A Proxy Signature-based Re-authentication Scheme for Secure Fast Handoff in Wireless Mesh Networks

Changsha Ma, Kaiping Xue, and Peilin Hong
(Corresponding author: Kaiping Xue)

The Information Network Lab of EEIS Department,

University of Science and Technology of China (USTC), Hefei 230027, China
(Email: kpxue@ustc.edu.cn)

(Received May. 24, 2012; revised and accepted July 30, 2012)

Abstract

In wireless mesh networks (WMNs), re-authentication guarantees the secure association between a roaming mesh host (MH) and a target mesh access point (MAP) in handoff process. However, due to the complex security mechanisms in re-authentication procedure, handoff delay is significantly extended, making it harder to guarantee the quality of service (QoS) of some mesh applications. In this paper, we propose a proxy signature-based re-authentication scheme for secure fast handoff in WMNs. To begin with, we designate the mesh portal (MPP) as the authenticator of the MH that initially accesses a certain mesh domain. After the successful initial association, the MH is authorized to obtain a temporal proxy delegation of the MPP for the preparation of handoff. Making use of the proxy delegation in handoff case, the MH can efficiently associate with a target MAP connecting to the MPP by performing the proposed re-authentication scheme, in which mutual authentication and pairwise master key (PMK) establishment are performed between the MH and the MAP in a three-way handshake procedure without involving any other parties. Benefiting from the reduced computation operations and message exchanges, the re-authentication delay of the proposed scheme is significantly reduced. Our theoretical analysis demonstrates that the proposed scheme is secure under common security attacks. Besides, the performance evaluation shows that the proposed scheme is more efficient than existing re-authentication schemes in terms of communication overhead, computation cost, and re-authentication delay.

Keywords: Handoff, re-authentication, proxy signature, wireless mesh networks

1 Introduction

Wireless mesh networks (WMNs) are promising to provide many kinds of applications in the near future, due to the features of convenient deployment, high bandwidth and flexible structure. In WMNs, nodes consist of a set of distributed mesh points (MPs) and mesh hosts (MHs). Specifically, the MPs providing additional access point functionality for serving MHs as points of network attachment are called mesh access points (MAPs). The MPs that bridge the WMN with other networks, i.e. Internet, are called mesh portals (MPPs) [1]. MPs form the backbone of WMNs and forward packets on behalf of other nodes that are not within direct wireless transmission range of the destinations. Unlike MPs that have minimal mobility, MHs can be either stationary or mobile.

An MH may move its association from one MAP to another, causing a period of communication disruption. This condition is called handoff, which can be divided into three stages: probe, re-authentication and re-association. A MH discovers a target MAP in the stage of probe, and gets through the authentication request of the target MAP in re-authentication stage. In re-association stage, the authenticated MH performs key materials derivation and trust relationship establishment with the target MAP. Among the three stages, re-authentication is the most essential stage of secure fast handoff. One important reason is that the re-authentication procedure is vulnerable to security attacks such as impersonation of communication entities and replay of exchanging messages [2, 3]. To resist such attacks, secure communication mechanisms between MAPs and MHs are necessary [4]. However, complex security mechanisms have significantly increased the handoff delay. In IEEE 802.11 mesh networks, the secure communication between MAPs and MHs during the handoff process is supported by IEEE 802.11i, which adopts IEEE 802.1X framework to provide authentication procedure [1]. However, in this case, re-authentication delay is of the order of 1000ms, which is too long to satisfy quality of service (QoS) demands of some mesh applications, especially the real-time applications. For instance, to guarantee the QoS of voice over Internet protocol (VoIP) applications, the overall handoff delay is recommended to be less than 50ms [5]. Therefore, it is important to design a re-authentication scheme that can guarantee security and reduce handoff delay for secure fast handoff.

Recently, many studies [6, 7, 8] have been focused on applying Fast BSS Transition (FT) authentication [9] to deal with the aforementioned challenges. FT authentication is proposed in the emerging IEEE 802.11r standard, which aims at supporting fast handoff. FT authentication schemes can be further divided into two subgroups: proactive neighbor caching [6, 7] and proactive key distribution [8]. The proactive neighbor caching schemes are based on proactive propagation of the MH context from the current associated MAP to the selected MAPs. In such FT authentication schemes, the handoff delay is largely reduced since a MH is allowed to perform authentication before handoff. However, the delay is reduced at the cost of dramatically increasing communication overhead in the network. The high communication overhead is especially intolerant when there are large amounts of users performing handoff in the network, e.g., in WMNs. In proactive key distribution schemes, the pairwise master keys (PMKs), which are shared by MHs, target MAPs and the authentication server (AS), are pre-distributed to reduce the transition messages overhead introduced in proactive neighbor caching schemes. Nonetheless, in WMNs, where MHs frequently join and leave the network, proactive key distribution approaches must keep updating the sharing relationships of PMKs constantly to achieve effective results [10]. Therefore, the efficiency of these schemes may be negatively impacted in large scale WMNs.

Some works that aim at reducing re-authentication delay while keeping low communication overhead during handoff are also proposed [1, 11, 12, 13]. In the dual re-authentication scheme [11], a MH is allowed to perform immediate authentication with a target MAP by virtue of a one-time ticket during handoff. Full IEEE 802.1X authentication is performed after the establishment of association between the MH and the target MAP. However, the re-authentication delay is reduced at the cost of sacrificing the security, since the one-time tickets in the network can be duplicated. In [1], repeated encryptions and decryptions during frame exchanges between MHs and MAPs can be substantially saved through extending access points (APs) security domains to a mesh network. Unfortunately, re-authentication delay of this scheme is at the same order of that of IEEE 802.1X authentication, which is still too high to satisfy QoS requirements of real-time mesh applications. In SFRIC [12], re-authentication is performed just between mobile nodes (MNs) and APs by employing their identities such as MAC addresses. However, private key generator (PKG) is required to be additionally designated for bringing SFRIC into effect, which requires significant changes in the current architecture of WMNs. Furthermore, the relatively costly bilinear mapping operations limit the improvement of authentication efficiency. In the scheme proposed in [13], i.e., HACCH, fast re-authentication is accomplished on the basis of a short-term credential that is issued by the AS for each MN. The scheme reduces the system complexity compared to the previous schemes. In addition, the re-authentication delay is further reduced compared to SFRIC scheme. However, since a MN or an AP has to apply a new credential from the AS each time when a credential is expired, the AS is laid a heavy burden to refresh credentials. More importantly, it is difficult to accomplish time synchronization among all parities in the whole network, which is necessary to verify the short-term credentials.

