A Unified Security Framework for Multi-domain Wireless Mesh Networks

Ze Wang[1, *], Maode Ma[2], Wenju Liu[1], and Xixi Wei[1]

[1] School of Comp. Science & Software,
Tianjin Polytechnic University, Tianjin, China
{wangze,liuwj,weixx}@tjpu.edu.cn
[2] School of EEE., Nanyang Technological University, Singapore
emdma@ntu.edu.sg

Abstract. The research issues of large scale wireless mesh networks (WMNs) have attracted increasing attention due to the excellent properties of WMNs. Although some proposals for WMN security framework with different security aspects have been put forward recently, it is a challenging issue of employing uniform public key cryptography to maintain trust relationships flexibly among domains and to achieve key-escrow-free anonymous access control. In this paper, a unified security framework (USF) for multi-domain wireless mesh networks is proposed, which unifies id-based encryption and certificateless signature in a single public key cryptography context. Trust relationship between different domains and anonymous access control of wireless clients can be realized by employing of cryptography operations on bilinear groups. To achieve perfect forward secrecy and attack-resilience, trust domain construction methods and authentication protocols are devised within the security framework without key escrow.

Keywords: Wireless mesh networks, security, identity-based cryptography, certificateless signature.

1 Introduction

Security issues inherent in Wireless mesh network (WMN) need be considered because of the intrinsically open and distributed nature. Be aware of the embarrassing situation of WMN security, state-of-the-art schemes [1-4] addressing different WMN security issues have been devised sophisticatedly. Special signature methods have been utilized in [1,2] to achieve security objectives, wherein conventional public key signature has been employed to build trust relationships. To mitigate complex conventional public key certificates management, authors in [3,4] have proposed WMN security architectures based on id-based cryptography (IBC) [5].

The proposal in [3] has attempted to apply IBC into the WMN security scheme while it has adopted a credit-card-based model for the inter-domain authentication. Focusing on anonymity, IBC and blind signature mechanism have been combined in

[*] Corrresponding author.

S. Qing et al. (Eds.): ICICS 2011, LNCS 7043, pp. 319–329, 2011.

one security architecture to achieve anonymity and traceability in [4]. Although IBC is promising with an attractive feature of public key self authenticity, it suffers from private key escrow problem. As a result, it is still a challenging issue of employing uniform public key cryptography without key escrow problem for flexible maintenance of domain trust relationships and anonymous access control.

To overcome the shortcomings of the existing solutions, in this paper, we propose to build a security framework in a unified cryptography context without key escrow while possessing anonymous and attack-resilient features. To obviate all the private keys of clients escrowing in a centralized private key generator (PKG), we adopt certificateless public key cryptography (CL-PKC) [6] to avoid possible keys leakage. We propose a unified security framework (USF) for multi-domain wireless mesh networks, which unifies IBC and CL-PKC in a single cryptography context where both IBC and CL-PKC master keys are generated with the same public cryptology parameters. Trust domain construction methods and anonymous authentication protocols with perfect forward secrecy are devised within the key-escrow-free framework to achieve attack-resilience.

The remainder of this paper is organized as follows. In Section 2, the system models are described. In Section 3, the details of the security framework are presented. In Section 4, the security analysis of our scheme is performed. Performance comparison is shown in Section 5. The paper is concluded with a summary in Section 6.

2 System Models

2.1 Network Model

Large scale WMNs are composed of a great number of WMN domains with different scales. As the fundamental components in a WMN, mesh routers have much more powerful computation and communication capacities than those of mesh clients. Mesh clients, which can choose a mesh router to access the Internet, are mobile nodes served by the networks. The traffics from mesh clients are mainly forwarded through mesh routers in WMN, which yields a natural design to control clients' access directly by a mesh router. In the WMN under the study, to show compatibility of the proposed solution, routing scheme is not specified and the clients may communicate with mesh routers through either a single hop or a multi-hop link.

2.2 Trust Model

A trust domain of a WMN covers the same area as a physical domain and includes all the member nodes in it. The domain operator (DO) is responsible for the management of the wireless clients and routers in the domain. In the deployment of the trust domain, a mesh router has to register with the domain operator and build secure associations with it and other neighbor mesh routers. Each mesh client has to first register with the domain operator which, in turn, issues a user access ticket (UAT) to the client. The entire WMN is composed of numerous such trust domains, among which the trust relationships may exist or not exist between each of two peers. An interdomain authentication is a necessary authentication process for a mesh client to obtain access to the mesh router belonging to a foreign domain of the client. Trust relationships among domains should be built to approve interdomain access requests.

