A novel ID-based multi-domain handover protocol for mesh points in WMNs

Xue Zhang, Guangsong Li, Wenbao Han and Huifang Ji
State Key Laboratory of Mathematical Engineering and Advanced Computing, Information Engineering University
Zhengzhou, 450002, P.R. China
[email: whity_zhang@163.com]
*Corresponding author: Xue Zhang

Received December 13, 2014; revised March 17, 2015; revised May 9, 2015; accepted June 8, 2015; published July 31, 2015

Abstract

Wireless mesh networks (WMNs) provide an efficient and flexible method to the field of wireless networking, but also bring many security issues. A mesh point may lose all of its available links during its movement. Thus, the mesh point needs to handover to a new mesh point in order to obtain access to the network again. For multi-domain WMNs, we proposed a new ID-based signcryption scheme and accordingly present a novel ID-based handover protocol for mesh points. The mutual authentication and key establishment of two mesh points which belong to different trust domains can be achieved by using a single one-round message exchange during the authentication phase. The authentication server is not involved in our handover authentication protocol so that mutual authentication can be completed directly by the mesh points. Meanwhile, the data transmitted between the two mesh points can be carried by the authentication messages. Moreover, there are no restrictions on the PKG system parameters in our proposed multi-domain ID-based signcryption scheme so our handover scheme can be easily applied to real WMNs circumstances. Security of the signcryption scheme is proved in the random oracle model. It shows that our protocol satisfies the basic security requirements and is resistant to existing attacks based on the security of the signcryption. The analysis of the performance demonstrates that the protocol is efficient and suitable for the multi-domain WMNs environment.

Keywords: wireless mesh networks, handover, ID-based, multi-domain, signcryption

This research is supported by the National Natural Science Foundation of China (Grant No.61201220).

http://dx.doi.org/10.3837/tiis.2015.07.10 **ISSN : 1976-7277**

1. Introduction

Wireless mesh networks (WMNs) [1] use a new crucial technology for wireless network structure, with many features including multi-hops, self-organization, low installation costs, large-scale deployment and fault-tolerance. Mesh nodes consist of mesh clients (MCs) and mesh points (MPs). The MCs are often laptops, cell phones and other wireless devices. The MPs form a wireless mesh backbone to provide network access from one mesh node to another or to the Internet. A subset of mesh points work as mesh access points (MAPs) to connect mesh clients to the WMNs. Due to the features of distributed architecture, multi-hop wireless backbone and dynamic network topology, the WMNs provide an efficient and flexible networking method, but also bring great security challenges.

The IEEE 802.11s [2] defines the security of WMNs that are still using the IEEE 802.11i [3] standards with IEEE 802.11x [4] and 4-way handshake protocols. Current research of WMNs is based on a shared key scheme or a public key system. The shared key scheme relies heavily on key management, and the conventional public key infrastructure (PKI) has a requirement for large storage and management of the public key certifications. The IEEE 802.11s presents a new security structure MSA (Mesh Security Association) [5], however, its key framework is quite complicated. Numerous security schemes for WMNs using identity-based (ID-based) cryptography have been proposed over the years. The concept of ID-based cryptography (IBC) [6] was first introduced by Shamir in 1984. The basic idea of ID-based cryptosystem is that the entity's public key is directly derived from its publicly known identity information such as an email address, an IP address, a telephone number or any other string of characters. The private key is issued by a trusted authority called the Private Key Generator (PKG). IBC completely eliminates the need for public-key distribution realized by conventional public-key certificates.

WMNs usually consist of several cooperating sub-networks called mesh trust domains. Establishing trust relationships between multi-domains is necessary and important in roaming scenarios. Most of the existing ID-based authentication protocols are based on the assumption that there exists only one single PKG. They consider the situation in which all the users belong to the same network. However, next generation wireless network is expected to establish a hybrid heterogeneous network with several types of wireless access technologies. In the circumstance of ubiquitous wireless network, there exists multiple independent and autonomous trust domains. It is unreasonable to assume that different trust domains use a single PKG. Different trust domains may be maintained by different PKGs in the real networks. Therefore, another kind of security handover scheme is needed for WMNs, namely an ID-based multi-domain security scheme with different PKGs.

A MP may lose all available current links when it moves away. Thus, it should be handed over to another MP in order to obtain access to the network again. Mutual authentication and key agreement are important for supporting the MPs' secure and fast roaming ability across different trust domains. We propose an ID-based multi-domain WMNs security structure. We will present a novel multi-domain handover protocol based on the ID-based multi-domain security structure. The scheme is quite suitable for real WMNs circumstances because the system parameters of the PKGs can be totally different. Multi-hops wireless communication between the Authentication Server (AS) and MPs would result in high latency, low stability and potential service interruption. In our protocol, the AS is not involved during the handover authentication process. Thus, the protocol is well suitable for self-organized WMNs. By using

the multi-domain ID-based signcryption technique we proposed, two MPs which belong to different trust domains will be able to achieve both a mutual authentication and an authenticated key establishment in a single one-round message exchange during the authentication phase. Furthermore, the transmitted data of both sides can be carried by the authentication messages.

2. Related Work

IEEE 802.11i defines a complete mutual authentication mechanism based on the EAP (Extensible authentication protocol) and IEEE 802.1x. However we believe it is not suitable for WMNs due to its centralized operations and multi-hops communication between the authentication server and the access points. The mutual re-authentication process still needs the AS to participate in executing the total IEEE 802.11i authentication procedures for any handover to occur. The IEEE 802.11s inherits the security architecture from IEEE 802.11i, so it will also suffer the above-mentioned drawbacks.

The shared key scheme has a key management burden, and the conventional public key infrastructure (PKI) has a large overhead storage requirement and has to deal with the management of the public key certifications. Shamir first presented the concept of ID-based cryptography in 1984. Several ID-based signature schemes have been proposed since then. It was not until 2001 that a satisfying ID-based encryption scheme was devised by Boneh and Franklin [7] using bilinear maps (the Wail or Tate pairing) over supersingular elliptic curves.

Confidentiality, integrity, non-repudiation and authentication are the important security attributes for many cryptographic applications. The traditional approach to achieve these security attributes is “sign-then-encrypt”. A new standard for data protection called signcryption [8] was proposed by Zheng in 1997. Signcryption simultaneously fulfills both the functions of digital signature and public key encryption in a single logical step, and with a cost significantly lower than that required by "signature followed by encyption". Signcryption plays an important part in the application environments which demand to complete both encryption and signature. A signcryption scheme is deemed to be secure if it possesses confidentiality, unforgeability and non-repudiation. Malone-Lee [9] first presented ID-based signcryption by using bilinear pairing. Li [10] presents ID-based multi-PKG signcryption schemes which can achieve multi-domain signcryption. But these schemes require an assumption that different domains own different master private keys but still share the same pairing parameters.