In this paper, we consider the secure fast handoff problem in a mesh domain that is comprised of an MPP, and the MPs (including MAPs) and the MHs connecting to the MPP. We propose a proxy signature-based re-authentication scheme to provide mutual authentication and key establishment between a roaming MH and the target MAP. The basic idea is as follows:

1) We designate the MPP in a mesh domain for authenticating an initially accessing MH, and for further authorizing the MH to obtain a proxy delegation for intra-domain fast handoff;

2) The MH can derive a proxy key pair (PKP) from the proxy delegation, and use the PKP for authenticating itself when associating with the target MAP in the case of intra-domain handoff;

3) In order to authenticate the target MAP, the MH needs to additionally acquire an access list, which includes the identities and elliptic curve cryptosystem (ECC) public keys of the MAPs in the mesh domain, from the MPP;

4) For further secure communication, a PMK is negotiated between the MH and the target MAP during the re-authentication process.

The aforementioned mutual authentication and PMK establishment between the roaming MH and the target MAP are accomplished in a three-way handshake procedure. The reduced computing operations and message exchanges contribute to the decreased re-authentication delay of the proposed scheme. The proposed scheme is also proved to be secure under common security attacks. Besides, the load of the AS is lightened since the AS is not involved in the re-authentication procedure. Although the MPP has to authenticate all of the initially accessing MHs in its domain, its burden of transmitting messages in the process of handoff is released. Therefore, no significant additional network overhead is brought in preparation for the fast handoff.

The rest of the paper is organized as follows. In Section 2, we introduce some preliminaries of the proposed scheme. Section 3 presents the proposed scheme in details. The security analysis of the proposed scheme is presented in Section 4. Performance evaluation, including computation cost, communication overhead, and re-authentication delay, is described in Section 5. Section 6 concludes this paper.

2 Preliminary

In this section, we present the following preliminaries, which are the related techniques of the proposed scheme.

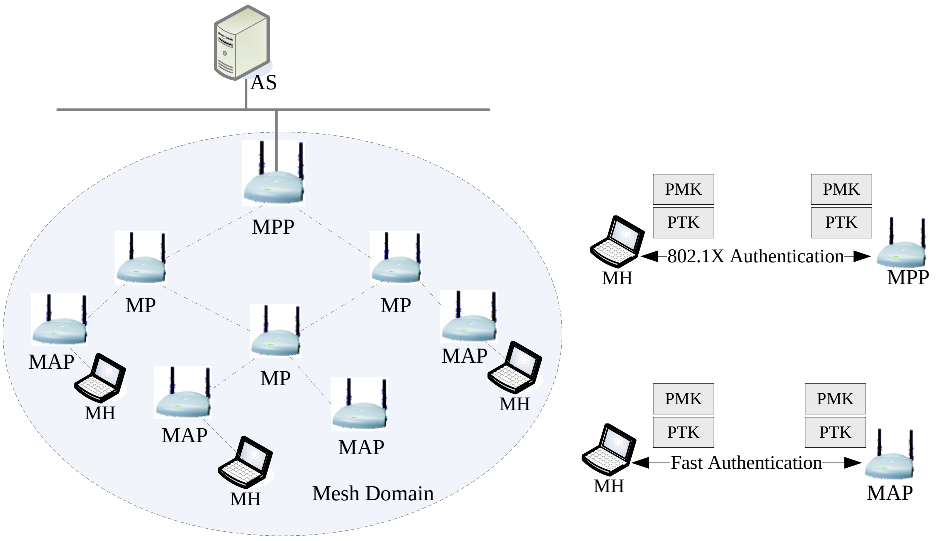

Figure1. The network model and trust model of the proposed scheme

2.1 IEEE 802.1X Framework

In IEEE 802.1X framework, the secure association between the MH and the MAP is established through extensible authentication protocol (EAP) interactions. Specifically, IEEE 802.1X authentication starts with the transmission of EAP-Request /Identity packet from the current associated MAP. Then the MH responds its identity to the MAP by sending EAP-Response/Identity packet to the MAP. When receiving the packet, the MAP encapsulates it into RADIUS-Access-Request packet and transmits it to the AS. The subsequent interactions are several rounds of challenge-response between the MH and the AS via the packet transformation by the MAP. The number of the round-trips depends on the specific EAP method. After the successful EAP interactions, a common master session key (MSK) is negotiated between the MH and the AS. The MSK will then be sent to the MAP by the AS in a RADIUS-Access-Accept message, for the purpose of deriving a PMK between the MAP and the MH. Finally, the MH and the MAP derive a pairwise transient key (PTK) from the PMK in a four-way handshake procedure, and accordingly the secure association is established.

In this paper, we adopt the IEEE 802.1X framework to authenticate each initially accessing MH. However, we designate the MPP, rather than the MAP, as the initial authenticator. In this way, MHs that have been successfully authenticated by the MPP can obtain the proxy delegation of the MPP, and can further perform fast re-authentication in the mesh domain. The details will be further described in Section 3.

2.2 Elliptic Curve Cryptosystem

ECC is more computationally efficient than RSA due to the smaller key size and lower computation overhead. For instance, 160-bit-ECC has the same security level as 1024-bit-RSA. An elliptic curve is an abelian group over a finite field $GF(q)$ with the order q. The point (x, y) in the group satisfies the long Weierstrass form as in Equation (1).

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ (a_i \in GF(q)) \quad (1)$$

In elliptic curve system, a point that is the result of the addition of two points on a curve is also on the curve. Such addition operation is called elliptic curve point addition (ECADD). The operation of adding a point to itself $i\ (i \geq 1)$ times is called scalar multiplication.

The security of ECC depends on the difficulty of the elliptic curve discrete logarithm problem, namely, given two points P_1 and P_2 in the group, it is hard to find a number j that satisfies $P_2=jP_1$.