A trusted third party (TTP) used to sponsor different trust domains registration should be built in the security framework, so as to establish trust relationships among trust domains. TTP generates global public parameters in the form of global access token (GAT), which should be easily obtained by any nodes in the network. Each domain operator has to first deliver the domain public parameters to the TTP which, in turn, issues a domain access token (DAT) to the operator. A trust domain list is used, which is a list of DATs stored by a DO, to record the domains, which the DO should trust. Considering domain A and domain B in a WMN, a domain operator DO_A can claim to trust domain B by insertion of DAT of DO_B into its local trust domain list. Vice versa, DO_B inserts DAT of DO_A into its local trust domain list to trust domain A. The easy yet flexible way of trust construction allows unidirectional or bidirectional trust relationship between peer domains.

The above trust model fits in well with the deployment structure of Wireless Internet Service Providers (WISPs) providing Internet access via WMNs.

2.3 Cryptographic Background

Let q be a large prime. Let G_1 and G_2 be an additive group and a multiplicative group, respectively, of the same prime order q. Bilinear map is denoted by $e: G_1 \times G_1 \to G_2$. Let $H_1:\{0,1\}^* \to G_1^*$, $H_2:\{0,1\}^* \to Z_q^*$ and $H_3: G_1^* \to \{0,1\}^n$ be three secure cryptographic hash functions. A trust authority chooses a random number $s \in Z_q^*$ and a generator P of G_1. It sets the system master public key $P_{pub} = sP$, master secret key as s and publishes $\{q, G_1, G_2, e, P, P_{pub}\ H_1, H_2, H_3\}$. The user ID chooses a random number $x_{ID} \in Z_q^*$ and sets x_{ID} as his secret value. Let $f(ID)$ denote a function that maps ID and other corresponding important information into an element in G_1^*. We can get certificateless public key as $x_{ID}P, f(ID)$ and private key as $x_{ID}, sf(ID)$ for certificatleless signature. Meanwhile, we can extract id-based public key $f(ID)$ and private key $sf(ID)$ for id-based encryption defined as in [7].

The second certifcateless signature and verification method in [8] is modified to fit in our security scheme, which is shown as follows.

Certificateless-Sign: For a message m, the user ID computes the signature $\sigma = (u,v,W)$ where:

$u = H_2(m \,\|\, f(ID) \,\|\, x_{ID}P \,\|\, r_1P \,\|\, e(P,P)^{r_2})$ for random numbers $r_1, r_2 \in Z_q^*$ which are chosen by user ID. $v = r_1 - ux_{ID} (\bmod q)$, $W = r_2P - usf(ID)$.

Certificateless-Verify: Given a message and signature pair $(m, \sigma = (u,v,W))$ and user ID's public key $x_{ID}P, f(ID)$, anyone can check whether $u = H_2(m \,\|\, f(ID) \,\|\, x_{ID}P \,\|\, vP + ux_{ID}P \,\|\, e(W,P)e(f(ID),P_{pub})^u)$. If the equation holds, results *true*. Otherwise, results *false*.

The common notation in our scheme are listed as follows.

- ***IDD$_i$*, *ID$_j$*, *IDR$_k$*:** The unique identity of a trusted domain *i*, a wireless client *j*, and a mesh router *k*, respectively.
- **||:** concatenation symbol.
- ***PK$_x$*, *SK$_x$*:** The certificateless public key and private key for entity *x*.
- ***Sig$_x$*(*m*):** The certificateless signature on a message *m* using the signer *x*'s certificateless private key.
- ***Ver$_x$*(σ):** The verification process of the above signature using the signer *x*'s certificateless public key, which returns *true* or *false*.
- ***Enc$_x$*(*m*):** The id-based encryption to a message *m* using the entity *x*'s id-based public key.
- ***Dec$_x$*(*c*):** The id-based decryption to a cipher text *c* using the entity *x*'s id-based private key.
- ***H$_{MIC}$*(*m*):** A hash function such as SHA-1.
- ***H$_{KD}$*(*m*):** A hash function for symmetric key generation, usually implemented by one to several rounds of hash operations on a message *m*.

