Computer Science and Information Systems 11(3):975–999 DOI: 10.2298/CSIS130917060G

PPS: A Privacy-Preserving Security Scheme for Multi-operator Wireless Mesh Networks with Enhanced User Experience

Tianhan Gao[1], Nan Guo[2], Kangbin Yim[3], and Qianyi Wang[4]

[1] Faculty of Software College, Northeastern University,
110819 Shenyang, China
gaoth@mail.neu.edu.cn
[2] Faculty of Information Science and Engineering College, Northeastern University,
110819 Shenyang, China
guonan@ise.neu.edu.cn
[3] Faculty of Information Security Engineering, Soonchunhyang University,
336745 Asan, Korea
yim@sch.ac.kr
[4] Faculty of Economics and Administration, University of Malaya,
50603 Kuala Lumpur, Malaysia
qianyiyouyou@sina.com

Abstract. Multi-operator wireless mesh networks (WMNs) have attracted increasingly attentions as a low-cost accessing approach for future large-scale mobile network. Security and privacy are two important objectives during the deployment of multi-operator WMNs. Despite the necessity, limited literature research takes both privacy and user experience into account. This motivates us to develop PPS, a novel privacy-preserving security scheme, for multi-operator WMNs. On one hand, most of the privacy needs are satisfied with the hybrid utilization of a tri-lateral pseudonym and a ticket based on proxy blind signature. On the other hand, the sophisticated unlinkability is implemented where mobile user is able to keep his pseudonym unchanged within the same operator in order to gain better user experience. PPS is presented as a suite of authentication and key agreement protocols built upon the proposed three-tire hierarchical network architecture. Our analysis demonstrates that PPS is secure and outperforms other proposal in terms of communication and computation overhead.

Keywords: Multi-operator wireless mesh network, privacy preservation, mutual authentication, security, user experience.

1. Introduction

Wireless mesh networks (WMNs) have recently emerged as a promising and competitive technology to cope with the challenges in next generation mobile network due to the features of self-organization, self-maintenance, as well as low upfront investment [1]. It can also be envisioned that the future large scale WMNs will be composed of a majority of autonomous domains managed by different operators as opposed to few ones today [2]. Typically, in the multi-operator WMNs scenario as Fig.1, each operator maintains its own mesh backbone including mesh gateway and mesh routers, or shares some of the infrastructure components with other operators to provide network services to the mesh clients. Whereas mesh client may be associated with one or more operators by contractual means and has the ability to roam to the rest of the cooperating operators, if necessary. Different operators in a given geographical area will cooperate with each other in order to obtain large scale coverage and more consecutive user experience. However, security issues inherited from the intrinsically dynamic and open nature of wireless networks are still the main obstacle for the wide deployment of WMNs since it is unappealing to subscribers to obtain access and service without security guarantees. In addition, different operators may hold different security management policies, which will make the security control more complicated in the multi-operator WMNs. To this end, some proposals on WMNs security [3-4] have been presented recent years. In [3], the authors developed a broker-based attack-resilient security architecture (ARSA) for WMNs to address a wide range of particular attacks. We [4] proposed a localized efficient mutual authentication scheme (LEAS) with identity-based proxy signature [5] for access security in multi-operator WMNs. Despite the necessity and importance, security of WMNs is still in its early stage and has gained little attention so far [6].

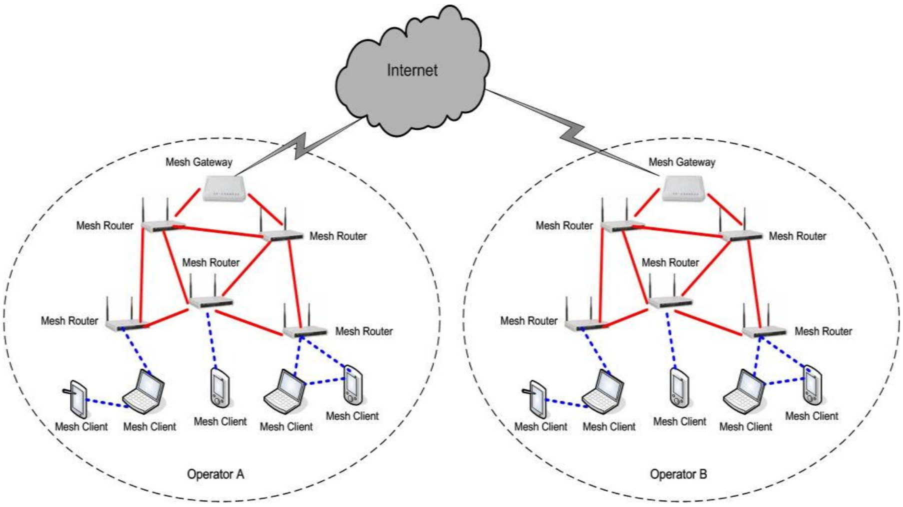

Fig.1. A typical architecture of multi-operator wireless mesh networks

Another big challenge for actually deploying WMNs with a multi-operator manner is how to provide adequate protection over user privacy since the communications contain various kinds of sensitive user information like personal identities, location information, financial information, social connections, and so on. Once disclosed to malicious attackers, the sensitive information could be illegally utilized or further be correlated together to compromise user privacy. Besides, the dynamic network architecture, hop-by-hop open wireless link, as well as autonomous yet cooperating operators render

WMNs highly vulnerable to various privacy-oriented attacks. Hence, privacy-preserving is of paramount practical importance in multi-operator WMNs.