2.3 Proxy Signature

In this paper, we utilize the proxy signature scheme for partial delegation with warrant [14] to design the fast re-authentication scheme. In the proxy signature scheme, the original signer, called Alice, delegates her signing capability to a proxy signer, called Bob, whose identity is ID_B. To prevent Bob from misusing the delegation, Alice creates a proxy warrant a_B, which demonstrates the proxy information [15], for Bob. Then Bob creates a signature on behalf of Alice. When receiving Bob's proxy signature, the receiver verifies the signature and the delegation of Alice together. Let p be a large prime, and g be a generator of a multiplicative subgroup of Z_p^* with order p. $h(\ )$ denotes a collision resistant hash function. The private key and the corresponding public key of Alice are x_A and y_A ($y_A = g^{x_A} \bmod p$), respectively. Then the proxy signature scheme can be described as follows:

1). Proxy generation: Alice generates a random number $k_B \in Z_{p-1}^*$, and computes the proxy delegation (r_B, s_B) as in Equation (2) and Equation (3).

$$r_B = g^{k_B} \bmod p \quad (2)$$

$$s_B = (h(a_B, r_B)x_A + k_B) \bmod (p-1) \quad (3)$$

Table 1: Relevant parameters of the proposed scheme

Notations	Meanings
σ	Authentication signature
Z_q^*	Positive integers less bigger than q
$(G,+)$	The selected cyclic group
q	The order of G
P	The generator of G
$\{0,1\}^*$	non-zero-length string
$\{0,1\}^n$	n-bit-size string
$H_1(\ )$	$G \rightarrow \{0,1\}^n$
$H_2(\ )$	$\{0,1\}^n \times \{0,1\}^n \rightarrow Z_q^*$
$h(\ )$	$\{0,1\}^* \rightarrow \{0,1\}^n$
PK	The pairwise key between the MH and the MAP
PuK_{MH}	The public key of the MH
PrK_{MH}	The private key of the MH
PuK_{MPP}	The public key of the MPP
PrK_{MPP}	The private key of the MPP
PuK_{MAP}	The public key of the MAP
PrK_{MAP}	The private key of the MAP
PuK_{MH_P}	The proxy public key of the MH
PrK_{MH_P}	The proxy private key of the MH
a_{MH}	The proxy warrant of the MH
r_{MH}	The public proxy delegation to the MH
s_{MH}	The private proxy delegation to the MH

$H_1(\ )$, $H_2(\ )$, $h(\ )$: strong one-way hash functions; PK, PMK, PuK_{MH}, PuK_{MPP}, PuK_{MAP}, PuK_{MH_P}, $r_{MH} \in G$; σ, PrK_{MH}, PrK_{MPP}, PrK_{MAP}, PrK_{MH_P}, $s_{MH} \in Z_q^*$; $a_{MH} \in \{0,1\}^n$, $Z_q^* \cdot P \rightarrow G$.

2). Proxy delivery: Alice sends the message (a_B, r_B, s_B) that contains the proxy warrant and the proxy delegation to Bob in a secure manner, and publishes the warrant a_B to the public.

3). Proxy verification: If the Equation (4) holds, Bob confirms the validity of the proxy delegation, and computes his PKP (x_{P_B}, y_{P_B}) as in Equation (5) and Equation (6), where x_{P_B} is the proxy private key, and y_{P_B} is the proxy public key.

$$g^{s_B} = (y_A^{h(a_B,r_B)} r_B) \bmod p \tag{4}$$

$$x_{P\_B} = s_B \tag{5}$$

$$y_{P\_B} \equiv g^{x_{P\_B}} = y_A^{h(a_B,r_B)} r_B \bmod p \tag{6}$$

In this paper, we reconstruct this proxy signature scheme on elliptic curve system to enhance its efficiency. Furthermore, we designate the MPP for authorizing the MH that has accomplished the initial association with the MPP to obtain a proxy delegation. The PKP that is derived from the proxy delegation helps the MH to perform fast re-authentication in the case of handoff. The detailed process will be described in Section 3.

3 The Proposed Scheme

In the proposed scheme, we adopt the IEEE 802.1X framework to perform the authentication on MHs that initially access a mesh domain. However, we designate the MPP in the domain, rather than the accessed MAPs, as the authenticator. A MH that has performed the complete IEEE 802.1X authentication procedure with the MPP can obtain the proxy delegation from the MPP. Furthermore, the MH can derive a PKP from the delegation, and use the PKP to make itself authenticated by the target MAP in the case of intra-domain handoff. To authenticate the target MAP, the MH needs to additionally acquire an access list, which includes the identities and ECC public keys of the MAPs in the mesh domain, from the MPP. For the subsequent secure communication, a PMK is also negotiated between the MH and the target MAP during the re-authentication process. The aforementioned mutual authentication and PMK establishment between the MH and the MAP are accomplished in a three-way handshake procedure.

In this section, we first introduce the network model and trust model of the proposed scheme. Then we will present the proposed scheme, including the initial access procedure of a MH in a mesh domain, and the fast re-authentication process of the MH in the domain, in details.

3.1 The Network Model and Trust Model

In this paper, we focus on the intra-mesh-domain handoff. A mesh domain, as is shown in Figure 1, consists of a MPP, and the MPs (including the MAPs) and the MHs directly or indirectly connecting to the MPP. Through the network attachment provided by the MAP and the message transmission provided by MPs, the MH that enters the mesh domain can communicate with the parties in other networks, which is connected with the mesh network via the MPP. Before accessing the mesh domain, a MH has no trust relationship with any entities in the mesh domain. However, a trust relationship can be built between the MH and the MPP after the successful initial association, which is accomplished through a complete IEEE 802.1X authentication process among the MH, the MPP, and the AS. Furthermore, the MH is also able to build a trust relationship with a target MAP after a successful re-association, which is accomplished through performing the proposed re-authentication scheme between the MH and the MAP. Note that although we merely consider the intra-domain handoff in this paper, the scheme can be easily extended into inter-domain handoff scheme. For example, a MH can pre-authenticate with the MPP in another mesh domain when inter-domain handoff occurs.

