any critical files previously stored at the server to the client. The decryption key is utilized to decrypt any material at the client which were encrypted when the client was locked, including any material sent from the server, thereby unlocking the client. The decryption key may be combined with untransmitted portions of the original coded input in a variety of ways to generate an encryption key for the next time the terminal is to be locked. When one of a variety of client locking conditions occurs, the previously generated encryption key is utilized to encrypt at least selected critical material at the client. Critical directories or the like in encrypted form may be sent to the server and a message is sent to the server that the client is locked, which message is utilized by the server to inhibit the client from further access to at least selected resources on the network.

A Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme is used. A trusted third party, certification authority (CA), 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, Warning List (WL) and Black List (BL), 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. The CA updates each list according to received control packets. Note that each neighbor is allowed to accuse a given node only once. Furthermore, the CA broadcasts the information of the WL and BL to the entire network in order to revoke the certificates of nodes listed in the BL and isolate them from the network.

VI. Conclusion and Future Enhancement

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] George Theodorakopoulos and John S. Baras, February 2006.,"On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks." IEEE JSAC, Vol.24. No.2,

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

[3] S.kannan,T.Kalaikumaran,S.Karthik and V.P.Arunachalam ,2011 "A Review on attack prevention methods in MANET" journal of Modern Mathematics and Statistics 5(1): 37-42.

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

[5] X. Li, Jun. 2009 "Multicast capacity of wireless ad hoc networks," IEEE/ACM Trans. Netw., vol. 17, no. 3, pp. 950–961.

[6] G. S. Mamatha1 and dr. S. C. Sharma2 , August 2010"analyzing the manet variations, Challenges, capacity and protocol issues" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.1.

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

[8] Ping Yi, Yue Wu and Futai Zou and Ning Liu, Jan-Feb 2010 "A Survey on Security in Wireless Mesh Networks", Proceedings of IETE Technical Review, Vol. 27, Issue 1.

[9] Revathi Venkataraman, M. Pushpalatha, 2006: "Security in Ad Hoc Networks: An extension of dynamic Source Routing in Mobile Ad Hoc Networks". In proceedings of the 10th IEEE International Conference on Communication Systems, Singapore.

[10] P. Sakarindr and N. Ansari, Oct. 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.