The most important requirement of user privacy is anonymity that is concerned with hiding the real identity information of a user from his activities unless it is intentionally disclosed by himself. Different communication sessions associated with the same user should also be unlinkable to prevent association analysis. In reality, anonymity is conflicted with authentication or access control. With perfect anonymity, a user can misbehave arbitrarily and avoid being traced even to the identity issuer. Therefore, accountability is highly desirable for detecting and tracing malicious users in case of disputes and frauds. In terms of the above privacy requirements, several schemes have been proposed recently that are surveyed by [1] to meet the privacy-preserving needs for WMNs. However, limited literature research has been conducted to multi-operator context where operators are geographically distributed yet cooperating with each other. While user roaming across different operator WMNs, novel security architecture should be set up and conscious tradeoffs must be made to achieve both privacy-preserving authentication and fine user experience. According to [7], a new plan declared by Disney World will track visitors with wireless bracelets. Imagine walking through Disney World, Snow White walks up to you and wishes your child a happy birthday by name. Something like that could make an already memorable trip even more amazing. The cost of such a program is that your privacy, such as name, age, or even the credit card information, will be encoded in the bracelets. So Disney is able to track you during your trip or later. How to make a balance between privacy and user experience, is really a new challenge in multi-operator WMNs.

In this paper, we propose a privacy-preserving security scheme for large-scale multi-operator WMNs upon a three-tire hierarchical security architecture. Broker, acts as the root trust on the top tire, is responsible for the security management of all the involved entities. Based on such architecture, a novel mutual authentication scheme equipped with key agreement ability is achieved that takes inter-operator and intra-operator roaming scenarios into account. The combination of pseudonym and ticket is introduced as the authentication credential in our scheme. In light of the privacy requirements, on one hand a tri-lateral pseudonym approach is presented to meet anonymity need without key escrow. On the other hand, a ticket based on proxy blind signature (PBS) [8] is designed for mobile user against being traced from operator and broker. Both the pseudonym and the ticket can be altered by mobile user at his will when roaming across different operators. Thus the sophisticated unlinkability is implemented where mobile user is able to keep his pseudonym unchanged within the same operator in order to gain better user experience. In addition, the accountability is also satisfied due to the salient features borrowed from e-cash system on PBS. The system analysis demonstrates that our scheme is secure and outperforms similar one in terms of communication and computation overhead.

Specifically, our contributions are 3-folded as follows:

- The variable tri-lateral pseudonym approach and PBS-based ticket are designed to deal with the anonymity and untraceability needs;
- Sophisticated unlinkability is achieved through the bind of pseudonym and operator-level ticket in order to gain enhanced user experience;
- Accountability property is incorporated with the idea inherited from e-cash system to detect malicious users.

To sum up, our research is mainly focus on the security and privacy issues in multi-operator WMNs. It should be noted that the implementation of routing security and anonymity is out of the scope of this paper, which is left as the future works.

The rest of this paper is organized as follows. Section 2 reviews the identity-based primitives. Section 3 presents the system model including the hierarchical network architecture. We propose the mutual authentication scheme in terms of different roaming scenarios in Section 4. In Section 5, we provide security and performance analysis of our scheme. Section 6 discusses the related work. Finally, we conclude the paper in Section 7.

2. The Cryptographic Background

2.1. Bilinear Pairing

Let G be an additive group and G_T be a multiplicative group of the same prime order q, I_G and I_{GT} is the generator of G and G_T respectively. Assume that the discrete logarithm problem [9] is hard on both G and G_T. A mapping $\hat{e}: G \times G \rightarrow G_T$ which satisfies the following properties is called bilinear pairing:

(1) Bilinear: For all $P, Q \in G$ and $a, b \in Z_q^*$, $\hat{e}(a \cdot P, b \cdot Q) = \hat{e}(b \cdot P, a \cdot Q) = \hat{e}(P, Q)^{ab}$;

(2) Non-degenerate: $\hat{e}(P, Q) \neq I_{GT}$;

(3) Computable : For all $P, Q \in G,$ there is an efficient approach to compute $\hat{e}(P, Q) \in G_T$.

The Weil and Tate [10] associated supersingular elliptic curve can be modified to construct such bilinear pairing.

2.2. Short Signature (BLS)

Boneh et al. [11] proposed short signatures (BLS) from the Weil pairing in 2001, which is a simple but efficient signature scheme. It is designed for systems where signatures are sent over a low-bandwidth channel. The scheme is specified as following algorithms.

