Computer Standards & Interfaces 36 (2014) 577–584

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Improved migration for mobile computing in distributed networks

Chien-Lung Hsu [a,b,*], Yu-Li Lin [c]

[a] Department of Information Management, Chang Gung University, Tao-Yuan 333, Taiwan, ROC
[b] Department of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL 32816-2362, United States
[c] Ministry of Justice, Investigation Bureau (MJIB), Taipei 231, Taiwan, ROC

ARTICLE INFO

Article history:
Received 14 January 2010
Received in revised form 3 October 2013
Accepted 15 October 2013
Available online 4 November 2013

Keywords:
Key management
Mobile agent
Elliptic curve
Migration
Mobile computing
MANET

ABSTRACT

A mobile ad hoc network (MANET) is a special type of wireless network in which a collection of mobile nodes with wireless network interfaces may form a temporary network, without the aids of any fixed infrastructure. Security has become a hot research topic in mobile ad hoc networks. In 1998, Volker and Mehrdad proposed a tree-based key management and access control scheme for the mobile agents to manage rights to access its own resources for the visited mobile nodes. Latter, Huang et al. showed that Volker and Mehrdad's scheme needs a large amount of storage and costs for managing and storing secret keys. Huang et al. further proposed a new and efficient scheme based on the elliptic curve cryptosystems to reduce costs and gain better efficiency. However, there is a security leak inherent in Huang et al.'s scheme that the malicious node can overstep his authority to access unauthorized information. This paper will propose a secure, robust, and efficient hierarchical key management scheme for MANETs. Some practical issues and solutions about dynamic key management are also considered and proposed. As compared with Huang et al.'s scheme, our proposed scheme can provide better security assurance, while requiring smaller key-size, lower computational complexities, and constant key management costs which is independent on the number of the confidential files and the visited nodes.

1. Introduction

A mobile ad hoc network (MANET) has caught the attention and provided anytime and anywhere networking services. It is a self-organized wireless network for mobile nodes without any fixed infrastructure. Such a network can be deployed rapidly and dynamically, and all mobile nodes are connected by wireless links. A group of mobile nodes can improve message delivery and save bandwidth effectively in a MANET. MANETs can provide self-organizing and infrastructure-less property, and hence they are widely used in varied applications such as military and commercial settings. In a MANET, each mobile node owns different resources and might allow the visited node to access them. A mobile node decides where to migrate and executes the tasks on the desired node. The mobile agent will return the result to the request node after it completes the intended tasks.

In a MANET, a mobile agent might have some valuable resources or information to share with authorized visited mobile nodes. All sensitive information might be sent via a general tunnel or over the air without any protection. Hence, it might suffer from some potential security threats such as compromising, eavesdropping, impersonating attacks, etc. Security is a significant issue for protecting the transmitted messages and providing access control to resources in constructing the MANET. The mobile agent must establish suitable security mechanisms to protect the resources from being disclosed and accessed by unauthorized mobile nodes. It is a challenge to dynamically manage the access rights to the resources for mobile nodes and protect them from being disclosed. A key management scheme is a cryptographic technique to manage cryptographic keys used to protect the confidentiality of the sensitive resources [1–4]. It allows only authorized mobile agents to access authorized resources and information with its own cryptographic key(s). A key management scheme can improve security and reduce the memory storage of keys, as presented in MANETs [5–7].

Recently, many scholars proposed various key management and access control schemes for MANETs [8–14]. In 1998, Volker and Mehrdad proposed a tree-based key management and access control scheme for the mobile agents to manage rights to access its own resources for the visited mobile nodes [8]. It allows that only the authorized visited mobile nodes can access some information according to the predetermined access control, while unauthorized visited mobile nodes cannot. Main drawback of their scheme is that it requires a large amount of storage and high computational complexities. To improve the performance of Volker and Mehrdad's scheme [8], Chang and Lin later proposed two key management schemes based on RSA cryptosystem, i.e. one is bottom-up approach and the other is top-down approach [11]. Chang and Lin's scheme requires less key management costs and fewer computational costs as compared with Volker and Mehrdad's scheme. However, their scheme is still inefficient from practical viewpoints since they require expensive exponential operations for key generation and derivation.

* Corresponding author at: Department of Information Management, Chang Gung University 259, Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan 333, Taiwan, ROC. Tel.: +86 3 211 8800x5827; fax: +86 3 211 8020.
E-mail address: clhsu@mail.cgu.edu.tw (C.-L. Hsu).

0920-5489/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.csi.2013.10.006

In 2009, Huang et al. proposed a practical and efficient hierarchical mobile agent framework for MANETs to handle key management and access control problems based on elliptic curve cryptosystems, one-way hash function and interpolating polynomials [11]. In Huang et al.'s scheme, each mobile agent must maintain an access control hierarchy to manage the access rights for visited mobile nodes. Such a hierarchy is a POSET (partially ordered set) hierarchy. Each confidential file owned by the mobile agent has a pair of secret keys, a decryption key and a superkey. The decryption key is used to encrypt/decrypt the confidential file. Only the mobile node with the decryption key can access the content of the confidential file. The superkey is used for deriving the decryption key according to the predetermined access control policies. The mobile agent can determine and assign a distinct superkey to a visited mobile node for accessing the confidential file(s) according to the predetermined hierarchy of access control. The authorized mobile node can use its given superkey to derive the decryption key of the intended confidential file and then use it to obtain the content. Attractive contribution of Huang et al.'s scheme [15] is to achieve the same security level while requiring smaller key-size and lower computational costs as compared with Chang and Lin's scheme [11].