3.2 The Proposed Scheme

The computations in the proposed scheme are carried out on the elliptic curve. We define $(G,+)$ as the cyclic group for the selected elliptic curve algorithm. Let the large prime p ($p \geq 2^{160}$) be the order of G, and P be the generator of G. The MH, the MPP, and the target MAP hold an ECC key

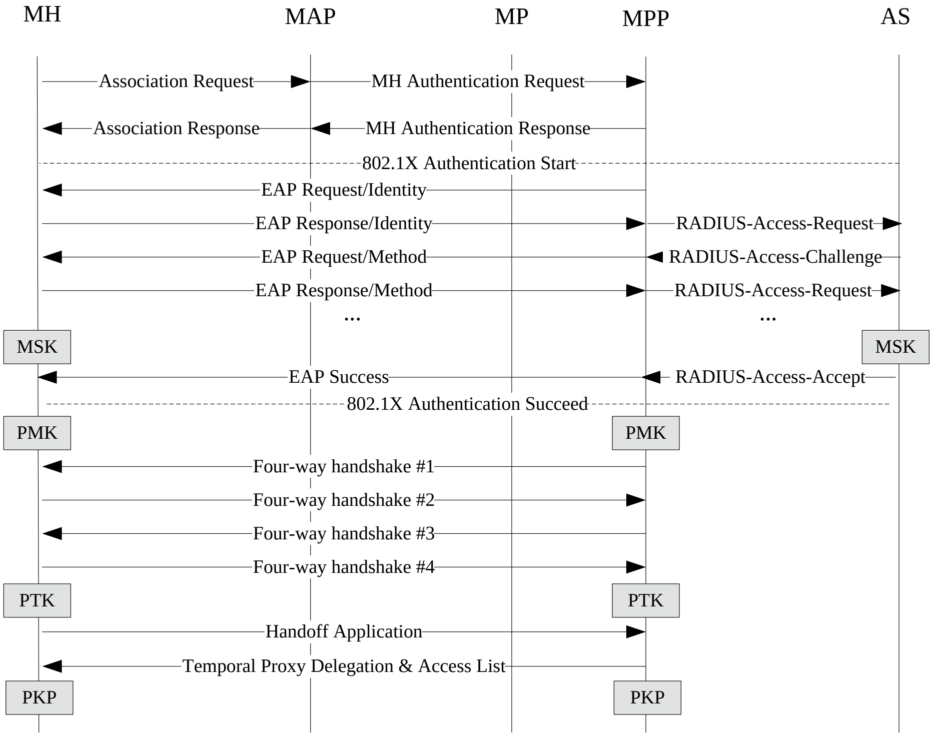

Figure2. Message flows in the process of initial access

pair (PrK_{MH}, PuK_{MH}), (PrK_{MPP}, PuK_{MPP}), and (PrK_{MAP}, PuK_{MAP}), respectively. The private keys PrK_I ($I=MH$, MPP, MAP) belong to Z_q^*, and the public keys PuK_I ($PuK_I = PrK_I P$) belong to G. The system defines three kinds of collision resistant hash functions. They are $h(\ )$: $\{0,1\}^* \to \{0,1\}^n$, $H_1(\ )$: $G \to \{0,1\}^n$, and $H_2(\ )$: $\{0,1\}^n \times \{0,1\}^n \to Z_q^*$. The system parameters are summarized in Table 1. We will present the proposed scheme in two steps, i.e. the initial access and the fast re-authentication.

1). The Initial Access

In the proposed scheme, when a MH initially accesses a mesh domain, it should be authenticated by the MPP in the domain. The authentication is accomplished through a complete IEEE 802.1X authentication procedure among the MH, the MPP, and the AS. The message flows of the initial access are shown in Figure 2, and the complete process is as follows.

a). The MH sends the association request to a MAP, which will transmit the MH authentication request to the MPP. The MPP will respond the MH authentication response if it accepts the MH authentication request. Then the MAP will respond the association response to the MH.

b). The MPP starts the initial authentication process by sending the EAP-Request/Identity packet to the MH. When receiving the packet, the MH responds the EAP-Response/Identity packet to the MPP to inform its identity. Then the MPP encapsulates the received EAP-Response/Identity packet into the RADIUS–Access-Request packet and transmits it to the AS. The subsequent interactions are rounds of challenge-response between the MH and the AS via the packet transmission performed by the MPP. After the successful EAP interactions, the MH is successfully authenticated, and a common master session key (MSK) is negotiated between the MH and the AS.

c). For the purpose of deriving a PMK between the MPP and the MH, the MSK is sent to the MPP by the AS in a RADIUS-Access-Accept message. Furthermore, the MH and the MPP derive a PTK from the PMK in a four-way handshake process. Thus the initial secure association is established.

d). In order to allow MHs to authenticate MAPs, the MPP transmits the access list, which includes the identities and public keys of the available MAPs in the domain, to the MH. To perform secure fast handoff, the MH should also apply a temporal proxy delegation from the MPP. The detailed procedure is described as follows.

- To prevent the MH from abusing the proxy delegation, the MPP first needs to choose a proxy warrant a_{MH} for the MH. This warrant is used to validate the effectiveness of the proxy delegation. A reasonable example of a_{MH} may be r_{MH} @ 24/09/10/2012 (the string length is n), which means that the proxy delegation with the public part of r_{MH} expires at 24:00 on September 10, 2012. Note that the timeliness verification only requires the time synchronism among the MPP and MAPs in the same mesh domain, rather than time synchronism among all parties in the whole network.

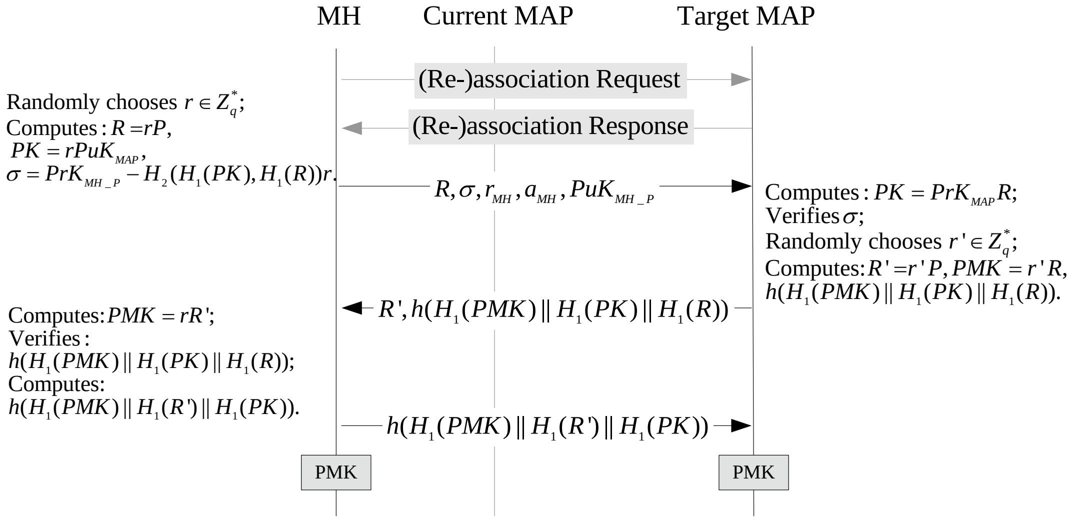
MH
Current MAP
Target MAP
(Re-)association Request
(Re-)association Response
Randomly chooses $r \in Z_q^*$;
Computes: $R = rP$,
$PK = rPuK_{MAP}$,
$\sigma = PrK_{MH\_P} - H_2(H_1(PK), H_1(R))r$.
$R, \sigma, r_{MH}, a_{MH}, PuK_{MH\_P}$
Computes: $PK = PrK_{MAP}R$;
Verifies σ;
Randomly chooses $r' \in Z_q^*$;
Computes: $R' = r'P, PMK = r'R$,
$h(H_1(PMK) \| H_1(PK) \| H_1(R))$.
$R', h(H_1(PMK) \| H_1(PK) \| H_1(R))$
Computes: $PMK = rR'$;
Verifies:
$h(H_1(PMK) \| H_1(PK) \| H_1(R))$;
Computes:
$h(H_1(PMK) \| H_1(R') \| H_1(PK))$.
$h(H_1(PMK) \| H_1(R') \| H_1(PK))$
PMK
PMK