Setup.

PKG chooses additive group G_1 and multiplicative group G_2, as well as a bilinear pairing $\hat{e}: G_1 \times G_1 \rightarrow G_2$; PKG chooses arbitrary $P \in G_1$ and a hash function $H_1: \{0,1\}^* \rightarrow G_1$.

Key Generation.

User selects random $x \in Z_q^*$ and computes $R = x \cdot P$. R is public key and x is private key.

Sign.

To sign a message m, signer computes $V = x \cdot H_1(m)$. V is the signature.

Verify.

To verify V, verifier checks whether $\hat{e}(R, H_1(m)) == \hat{e}(P, V)$.

2.3. Identity-based Proxy Signature

The concept of proxy signatures was first introduced by Mambo et al. [12] in 1996. A proxy signature scheme permits an original signer to delegate its signing rights to a proxy signer so that it can sign on behalf of the original signer within a given context. Holding a proxy signature, anyone can verify both the delegation of original signer and the digital signature from proxy signer. Bo Gyeong Kang et al. [5] constructed a concrete identity-based proxy signature (IBPS) which is derived from BLS and CBE [13] as below.

Setup.
Assume Alice (original signer) and Bob (proxy signer) have private/public key pairs $(s_A,\ s_A \cdot P)$ *and* $(s_B,\ s_B \cdot P)$ respectively and the common system parameters $PARA = (G_1, G_2, \hat{e},\ P, H_1, H_2)$, where two hash functions $H_1 : \{0,1\}^* \to G_1$ *and* $H_2 : \{0,1\}^* \times G_1 \to Z_q^*$ *are defined*.

Delegation.
In order to delegate signing right to Bob, Alice sends to Bob a warrant ω together with a BLS signature $Cert_B = s_A \cdot P_B,$ *where* $P_B = H_1(PK_A \| PK_B \| \omega).$ The corresponding proxy signing key of Bob is $SKP_B = Cert_B\ +\ s_B \cdot P_B.$

Sign.
To sign message m on behalf of Alice, Bob selects secrect random $r \in Z_q^*$ and computes $\sigma =$ $(U,V),$ where $U = r \cdot P_B,\ h =\ H_2(m,U)$, and $V = (r+h)SKP_B.$

Verify.
To verify signature $\sigma,$ verifier checks whether $\hat{e}(PK_A + PK_B, U + h \cdot P_B) == \hat{e}(P,V),$ *where* $h = H_2(m,\ U).$

3. System Model

Our concrete privacy-preserving security scheme is based on the following system model which contains network architecture, trust model, as well as privacy model. After some definitions of handover types and credentials, a three-tire hierarchical network architecture is first presented to support different kinds of handovers in multi-operator WMNs. Both trust and privacy model are then illustrated making the trust hypothesis and privacy needs explicit. The system is also initialized to develop the later proposed security scheme.

3.1. Definitions and Notations

Definitions. Some definitions that are frequently used in this paper are given in this subsection.

Inter-operator handover. Inter-operator handover occurs when mesh client roams from one operator WMNs to another under the same trust broker.

Intra-operator handover. Intra-operator handover refers that mesh client handoffs from one mesh router to another within the same operator WMNs.

Certificate. The certificate here is different from the X.509 public key certificate in PKI [14] which manifests the binding of owner's identity and public key. In contrast, our certificate is a delegation from issuer to owner and used in IBPS.

*Pseudonym***.** Pseudonym, generated by some cryptographic primitives, is one of user's authentication credentials whereas contains no essential identity information (e.g. SSN or driver's license) of user.

*Ticket***.** Ticket is the other authentication credential hold by mesh router or mesh client. We define three types of ticket for the later proposed authentication scheme.

(1) RTK: Mesh router's ticket which has long-term validity throughout multi-operator WMNs.

(2) CTK: Mesh client's ticket which has long-term validity throughout multi-operator WMNs.

(3) OTK: Mesh client's operator-level ticket which has short-term validity within operator WMNs.

Double deposit. A type of misbehavior that refers to mesh client's double depositing his CTKs at the same visiting mesh router.

Notations. To simplify the hereafter descriptions, we make some notations in Table 1.

Table 1. Notations and explanations

Notation	Meaning
B	Broker
OM (O)	operator manager
MR (R)	mesh router
MC (C)	mesh client
ID_X	real identity of entity X
PS_X	pseudonym of entity X
Cert_X	certificate of entity X
RTK_X	ticket of mesh router X
CTK_X	ticket of mesh client X
OTK_X	operator-level ticket of mesh client X
A_M	account of mesh client
PK_X /SK_X	public and secret key of entity X

$\overrightarrow{PK_X} / \overrightarrow{SK_X}$	self-generated public and secret key of entity X from PS_X
PARA	system parameters
X_{INFO}	Related information of entity X
P_X	Hash value of X_{INFO}
$\{M\}_{\alpha\_Sign\_SK}$	sign message M with algorithm α and secret key SK
$\{\sigma\}_{\beta\_Verify\_PK}$	verify signature σ with algorithm β and public key PK
$K_{X\text{-}Y}$	shared key between entity X and entity Y
$SEK_{X\text{-}Y}$	session key between entity X and entity Y
SKP_X	proxy signing key of entity X
TS	timestamp
Exp	expiration time of ticket or certificate
X→Y:[M]	entity X sends message M to entity Y
M1||M2	concatenation of two messages M1 and M2

3.2. Network Architecture

The three-tire hierarchical network architecture in Fig.2 is set up for multi-operator large-scale WMNs where each operator WMNs is taken as an administrative domain.

