A New Method for Key Sharing in Wireless Mesh Networks

Peng Xiao¹, Jingsha He², and Yingfang Fu³

¹ College of Computer Science and Technology, Beijing University of Technology
   Beijing 100124, China
   xp4523@emails.bjut.edu.cn
² School of Software Engineering, Beijing University of Technology
   Beijing 100124, China
   jhe@bjut.edu.cn
³ Fantai Lingshi Technology (Beijing) Limited, Beijing 100044, China
   fuyingfang@bjut.edu.cn

Abstract. Combining the advantages of WLANs and ad hoc networks, wireless mesh networks (WMNs) are wireless access networks based on IP technologies and have become effective broadband access networks with high capacity, high speed and wide coverage. Security is a crucial and urgent problem in WMNs as in other types of networks and a simple and effective distributed key management is essential for the establishment of secure WMNs. In this paper, we present an effective distributed key management scheme based on several technologies, such as ad hoc network model, ECC, (t, n) threshold cryptographic method, verifiable secret sharing and so on.

Keywords: Wireless mesh networks; distributed key management; cheater identification; ECC; cryptography

1 Introduction

Combining the advantages of WLANs and ad hoc networks, WMNs are wireless broadband access networks completely based on IP packet networks and have quickly become effective broadband access networks with high capacity, high speed and wide coverage. Security is a crucial and urgent problem in WMNs as in any other types of networks [1]. A simple and effective distributed key management is crucial for the establishment of secure WMNs.

2 Related Work

Hong et al. proposed an efficient key distribution scheme with self-healing property, which is optimal in terms of user memory storage and more efficient in terms of communication complexity [2]. IEEE P802.11s™/D1.01 provides efficient mesh security association (EMSA) [3] based on the IEEE 802.11i standard in which the
802.1x scheme and four handshakes are used to implement access authentication and key establishment. Fu et al. proposed a mutual authentication in WMNs [4] based on a \((t, n)\) cryptography method but without verifiable secret sharing. Duan et al. proposed an efficient location-based compromise-tolerant key management scheme for sensor networks based on sensor deployment and localization [5]. Dahshan et al. proposed an elliptic curve distributed key management scheme for mobile Ad Hoc networks based on ECDLP and \((t,n)\) threshold cryptography [6]. But they are all suitable for certain type of networks only and don’t support cheater identification for locating the malicious node. In relatively complex hybrid WMNs, they need to be improved to adapt to the networks.

3 Distributed Group Key Management

In this paper, we use traditional Lagrange interpolation to implement secret key sharing and elliptic curve cryptography (ECC) to generate authorized certificates.

3.1 Cheater Detection

In the initial stage of key establishment in our scheme, a public key piece \((d_v, SK_v)\) generated by the offline CA is broadcast to the whole network. When \(t\) key pieces are collected, a new matrix equation \(D' \cdot A' = S'\) is established,

\[
D' = \begin{bmatrix}
    d_1^{-1} & \ldots & d_1 & 1 \\
    d_2^{-1} & \ldots & d_2 & 1 \\
    \vdots & \ddots & \vdots & \vdots \\
    d_t^{-1} & \ldots & d_t & 1
\end{bmatrix} \quad A' = \begin{bmatrix}
    a_1 \\
    a_2 \\
    \vdots \\
    a_t
\end{bmatrix} \quad S' = \begin{bmatrix}
    SK_1 \\
    SK_2 \\
    \vdots \\
    SK_t
\end{bmatrix} \quad \text{and} \quad \overrightarrow{D} = \begin{bmatrix}
    d_1^{-1} & \ldots & d_1 & 1 & SK_1 \\
    d_2^{-1} & \ldots & d_2 & 1 & SK_2 \\
    \vdots & \ddots & \vdots & \vdots & \vdots \\
    d_t^{-1} & \ldots & d_t & 1 & SK_t
\end{bmatrix}
\]

At the moment, we can deduce that \(R(\overrightarrow{D}) = R(D) \leq t + 1\). So,

1. If \(R(\overrightarrow{D}) = R(D) < t\), there are more than one solutions for the equation. So, more key pieces need to be gathered to get the unique solution until \(R(\overrightarrow{D}) = R(D) = t\).
2. If \(R(\overrightarrow{D}) = R(D) = t\), there is a unique solution for the equation. So, a correct secret key \(SK\) will be reconstructed.
3. If \(R(\overrightarrow{D}) = R(D) = t + 1\), there is no feasible solution for the equation. So, there exists at least one incorrect key piece in the participants. Hence, a cheater is detected.

3.2 Cheater Identification

Once detected, the cheater must be identified. When a new participant is acquiring a key piece from an existing participant, the latter must deliver its own key piece along
with its digital signature to the former. So, after the new participant has collected \( t \) key pieces and found a cheater in the network, as described in the last section, it will broadcast a request to arouse the offline CA. Then, it will deliver all the collected key pieces with its digital signature to the offline CA. The CA can verify which key pieces are incorrect through the pre-selected \((t-1)\)-degree polynomial \( f(x) \) and which participants are dishonest through their registered certificates.

4 Conclusions

We presented an effective distributed key management scheme for the establishment of a secure WMN in this paper, which is based on several technologies, such as ad hoc network model, ECC, \((t, n)\) threshold cryptographic, verifiable secret sharing. In the future, we will consider distributed key management in the handoff and roaming scenario in WMNs to further improve our protocol [7].

References