Caimu Tang et al. [11] presented a mobile authentication scheme for wireless networks. In his protocol, a MC is registered to its home network and can be authenticated by visiting a network through a delegation passcode. However, the communication between the HLR (home location register) and the VLR (visited location register) will lead to high latency and low stability. Li et al. [12] proposed a ticket-based authentication protocol to support a faster handover in wireless local area networks. The authentication server pre-distributes the tickets to clients, one for each neighbor AP of the current AP. The client will deliver the corresponding ticket to the target AP for mutual authentication when it moves to the target AP. The protocol does not apply any public-key cryptography in order to minimize the re-authentication latency. But their schemes may not be suitable for all WMNs circumstances, for risk and cost caused by the multi-hop communication should be considered. Celia Li et al. [13, 14] proposed a mesh handover scheme, in which the AS is not required. But the major problem of the protocol for handover authentication is that all the neighbours of the current

MAP share the same keys for handover authentication. For this reason, the client can not verify the AP's identity because any AP that owns the authentication keys can impersonate the target AP. Li et al. [15] achieved roaming authentication without any home AS's participation, which can not be applied in the environment of multi-domain wireless networks.

Zhu et al. [16] presented a more secure scheme for multi-domain wireless mesh networks combing PKI and IBC techniques. The MC which belongs to trust domain B can be authenticated by the target network of trust domain A. However, trusted authorities of both sides need to be involved during the authentication process, and the trust relationship between home domain and visited domain should be negotiated through PKI. He et al. [17] accomplished the authentication between mesh nodes belongs to different trust domains, but the home AS still needs to be involved, and system time synchronization is required. The interaction between home domain and visited domain causes high latency and low efficiency. A non-repudiable authentication scheme for wireless mesh networks was proposed in paper [18]. Although inter-domain authentication in the scheme is actualized by an ID-based signature, the author assumes that different domains share the same PKG system parameters. Gao et al. [19] applied ID-based proxy signature to multi-domain authentication protocols for WMNs. Authentication and key agreement depend on a trust relationship between the broker and the domain. Besides that, delegating the signing rights from the original signer to a proxy signer would result in more security risks. And proxy signature mechanism is sure to increase system complexity. As discussed above, the ID-based multi-domain authentication schemes, except Zhu's, are based upon the assumption that: all the different domains share the same pairing parameters. The assumption limits the application scalabilities of these schemes. It is infeasible to satisfy the above assumption for real networks especially heterogeneous networks.

We are proposing a novel ID-based multi-domain handover protocol for mesh points in WMNs in which there are no restrictions on the PKG system parameters. As a result different domains may have totally different PKG system parameters including public system parameters, master keys and system public keys.

3. ID-based multi-domain handover protocol for mesh points in WMNs

Preliminaries

(1) Bilinear pairings: Let G_1 be an additive group and G_2 be a multiplicative group of the prime order q. Let P be an arbitrary generator of G_1. The pairing $e: G_1 \times G_1 \to G_2$ is called an admissible bilinear map if it has the following properties:

1) Bilinear: For $\forall P, Q \in G_1$ and $a, b \in Z_q^*$, $e(aP, bQ) = e(P, Q)^{ab}$.

2) Non-degenerate: $\forall P, Q \in G_1$, $e(aP, bQ) \neq 1_{G_2}$, for 1_{G_2} is an arbitrary generator of G_2.

3) Computable: For $\forall P, Q \in G_1$, there exists an efficient algorithm to compute $e(P, Q)$.

(2) Decisional Bilinear Diffie-Hellman Problem (DBDHP): Given (P, aP, bP, cP), for some $a, b, c \in Z_q^*$ and an element $\theta \in G_2$, decide whether $\theta = e(P, Q)^{abc}$.

3.1 ID-based multi-domain security structure of WMNs

The network model we considered in this paper is portrayed in **Fig. 1**. There are multiple independent and autonomous trust domains in the WMNs. Each domain has its own PKG which generates and distributes the private keys for the nodes in the domain. The PKGs are

supposed to be trusted. In order to make our scheme applicable in real WMNs circumstances, we have allowed each PKG to use totally different system parameters, including different public parameters $<G_1, G_2, e, P, H_1, H_2, H_3>$, system master key s and system public key $Pub = sP$. For each node in the domain, the public key is its identity information, and the private key is generated by PKG using its identity information.

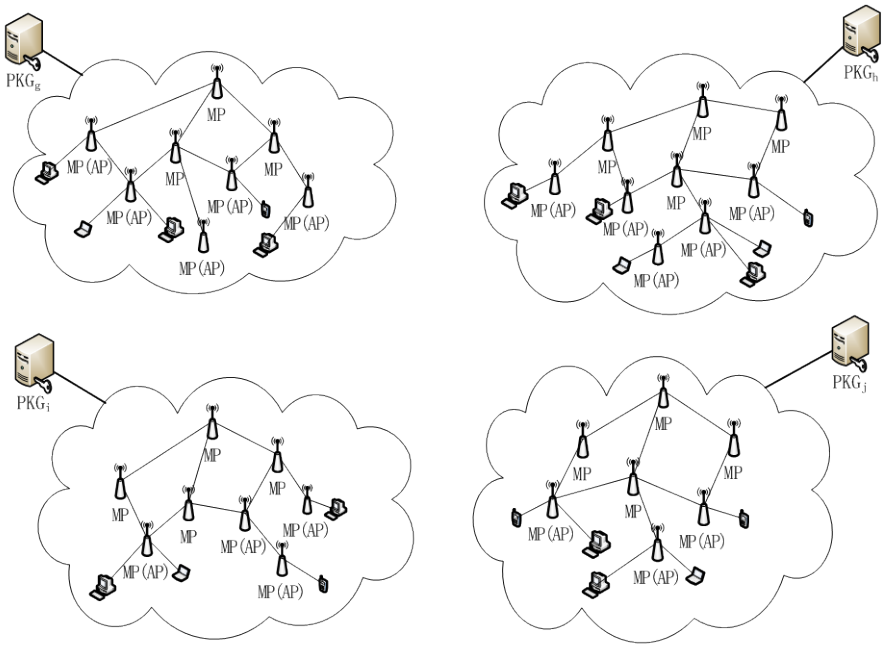

Fig. 1. ID-based multi-domain security structure of WMNs

A MP may lose all currently available links during its movement. Thus, the MP must handover to another MP in order to obtain access to the network again. **Fig. 2** shows the ID-based multi-domain handover for MPs in WMNs. We take the networks U and V for instance.

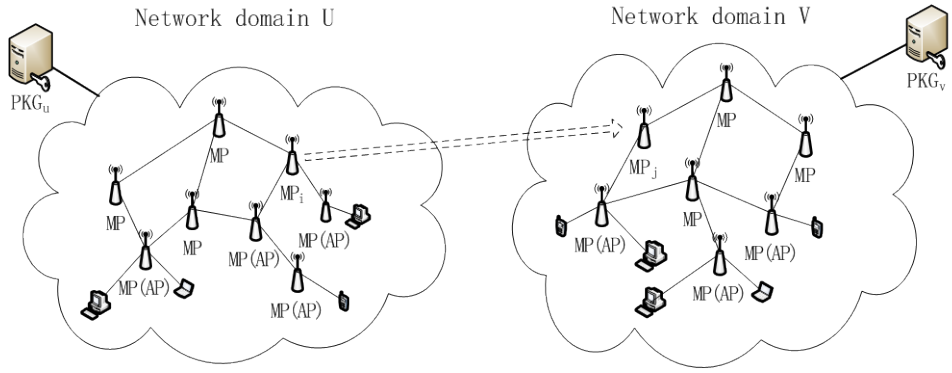

Fig. 2. ID-based multi-domain handover for mesh points in WMNs

3.2 ID-based multi-domain signcryption protocol

The encrypted random numbers used as challenges will enhance the security during the handover protocol. However, a simple signature scheme cannot implement random numbers encryption. Both signature and encryption should be considered in the scheme. Signcryption simultaneously fulfills both signature and public key encryption in a single logical step with a cost significantly lower than that required by "signature followed by encyption". Therefore, we have proposed a novel ID-based multi-domain signcryption scheme which can be used to achieve secure handovers for MPs in WMNs in the future. There are no restrictions on PKG system parameters so they can be totally different in the different trust domains. Let us describe the signcryption scheme before representing the handover protocol. The scenario studied in this section is pictured in **Fig. 2**.