Figure3. Message flows in the process of fast re-authentication

- Then the MPP randomly chooses a value $k\ (k \in Z_q^*)$, and computes a proxy delegation pair (r_{MH}, s_{MH}) as in Equation (7) and Equation (8). Then the MPP sends the proxy delegation to the MH securely by virtue of the PTK between them.

$$r_{MH} = kP \tag{7}$$

$$s_{MH} = PrK_{MPP}H_2(a_{MH}, H_1(r_{MH})) + k \tag{8}$$

- The MH checks the validity of the delegation by checking if Equation (9) satisfies.

$$s_{MH}P = PuK_{MPP}H_2(a_{MH}, H_1(r_{MH})) + r_{MH} \tag{9}$$

- After the confirmation, the MH computes the PKP (PrK_{MH_P}, PuK_{MH_P}) as in Equations (10) and (11).

$$PrK_{MH\_P} = s_{MH} \tag{10}$$

$$PuK_{MH\_P} = PuK_{MPP}H_2(a_{MH}, H_1(r_{MH})) + r_{MH} \tag{11}$$

After the aforementioned operations, the MH is prepared for the fast handoff.

2). The Fast Re-authentication

When performing handoff, the MH first probes a MAP that can associate with it. After receiving the response from a target MAP, the MH starts the (re-)authentication with the MAP in the form of a three-way handshake procedure. The process is presented in Figure 3, and the detailed three-way handshake process is as follows.

a). The first handshake: In this handshake, the MH generates the pairwise key used to authenticate the target MAP, and the authentication signature used to make itself authenticated by the MAP. Specifically, the MH randomly chooses a value $r\,(r \in Z_q^*)$, and computes the pairwise key used for MAP authentication, i.e. *PK*, according to Equation (12). In addition, it generates the authentication signature σ according to Equation (13) and Equation (14). Then the MH sends the message ($R, \sigma, r_{MH}, a_{MH}, PuK_{MH\_P}$) to the MAP.

$$PK = rPuK_{MAP} \tag{12}$$

$$R = rP \tag{13}$$

$$\sigma = PrK_{MH\_P} - H_2(H_1(PK), H_1(R))r \tag{14}$$

b). The second handshake: When receiving the message, the MAP first checks if the proxy delegation is overdue according to the proxy warrant. If the proxy delegation is overdue, the MAP will terminate the fast authentication procedure. In this case, the MH has to renew the proxy delegation from the MPP. If the association between the MH and the MPP has been broken down, the MH is required to perform another complete IEEE 802.1X authentication with the MPP. Otherwise, the MAP computes *PK* according to Equation (15) and then verifies the authentication signature σ by checking if Equation (16) satisfies. The successful confirmation means that the MH is authenticated by the MAP. For the purpose of negotiating the PMK with the MH, the MAP randomly chooses a value $r'(r' \in Z_q^*)$, and computes R' and PMK as in Equation (17) and Equation (18). In order to make itself authenticated by the MH, the MAP should further compute $h(H_1(PMK) \| H_1(PK) \| H_1(R))$. Then the MAP sends the message ($R', h(H_1(PMK) \| H_1(PK) \| H_1(R))$) to the MH.

$$PK = PrK_{MAP}R \tag{15}$$

$$\sigma P + H_2(H_1(PK), H_1(R))R = PuK_{MPP}H_2(a_{MH}, H_1(r_{MH})) + r_{MH} \tag{16}$$

$$R' = r'P \tag{17}$$

$$PMK = r'R \tag{18}$$

c). The third handshake: When receiving the response, the MH firstly computes *PMK* as in Equation (19), and computes $h(H_1(PMK) \| H_1(PK) \| H_1(R))$ and compares the result with that in the response. If the two results are equal, the MAP will be successfully authenticated by the MH, and the MH will accept the *PMK*. Then the MH computes $h(H_1(PMK) \| H_1(R') \| H_1(PK))$, and sends the result as a message to the MAP for confirming the *PMK*.

$$PMK = rR' \tag{19}$$

Through the three-way handshake, the MH and the MAP have accomplished the mutual authentication and have built a PMK with each other. Hence, the MH successfully accomplished the re-authentication with the MAP. In order to further build a trust relationship, the two parties can derive a PTK from the PMK, which belongs to the re-association stage and is out of the scope of our discussion. Additionally, to avoid the key leaking caused by compromise of communication parties, the historical PMKs should not be stored in the MAP or the MH and hence the MH should negotiate a new PMK with the MAP each time when handoff occurs.

4 Correctness Proof and Security Analysis

In this section, we will prove the correctness and present the security analysis of the proposed scheme.

4.1 Correctness Proof

1). Correctness of Proxy Delegation Verification

In the initial access procedure, we mentioned that the MH verifies the proxy delegation by checking if Equation (9) satisfies. This is correct because, if Equation (7) and Equation (8) holds, then according to the commutative law of multiplication in Z_q^*, the following equations will hold.

$$\begin{aligned} s_{MH}P &= (PrK_{MPP}H_2(a_{MH}, H_1(r_{MH})) + k)P \\ &= H_2(a_{MH}, H_1(r_{MH}))PrK_{MPP}P + kP \\ &= PuK_{MPP}H_2(a_{MH}, H_1(r_{MH})) + r_{MH} \end{aligned}$$

Therefore, the MH can confirm the correctness of the proxy delegation provided by the MPP.