3 Proposed Security Framework

The essential components of the proposed framework are intradomain authentication and interdomain authentication protocols based on trust among domains. The prerequisite to execution of the authentication protocols is the initialization of the TTP and DOs at the very beginning followed by the construction of trust relationships and registration of intradomain wireless nodes. In the following, we will describe the initialization, registration and authentication protocols in detail, together with the master key generation, session key agreement, and confidential communications that may take place during the execution of these protocols.

3.1 Trust Domain Initialization

The trust domains should be initialized before wireless clients gain the opportunities of access by registration on the operator of certain domain. At the very beginning, a trusted third party *TTP* should be constructed to build authenticity of trust domain parameters. *TTP* generates global parameters and the global public access token *GAT* as follows:

$$GAT = global-params \,||\, \Gamma\tilde{H}_1(global-params)$$
$$global-params = \{\tilde{q}, \tilde{G}_1, \tilde{G}_2, \tilde{e}, \tilde{P}, \tilde{P}_{pub}, \tilde{H}_1, \tilde{H}_2, \tilde{H}_3\}$$

The global secret $\Gamma \in Z_{\tilde{q}}^*$ is random selected by TTP. The *GAT*, which contains global public parameters, should be distributed freely to each node in the WMNs. However, *GAT* is not an essential element if a wireless client is expected to keep inside the master domain.

TTP generates the public domain cryptography parameters $(q, G_1, G_2, e, P, H_1, H_2, H_3)$ and domain operator DO_i picks a random $s_i \in Z_{\tilde{q}}^*$ as the domain secret whereby to compute a domain public key as $P_{pub} = s_i P$.

Next DO_i registers its domain public parameters *domain-params* to *TTP*, whereby *GAT* and domain access token *DAT* are returned. The domain access token *DAT* is defined as follows:

$$DAT = domain - params \parallel \Gamma \tilde{H}_1(domain - params)$$
$$domain - params = \{IDD_i, Exp_i, q, G_1, G_2, e, P, P_{pub}, H_1, H_2, H_3\}$$

IDD_i is the global unique identity of domain *i* provided by the TTP. Exp_i is the expiration time of DAT for domain *i.* If $e(\Gamma \tilde{H}_1(domain - params), \tilde{P}) = e(domain - params, \tilde{P}_{pub})$ holds, it is the authenticity evidence of *domain-params*. *DAT* is the unique representation of a domain. *DO* should determine whether to insert *DAT* of another domain *B* into its local trust domain list in order to approve the access requests from the clients belonging to domain *B*. Thus, registered domains will build their trust relationships to enable interdomain access.

3.2 Intradomain Registration

After the domain is initialized, DO takes the responsibility of domain security management. A wireless client must register to DO through a secure link for future network access. Registration steps are as follows.

1. *CL→DO*: *SSN, credentials,* etc.
2. *DO→CL*: *GAT, DAT,* ID_j, exp_j, c_j
3. *CL→DO*: x_jP, $f(ID_j)$
4. *DO→CL*: $s_if(ID_j)$, *UAT*

A wireless client CL_j supplies personal information such as social security number (SSN), date of birth, telephone number and other identity credentials in message 1 to a domain operator DO_i. After examining the credentials, DO_i generates a unique identity ID_j, expiration time exp_j and a service contract c_j and sends them together with *GAT* in message 2 to CL_j. After approving the service contract and validating *DAT* through *GAT*, CL_j chooses a random number $x_j \in Z_q^*$, calculates x_jP and $f(ID_j) = H_1(IDD_i \parallel H_1(ID_j) \parallel x_jP \parallel exp_j \parallel c_j)$. CL_j sends $PK_j=(x_jP, f(ID_j))$ in message 3 to DO_i. In turn, DO_i issues an user access ticket *UAT* and parital secret $s_if(ID_j)$ in message 4 to CL_j where $UAT = \{IDD_i, H_1(ID_j), exp_j, c_j, PK_j\}$.