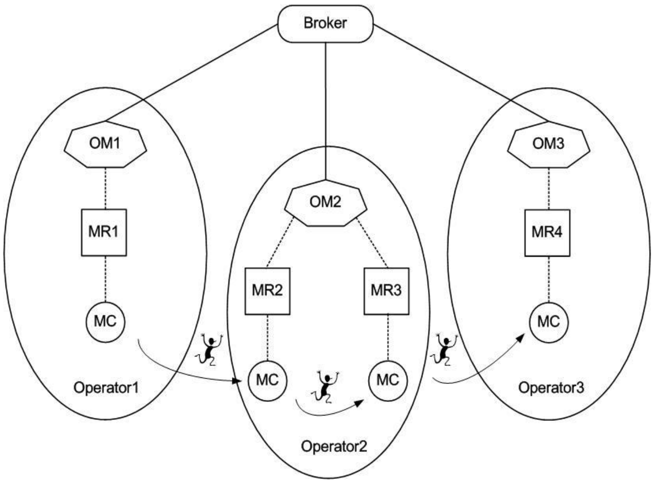

Fig.2 Hierarchical network architecture for multi-operator WMNs, which is composed of three administrative domains

Broker on the top tier of the hierarchical architecture is introduced as a trusted anchor for all domains. The second tier of the architecture is composed of OMs who take the role of connectors between operator domain and broker and is in charge of the registration and trust management for MRs, as well as MCs inside operator domain. In reality, the functionalities of OM can be achieved into mesh gateway who shares reachability to all MRs through either direct or multi-hop wireless links as shown in Fig.1. MRs form the third tire of our security architecture and can provide access service for both local and roaming MCs. MC associated with certain operator may take arbitrary handover across different operator domains under the hierarchical architecture.

From the collaboration point of view, any operator domain in our architecture is able to create relationship with others in order to provide larger-scale coverage and more access opportunities through signing service level agreements (SLAs) by the OMs.

3.3. Trust Model

In the context of multi-operator WMNs, the main security goals include:

- Mutual authentication. Users and visiting network should authenticate each other before user's access to avoid both malicious users and rouge routers.
- Confidentiality. After a successful user access, the subsequent communications between user and entities in the visiting network should be further protected to prevent different attacks such as eavesdropping and modification.

Due to the above security goals and the intrinsically open and collaborative features of multi-operator WMNs, it is essential to establish trust relationships among entities against free riders and malicious attackers.

As shown in Fig.3, our trust model is constructed in terms of the proposed hierarchical network architecture. The trust relationships among entities are defined and elaborated as follows:

- Broker, functions as a trustworthy administrator, is the root trust for all operator domains.
- OMs have long-term trust relationship with broker. Meanwhile, two OMs may also trust each other if they have signed SLA before. The SLA contains all the credible public keys of OM and MRs (PK_O and PK_R) in the other operator domain.
- MRs have long-term trust relationship with the OM in the same operator domain.
- MCs have long-term trust relationship with the OM in their home operator domain.
- There is no trust relationship between MC and MR before MC's access. Two MCs do not trust each other.

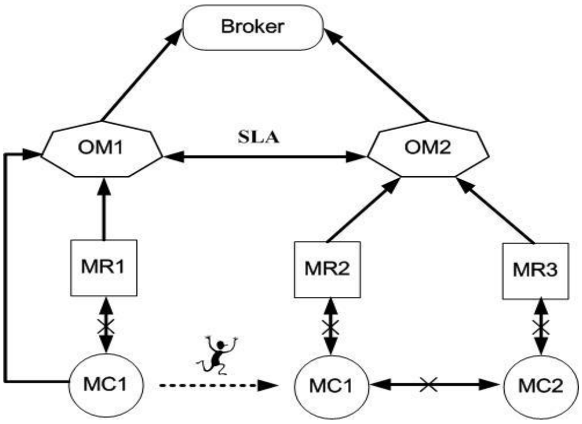

Fig.3 Broker-based trust model

The trust relationship above means that there is a pre-established secure channel between two entities. The later proposed mutual authentication scheme is based on this trust model and the objective is how to build trust relationship between MC and access MR as well as the trust relationships amongst MCs.