2). Correctness of Authentication Signature Verification

In the second handshake of the (re-)authentication procedure, the verification of the MH's authentication signature is carried out through checking if Equation (16) satisfies. This is correct because, if the signature is generated by the authorized MH and the proxy delegation is valid, the following equations will hold.

$$\begin{aligned} &\sigma P + H_2(H_1(PK), H_1(R))R \\ &= (PrK_{MH\_P} - H_2(H_1(PK), H_1(R))r)P + H_2(H_1(PK), H_1(R))R \\ &= PrK_{MH\_P}P - H_2(H_1(PK), H_1(R))rP + H_2(H_1(PK), H_1(R))R \\ &= PuK_{MH\_P} - H_2(H_1(PK), H_1(R))R + H_2(H_1(PK), H_1(R))R \\ &= PuK_{MH\_P} = PuK_{MPP}H_2(a_{MH}, H_1(r_{MH})) + r_{MH} \end{aligned}$$

3). Correctness of the *PK* Verification

In the first handshake, the MH computes *PK* according to Equation (12). In the third handshake, the MH authenticates the MAP by verifying the *PK* sent back from the MAP, which is computed by the MAP according to Equation (15). The verification of *PK* is correct, since according to the commutative law of multiplication in Z_q^*, the following equations will hold.

$$rPuK_{MAP} = rPrK_{MAP}P = PrK_{MAP}rP = PrK_{MAP}R$$

4). Correctness of the PMK Establishment

The MAP computes the PMK shared with the MH according to Equation (18) in the second handshake, whereas the MH computes it according to Equation (19) in the third handshake. Through the above operations, the MH and the MAP can build a common PMK, since according to the commutative law of multiplication in Z_q^*, the following equations hold.

$$r'R = r'rP = rr'P = rR'.$$

5). Correctness of Mutual Authentication

On the one hand, the MAP authenticates the MH by verifying the authentication signature sent by the MH, which is proved to be correct as mentioned above. On the other hand, the MH authenticates the MAP by confirming that the MAP can return the right computation result of *PK*. This is correct because only the MAP with the corresponding private key can return the right *PK*. Therefore, the proposed scheme provides mutual authentication between a roaming MH and the target MAP.

4.2 Security Analysis

In this part, we present the security analysis of the proposed scheme. Since the security of the initial access part of the proposed scheme is guaranteed by IEEE802.1X, which can be found in [1], we do not include the analysis in this paper. Instead, we focus on the security analysis of the fast re-authentication part of the proposed scheme. The proposed scheme provides functionalities, including the authenticatablity of the MH and the MAP, and the secure PMK establishment. On the basis of the appropriate use of the proxy signature, the elliptic curve public-key algorithm, and the strong one-way hash functions, the proposed scheme can resist attacks, including proxy delegation forgery, man-in-the-middle attacks, and replay attacks. Besides, the proposed scheme provides forward security, which means that the historical data will not leak out even if some communication parties are compromised. We give the security proof of the proposed scheme as follows.

(1). Proxy delegation forgery

According to the initial access part of the proposed scheme mentioned above, a MH that holds a valid proxy delegation from the MPP can perform fast re-authentication with a target MAP in a mesh domain. Hence, it is possible for unauthorized MHs to forge proxy delegations in order to perform (re-)authentication with MAPs. However, since each valid proxy delegation is generated using the private key of the MPP, the proxy delegation is able to be verified by using the public key of the MPP. Therefore, the forgery of proxy delegation is infeasible as long as the private key of the MPP has not leaked out.

(2). The authenticatablity of MH

Since the proxy delegation parameters are uniquely chosen or generated by the MPP for a given MH, and the forgery of proxy delegation is infeasible according to the security analysis as aforementioned, only the MH that holds the specific proxy private key can create the specific authentication signature. The authentication signature of the MH can be further verified by recovering the MH's proxy public key using the proxy delegation parameters, i.e., a_{MH} and r_{MH}. Therefore, a MH can be authenticated by handing over its authentication signature that is signed by his or her proxy private key to the target MAP.

(3). The authenticatablity of MAP

Since a MH can extract the public key of the target MAP from the access list sent by the MPP, it can authenticate the target MAP by learning whether the MAP holds the corresponding private key. This is done by checking if the MAP can compute the correct *PK*, which is indirectly accomplished through checking $h(H_1(PMK)\,||\,H_1(PK)\,||\,H_1(R))$ as described in the third handshake of the fast re-authentication procedure.

(4). The security of PMK establishment

In order to prove the security of the PMK establishment, we first introduce two definitions [16] as follows.

Definition 1. *Computational Elliptic Curve Diffie-Hellman (CECDH) Problem. Let P be a CECDH parameter generator, p be the corresponding order. Given ($P,aP,bP \in G$) for some unknown $a,b \in Z_p$, compute abP. The success probability of a polynomial algorithm A in solving CDH problem is denoted as:*

$$Win_{A,G}^{CECDH} = Pr[A(P,aP,bP) = abP : a,b \in Z_p].$$

Definition 2. *Computational Elliptic Curve Diffie-Hellman (CECDH) Assumption. Let P be a CECDH parameter generator, p be the corresponding order. Given ($P,aP,bP \in G$) for some unknown $a,b \in Z_p$, $Win_{A,G}^{CECDH}$ is negligible.*

According to the (re-)authentication procedure, the Diffie-Hellman public parameters used for constructing the PMK are R and R', in which, $R = rP$, $R' = r'P$, and $PMK = rR' = r'R$. Therefore, the extraction of PMK using R and R' is a CECDH problem, which is infeasible due to the CECDH assumption.