CL_j checks whether $e(f(ID_j), P_{pub}) = e(s_if(ID_j), P)$ and stores ID_j, certificateless private key $SK_j=(x_j, s_if(ID_j))$ and *UAT*. DO_i will save ID_j, *UAT* and identity credentials as a user record. As a proof of CL_j's legality, *UAT* contains the certificateless public key and the master domain identity IDD_i. To implement anonymous access control, CL_j's identity ID_j is not included in *UAT*. Validity of *UAT* is restricted by the field exp_j so that CL_j must renew registration for a new valid *UAT* when the old one expired. Through registration, CL_j gets the certificateless public key $(x_jP, f(ID_j))$ and private key $(x_j, s_if(ID_j))$, from which the id-based public key $f(ID_j)$ and private key $s_if(ID_j)$ can be naturally extracted. CL_j must keep x_j secret to ensure the confidentiality of certificateless private key to DO_i.

For mesh routers, similar registration steps are as follows.

1. $MR \rightarrow DO$: *MAC, SN, credentials,* etc.
2. $DO \rightarrow MR$: GAT, DAT, IDR_k, exp_j
3. $MR \rightarrow DO$: x_kP, $g(IDR_k)$
4. $DO \rightarrow MR$: $s_ig(IDR_k)$, RAT

Different from a mesh client, a mesh router should supply the MAC address, the sequence number (SN), and other corresponding credentials. At the end of the registration, a mesh router obtains certificateless private key $(x_k,s_ig(IDR_k))$ and router access ticket (RAT) as follows:

$$RAT = \{IDD_i \,||\, IDR_k, exp_k, PK_k\}$$
$$PK_k = (x_kP, g(IDR_k))$$
$$g(IDR_k) = H_1(IDD_i \,||\, IDR_k \,||\, x_kP \,||\, exp_k)$$

DO allocates a unique identity IDR_k for the mesh router and sets expiration time in exp_k. The length of IDR_k must be different from that of $H_1(ID_i)$ to distinguish UAT and RAT. Certifcateless public key PK_k and id-based public key $g(IDR_k)$ are generated in a similar way but with a different function $g(ID)$. The identity of a mesh router is explicitly given in RAT since a client would be reluctant to access via an anonymous mesh router.

3.3 Intradomain Authentication Protocols

A registered client may access the network after authentication with a mesh router belonging to the same master domain. When a wireless client moves into the coverage of a mesh router, the intradomain authentication could be carried out to complete bidirectional authentication and session key agreement between them.

The intradomain authentication protocol between a CL and a MR is described as follows.

1. $MR \rightarrow *$: RAT
2. $CL \rightarrow MR$: $UAT, aP, N_1, Sig_{CL}(UAT \,||\, aP \,||\, N_1)$
3. $MR \rightarrow CL$: $RAT, bP, N_2, Sig_{MR}(RAT \,||\, aP \,||\, bP \,||\, N_1 \,||\, N_2)$, $H_{MIC}(abP \,||\, N_1 \,||\, N_2 \,||\, bP)$
4. $CL \rightarrow MR$: $H_{MIC}(abP \,||\, N_2 \,||\, N_1 \,||\, aP)$

The MR periodically broadcasts a beacon in message 1 to announce its presence. The beacon should include RAT. Upon receiving message 1, a client CL may first check the IDD_i field in the RAT to confirm he is within the scope of a master domain router and then justify the legality of the RAT by computing $g(IDR_k)$ and examining its exp_k field. If tests passed, CL selects random numbers $a, N_1 \in Z_q^*$, computes key negotiation factor aP and sends UAT, aP, N_1 and certificateless signature via message 2. Upon receipt of message 2, MR first justifies the legality of UAT and then verifies the signature. In case of passed, MR selects random numbers $b, N_2 \in Z_q^*$, computes bP, *abP* and calculates signature and message integration code (MIC) $H_{MIC}(abP||N_1||N_2||bP)$ to form and send message 3. When the message 3 arrives, *CL* computes *abP* with obtained *bP* and secret number *a* after the verification to the signature succeeded. *CL* confirms the session key by checking $MIC = H_{MIC}(abP \,||\, N_1 \,||\, N_2 \,||\, bP)$, then calculates session key $K_s = H_{KD}(abP \,||\, N_1 \,||\, N_2)$ and stores it for future secure communication. Finally, *CL* calculates and sends $MIC = H_{MIC}(abP \,||\, N_2 \,||\, N_1 \,||\, aP)$ to *MR*. Upon receipt of message 4, *MR* confirms the session key through *MIC* and computes session key K_s with the knowledge of *aP* and secret number *b*.

