Distributed Group Key Management in Wireless Mesh Networks

Peng Xiao[1], Jingsha He[2] and Yingfang Fu[3]

[1]*Computer Science and Technology, Beijing University of Technology, Beijing 100124, China*
[2]*School of Software Engineering, Beijing University of Technology, Beijing 100124, China*
[3]*Fantai Lingshi Technology (Beijing) Limited, Beijing 100044, China*
[1]*xp4523@emails.bjut.edu.cn, {*[2]*jhe,* [3]*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, and demonstrate its effectiveness through analysis and experiment.*

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

1. Introduction

Wireless mesh networks (WMNs) are a new technology of wireless networks, which can remove specific restrictions of ad hoc networks, wireless local area networks (WLANs), wireless personal area networks (WPANs) and wireless metropolitan area networks (WMANs), and can be used to establish commercial wireless mobile networks. 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. In essence, WMNs are a network design that can offer such features as no central control, self-organization, multi-hop, best routing-judgment, etc.

Security is a crucial and urgent problem in WMNs as in any other types of networks [1]. In a wired network, data are transmitted to their destination through electric cables, so disclosure can happen only when the physical links are under attack. In a wireless network, data are transmitted through an open space and any node in the coverage area can receive the radio signals. Moreover, in WMNs, the external environment can be much harsher due to the lack of central administration. Therefore, 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]. But it requires that there exist a group manager for a

network with a finite number of users and is mainly useful in a wired network. It also lacks verification on the correctness of the received keys.

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. However, it requires that some special wireless nodes called mesh key distributor (MKD) be present in WMNs to generate, distribute and store keys. The MKD breaks the equality of nodes in WMNs and, in addition, if it is compromised, the keys stored in it might be compromised.

Fu et al. proposed a mutual authentication in WMNs [4] based on a (*t, n*) cryptography method but without verifiable secret sharing. Therefore, if there is any dishonest node, there is no way of detecting and identifying such a node, and, as the result, an incorrect key can be constructed. For example, one can forge an invalid sub signature once the secret random integer b_r becomes known, which can be calculated if a valid signature is intercepted.

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. Preliminaries

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

3.1. Traditional Secret Sharing

A (t, n) threshold secret sharing method is comprised of three parts: system parameters, secret distribution algorithm and secret reconstruction algorithm [7].

(1) System parameters: private key SK is the secret to be shared which is defined in a finite field $GF(p)$ where p is a prime number greater than SK and n; $d_1, d_2, ..., d_n$ are different integers defined in $GF(p)$ that represent the public identification of n participants.

(2) Secret distribution algorithm: a polynomial of degree (t-1) $f(x) = a_{t-1}x^{t-1} + ... + a_1 x + a_0 \mod p$ in the finite field $GF(p)$ is chosen, where $a_{t-1}, ..., a_1$ are random integers and $a_0 = SK$. Then, the key pieces $SK_i = f(d_i) \mod p$ can be calculated and delivered to each and every responding participant through secure channels.

(3) Secret reconstruction algorithm: t coordinates (d_1, SK_1), (d_2, SK_2), ..., (d_t, SK_t) can be acquired through the cooperation from any t participants. According to Lagrange interpolation polynomial, $SK = f(0) = \sum_{i=1}^{t} SK_i \prod_{j \neq i, j=1}^{t} \frac{d_j}{d_j - d_i} \mod p$.

3.2. ECC

ECC can offer the same level of security with smaller key sizes and faster computation time, which leads to less power consumption than other public-key cryptographic algorithms such as the RSA.

The cryptography is built on a suitably chosen elliptic curve E defined over a finite field F_q of characteristic p and a base point $P \in E(F_q)$. Some domain parameters can be defined as described in [8]. Given a valid set domain parameters (q, FR, a, b, P, n, h), an entity A's private key is a random integer $\omega_A \in_R [1, n-1]$ while its public key is the point $W_A = \omega_A P$.

4. Distributed Group Key Management

Before accessing the network, all mesh nodes need to acquire a legal certificate from the offline CA, which is supported by an ISP or network carrier [9]. And as there is no CA or administrator center online in the backbone mesh networks, n mesh routers with higher performance will form a virtual CA and group key management (GKM) to manage the keys using the (t, n) threshold cryptographic method [10].

There are several disadvantages when traditional secret sharing is used in WMNs:

(1) If a dishonest participant may deliver an incorrect key piece or if there is anything wrong in date transmission, the correct secret key SK cannot be reconstructed.

(2) If there is a malicious attacker among the n participants, it may deliberately deliver a faked key piece to others and, at the same time, receive all the correct key pieces from others. Then, only it can reconstruct the correct secret key SK while all the others who receive a faked piece cannot.

(3) In a wireless mobility environment, an attacker can attack a holder and break one key piece in a limited time and then move to attack the next holder. So in a long enough time, the attacker may attack all t holders and acquire the t key pieces so as to calculate the shared secret key SK.