It is also worth noting that our trust model is different from the one presented in [3], where broker and operator issue authentication credentials to MCs and MRs separately. Different trust anchors make the trust management more implicit. In contrast, broker takes the role of root trust in our trust model. Any operator could not issue credentials to MRs or MCs without broker's permission and delegation. The trust management is thus more explicit and is suitable for the security control in multi-operator WMNs.

3.4. Privacy Model

In addition to keep access and communication secure, privacy provision is another critical issue to be considered for WMNs deployment. However, privacy is difficult to achieve even if traffics are protected since users' activities can be easily monitored or traced with regard to their movement, which may cause the exposure of the sensitive information. Therefore, the establishment of a practical privacy model is necessary to provide adequate privacy concerns and detect malicious users simultaneously.

Anonymity. User's activities, during the roaming procedure, should not be correlated to his real identity (e.g. SN or driver's license). In our privacy model, we utilize pseudonym and ticket as hybrid authentication credential to achieve user anonymity. Neither pseudonym nor ticket contains real identity of user so that user can roam anonymously in multi-operator WMNs.

Untraceability. For untraceability, it is required that the credential issuer can't trace user's activity during the roaming procedure. Thus both the pseudonym and the ticket should be alerted by user while roaming.

Sophisticated unlinkability. On one hand, from the privacy-preserving point of view, different communication sessions from the same user should not be linked against association analysis. On the other hand, from the user experience point of view, the recognizable credential is preferable in the same operator WMNs or collaborative operator WMNs. For such sophisticated unlinkability, user is equipped with variable pseudonym and temporary operator-level ticket in our privacy model to keep balance between privacy and user experience.

Accountability. Unconditional anonymity may result in perfect crimes since misbehaving users are no longer traceable. Therefore, accountability is highly desirable for detecting and tracing malicious users. We borrow the idea from e-cash system to form a novel ticket management scheme. The real identity of misbehaving user, who double deposits his CTK at the same MR, could be disclosed with the help of broker and OM.

In summary, our privacy model aims at the above privacy guarantees meanwhile takes user experience into account. It's a trade off: giving up some privacy in return for an enhanced user experience.

3.5. System Initialization

In order to support the proposed security framework, our system must be initialized to distribute indispensable system parameters, certificates, as well as key materials to involved entities. Specifically, the following system initialization steps should be performed when the network bootstrapped.

System parameter generation

(1) Broker generates parameter tuple $(G_1, G_2, \hat{e}, P, Q, H, H_1, H_2)$, where P and Q are generators of G_1, $\hat{e}$ is a billiner pairing, hash functions $H : G_2 \to Z_q^*$, $H_1 : \{0,1\}^* \to G_1$, $H_2 : \{0,1\}^* \times G_1 \to Z_q^*$.

(2) Broker randomly selects a master secrect key $SK_B = S_B \in Z_q^*$ and calculates the public key $PK_B = S_B \cdot P$, then publishes the system parameter $PARA$=$(G_1, G_2, \hat{e}, P, Q, H, H_1, H_2, PK_B)$.

OM certificate insurance

(1) Each OM randomly selects a secrect key $SK_O = S_O \in Z_q^*$ and calculates its public key $PK_O = S_O \cdot P$ according to $PARA$.

(2) $O \to B : [PK_O]$

(3) Broker generates certificate for OM: $Cert\_O = S_B \cdot P_O, where\ P_O = H_1(PK_B \,||\, PK_O \,||\, Exp)$.

(4) $\mathrm{B} \to O : [Cert\_O]$

(5) OM calculates the proxy signing key: $SKP_O = Cert\_O + S_O \cdot P_O = (S_B + S_O)P_O$.

MR ticket insurance

(1) Each MR randomly selects a secrect key $SK_R = S_R \in Z_q^*$ and calculates its public key $PK_R = S_R \cdot P$ according to $PARA$.

(2) $\mathrm{R} \to \mathrm{O} : [PK_R]$

(3) OM generates certificate and RTK for managed MR: $Cert\_R = S_O \cdot P_R, where\ P_R = H_1(PK_O \,||\, PK_R \,||\, Exp)$; $RTK\_R =< Exp, PK_B, PK_O, PK_R, \ \sigma >$, where σ=$\{Exp||PK_B||PK_O||PK_R\}_{IBPS\_Sign\_SKP_O}$.

(4) $\mathrm{O} \to \mathrm{R} : [Cert\_R,\ RTK\_R]$

(5) MR calculates the proxy signing key $SKP_R = Cert\_R + S_R \cdot P_R = (S_O + S_R) \cdot P_R$.

Through the above system initialization, OMs and MRs obtain their certificates and proxy signing keys with the delegated right from broker. Besides, MRs are also equipped with the RTKs which will be applied into the following proposed mutual authentication scheme.