Setup:

The system parameters for network domain U are generated as follows. Define G_1^U be an additive group and G_2^U be a multiplicative group of the prime order q_U. P_U is an arbitrary generator of G_1^U. The pairing $e_U : G_1^U \times G_1^U \to G_2^U$ is a bilinear map. Let H_1^U, H_2^U and H_3^U be three cryptography hash functions where $H_1^U : \{0,1\}^* \to G_1^U$, $H_2^U : G_2^U \to \{0,1\}^*$, $H_3^U : \{0,1\}^* \times G_1^U \to Z_{q_U}^*$. The PKG_U chooses a master private key $s_U \in Z_{q_U}^*$ randomly and computes a corresponding system public key $Pub_U = s_U P_U$. The PKG_U publishes Pub_U and keeps the master private key s_U secret. The public system parameters of PKG_U are $< G_1^U, G_2^U, q_U, P_U, Pub_U, e_U, H_1^U, H_2^U, H_3^U >$.

The similar process is implemented for network domain V. Define G_1^V be an additive group and G_2^V be a multiplicative group of the prime order q_V. P_V is an arbitrary generator of G_1^V. The pairing $e_V : G_1^V \times G_1^V \to G_2^V$ is a bilinear map. Let H_1^V, H_2^V and H_3^V be three cryptography hash functions where $H_1^V : \{0,1\}^* \to G_1^V$, $H_2^V : G_2^V \to \{0,1\}^*$, $H_3^V : \{0,1\}^* \times G_1^V \to Z_{q_V}^*$. The PKG_V chooses a master private key $s_V \in Z_{q_V}^*$ randomly and computes a corresponding system public key $Pub_V = s_V P_V$. The PKG_V publishes Pub_V and keeps the master private key s_V secret. The public system parameters of PKG_V are $< G_1^V, G_2^V, q_V, P_V, Pub_V, e_V, H_1^V, H_2^V, H_3^V >$.

Extract:

Suppose Alice that registers with PKG_U and gets its private key $S_{Alice} = s_U Q_{Alice}$, where $Q_{Alice} = H_1^U(ID_{Alice})$, $ID_{Alice} \in \{0,1\}^*$.

Suppose Bob that registers with PKG_V and gets its private key $S_{Bob} = s_V Q_{Bob}$, where $Q_{Bob} = H_1^V(ID_{Bob})$, $ID_{Bob} \in \{0,1\}^*$.

Signcrypt:

To send a message m to Bob,

Alice operates as follows.

1. Choose random numbers $a_1 \in Z_{q_U}^*$, $a_2 \in Z_{q_V}^*$ and compute $TA_1 = a_1 P_U$, $TA_2 = a_2 P_V$.
2. Compute $w = e_V(a_2 Pub_V, Q_{Bob})$.
3. Compute $c = H_2^V(w) \oplus m$. (The plaintext m is encrypted by Bob's public key Q_{Bob}.)

4. Compute $h = H_3^U(c, TA_1)$.
5. Compute $\sigma = a_1 Pub_U + hS_{Alice}$. (The ciphertext c is signatured by Alice using its private key S_{Alice}.)

The $Signcrypt_{Alice,Bob}(m)$ is $\{c, TA_1, TA_2, \sigma\}$.

Unsigncrypt:

When receiving $Signcrypt_{Alice,Bob}(m)$, Bob operates as follows.

1. Compute $e_U(P_U, \sigma) = e_U(TA_1, Pub_U) e_U(Pub_U, Q_{Alice})^{H_3^U(c, TA_1)}$. (Bob checks Alice's signature using Alice's public key Q_{Alice} to make sure that the message is from Alice indeed.) Bob accepts the ciphertext c if and only if the above equation holds.
2. Compute $w^* = e_V(TA_2, S_{Bob})$.
3. Recover $m = H_2^V(w^*) \oplus c$. (The plaintext m is recovered from the ciphertext c by Bob's private key S_{Bob}. Thus no one but Bob is able to obtain m.)

The correctness can be easily verified by the following equations.

$$e_U(P_U, \sigma) = e_U(P_U, a_1 Pub_U + hS_{Alice}) = e_U(P_U, a_1 Pub_U) e_U(P_U, hS_{Alice})$$
$$= e_U(a_1 P_U, Pub_U) e_U(P_U, S_{Alice})^h = e_U(a_1 P_U, Pub_U) e_U(P_U, s_U Q_{Alice})^h \quad ,$$
$$= e_U(TA_1, Pub_U) e_U(s_U P_U, Q_{Alice})^h = e_U(TA_1, Pub_U) e_U(Pub_U, Q_{Alice})^{H_3^U(c, TA_1)}$$
$$w^* = e_V(TA_2, S_{Bob}) = e_V(a_2 P_V, s_V Q_{Bob}) = e_V(a_2 s_V P_V, Q_{Bob}) = e_V(a_2 Pub_V, Q_{Bob}) = w.$$

A brief security analysis is described as follows. Our signcryption scheme possesses confidentiality, unforgeability and non-repudiation. More details see in Section 4.1.

confidentiality

It is computationally infeasible for an attacker who may be anyone other than Alice and Bob to obtain any partial information on the contents of a signcrypted text. No one except Bob can achieve m from $\{c, TA_1, TA_2, \sigma\}$, because only Bob owns S_{Bob} to calculate the decryption key $w^* = e_V(TA_2, S_{Bob})$.

unforgeability

It is computationally infeasible for an attacker to impersonate Alice in creating a signcrypted text. An attacker can obtain Pub_U and h, but cannot get a_1 nor S_{Alice}. For $\sigma = a_1 Pub_U + hS_{Alice}$, no one can forge a Alice's signature.

non-repudiation

It is computationally infeasible for anyone to deny the fact that they are the originator of a signcrypted text. Once Bob verifies Alice's signature, Alice cannot repudiate the signature because nobody is able to forge her signature.

3.3 ID-based multi-domain handover protocol

We propose an ID-based multi-domain handover protocol for mesh points in WMNs based upon the signcryption scheme in 3.2. A MP loses all links with other MPs in its home domain U if it roams to visited domain V. It should handover to one MP in domain V to acquire network service. Thus a fast and secure handover authentication process is needed to avoid a great deal of data loss. The detailed procedure of the protocol is described in **Fig. 3**.