(5). Man-in-the-middle attack

Generally, Diffie-Hellman key exchange is vulnerable to the man-in-the-middle attack. However, the man-in-the-middle attack is infeasible in the proposed scheme. This is attributed to the fact that the *PMK* is confirmed by the MH and the MAP through checking the correctness of *PK* and Diffie-Hellman public parameters, which are confirmable and cannot be tampered by the attacker without causing awareness of victims. For example, the man-in-the-middle attacker tampers R and R' in the message flows of fast re-authentication, to be R_w and R_w', where $R_w = r_wP$, and $R_w' = r_w'P$. In this way, the attacker wants to successfully make the MAP accept R_w and wrongly compute the PMK_w according to $PMK_w = r'R_w$, and also to make the MH accept R_w' and wrongly compute the PMK_w' according to $PMK_w' = rR_w'$. However, the MAP will refuse R_w, since the authentication signature in the message cannot be successfully verified. It is also infeasible for the attacker to generate a correct authentication signature on R_w, since the attacker does not know the proxy private key of the MH. In addition, the MH will not accept R_w' either, because the result of $h(H_1(PMK_w)\,||\,H_1(PK)\,||\,H_1(R_w))$ that is computed by the MH is not equal to $h(H_1(PMK)\,||\,H_1(PK)\,||\,H_1(R))$ in the message sent by the MAP to the MH. Since the attacker is unable to compute the correct PK because of the lack of corresponding private keys, it's also infeasible for the attacker to tamper $h(H_1(PMK)\,||\,H_1(PK)\,||\,H_1(R))$ in the message sent by the MAP to the MH to be $h(H_1(PMK_w)\,||\,H_1(PK)\,||\,H_1(R_w))$. Therefore, the proposed scheme can resist the man-in-the-middle attack.

(6). Replay attack

The replay attack cannot be carried out in the proposed scheme resulting from random values added in each handshake. If the attacker replays the message sent in the first handshake, it cannot respond the feedback of the MAP, since the PMK or PK cannot be computed correctly. If the attacker replays the message sent in the second or the third handshake, the behavior will be meaningless since the right PMK cannot be derived from the message.

(7). Forward security

If a MAP or a MH is compromised by the attacker, the corresponding private key will leak out. In this case, the attackers that have intercepted the compromised entity's historical message exchanges may try to obtain the historical data by recovering historical PMKs by virtue of the compromised private key. However, since the temporal Diffie-Hellman parameters used to negotiate a PMK is randomly chosen, and is unrelated to the private key, it's infeasible for the attacker to recover historical PMKs. Therefore, the historical data will not leak out because of the compromise of communication entities, namely, the proposed scheme provides forward security.

5 Performance Evaluation

In this section, we evaluate the performance of the proposed scheme in terms of computation cost, re-authentication delay, and communication overhead. The computation cost and the re-authentication delay are compared with SFRIC [12] and HACCH [13]. We choose these two schemes rather than FT-based schemes and other schemes mentioned in Section 1 for two reasons. Firstly, the communication with an AS is not required in both SFRIC and HACCH, which is similar to the proposed scheme. However, the AS is involved in the process of handoff in other schemes. Secondly, the re-authentication procedures of SFRIC, HACCH, and the proposed scheme are all three-way handshake processes, rather than tedious message flows in IEEE802.1X architecture. In addition, the communication overhead is compared with SFRIC and HACCH, as well as two schemes in [1] and [8]. The latter two schemes for comparison are both based on IEEE 802.1X. Since the communication overhead of FT-based schemes is consumed in the process of proactive context propagation, rather than the re-authentication procedure when handoff occurs, we don't choose such schemes for comparison.

The parameters of the performance evaluation are summarized in Table 2. Note that the computation operations listed in the table are relatively costly, whereas the much less costly operations that have negligible impact on the performance of a certain scheme are not listed in the table. For example, since hash and ECADD operations are much less costly than scalar multiplication operation, we only consider the number of scalar multiplication operations performed by communication parties when evaluating the computation cost. The estimated values of time cost of different operations are from [13], in which primitive cryptography operations are performed on an Intel P III Mobile 733MHz processor (as a MH) and Intel P IV 3GHz (as a MAP) using the MIRACL library. The values are further verified to be valid according to [17]. The computation cost of the MH is defined as the total time of its cryptography operations, which is directly related to its energy consumption. The re-authentication delay is defined as the time of optimized cryptography operations of the MH and the MAP. The optimization is accomplished through pre-computation. For communication overhead, since all of the schemes for comparison and the proposed scheme do not involve communication among MAPs, we only need to consider communication between the MH and the MAP, and that between the MAP and the AS. Additionally, we assume that the average message delivery cost for each message exchange between the MH and the MAP, or between the MAP and the AS, is a constant value, i.e. $E_{MH\text{-}MAP}$ and $E_{MAP\text{-}AS}$, respectively.

Table 2: Parameters of performance evaluation

Notation	Definition	Estimated value (ms)
T_E	Time for modular exponent	MH/MAP: 1.1/0.5
T_{RV}	Time for RSA verification	MH/MAP: 0.4/0.2
T_M	Time for scalar multiplication on elliptic curve	MH/MAP: 1.1/0.4
T_P	Time for tate pairing	MH/MAP: 34/13
T_{MH_or}	Computation time for the MH	Variable
T_{MH_op}	Computation time for the MH with pre-computation	Variable
T_{MAP_op}	Computation time for the MAP with pre-computation	Variable
$E_{MH\text{-}MAP}$	Message delivery cost of once message exchange between the MH and the MAP	——
$E_{MAP\text{-}AS}$	Message delivery cost of once message exchange between the MAP and the AS	——

Section size: RSA-1024 bits, ECC-160 bits.

The comparison results of computation cost and re-authentication delay are concluded in Table 3. According to the table, the computation cost of the MH in the proposed scheme is far less than that in SFRIC scheme, and is also less than that in HACCH scheme. This is significant for the MH, which does not have sufficient power to persistently connect with the MAP. The low computation cost of the proposed scheme results from the efficient computations on elliptic curve system. Furthermore, due to the reduced computation time, the re-authentication delay is also obviously reduced in the proposed scheme compared to the other two schemes.

We show the comparison result of communication overhead in Table 4. Since SFRIC scheme, HACCH scheme and the proposed scheme all involve three message exchanges between the MH and the MAP, and the message sizes of the three schemes are comparable, their communication overhead is approximately equal. Generally, $E_{MH\text{-}MAP}$ is lower than $E_{MAP\text{-}AS}$, since the message delivery from the MAP to the AS involves several hops [13].

Therefore, the communication overhead of the proposed scheme is much lower than those schemes in which the AS is involved in authentication procedure, e.g., schemes in [1], [8]. The low communication overhead of the proposed scheme is due to the idea that we utilize proxy signature to save the message exchanges with the AS.