4. PPS: The Proposed Scheme

To address the security and privacy concerns in multi-operator WMNs with enhanced user experience, we propose a privacy-preserving mutual authentication scheme, upon the security system, together with accountability capability. The scheme is based on the hybrid employment of pseudonym and ticket to achieve anonymity, untraceability, as well as sophisticated unlinkability. In light of the handover types defined in section 3.1, we take two authentication scenarios (as shown in Fig.2) into account: inter-operator authentication and intra-operator authentication. Shared key establishment is also integrated into PPS to protect subsequent communications in the air and gain more efficiency. In addition, we also consider MC-MC authentication and user accountability issues in multi-operator WMNs. In this section, we will give the details of PPS.

4.1. Pseudonym Generation

The pseudonym is used to hide the real identity of user during the roaming procedure, which is necessary for both anonymity and user experience. Moreover, in order to meet the sophisticated unlinkability need, the pseudonym should also be variable in our design. The widely adopted way to achieve that is to assign a batch of pseudonyms to user and showing one each time [15, 16]. However, the communication and update cost are the main obstacles. In [6], the authors presented a more efficient method. The pseudonym is generated with the help of an authority while can be alerted by user whenever needed. As such, user is able to frequently update his pseudonym to enhance unlinkability. Unfortunately, the authority may learn user’s secret key which is derived from the pseudonym, thus results in the key-escrow problem and violates the untraceability requirement.

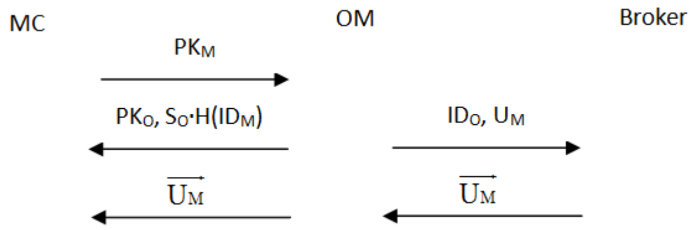

Fig. 4 Workflow of tri-lateral pseudonym generation among MC, OM and Broker

To address the above issues, we propose a tri-lateral pseudonym generation approach as shown in Fig.4. Before the approach bootstrapping, MC first registers the real identity (ID_M) to the home domain OM through either offline method or the pre-established secure channel. Afterwards the following steps are executed for the pseudonym generation.

(1) MC randomly selects a secrect key $SK_M = S_M \in Z_q^*$ and calculates its public key $PK_M = S_M \cdot P$ according to *PARA*.

(2) $\mathrm{M} \rightarrow \mathrm{O} : \left[PK_M \right]$

(3) OM computes $K_{O-M} = \hat{e}(S_O \cdot Q,\ PK_M),$ then derives $k_M = H(K_{O-M}),\ U_M = k_M \cdot H_1(ID_M),\ A_M = S_O \cdot U_M,$ where A_M is MC's account at OM. OM further stores the binding relation $<ID_M,\ A_M,\ k_M,\ U_M>$ for MC.

(4) $\mathrm{O} \rightarrow \mathrm{M} : \left[PK_O,\ A_M,\ S_O \cdot H_1\left(ID_M \right) \right]$

(5) MC computes $K_{M-O} = \hat{e}(S_M \cdot Q, PK_O),$ then derives $k_M = H(K_{M-O}).$

(6) $\mathrm{O} \rightarrow B:\left[ID_O,\ U_M\right]$

(7) Broker computes $\overrightarrow{U_M} = S_B \cdot U_M$

(8) $\mathrm{B} \rightarrow \mathrm{O} \rightarrow \mathrm{M}:\left[\overrightarrow{U_M}\right]$

(9) MC computes $\overrightarrow{U_M} \cdot k_M{}^{-1} = S_B \cdot H_1(ID_M),$ then generates the pseudonym $PS_M = S_M \cdot H_1(ID_M)$ and the correspoding key pair: $\overrightarrow{PK_M} = (S_B + S_O) \cdot H_1(ID_M),\ \overrightarrow{SK_M} = S_M \cdot \overrightarrow{PK_M} = (S_B + S_O) \cdot PS_M.$

A pairing-based key agreement method is incorporated into the above procedure. It can be easily proved that:

$$K_{O\text{-}M} = \hat{e}(S_O \cdot Q, PK_M) = \hat{e}(Q,P)^{S_O \cdot S_M} = \hat{e}(S_M \cdot Q, PK_O) = K_{M\text{-}O}$$

The agreed key ($K_{O\text{-}M}/K_{M\text{-}O}$) and the relevant key material (k_M) are the building blocks of our tri-lateral pseudonym generation approach. Such keys are the secret knowledge shared between MC and OM. We can also find that the pseudonym is self-generated by user with his own secret (S_M) thus can be altered at his will. Meanwhile, the secret key with regard to the pseudonym is composed of broker's secret (S_B) and OM's secret (S_O). The key escrow problem is averted as neither broker nor OM knows the secret key of the other party. Moreover, any MC can sign a message (m) with the generated $\overrightarrow{SK_M}$ using BLS: $\sigma = \{m\}_{\mathrm{BLS\_Sign\_}\overrightarrow{\mathrm{SK_M}}} = \overrightarrow{SK_M} \cdot H_1(m)$. Any party may verify σ using BLS: $\{\sigma\}_{\mathrm{BLS\_Verify\_PS_M\&PK_B\&PK_O}}$.