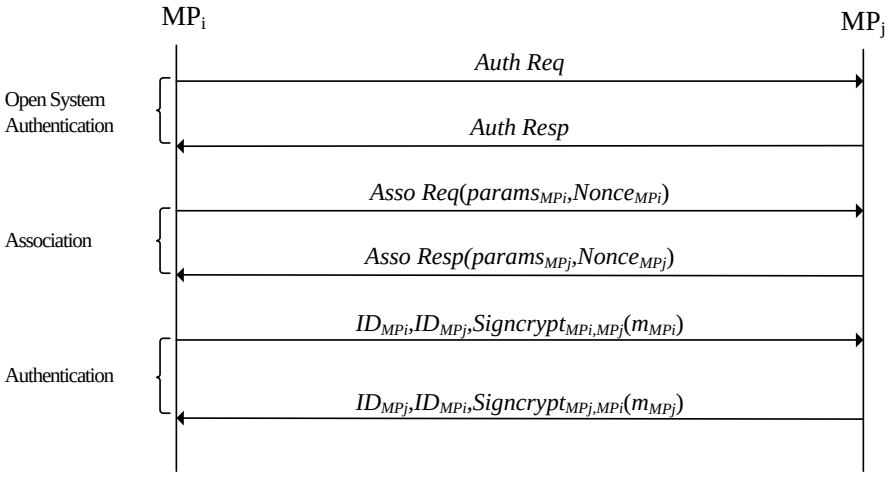

Fig. 3. Procedures for the ID-based multi-domain handover protocol for the mesh points in WMNs

When MP_i moves to the visited network V, it can obtain the identifiers, frequencies and link qualities of its surrounding mesh access points. According to some decision algorithms, MP_i chooses only one mesh access point. Let us take the access point MP_j for example. The detailed description of cross-domain handover authentication protocol is as follows.

In the open system authentication phase, MP_i sends an association requirement message to MP_j. MP_j then replies to MP_i's requirement with an association response message indicating acceptance or rejection. MP_i and MP_j generate random numbers $Nonce_{MP_i}$ and $Nonce_{MP_j}$ respectively. The random numbers are used as challenges for authentication. Then MP_i and MP_j exchange the random numbers and their respective public system parameters of PKGs: $< G_1^U, G_2^U, q_U, P_U, Pub_U, e_U, H_1^U, H_2^U, H_3^U >$ and $< G_1^V, G_2^V, q_V, P_V, Pub_V, e_V, H_1^V, H_2^V, H_3^V >$.

In the authentication phase, the procedure is described below.

1. $MP_i \rightarrow MP_j : \{ID_{MP_i}, ID_{MP_j}, Signcrypt_{MP_i,MP_j}(m_{MP_i})\}$.

MP_i signcrypts m_1 and $Nonce_{MP_j}$ with its own private key S_{MP_i} and MP_j's public key Q_{MP_j}. m_1 is a plaintext to be transferred from MP_i to MP_j, and its value is null if there is no message to be delivered.

(1) Choose $a_1 \in Z_{q_U}^*$, $a_2 \in Z_{q_V}^*$ randomly and compute $TA_1 = a_1 P_U$, $TA_2 = a_2 P_V$.

(2) Compute $w_{MP_i} = e_V(a_2 Pub_V, Q_{MP_j})$.

(3) Compute the ciphertext $c_{MP_i} = H_2^V(w_{MP_i}) \oplus m_{MP_i}$, where $m_{MP_i} = m_1 \| Nonce_{MP_j}$. ($MP_i$ encyptes the m_{MP_i} by using MP_j's public key Q_{MP_j}, thus only MP_j is able to decypt the ciphertext c_{MP_i}.)

(4) Compute $h_{MP_i} = H_3^U(c_{MP_i}, TA_1)$.

(5) Compute the signature $\sigma_{MP_i} = a_1 Pub_U + h_{MP_i} S_{MP_i}$. (The ciphertext c_{MP_i} is signed by MP_i using its private key S_{MP_i}.)

Then MP_i sends to MP_j the message: $\{ID_{MP_i}, ID_{MP_j}, Signcrypt_{MP_i,MP_j}(m_{MP_i})\}$, where $Signcrypt_{MP_i,MP_j}(m_{MP_i}) = \{c_{MP_i}, TA_1, TA_2, \sigma_{MP_i}\}$.

2. When receiving the message: $\{ID_{MP_i}, ID_{MP_j}, Signcrypt_{MP_i,MP_j}(m_{MP_i})\}$ from MP_i, MP_j follows these steps;

(1) Validate ID_{MP_i} and ID_{MP_j} to confirm the identity of each other.

(2) Compute $e_U(P_U, \sigma_{MP_i}) = e_U(TA_1, Pub_U) e_U(Pub_U, Q_{MP_i})^{H_3^U(c_{MP_i}, TA_1)}$. Accept the message c_{MP_i} if and only if the equation holds. (MP_j checks MP_i's signature using MP_i's public key Q_{MP_i} to make sure that the message is indeed from MP_i.)

Step (2) is using MP_i's public key Q_{MP_i} to confirm MP_i's signature of the message in order to authenticate the identity of MP_i.

(3) Compute $w_{MP_i}{}^* = e_V(TA_2, S_{MP_j})$.

(4) Recover $m_{MP_i} = H_2^V(w_{MP_i}{}^*) \oplus c_{MP_i}$. (The plaintext m_{MP_i} is recovered from the ciphertext c_{MP_i} by MP_j's private key S_{MP_j}. Thus no one but MP_j is able to obtain m_{MP_i}.)

Step (3) (4) is using MP_j's private key S_{MP_j} to recover the message m_{MP_i}, $m_{MP_i} = m_1 \| Nonce_{MP_j}$. MP_j then gets data m_1 and random number $Nonce_{MP_j}$.

(5) Confirm the challenge number $Nonce_{MP_j}$.(MP_j decides whether $Nonce_{MP_j}$ is the challenge number it sent to MP_i. This step is to resist replay attacks.)

At this point the identity of MP_i is confirmed by MP_j. Meanwhile, the data m_1 is successfully received by MP_j.

3. MP_j ® MP_i : $\{ID_{MP_j}, ID_{MP_i}, Signcrypt_{MP_j,MP_i}(m_{MP_j})\}$.

MP_j signcrypts m_2 and $Nonce_{MP_i}$ with its own private key S_{MP_j} and MP_i's public key Q_{MP_i}. m_2 is a plaintext to be transferred from MP_j to MP_i, and its value is null if there is no message to be delivered.

(1) Choose $b_1 \in Z_{q_V}^*$, $b_2 \in Z_{q_U}^*$ randomly and compute $TB_1 = b_1 P_V$, $TB_2 = b_2 P_U$.

(2) Compute $w_{MP_j} = e_U(b_2 Pub_U, Q_{MP_i})$.

(3) Compute the ciphertext $c_{MP_j} = H_2^U(w_{MP_j}) \oplus m_{MP_j}$, where $m_{MP_j} = m_2 \| Nonce_{MP_i}$. ($MP_j$ encyptes the m_{MP_j} by using MP_i's public key Q_{MP_i}, thus only MP_i is able to decrypt the ciphertext c_{MP_j}.)

(4) Compute $h_{MP_j} = H_3^V(c_{MP_j}, TB_1)$.

(5) Compute the signature $\sigma_{MP_j} = b_1 Pub_V + h_{MP_j} S_{MP_j}$. (The ciphertext c_{MP_j} is signed by MP_j using its private key S_{MP_j}.)