After the above process of authentication protocol, both sides have completed the bidirectional authentication and session key agreement. Compared to ARSA [3], in our scheme a wireless client needs not to launch an interdomain protocol before intra-domain access. The localized intradomain authentication process is carried out without participation of a trust authority e. g. DO or authentication server (AS) in comparison to EAP-TLS protocol of 802.11i [9].

For registered mesh clients in a certain domain, owning *DAT*, *UAT* and corresponding keys enables authentication between any neighbor peers. Suppose CL_1 and CL_2 are two adjacent wireless clients. They can share a common session key $K = e(f(ID_{CL_2}), s_i f(ID_{CL_1})) = e(f(ID_{CL_1}), s_i f(ID_{CL_2}))$ with solely the knowledge of each other's public key just as [3]. However, we prefer to carry out session key negotiation process to mitigate possible leakage problem of master private keys. The authentication protocol between adjacent clients is as followed:

1. $CL_1 \rightarrow CL_2$: $UAT_1, aP, N_1, Sig_{CL_1}(UAT_1 \,||\, aP \,||\, N_1)$
2. $CL_2 \rightarrow CL_1$: $UAT_2, bP, N_2, Sig_{CL_2}(UAT_2 \,||\, aP \,||\, bP \,||\, N_1 \,||\, N_2)$, $H_{MIC}(abP \,||\, N_1 \,||\, N_2 \,||\, bP)$
3. $CL_1 \rightarrow CL_2$: $H_{MIC}(abP \,||\, N_2 \,||\, N_1 \,||\, aP)$

During the authentication process, the adjacent clients verify the certificateless signatures and build the session key $K_S = H_{KD}(abP \,||\, N_1 \,||\, N_2)$ just like the process between *CL* and *MR*. It should be noted that the authentication initiator needs to launch an interdomain authentication at first when the target client doesn't belong to the same domain.

3.4 Interdomain Authentication Protocol

Wireless clients may access a foreign domain which trusts their master domain by finishing an interdomain authentication process. When a wireless client sends an access request to a mesh router in a foreign domain, the mesh router will forward the request to *DO* of that domain for verification. The verification includes to retrieve the client's DAT_h in the trust domain list and to verify UAT_h through DAT_h. In case the verification passed, *DO* would issue a temporal user access ticket UAT_f including the hash value $H_1(ID_f)$ for a unique temporal idenity ID_f to the client. The field c_j in UAT_f should indicate temporality of the ticket. Holding a valid temporal ticket, mesh client may access through other mesh routers in that domain by only finishing an intradomain authentication process.

Let IDD_h denotes the master domain identity and IDD_f denotes the foreign one. UAT_h represents the access ticket in the master domain and UAT_f represents the temporal access ticket in the foreign domain. Suppose *MR* and *DO* trust each other and build a secure link between them. The interdomain authentication protocol among *CL*, *MR* and *DO* is showed as follows:

1. $MR \rightarrow *$: RAT
2. $CL \rightarrow MR$: $UAT_h, aP, x_fP, N_1, AUTH_{CL}$
3. $MR \rightarrow DO$: $UAT_h, aP, x_fP, N_1, AUTH_{CL}$
4. $DO \rightarrow MR$: $UAT_f, Enc_{CL}(s_ff(ID_f))$
5. $MR \rightarrow CL$: $DAT_f, UAT_f, Enc_{CL}(s_ff(ID_f)), bP, N_2, AUTH_{MR}, H_{MIC}(abP \| N_1 \| N_2 \| bP)$
6. $CL \rightarrow MR$: $H_{MIC}(abP \| N_2 \| N_1 \| aP)$