4.1. Cheater Detection

The key question is how to detect whether an incorrect key piece comes from a potential cheater. Let us consider the matrix equation of the form: $D \bullet A = S$, in which

$$D = \begin{bmatrix} d_1^{t-1} & \ldots & d_1 & 1 \\ d_2^{t-1} & \ldots & d_2 & 1 \\ \ldots & \ldots & \ldots & \ldots \\ d_t^{t-1} & \ldots & d_t & 1 \end{bmatrix}, A = \begin{bmatrix} a_{t-1} \\ a_{t-2} \\ \ldots \\ a_0 \end{bmatrix}, S = \begin{bmatrix} SK_1 \\ SK_2 \\ \ldots \\ SK_n \end{bmatrix} \text{ and } \overline{D} = \begin{bmatrix} d_1^{t-1} & \ldots & d_1 & 1 & SK_1 \\ d_2^{t-1} & \ldots & d_2 & 1 & SK_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ d_t^{t-1} & \ldots & d_t & 1 & SK_t \end{bmatrix}.$$

The substance of the Lagrange interpolation polynomial is that there exists a unique feasible solution A in the matrix equation when D and S are given. A necessary and sufficient condition is that the rank of the augmented matrix $\overline{D}$ is the same as that of D which is equal to t, hereby marked as $R(\overline{D}) = R(D) = t$. If there exists an incorrect key piece (d_i, SK_i) and the condition $R(\overline{D}) = R(D) = t$ is satisfied, then a incorrect secret key SK will be reconstructed.

Therefore, in the initial stage of key establishment in our scheme, a public key piece (d_0, SK_0) generated by the offline CA is broadcast to the whole network. When t key pieces are collected, a new matrix equation $D' \bullet A' = S'$ is established,

where $D' = \begin{bmatrix} d_1^{t-1} & ... & d_1 & 1 \\ d_2^{t-1} & ... & d_2 & 1 \\ ... & ... & ... & ... \\ d_t^{t-1} & ... & d_t & 1 \\ d_0^{t-1} & ... & d_0 & 1 \end{bmatrix}$, $A' = \begin{bmatrix} a_{t-1} \\ a_{t-2} \\ ... \\ a_0 \end{bmatrix}$, $S' = \begin{bmatrix} SK_1 \\ SK_2 \\ ... \\ SK_n \\ SK_0 \end{bmatrix}$ and $\overline{D}' = \begin{bmatrix} d_1^{t-1} & ... & d_1 & 1 & SK_1 \\ d_2^{t-1} & ... & d_2 & 1 & SK_2 \\ ... & ... & ... & ... & ... \\ d_t^{t-1} & ... & d_t & 1 & SK_t \\ d_0^{t-1} & ... & d_0 & 1 & SK_0 \end{bmatrix}$. At the moment, we can deduce that $R(\overline{D}) = R(D) \le t+1$. So,

(1) If $R(\overline{D}) = R(D) < t$, there are more than one solutions for the equation. So, more key pieces need to be gathered to get the unique solution until $R(\overline{D}) = R(D) = t$.

(2) If $R(\overline{D}) = R(D) = t$, there is a unique solution for the equation. So, a correct secret key SK will be reconstructed.

If $R(\overline{D}) = R(D) = t+1$, there is no feasible solution of the equation. So, there exists at least one incorrect key piece in the participants. Hence, a cheater is detected.

4.2. 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.

(1) If there are indeed some faked key pieces that cannot satisfy $f(x)$, those who generated them are dishonest cheaters. And they cannot deny the fact due to their digital signatures. In this case, the group key must be updated and the offline CA will revoke the current group key SK and start a new key establishment.

(2) If there is no faked key piece, which means all the key pieces satisfy $f(x)$, the new participant who provided them is the cheater. In this case, the group key doesn't need to be updated.

Once a cheater is identified, some actions must be taken in the network. In a strict security policy, the cheater will be disassociated from the network and its certificate will be revoked by the offline CA. In a weaker security policy, the cheater will be recorded by the offline CA and its credit will be reduced. And after losing its credit for a few times so that a threshold pre-set is reached in the network, it will be disassociated with its certificate being revoked. Sometimes, something wrong may happen during data transmission or an unwitting mistake might take place in the participants.

4.3. Key Update

There are several conditions in which the group key needs to be updated.

(1) A new mesh router accesses the backbone network;

(2) An existing mesh router leaves the backbone network;

(3) A cheater is detected in the network as described in the last section.

To prevent a mobile attacker from breaking *t* key pieces in a long enough time, every key piece should be updated within a defined cycle *T*. Only when at least *t* key pieces are gained in the same cycle, can the secret be reconstructed.

The following four steps are executed in order to update a key:

(1) The offline CA is aroused in the network;

(2) The CA constructs a new group key SK' and selects a new polynomial $f'(x)$. The new key pieces (d_i, SK_i') are calculated and delivered to *n* selected mesh routers. Then CA disconnects itself from the network and remains offline.

(3) A mesh router requires (*t-1*) key pieces from other mesh routers.

(4) After *t* key pieces are collected that include its own, the mesh router can then reconstruct the new group key SK'. And cheater detection and identification is carried out as described above.