Then MP_j sends to MP_i the message: $\{ID_{MP_j}, ID_{MP_i}, Signcrypt_{MP_j,MP_i}(m_{MP_j})\}$, where $Signcrypt_{MP_j,MP_i}(m_{MP_j}) = \{c_{MP_j}, TB_1, TB_2, \sigma_{MP_j}\}$.

In addition, MP_j is able to calculate the session key between MP_i and MP_j. MP_j

computes $K_{MP_j,MP_i} = e_V(S_{MP_j}, TA_2)e_U(Q_{MP_i}, b_2 Pub_U)$, $K_1^{MP_j} = b_2 TA_1$, $K_2^{MP_j} = b_1 TA_2$, and then gets the session key $sk_{MP_j,MP_i} = H(K_{MP_j,MP_i}, K_1^{MP_j}, K_2^{MP_j}, TA_1, TA_2, TB_1, TB_2, ID_{MP_i}, ID_{MP_j})$, where $H: \{0,1\}^* \to \{0,1\}^k$, k is the length of the session key.

4. When receiving the message: $\{ID_{MP_j}, ID_{MP_i}, Signcrypt_{MP_j,MP_i}(m_{MP_j})\}$ from MP_j, MP_i follows these steps;

(1) Validate ID_{MP_j} and ID_{MP_i} to confirm the identity of each other.

(2) Compute $e_V(P_V, \sigma_{MP_j}) = e_V(TB_1, Pub_V)e_V(Pub_V, Q_{MP_j})^{H_3^V(c_{MP_j}, TB_1)}$. Accept the ciphertext c_{MP_j} if and only if the equation holds. (MP_i checks MP_j's signature using MP_j's public key Q_{MP_j} to make sure that the message is indeed from MP_j.)

Step (2) is using MP_j's public key Q_{MP_j} to confirm MP_j's signature of the message in order to authenticate the identity of MP_j.

(3) Compute $w_{MP_j}{}^* = e_U(TB_2, S_{MP_i})$.

(4) Recover $m_{MP_j} = H_2^U(w_{MP_j}{}^*) \oplus c_{MP_j}$. (The plaintext m_{MP_j} is recovered from the ciphertext c_{MP_j} by MP_i's private key S_{MP_i}. Thus no one but MP_i is able to obtain m_{MP_j}.)

Step (3) (4) is using MP_i's private key S_{MP_i} to recover the message m_{MP_j}, $m_{MP_j} = m_2 \| Nonce_{MP_i}$. MP_i then gets data m_2 and random number $Nonce_{MP_i}$.

(5) Confirm the challenge number $Nonce_{MP_i}$. (MP_i decides whether $Nonce_{MP_i}$ is the challenge number it sent to MP_j. The step is to resist replay attacks.)

At this point the identity of MP_j is confirmed by MP_i. Meanwhile, the data m_2 is successfully received by MP_i.

MP_i is able to calculate the session key between MP_i and MP_j. MP_i computes $K_{MP_i,MP_j} = e_U(S_{MP_i}, TB_2)e_V(Q_{MP_j}, a_2 Pub_V)$, $K_1^{MP_i} = a_1 TB_2$, $K_2^{MP_i} = a_2 TB_1$, and then gets the session key $sk_{MP_i,MP_j} = H(K_{MP_i,MP_j}, K_1^{MP_i}, K_2^{MP_i}, TA_1, TA_2, TB_1, TB_2, ID_{MP_i}, ID_{MP_j})$, where $H: \{0,1\}^* \to \{0,1\}^k$, k is the length of the session key.

To this, mutual authentication between MP_i and MP_j is completed.

The correctness of the session key can be easily verified. It is easy to verify $K_{MP_i,MP_j} = K_{MP_j,MP_i}$, $K_1^{MP_i} = K_1^{MP_j}$ and $K_2^{MP_i} = K_2^{MP_j}$ by the following equations.

$$K_{MP_i,MP_j} = e_U(S_{MP_i}, TB_2)e_V(Q_{MP_j}, a_2 Pub_V) = e_U(s_U Q_{MP_i}, b_2 P_U)e_V(Q_{MP_j}, a_2 s_V P_V)$$
$$= e_U(Q_{MP_i}, P_U)^{s_U b_2} e_V(Q_{MP_j}, P_V)^{a_2 s_V},$$

$$K_{MP_j,MP_i} = e_V(S_{MP_j}, TA_2)e_U(Q_{MP_i}, b_2 Pub_U) = e_V(s_V Q_{MP_j}, a_2 P_V)e_U(Q_{MP_i}, b_2 s_U P_U)$$
$$= e_V(Q_{MP_j}, P_V)^{s_V a_2} e_U(Q_{MP_i}, P_U)^{b_2 s_U},$$

$$K_1^{MP_i} = K_1^{MP_j} = a_1 b_2 P_U,$$

$$K_2^{MP_i} = K_2^{MP_j} = a_2 b_1 P_V.$$

For $sk_{MP_i,MP_j} = sk_{MP_j,MP_i}$, MP_i and MP_j share the same session key.

4. Security analysis

4.1 Security analysis of the ID-based multi-domain signcryption protocol

First of all, the security definitions for multi-domain ID-based signcryption scheme (MPIDSC) are described in [10].

Definition 1 (Confidentiality). A multi-PKG ID-based signcryption scheme is said to have indistinguishability against adaptive chosen ciphertext attacks (IND-MPIDSC-CCA2) if no polynomially bounded adversary has a non-negligible advantage in the game. (More details about the game are given in definition3 of [10]).

Definition 2 (Unforgeability). A multi-PKG ID-based signcryption scheme is said to have existential unforgeability against adaptive chosen message attacks (EUF-MPIDSC-CMA) if no polynomially bounded adversary has a non-negligible advantage in the game. (More details about the game are given in definition4 of [10]).

Similarly, we can prove that our scheme is both IND-MPIDSC-CCA2 and EUF-MPIDSC-CMA secure.

Theorem 1 (Confidentiality). In the random oracle model, we assume we have an IND-MPIDSC-CCA2 adversary called A that is able to distinguish ciphertext during the game of Definition 1 with an advantage ε when running in a time t and asking at most $q_{H_i^j}$ times H_i^j ($i=1,2,3$, $j=U,V$) queries, at most q_S times signcryption queries and q_U times unsigncryption queries. And there exists a distinguisher X that can solve the DBDH problem in a time $t'=t+(q_S+4q_U)t_e$ with an advantage $\varepsilon\frac{1}{q_{H_1^V}q_{H_2^V}}$, where t_e denotes the computation time of the bilinear map.

Proof. We assume that the distinguisher X receives a random instance $(P_V, aP_V, bP_V, cP_V, h)$ of the DBDH problem to decide whether $h=e_V(P_V,P_V)^{abc}$ is true or not. X will run A as a subroutine and act as A's challenger in the IND-MPIDSC-CCA2 game. A will consult X for answers to queries of random oracles H_i^j ($i=1,2,3$, $j=U,V$), signcryption and unsigncryption. Correspondingly, X maintains 10 lists to store the answers. The lists are L_i^j （ $i=1,2,3$, $j=U,V$ ） , L_S^U , L_S^V , L_{Un}^U , L_{Un}^V respectively.