Therein, $AUTH_{CL} = Sig_{CL}(UAT_h \| aP \| x_f P \| N_1)$ and $AUTH_{MR} = Sig_{MR}(DAT_f \| UAT_f \| ENC_{CL}(s_f f(ID_f)) \| aP \| bP \| N_1 \| N_2)$. The MR periodically broadcasts a beacon frame including *RAT* to announce its presence. Upon receipt of message 1, a client *CL* may first check the IDD_i field in the *RAT* to confirm that he is in the scope of a foreign domain router and then justify the legality of *RAT* through examination of $g(IDR_k)$ and exp_k. If the verification successful, *CL* selects random numbers a, N_1, $x_f \in Z_q^*$, computes aP, x_fP and sends UAT_h, aP, x_fP, N_1 and certificateless signature via message 2. Upon receipt of message 2, *MR* first checks the IDD field of UAT_h to confirm that the request is from a foreign domain client and then justify the legality of UAT_h. In case of success, *MR* forwards UAT_h, aP, x_fP, N_1 and the signature to *DO*. After retrieving DAT_h in the local trust domain list by IDD_h, *DO* justifies the legality of UAT_h and verifies the signature. If all success, *DO* generates a unique temporal indentity ID_f, calculates partial secret $s_ff(ID_f)$ and encrypts it with *CL*'s id-based public key in the master domain before generating a temporal access ticket UAT_f including $H_1(ID_f)$. DO sends back UAT_f and the encrypted partial secret encapsulated in message 4. Upon receiving message 4, *MR* collects UAT_f as the proof of approval of the access request and then generates session key negotiation element bP, nonce N_2, signature to the message and *MIC* for session key confirmation, then sends all of them together with DAT_f in message 5. CL gets UAT_f and corresponding partial secret $s_ff(ID_f)$ by decrypting with id-based private key in the master domain h after verifing DAT_f through *GAT* and the certificateless signature, then checks authenticity of the partial secret by examining $e(f(ID_f),P_{pub}) = e(s_ff(ID_f),P)$. If the equation holds, *CL* stores DAT_f, UAT_f and corresponding private key and sends *MIC* in message 6. After the final session key confirmation message 6 is approved, a shared session key will be built between the peers. Holding UAT_f and corresponding certificateless private keys, the client will access any mesh router in foreign domain f after carrying out a more simplified intradomain authentication whenever necessary.

4 Security Analysis

In the proposed framework, DO plays an important role to safeguard the domain security through administration to all the wireless nodes inside the master domain and authentication to foreign domain clients. The costs for the intradomain authentication will be distributed to mesh routers to remove the bottleneck caused by a centralized authentication scheme. Another advantage for the localized authentication is that suppose DO fails in an accident, the survival parts of the domain may still work in a local area. Free of key escrow, our scheme renders survivability even when the master key of DO is exposed, which will guarantee the confidentiality of certificateless private keys and the session keys by the authentication protocols. This is a security improvement over those pure IBC based schemes. Further more, the embedded session key agreement in our authentication protocol yields the attribute of perfect forward secrecy (PFS) [10]. When all the master private keys of communication participants are exposed, the previous session keys will not be affected. In contrast to existing IBC based schemes [3,4], if the master private key of a wireless client is leaked or the master key of the trust authority is disclosed, the confidentiality of exchanged data encrypted with the session key will still be kept by our scheme.

Different from the schemes combining special signature mechanism and conventional public key signature mechanism [1,2], IBC and CL-PKC have been integrated into a single cryptography context to exempt complex management of public key certificates by our proposed scheme. Furthermore, the clients or mesh routers can have id-based encryption/decryption or certifcateless signature/verification with consistent keying material, bilinear groups and hash functions, which renders the uniformity of cryptography operations. Besides its fundamental security functionality, other security aspects of our scheme can be deduced as follows.

Identity and Location Privacy Protection: Identity and location privacy is a growing concern to wireless network users. To keep anonymity of a client, since only hash value of the identity is used to generate part of the public key in the *UAT*, from it the real identity cannot be inferred. When a wireless client accesses a foreign domain, identity will not be disclosed due to the anonymous design of *UAT* which is shown as interdomain access admission. Moreover, a wireless client cannot link any meaningful identity with a neighbor client's location. Furthermore, it is difficult to link a master domain *UAT* to a temporal *UAT* of a foreign client except for the *DO* and the mesh router firstly accessed in the corresponding domain. It should be noted that absolute anonymity and location privacy is impossible to achieve because the administrators of wireless networks would prefer to reserve the rights of tracing malicious nodes, which could be realized by retrieving the original credentials from DO's user records.

Impersonation Attack Protection: A legal wireless client cannot impersonate another legal client because a legal *UAT* is bound to a unique identity by partial private key generated by *DO*. A legal wireless client cannot impersonate a legal mesh router to phish other clients because the partial public key generation function *g(ID)* of the *RAT* is different from the function *f(ID)* of the *UAT*. By our scheme, the identity of a mesh router is explicitly given in the *RAT* while the identity of a client is disguised in the *UAT*. Due to its authoritative status, DO is capable of generating a legal *UAT* with the same identity as an existing legal client, but it cannot forge a legal certificatelss signature related to the existing *UAT* without the knowledge of the secret value x_j selected by the client *j*.