Table 3: Computation cost and delay comparison

Items	SFRIC	HACCH	Ours
Computation cost of the MH (T_{MH_or})	$1T_M+2T_P \approx 69$ms	$4T_E+1T_{RV} \approx 4.8$ms	$3T_M \approx 3.3$ms
Re-authentication delay ($T_{MH\_op} + T_{MAP\_op}$)	$(1T_P)+(2T_P) \approx 60$ms	$(3T_E+1T_{RV}) + (3T_E+1T_{RV}) \approx 5.4$ms	$(1T_M)+(3T_M) \approx 2.3$ms

Table 4: Communication overhead comparison

[1]	[6]	SFRIC	HACCH	Ours
$7E_{MAP\text{-}AS}+8E_{MH\text{-}MAP}$	$3E_{MAP\text{-}AS}+3E_{MH\text{-}MAP}$	$3E_{MH\text{-}MAP}$	$3E_{MH\text{-}MAP}$	$3E_{MH\text{-}MAP}$

6 Conclusions

In this paper, we propose a novel proxy signature-based re-authentication scheme for secure fast handoff in WMNs. We designate the MPP in a mesh domain for authenticating MHs that initially access the domain, and for further authorizing the MHs to obtain proxy delegation. By utilizing proxy signature, a roaming MH is able to only communicate with the target MAP when performing handoff. Hence the message exchanges with the AS are saved. We have analyzed the security of the proposed scheme by discussing potential threat models. The security analysis shows that the scheme is secure considering common attacks. We have also evaluated the performance of the proposed scheme by comparing it with existing schemes. The performance evaluation shows that the proposed scheme is more efficient than existing schemes, in terms of computation cost, re-authentication delay and communication overhead.

Acknowledgments

This work is supported by the National S&T Major Project of China under Grant No. 2011ZX03005-006, the National Natural Science Foundation of China under Grand No. 60832005, and the Research Cooperation Project of Guangdong Province and the Ministry of Education under Grant No.2011B090400250.

References

[1] K. H. Chi, Y. C. Shih and H. H. Liu, “Fast Handoff in Secure IEEE 802.11s Mesh Networks,” IEEE transactions on vehicular technology, vol. 60, no. 1, pp.219-232, 2011.

[2] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Standard 802.11i Part 11, 2004.

[3] M. S. Bouassida, “Authentication vs. Privacy within Vehicular Ad Hoc Networks,” I*nternational Journal of Network Security*, vol.13, no.3, pp.121-134, 2011.

[4] R. Kandikattu and L. Jacob, “Comparative Analysis of Different Cryptosystems for Hierarchical Mobile IPv6-based Wireless Mesh Network,” I*nternational Journal of Network Security*, vol. 10, no. 3, pp. 190-203, 2010.

[5] A. Mishra, M. Shin, and W. Arbaugh, “An empirical analysis of the IEEE 802.11 MAC layer handoff process,” *ACM SIGCOMM Computer Communications Review*, vol. 33, no. 2, pp. 93-102, 2003.

[6] S. Shin, A. Forte, A. Rawat, and H. Schulzrinne, “Reducing MAC Layer handoff Latency in IEEE 802.11 Wireless LANs,” *The 2nd ACM International Symposium on Mobility Management and Wireless Access (ACM MobiWac2004)*, pp. 19-26, 2004.

[7] S. Pack, J. Choi, T. Kwon, and Y. Choi, “Fast-handoff support in IEEE 802.11 wireless networks,” *IEEE Communications Surveys and Tutorials*, vol. 9, no. 1, pp. 2–12, 2007.

[8] A. Mishra, M. Shin and W. Arbaugh, “Proactive Key Distribution using Neighbor Graphs,” *IEEE Wireless Communications*, vol. 11, no. 1, pp. 26-36, 2004.

[9] Amendment 2: Fast BSS Transition, IEEE Std. P802.11r, 2008.

[10] X. Chen and D. Qiao, “HaND : Fast Handoff with Null Dwell Time for IEEE 802.11 Networks,” *ACM INFOCOM Computer Communications*, pp. 1–9, 2010.

[11] Y. Yan, J. Cao, C. Liu, S. Kim, and W. Wu, “A Dual Re-authentication Scheme for Fast Handoff in IEEE 802.11 Wireless Mesh Networks,” *IEEE Wireless Communications and Networking Conference (WCNC2009)*, pp. 1-5, 2009.

[12] Y. Kim,W. Ren, J. Jo, M. Yang, Y. Jiang, and J. Zheng, “SFRIC: a secure fast roaming scheme in wireless LAN using ID-based cryptography,” *IEEE International Conference on Communications (ICC)*, pp. 1570-1575, 2007.

[13] J. Choi and S. Jung, “A handover authentication using credentials based on chameleon hashing,” *IEEE communications letters*, vol. 14, pp. 54–56, 2010.

[14] S. Kim, S. Park, D. Won, “Proxy signatures, revisited,” *International Conference on Information and Communication Security (ICICS1997)*, Lecture Notes in Computer Science, Springer, pp. 223-232, 1997.

[15] B. Lee, H. Kim, K. Kim, “Strong Proxy Signature and its Applications,” *The 2001 Symposium on Cryptography and Information Security (SCIS2001)*, pp. 603-608, 2001.

[16] B. Libert, J.J. Quisquater, “Efficient Signcryption with Key Privacy from Gap Diffie-Hellman Groups,” *Public Key Cryptography (PKC2004)*, Lecture Notes in Computer Science, Springer, pp. 187-200, 2004.

[17] Shamus Software Ltd - MIRACL, accessed in February, 2007

http://www.shamus.ie/index.php?page=Benchmarks

Changsha Ma received the Bachelor degree of Information Engineering from Southeast University, China, in 2010. Now she is a Postgraduate Student majoring in Information Security in University of Science and Technology of China (USTC). Her research interest is Network Security.

Kaiping Xue received the Ph.D. degree of Communication and Information Systems from University of Science and Technology of China (USTC) in 2007. Now he works as a Lecturer at Department of Infosec and EEIS of USTC. His research interests include Distributed Network and Network Security.

Peilin Hong is a Professor in the Department of EEIS, University of Science and Technology of China (USTC). Her research interests include Next Generation Internet, Policy Control, IP QoS and Information Security. She has published 2 books and over 100 academic papers in journals and conference proceedings.