At the beginning of the game, X gives A the system parameters with $Pub_V=cP_V$ and $Pub_U=dP_U$, where c and d respectively simulate the master key for PKG_V and PKG_U. c and d are not known to X.

H_1^V queries: X chooses a random number $l\in\{1,2,...,q_{H_1^V}\}$. At the u-th H_1^V query, if $u=l$, then X answers $H_1^V(ID_u)=bP_V$; if $u\neq l$, X chooses a random number $x\in Z_{q_V}^*$, answers $H_1^V(ID_u)=xP_V$ and then puts (ID_u,x) in the list L_1^V .

H_1^U queries: X chooses a random number $x\in Z_{q_U}^*$, answers $H_1^U(ID_u)=xP_U$ and then puts (ID_u,x) in the list L_1^U .

H_2^U / H_2^V queries: When A asks the queries, X will check the list L_2^U / L_2^V . If the corresponding hash value exists, the hash value will be returned to A; otherwise, a random value $h_2\in(0,1)^*$ will be chosen by X, and X then stores the query and answer in the list.

H_3^U / H_3^V queries: When A asks the queries, X will check the list L_3^U / L_3^V. If the corresponding hash value exists, the hash value will be returned to A; otherwise, a random value h_3 will be chosen by X, and X then stores the query and answer in the list.

$Extract_V$ queries: If $ID_u = ID_l$, then X fails. Otherwise, X finds entry (ID_u, x) from list L_1^V, computes the private key corresponding to ID_u: $S_{ID_u} = cxP_V$, and returns to A.

$Extract_U$ queries: X finds entry (ID_u, x) from list L_1^U, computes the private key corresponding to ID_u: $S_{ID_u} = dxP_U$, and returns to A.

Singcrypt queries: Let ID_1 and ID_2 denote the sender and the receiver respectively and m is the plaintext. There are two cases to consider.

Case 1: $ID_1 \neq ID_l$. X can get the private key of ID_1: S_{ID_1}. X chooses random numbers $a_1 \in Z_{q_U}^*$ and $a_2 \in Z_{q_V}^*$ randomly and computes $TA_1 = a_1 P_U$, $TA_2 = a_2 P_V$. Then X calculates $w = e_V(a_2 Pub_V, Q_{ID_2})$, $c = m \oplus H_2^V(w)$, $h = H_3^U(c, TA_1)$, $\sigma = a_1 Pub_U + hS_{ID_1}$. X returns message: $\{c, TA_1, TA_2, \sigma\}$ to A.

Case 2: $ID_1 = ID_l$. X cannot get S_{ID_1}, but can obtain S_{ID_2}. X chooses random numbers $a_1, h \in Z_{q_U}^*$ and $a_2 \in Z_{q_V}^*$ randomly. Then X computes $TA_2 = a_2 P_V$, calculates $w = e_V(TA_2, S_{ID_2})$, and runs $c = m \oplus H_2^V(w)$. X computes $TA_1 = a_1 P_U - hQ_{ID_1}$ and $\sigma = a_1 Pub_U$. X returns $\{c, TA_1, TA_2, \sigma\}$ to A and puts it to list L_3^U.

Unsingcrypt queries: For an unsigncryption query on ciphertext $\{c, TA_1, TA_2, \sigma\}$, there are two cases to consider.

Case 1: $ID_2 \neq ID_l$. X checks if $e_U(P_U, \sigma) = e_U(TA_1, Pub_U) e_U(Pub_U, Q_{ID_1})^{H_3^U(c, TA_1)}$ holds. If the equation holds, X can get the private key of ID_2: S_{ID_2} to compute $w = e_V(TA_2, S_{ID_2})$, and retruns $m = c \oplus H_2^V(w)$ to A.

Case 2: $ID_2 = ID_l$. X always answers A that the ciphertext: $\{c, TA_1, TA_2, \sigma\}$ is invalid.

A can ask a polynomially bounded number of queries adaptively again as in the first stage. Then A will pick a challenged pair of identities : $\{ID_A, ID_B\}$ and output two messages: $\{m_0, m_1\}$. X chooses $v \in \{0,1\}$ and signcrypts m_v. Then X randomly chooses $\sigma^* \in G_1^U$, $TA_1^* \in G_1^U$, sets $TA_2^* = aP_V$, $\theta = w$ (θ is the candidate answer for the DBDH problem). Finally, X computes $c^* = H_2^V(w) \oplus m_v$ and returns to A.

A runs a second series of queries which are the same as the first stage. At the end of the simulation, A outputs $v' \in \{0,1\}$, if $v' = v$, X outputs $\theta = e_V(TA_2^*, S_{ID_l}) = e_V(aP_V, cQ_{ID_l}) = e_V(aP_V, cbP_V) = e_V(P_V, P_V)^{abc}$ as a solution of the DBDH problem, otherwise X fails.

The probability that A picks ID_l as challenged identity is at least $\frac{1}{q_{H_1^V}}$. The probability that A does not submit H_2^V query is at least $\frac{1}{q_{H_2^V}}$. Every signcryption query requires one pairing operation and every unsigncryption query requires three pairing operations. Thus X can solve

the DBDH problem in a time $t' = t + (q_S + 4q_U)t_e$ with an advantage $\varepsilon \frac{1}{q_{H_1^V} q_{H_2^V}}$.

Theorem 2 (Unforgeability). The scheme is EUF-MPIDSC-CMA secure.

Proof. If an attacker is able to forge a signature for our scheme, he must be able to forge a signature for the following scheme. The signature scheme is a variant of Hess's signature [20]. It has been proved that Hess's signature and its variants have unforgeability against adaptive chosen ciphertext attacks, therefore our scheme is EUF-MPIDSC-CMA secure.

Sign: To sign a message m, ID_1 follows these steps;

1. Choose random number $a_1 \in Z_{q_U}^*$ and compute $TA_1 = a_1 P_U$.
2. Compute $h = H_3^U(m, TA_1)$.
3. Compute $\sigma = a_1 Pub_U + hS_{ID_1}$.

The signature is $\{TA_1, \sigma\}$.

Verify: When receiving the signature: $\{TA_1, \sigma\}$, the verifier ID_2 accept the signature if and only if the equation holds. $e_U(P_U, \sigma) = e_U(TA_1, Pub_U) e_U(Q_{ID_2}, Pub_U)^{H_3^U(m, TA_1)}$.

4.2 Security analysis of ID-based multi-domain handover protocol

The security analysis of our proposed ID-based multi-domain signcryption is proved in section 4.1. Based on the security properities of the signcryption, the security of our handover protocol is discussed below.

1.Mutual authentication

Signcryption simultaneously fulfills both the functions of digital signature and public key encryption in a single logical step. MP_i signcrypts m_{MP_i} with its private key S_{MP_i} and MP_j's public key Q_{MP_j}, and then sends to MP_j the message: $\{ID_{MP_i}, ID_{MP_j}, Signcrypt_{MP_i, MP_j}(m_{MP_i})\}$. MP_j confirms MP_i's signature of the message using MP_i's public key Q_{MP_i}, the identity of MP_i is thus authenticated. In the same way, the identity of MP_j is authenticated by MP_i. Hence the mutual authentication is accomplished in a one-round signcryption message interaction between MP_i and MP_j during the authentication phase.