Bogus data injection attacks can be easily thwarted by the access control based on the essential authentication and session key negotiation. To deal with DoS attacks, mesh routers can limit the frequency of authentication requests from the clients belonging to foreign domains to reduce the possibility of DoS attacks to a centralized domain operator. From above, we claim that security functionality of our scheme is strong even when the trust authority has been compromised. Due to the space limit, a formal verification on our protocols are not shown in this paper.

In the Table 1, we present the security comparison of intradomain authentication protocols among different security schemes. Other two IBC based schemes, ARSA and SAT, don't possess key-escrow-free and perfect forward secrecy for the authentication protocol as our scheme. By consolation from a compromised operator, wireless nodes can still perform confidential communication in a local area by both PEACE and USF schemes. However, different from other three IBC based schemes, PEACE must support both conventional signature cryptography operations and special signature cryptography operations based on bilinear groups.

Table 1. Security attributes comparison for intradomain authentication

Attributes	ARSA	PEACE	SAT	USF
Key-escrow-free				√
Perfect forward secrecy		√		√
Independent from PKI	√		√	√
Anonymity		√	√	√
Attack resilience	√	√	√	√

Table 2. Performance comparison for intradomain authentication

Attributes	ARSA	PEACE	SAT	USF
Message counts	2	3	4	4
Signing/verifying counts (client side)	1V	1S+2V	1S+1V	1S+1V
Signing/verifying counts (network side)	1S	1S+1V	1S+1V	1S+1V

5 Performance Analysis

In the Table 2, we present the performance comparison among different security schemes. Among the four schemes, ARSA needs the least authentication messages and the least computation overhead at the cost of ignoring key escrow problem. For the scheme PEACE, the message counts are the second least. However, a client has to perform one more verification process for validating the public key certificate of the mesh router. As a result, the computation and communication overhead of intradomain protocols in PEACE, SAT and USF are nearly in the same level.

6 Conclusion

In this paper, we have proposed a unified security framework for multi-domain wireless mesh networks by integration of id-based encryption and certificateless signature in a unified cryptography context. Trust relationships among WMN domains can be constructed in a simple yet flexible way. The certificateless key generation scheme can be free of key escrow while anonymity of wireless clients is guaranteed.

Acknowledgements. This work was supported in part by the National Natural Science Foundation of China under grant 60970016 and Natural Science Foundation of Tianjin under grant 11JCYBJC00800.

References

1. Zhu, H., Lin, X., Lu, R., Ho, P., Shen, X.: SLAB: A Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks. IEEE Trans. Wireless Communications 7(10), 3858–3868 (2008)
2. Ren, K., Yu, S., Lou, W., Zhang, Y.: PEACE: A Novel Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks. IEEE Trans. Parallel and Distributed Systems 21(2), 203–215 (2010)
3. Zhang, Y., Fang, Y.: ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks. IEEE J. Selected Areas Comm. 24(10), 1916–1928 (2006)
4. Sun, J., Zhang, C., Zhang, Y., Fang, Y.: SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks. IEEE Trans. Dependable and Secure Computing 8(2), 295–307 (2011)
5. Shamir, A.: Identity-based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
6. Al-Riyami, S.S., Paterson, K.G.: Certificateless Public Key Cryptography. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 452–473. Springer, Heidelberg (2003)
7. Dutta, R., Barua, R., Sarkar, P.: Pairing-based Cryptography: A Survey. Cryptology ePrint Archive Rep. 2004/064 (2004)
8. Huang, X., Mu, Y., Susilo, W., Wong, D., Wu, W.: Certificateless Signature Revisited. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, pp. 308–322. Springer, Heidelberg (2007)
9. IEEE Standard Supplement to Standard for Telecommunications and Information Exchange between Systems—LAN/MAN Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security: IEEE 802.11i. IEEE, Piscataway (2004)
10. Canetti, R., Krawczyk, H.: Analysis of Key-exchange Protocols and Their Use for Building Secure Channels. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 453–474. Springer, Heidelberg (2001)