There, however, is a security leak inherent in Huang et al.'s scheme [15] that the malicious node can overstep his authority to access unauthorized information, which violates the claimed security requirements. Moreover, Huang et al.'s scheme does not consider some practical dynamic key management problems. For example, it does not provide an access control updating mechanism for the mobile nodes leaved from the access control hierarchy. This paper will propose a secure, robust, and efficient hierarchical key management scheme for MANETs. Each node of the proposed scheme maintains only *one* secret key which is used to help the visited node to derive decryption key(s) of authorized confidential file(s). This will reduce the key management costs. Some practical issues and solutions about dynamic key management are also considered. We also provided practical and efficient solution to deal with dynamic key management problem for migration for mobile computing in MANETs.

The rest of this paper is sketched as follows. In Section 2, we briefly reviewed MANET technologies, elliptic curve cryptosystem, and Huang et al.'s scheme [15]. Security leak inherent in Huang et al.'s scheme is also discussed in Section 2. In Section 3, we proposed a new key management and access control scheme based on a one-way hash function and discussed the solutions to dynamic access control problems. Security analysis and performance evaluations of the proposed scheme are given in Sections 5 and 6, respectively. Finally, we gave conclusions in Section 5.

2. Related works

2.1. MANET technologies

A mobile ad hoc network (MANET) is a self-configuring and infrastructureless wireless network for mobile devices. In such a wireless network, all mobile devices can move freely in any direction and they will therefore be frequently connected by wireless. Characteristics of MANETs are infrastructureless network, ease of deployment, speed of deployment, multi-hop network, dynamic changing topology of mobile devices, etc. MANETs are expected to become an important part of the future 4G architecture for providing pervasive computing services. Users can accomplish their tasks, accessing information, and communicating anytime, anywhere and by any device in MANET environment. Applications of a mobile ad hoc network include tactical networks, emergency services, commercial and civilian environments, home and enterprise networking, mobile education, sensor networks, context aware services, and so on. General challenging issues in MANETs include distributed congestion control [16–18], load balancing [19], admission control [20], routing [21,22], security [23], etc. MANET has higher security risks than conventional infrastructure network.

The mobile agents of mobile devices are software programs that act on behalf of users or other software programs in MANET environment. A mobile agent can achieve one or more tasks automatically, clone itself and propagate, collaborate and communicate with other ones and so on. Some sensitive and confidential information might be stored in the agent and hence, the agent might be suffered from many security threats [24–26] such as unauthorized access, malicious impersonation, disclosing or tampering attacks in open MANETs. Hence, the agent must authenticate its visited host or agents according to some proper security policies [27].

In 1998, Volker and Mehrdad proposed a tree-based key management and access control scheme for the mobile agents to manage rights to access its own resources for visited mobile nodes as illustrated in Fig. 1 [8]. In Fig. 1, nodes of the tree might either be folders or files and each node has a unique identifier. If a node is labeled *encrypted*, then its folders or files are encrypted from being disclosed. An encrypted node is tagged with the name of the decryption key for the valid readers to read its content. If a node is labeled *signed* then a digital signature is applied for the content of the node and integrity is protected. The signer of node is regarded as the rightful owner of the agent and a signed node is tagged with the signer's identity. Security policy of the agent is stored in the security context of the static branch. If an agent owner wants to send the mobile agent carried with the assigned tasks onto Internet, the agent owner encrypts its confidential file with a secret key using a symmetric cryptosystem. Then, a secret key is assigned by the owner to each host according to the access policies, and such secret keys are stored in the respective folders of each host. Furthermore, the respective folders are also be encrypted by the public key of each host. When the mobile agent visits the hosts and interacts with them, the host can decrypt its folder with its private key and then retrieves its secrete key to decrypt the confidential file according to its rights.

2.2. Elliptic curve cryptosystem

An elliptic curve cryptosystem (ECC) is first proposed by Miller [28] and Koblitz [29] in 1985. Attractive advantage of the ECC is that it can achieve the same level of security while requiring shorter key-size as compared with transitional cryptosystems. For example, the ECC with 160-bits key size is as secure as the RSA cryptosystem with 1024-bits one. This also implies that it requires lower memory and has greater execution speed. Since then, many standards are developed for the ECC, such as ISO 11770-3, ANSI X.9.62, IEEE P1363, FIPS 186-2, etc.

Typically, there are two types of the elliptic curves used in cryptography: the prive curves over Z_p for software applications and the binary curves over $GF(2^n)$ for hardware application. In the finite field, an elliptic curve is typically defined as E: $y^2 = x^3 + ax + b$, where $(a, b) \in Z_p$ and $4a^3 + 27b^2 \neq 0 \pmod{p}$. The elliptic curve $E_p(a, b)$ is the set of the integer points over the elliptic curve over Z_p and a point of infinity O. It forms a commutative finite group under the rules of addition operation. In $E_p(a, b)$, addition of any two points $P = (x_P, y_P)$ and $Q = (x_P, y_P)$ is denoted as $P + Q = R = (x_R, y_R)$ such that

$$\begin{cases} x_R = \lambda^2 - x_P - x_Q \\ y_R = \lambda(x_P - x_R) - y_P \end{cases}, \text{where} \begin{cases} \lambda = \frac{y_Q - y_P}{x_Q - x_P} & \text{if } P \neq Q \\ \lambda = \frac{3x_P^2 + a}{2y_P} & \text{if } P = Q \end{cases}.$$

The negative point of $P = (x_P, y_P)$ is defined as $-P = (x_P, -y_P)$ and the multiplication operation by an integer for the point P over $E_p(a, b)$ is defined as $Q = kP$, which repeats elliptic curve addition operations. In addition, $E_p(a, b)$ forms a commutative finite group under the following rules of addition operation:

1. $O + P = P$ and $P + O = P$, where O is regarded as the additive identity,
2. $P + (-P) = (-P) + P = O$, where $-P$ is defined as the negative point of the point P over $E_p(a, b)$,