2. Key freshness

The session key sk is calculated from the hash function $H(K, K_1, K_2, TA_1, TA_2, TB_1, TB_2, ID_{MP_i}, ID_{MP_j})$, where $K = K_{MP_i, MP_j} = K_{MP_j, MP_i}$, $K_1 = K_1^{MP_i} = K_1^{MP_j}$, $K_2 = K_2^{MP_i} = K_2^{MP_j}$. K_1 and K_2 are derived from the random temporary keys a_1, a_2, b_1, b_2. The freshness of the random temporary keys ensures the freshness of the session key sk. Because the random temporary keys are generated by MP_i and MP_j respectively, neither of them can control the choice of the session key sk independently. Owing to mutual authentication between MP_i and MP_j, any attacker cannot impersonate MP_i and MP_j to generate a_1, a_2, b_1, b_2. Therefore, the sk is confidential and only MP_i and MP_j can know it. Each session key is fresh, random and independent.

3. Forward Secrecy

The random temporary keys are unpredictable for any party except MP_i and MP_j. Even if the intruder obtains secret information MP_i and MP, he cannot obtain the past temporary keys and the past session key.Therefore, the scheme has the property of perfect forward secrecy.

Furthermore, even if the PKGs are captured, the attacker can only get the long-term private keys of MP_i and MP_j but not the past temporary keys and the past session keys. Hence it also has the property of PKG perfect forward secrecy.

4. Known Key Security

Each run of authentication protocol chooses different random temporary keys to generate session keys as below.

$sk = H(K, K_1, K_2, TA_1, TA_2, TB_1, TB_2, ID_{MP_i}, ID_{MP_j})$, where $K = K_{MP_i,MP_j} = K_{MP_j,MP_i}$, $K_1 = K_1^{MP_i} = K_1^{MP_j}$, $K_2 = K_2^{MP_i} = K_2^{MP_j}$.

$$K_{MP_i,MP_j} = e_U(S_{MP_i}, TB_2)e_V(Q_{MP_j}, a_2 Pub_V) = e_U(s_U Q_{MP_i}, b_2 P_U)e_V(Q_{MP_j}, a_2 s_V P_V)$$
$$= e_U(Q_{MP_i}, P_U)^{s_U b_2} e_V(Q_{MP_j}, P_V)^{a_2 s_V} ,$$

$$K_{MP_j,MP_i} = e_V(S_{MP_j}, TA_2)e_U(Q_{MP_i}, b_2 Pub_U) = e_V(s_V Q_{MP_j}, a_2 P_V)e_U(Q_{MP_i}, b_2 s_U P_U)$$
$$= e_V(Q_{MP_j}, P_V)^{s_V a_2} e_U(Q_{MP_i}, P_U)^{b_2 s_U} ,$$

$K_1^{MP_i} = K_1^{MP_j} = a_1 b_2 P_U$,

$K_2^{MP_i} = K_2^{MP_j} = a_2 b_1 P_V$.

If the past session key is exposed, the intruder can get the past session key: $sk^* = H(K^*, K_1^*, K_2^*, TA_1^*, TA_2^*, TB_1^*, TB_2^*, ID_{MP_i}, ID_{MP_j})$, where

$K^* = K_{MP_i,MP_j}{}^* = K_{MP_j,MP_i}{}^* = e_U(Q_{MP_i}, P_U)^{s_U b_2^*} e_V(Q_{MP_j}, P_V)^{a_2^* s_V}$,

$K_1^{MP_i*} = K_1^{MP_j*} = a_1^* b_2^* P_U$, $K_2^{MP_i*} = K_2^{MP_j*} = a_2^* b_1^* P_V$.

$a_1^*, a_2^*, b_1^*, b_2^*$ is the past random temporary keys. The current session key is generated by fresh random temporary keys a_1, a_2, b_1, b_2 . The non-correlation of random numbers assures the intruder cannot obtain any current session key even if its past session key is exposed.

5. Resistance to Replay Attack

An intruder may record message flows and then retransmit them to trick the target MP for false authentication. In the association phase, MP_i and MP_j exchange the random numbers $Nonce_{MP_i}$ and $Nonce_{MP_j}$. During the procedure of authentication, both sides of MP_i and MP_j should check the challenge numbers. Thus, this replay attack can be prevented since $Nonce_{MP_i}$ and $Nonce_{MP_j}$ are fresh and unpredictability.

6. Resistance to Man-in-the-Middle Attack

This protocol is proposed based on the IBC and ID-based signcryption. The entity's public key is directly derived from the publicly known identity information in IBC and signcryption combines the functions of digital signature and public key encryption in a single step. The attacker can intercept the signcryption messages between MP_i and MP_j. But he can not obtain the real data in the signcryption messages because the data is encrypted by the private key of the receiver, and then the attacker could not be able to modify the data. The malicious middle-man cannot establish the secure association on behalf of the legitimate MP_i and MP_j.

5. Performance analysis

1. Low management overhead

The shared key scheme relies heavily on key management, and the conventional PKI has a large overhead storage requirement and has to deal with the management of the public key certifications. These will impose a heavy burden on management of WMNs. IBC has simplified the difficult task of issuing public keys, eliminated dependency on certification authority. Using an ID-based scheme, our handover protocol overcomes the drawbacks of the symmetric key system and the conventional PKI system.

2. Low communication cost

The mutual authentication and authenticated key establishment of two MPs which belong to different trust domains can be achieved in a single one-round message exchange during the authentication phase based on our proposed multi-domain ID-based signcryption scheme. Authentication directly between two MPs avoids multi-hop wireless communication which will result in high latency and heavy cost. Using features of signcryption, our protocol can accomplish exchange of temporary keys during the process of authentication in order to establish a session key.

3. No AS involvement

Most current handover schemes in WMNs need AS to act as a trust authority. Multi-hop wireless communication is demanded because AS is in general several hops away from MPs. As we all know, muti-hop communications may result in high delay, low stability and potential service interruption. We use IBC whose basic idea is that the entity's public key is directly derived from its publicly known identity information. MP_i and MP_j exchange their respective public system parameters of PKGs. Therefore MP_i and MP_j can obtain public key of the other side. Making use of our ID-based multi-domain signcryption scheme, handover authentication between MP_i and MP_j can be completed directly by the two MPs. Authentication severs of both sides do not need to participate in handover protocols. It is suitable for application in WMNs with characters of self-organization.

4. No PKG parameters restricted

Almost all the ID-based multi-domain handover schemes are based upon the same assumption that all the different domains share the same pairing parameters. The applications of the schemes based on the assumption are limited because different domains may have totally different PKG system parameters including public system parameters, system master keys and system public keys in real WMNs environments. There are no restrictions on PKG system parameters in our proposed multi-domain ID-based signcryption scheme so that our handover scheme can be well applied to real WMNs circumstance.

5. Transmission data carried

Data transmission must be implemented after the authentication procedure in conventional handover schemes. In our handover scheme, data transmitted between two MPs can be carried by the authentication messages preventing transmission interruption on both sides owing to signcryption. Signcryption simultaneously fulfills both the functions of a digital signature and a public key encryption in a single logical step.