5. Simulation Results

We performed some simulation using OPNET 14.5 to prove the correctness and the reliability of our scheme. The simulation scenario assumes an area of $1000 \times 1000m^2$ and all the mobile nodes use a protocol based on IEEE 802.11b.

Fig. 1 shows the success ratio of key distribution and reconstruction when n values from *1* to *16* and *t=2, 4, 8*. As we can see if *n<t*, the key reconstruction cannot be implemented; and while the threshold *t* is increasing, the success ratio is getting lower because of radio collision and transmission delay. And Fig. 5 shows the time to identify a cheater when there is a malicious node existing in the network. We predesigned a malicious node in the network, which will give out an incorrect key piece to others, and the RSA verifying process costs about *30* million seconds through experiments. As the threshold *t* is increasing, there are more key pieces need to be verified, and then more cheater indentifying time will be expended.

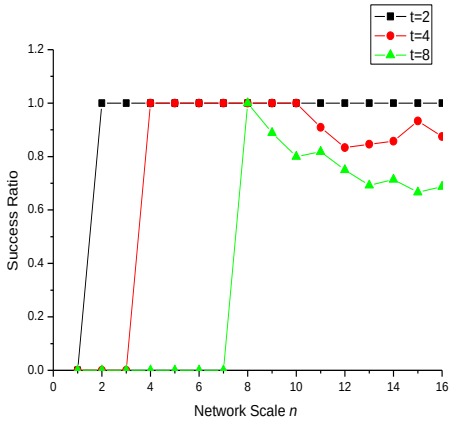

Figure 1. Key Pieces Distribution

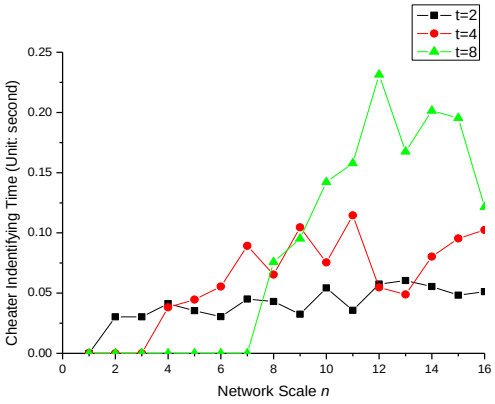

Figure 2. Group Key Reconstruction

6. 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 [11].

References

[1] M. Cesana1, A. Boukerche and A. Zomaya, "Security for QoS Assured Wireless and Mobile Networks", J. Security and Communication Networks, 4(3), pp. 239–241 **(2011)**.

[2] D. Hong and J. S. Kang, "An Efficient Key Distribution Scheme with Self-healing Property", J. IEEE Communications Letters, 9(8), pp. 759-761 **(2005)**.

[3] 802.11 Working Group of the IEEE 802 Committee: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE P802.11s™/D1.01, 1-780 **(2007)**.

[4] Y. Fu, J. He, L. Luan, R. Wang and G. Li, "A Zone-based Distributed Key Management Scheme for Wireless Mesh Networks", In: 32nd Annual IEEE International Computer Software and Applications Conference, pp. 68-71. IEEE Computer Society Washington, DC, USA **(2008)**.

[5] M. J. Duan and J. Xu, "An Efficient Location-based Compromise-tolerant Key Management Scheme for Sensor Networks", J. Information Processing Letters, 111(11), pp. 503-507 **(2011)**.

[6] H. Dahshan and J. Irvine, "An Elliptic Curve Distributed Key Management for Mobile Ad Hoc Network", In: 2010 IEEE 71st Vehicular Technology Conference, pp. 1-5. IEEE Xplore, Taipei **(2010)**.

[7] A. Shamir, "How to Share a Secret", J. Communications of the ACM, 22(11), pp. 612-613 **(1979)**.

[8] L. Law, "An Efficient Protocol for Authenticated Key Agreement", J. Designs, Codes and Cryptography, 28(2), pp. 119-134 **(2003)**.

[9] I. F. Akyildiz, X. D. Wang and W. L. Wang, "Wireless Mesh Networks: a Survey", J. Computer Networks, 47(4), pp. 445-487 **(2005)**.

[10] Y. Fu, J. He, R. Wang and G. Li, "Mutual Authentication in Wireless Mesh Networks", In: 2008 International Conference on Communications, pp. 2606-2610. IEEE Xplore, Beijing **(2008)**.

[11] A. P. Shrestha, D. Y. Choi, G. R. Kwon and S. J. Han, "Kerberos based Authentication for Inter-domain Roaming in Wireless Heterogeneous Network", J. Computers and Mathematics with Applications, 60(2), pp. 245-255 **(2010)**.

Authors

Peng Xiao is currently a Ph.D. candidate in the College of Computer Science and Technology at Beijing University of Technology. His research interests include network security, trusted authentication in WMNs and Ad Hoc networks.

Jingsha He is currently a professor of the School of Software Engineering at Beijing University of Technology. His research interests include network security and wireless communication technologies.

Yingfang Fu is currently a researcher in Fantai Lingshi Technology (Beijing) Limited, Beijing 100044, China. Her research interests include network security and trusted computing in WMNs.