4.2. Ticket Insurance

Ticket is the other authentication credential in PPS. The insurance of RTK has been presented by in section3.5. We will elaborate CTK's insurance procedure in this section.

PBS is borrowed for the generation and insurance of CTK. The insurance procedure can be carried out locally between MC and OM who owes the delegation from broker. The detailed procedure is demonstrated through the following steps.

(1) OM randomly selects $r \in Z_q^*$ and calculates $R = r \cdot P.$

(2) $\mathrm{O} \rightarrow \mathrm{M}:\left[R,\ O_{INFO}\right],$ where O_{INFO}=<$PK_B,\ PK_O$>.

(3) MC randomly selects $a,\ b,\ \alpha,\ \beta \in Z_q^*$ and $\omega,$ where ω is an agreement between MC and OM such as *Exp* or other restrictions on the CTK.

(4) MC calculates: $d1 = \alpha \cdot PK_O,\ d2 = \beta \cdot PK_O,\ d = \beta \cdot A_M,\ P_O = H_1(PK_B \,\|\, PK_O),\ t = \hat{e}(R + a \cdot P, PK_O) \cdot \hat{e}(b \cdot P_O,\ PK_B + PK_O),\ C' = H_2(d \,\|\, d1 \,\|\, d2 \,\|\, \omega \,\|\, O_{INFO} \,\|\, t) + b$

(5) $\mathrm{M} \rightarrow \mathrm{O}:\left[C'\right].$

(6) OM caculates $S' = C' \cdot SKP_O + r \cdot PK_O.$

(7) $\mathrm{O} \rightarrow \mathrm{M}:\left[S'\right].$

(8) MC first calculates: $S = S' - a \cdot PK_O,\ C = C' - b,\ t' = \hat{e}(S,P) \cdot \hat{e}(-C \cdot P_O,\ PK_B + PK_O),$ then checks whether $C == H_2(d \,\|\, d1 \,\|\, d2 \,\|\, \omega \,\|\, O_{INFO} \,\|\, t'),$ if the equation holds, MC obtains the CTK=<$d,\ d1$, d2,$\omega,\ O_{INFO}$, S, C>; Otherwise, MC quits the procedure.

Actually, <S, C> in CTK is the signature result of PBS on $< d,\ d1$, d2,$\omega,\ O_{INFO} >$ and step (8) is the PBS verification process. CTK together with pseudonym will be utilized during the authentication between MC and visiting MR in PPS.

4.3. Inter-operator Authentication

In Fig.2, while a MC (M), registered with OM1 (O1) in operator1 domain, entering operator2 domain managed by OM2 (O2) and accessing MR2 (R2), inter-operator authentication protocol is executed between MC and MR2 as below.

(1) $\mathrm{R2} \rightarrow \mathrm{M} : [\mathrm{RTK\_R2} =< Exp, PK_B, PK_{O2}, PK_{R2}, \sigma 1 = \{Exp \| PK_B \| PK_{O2} \| PK_{R2}\}_{\mathrm{IBPS\_Sign\_SKP_{O2}}} >]$ through beacon message.

(2) MC executes the following operations:

- Check the validity of Exp in RTK_R2;
- Verify $\sigma 1$ with PK_B and PK_{O2} : $\{\sigma 1\}_{\mathrm{IBPS\_Verify\_PK_B\&PK_{O2}}}$;
- Computes $K_{M\text{ - }R2} = \hat{e}(\overrightarrow{SK_M}, PK_{R2})$.

(3) $\mathrm{M} \rightarrow \mathrm{R2} : [PS_M,\ \mathrm{CTK\_M} =< d,\ d1,\ \mathrm{d}2,\ \omega{=}Exp,\ O1_{INFO} =< PK_B,\ PK_{O1} >, S,\ C>,\ t1,\ \sigma 2 = \{\mathrm{CTK\_M} \,\|\, t1\}_{BLS\_Sign\_\overline{SK_M}}]$, where $t1$ is the current timestamp.

(4) MR2 executes the following operations:

- Check the validity of Exp in CTK_M and the freshness of $t1$;
- Verify $\sigma 2$ with $PK_B,\ PK_{O1},\ PS_M$: $\{\sigma 2\}_{\mathrm{BLS\_Verify\_PK_B\&PK_{O1}\&PS_M}}$;
- Verify $< S,\ C >$ in CTK_M with $\mathrm{PK_B}$, $\mathrm{PK_{O1}}$: $\{\mathrm{S, C}\}_{\mathrm{PBS\_Verify\_PK_B\&PK_{O1}}}$;
- Compute $K_{R2-M} = \hat{e}(S_{R2} \cdot PS_M, PK_B + PK_{O1})$.