The receiver accepts the ciphertext signcrypted if and only if the following equation holds. $e_U(P_U, \sigma_{MP_i}) = e_U(TA_1, Pub_U) e_U(Pub_U, Q_{MP_i})^{H_3^U(c_{MP_i}, TA_1)}$. Then the receiver recovers the data $m_{MP_i} = H_2^V(w^*) \oplus c_{MP_i}$. Note that no one except the right receiver can recover the data since only the right receiver MP_j knows the private key S_{MP_j} to compute $w^* = e_V(TA_2, S_{MP_j})$.

Finally, we analyze the communication cost and computational cost of our protocol in **Table 1**. The operations with low computation complexity such as random number generation and hash function are trivial in comparison with bilinear pairing, thus can be omitted. The involved operations consist of bilinear pairing (BP) and scalar multiplication (SM). Although there are several pairing operations for MPs, they have enough computational capabilities and power supplies. Moreover, authentication directly between two MPs avoids multi-hop wireless communication between MP and AS. The communication latency between MPs is much lower than that between MP and AS, because AS is in general several hops away from the MPs. Muti-hop communication may result in long delays, low stability and potential service interruption. Therefore we get low communication latency in return for increased bilinear pairing operations. Meanwhile, the signcryption to which the bilinear pairing operations are applied make the data transmitted between the two mesh points able to be carried by the authentication messages. In a sense, the bilinear pairing operations should be considered acceptable.

Table 1. Numbers of messages and computational cost

Total numbers of messages between MP_i and MP_j	**Computational cost of MP_i**		**Computational cost of MP_j**	
	BP	**SM**	**BP**	**SM**
6	5	7	5	7

6. Conclusion

In this paper, we have proposed a new ID-based multi-domain signcryption scheme and accordingly presented a novel ID-based multi-domain handover protocol for mesh points in WMNs. Our handover scheme can be well applied to real WMNs circumstance. Security and performance analysis shows that our protocol is secure and efficient. We plan to design a lightweight ID-based handover protocol for mesh clients which are common devices with low computational power.

References

[1] I. Akyildiz and X. Wang, *Wireless Mesh Networks*, Wiley, 2009. Article (CrossRef Link)
[2] "IEEE Draft Amendment: ESS Mesh Networking," *IEEE 802.11s. Draft 1.00*, 2006.
[3] "IEEE 802.11i Amendment 6: Medium Access Control (MAC) Security Enhancements," *IEEE standards*, 2004.
[4] "IEEE 802.11x: IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control," *IEEE standards*, 2001.
[5] T. Braskich and S. Emeott, "Initial MSA Comment Resolution," *IEEE 802.11-07/0564r2*, May, 2007. Article (CrossRef Link)
[6] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Proc. of Crypto'84*, vol. 196, pp. 47-53, 1985. Article (CrossRef Link)
[7] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in *Proc. of Crypto'01*, vol. 2139, pp. 213-229, August 19-23, 2001. Article (CrossRef Link)
[8] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)," in *Proc. of Crypto'97*, vol.1294, pp. 165-179, August 17-21, 1997. Article (CrossRef Link)
[9] J. Malone-Lee, "Identity-based signcryption," *Cryptology ePrint Archive, Report 2002/098*, 2002.

Article (CrossRef Link)
[10] F. Li, M. Shirase, and T. Takagi, "Efficient Multi-PKG ID-based Signcryption for Ad Hoc Networks," *Information Security and Cryptology*, vol. 5487, pp. 289-304, 2009. Article (CrossRef Link)
[11] C. Tang and D.O. Wu, "An efficient mobile authentication scheme for wireless network," *IEEE Transaction on Wireless Communications*, vol.7, no. 4, pp.1408-1416, April, 2008. Article (CrossRef Link)
[12] G. Li, X. Chen and J. Ma, "A ticket-based re-authentication scheme for fast handover in wireless local area networks," in *Proc. of the 6th International Conference on Wireless Communications Networking and Mobile Communication*, pp. 1-4, September 23-25, 2010. Article (CrossRef Link)
[13] C. Li and U. T. Nguyen, "Fast authentication for mobile clients in wireless mesh networks," in *Proc. of the 23rd Canadian Conference on Electrical and Computer Engineering*, pp. 1-8, May 2-5, 2010. Article (CrossRef Link)
[14] C. Li, U. T. Nguyen, H. L. Nguyen and N. Huda, "Efficient authentication for fast handover in wireless mesh networks," *Computer &Security*, vol. 37, pp. 124-142, September, 2013. Article (CrossRef Link)
[15] X. Li, Y. Zhang, X. Liu, J. Cao and Q. Zhao, "A new roaming authentication framework for wireless communication," *KSII TRANSACTION ON INTERNET AND INFORMATION SYSTEM*, vol.7, no. 8, pp. 2061-2080, 2013. Article (CrossRef Link)
[16] X. Zhu, Y. Fang and Y. Wang, "How to secure multi-domain wireless mesh networks," *Wireless Networks*, vol.16, no. 5, pp. 1215-1222, July, 2010. Article (CrossRef Link)
[17] B. He and D. P. Agrawal, "An identity-based authentication and key establishment scheme for multi-operator maintained wireless mesh networks," in *Proc. of IEEE 7th International Conference on Mobile Ad hoc and Sensor Systems*, pp. 71-78, November 8-12, 2010. Article (CrossRef Link)
[18] R.C.-W. Phan, "Non-repudiable authentication and billing architecture for wireless mesh networks," *Wireless Networks*, vol. 17, no. 4, pp. 1055-1061, May, 2011. Article (CrossRef Link)
[19] T. Gao, N. Guo and K. Yim, "LEAS: Localized efficient authentication scheme for multi-operator wireless mesh network with identity-based proxy signature," *Mathematical and computer modelling*, vol. 58, no. 5-6, pp. 1427-1440, September, 2013. Article (CrossRef Link)
[20] F. Hess, "Efficient identity based signature scheme based on pairings," in *Proc. of the 9th Workshop on Selective Areas on Cryptography*, vol. 2595, pp. 310-324, August 15-16, 2002. Article (CrossRef Link)

Xue Zhang received the B.E. degree and M.E. degree in Computer Science and Technology from Engineering University, Xi'an, P.R. China in 2006 and 2009 respectively. Now she is a Ph.D. Candidate in Zhengzhou Information Science and Technology Institute. Her current interests include wireless network security, and information security.

Guangsong Li received the B.S. degree in applied mathematics from Information Engineering University, Zhengzhou, P. R. China in 1999, and M. S. degree in applied mathematics from Information Engineering University in 2002, and the Ph. D. degree in Cryptography from Information Science and Technology Institute, Zhengzhou, P. R. China, in 2005. Now he is an associate professor of State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou. His current interests include mobile communication, wireless security, and digital rights management.

Wenbao Han received the B.S. degree in applied mathematics from Zhengzhou Information Science & Technology Institute, Zhengzhou, P. R. China in 1982. He recieved the M.S. degree and Ph. D. degree in applied mathematics from Sichuan University in 1989 and in 1992 respectively. Now he is a professor of State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou. His research interests are cryptography and information security.

Huifang Ji received the B.S. degree in applied mathematics from Information Engineering University, Zhengzhou, P. R. China in 2004, and M. S. degree in applied mathematics from Information Engineering University in 2007, and the Ph. D. degree in Cryptography from Information Science and Technology Institute, Zhengzhou, P. R. China, in 2011. Now she is a lecturer of State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou. Her current interests include cryptography and information security.