(5) $\mathrm{R2} \rightarrow \mathrm{M} : \left[e,\ t2,\ \sigma 3 = \{e \,\|\, t2\}_{\mathrm{HMAC\_Sign\_K_{R2\text{-}M}}}\right],$ where e is a challenge selected from $\{0,1\}^*$ and $t2$ is the current timestamp.

(6) MC executes the following operations:

- Check the freshness of t2;
- Verify $\sigma 3$ with $K_{M\text{ - }R2}$: $\{\sigma 3\}_{\mathrm{HMAC\_Verify\_K_{M\text{-}R2}}}$. If the verification success, MC regards MR2 as a legitimate MR.
- Computes: $u = H_2(CTK\_M \,\|\, e \,\|\, d2), v = \beta + \alpha \cdot u.$

(7) $\mathrm{M} \rightarrow \mathrm{R2} : [u,\ \mathrm{v},\ \mathrm{t3},\ \sigma 4 = \{u \,\|\, v \,\|\, t3\}_{\mathrm{HMAC\_Sign\_K_{M\text{-}R2}}}]$, where $t3$ is the current timestamp.

(8) MR2 executes the following operations:

- Check the freshness of t3;
- Verify $\sigma 4$ with K_{R2-M}: $\{\sigma 4\}_{\mathrm{HMAC\_Vverify\_K_{R2\text{-}M}}}$;
- Compute $t' = \hat{e}(S,P) \cdot \hat{e}(-C \cdot P_{O1},\ PK_B + PK_{O1})$;
- Check whether $u == H_2(CTK\_M \,\|\, e \,\|\, v \cdot PK_{O1} \text{-} u \cdot d1)$ and $C == H_2(d \,\|\, d1 \,\|\, v \cdot PK_{O1} \text{-} u \cdot d1 \,\|\, Exp \,\|\, O1_{INFO} \,\|\, t')$.
- If all the equations hold, MR2 regards MC as a legitimate user and stores <CTK_M, e, u, v > for MC.

(9) $\mathrm{R2} \rightarrow \mathrm{M} : [OTK\_M =< PS_M,\ R2_{INFO},\ PK_{O1}, Exp,\ t4,\ \sigma 5 = \{PS_M || R2_{INFO} || Exp || t4\}_{\mathrm{IBPS\_Sign\_SKP_{R2}}} >]$, where $R2_{INFO} =< PK_{O2},\ PK_{R2} >$ and $t4$ is the current timestamp.

(10) MC does the followings:

- Check the freshness of t4;
- Verify $\sigma 5$ in OTK_M with PK_B, PK_{O2}, and PK_{R2} : $\{\sigma 5\}_{\mathrm{IBPS\_Verify\_PK_{O2}\&PK_{R2}}}$. If the verification success, MC obtains OTK_M as a legitimate OTK.

After the inter-operator authentication, MC and MR2 are able to generate their session key $\mathrm{SEK_{M\text{-}R2}=H(K_{M\text{-}R2}||t1||t2)}$ respectively to protect the subsequent communications.

It should be noted that the HMAC [17] operations introduced above are symmetric-key method which is much more efficient than the public-key ones as BLS, IBPS, as well as PBS. In addition, in order to achieve untraceability and unlinkability across operators, the pseudonym should be altered by MC each time when accessing a new operator domain. After successful mutual authentication between MC and MR2 through steps (1)-(8), MR2 directly issues OTK to MC (by step (9)) with the proxy signing key ($\mathrm{SKP_{R2}}$) delegated from OM2 and broker. This OTK will be utilized as an authentication credential during the following intra-operator authentication scheme.

4.4. Intra-operator Authentication

Intra-operator authentication occurs while MC (M) moves from MR2 (R2) to MR3 (R3) within operator2 domain managed by OM2 (O2) as shown in Fig.2. The authentication protocol is as below.

(1) $\mathrm{R3} \rightarrow \mathrm{M} : [\mathrm{RTK\_R3} =< Exp, PK_B, PK_{O2}, PK_{R3}, \sigma 6 = \{Exp || PK_B || PK_{O2} || PK_{R3}\}_{\mathrm{IBPS\_Sign\_SKP_{O2}}} >]$ through beacon message.

(2) MC verifies $\sigma 6$ in RTK_R3 with PK_B and PK_{O2} : $\{\sigma 6\}_{\mathrm{IBPS\_verify\_PK_B\&PK_{O2}}}$, then computes $K_{M\text{ - }R3} = \hat{e}(\overrightarrow{SK_M}, PK_{R3})$.

(3) $\mathrm{M} \rightarrow \mathrm{R3} : [\mathrm{OTK\_M} =< PS_M, PK_{O1}, R2_{INFO},\ Exp,\ t4, \sigma 5 = \{PS_M || PK_{O1} || R2_{INFO} || Exp || t4\}_{\mathrm{IBPS\_Sign\_SKP_{R2}}}>,$ $t5,\ \sigma 7 = \{\mathrm{OTK\_M} || t5\}_{HMAC\_Sign\_K_{M-R3}}]$, where $t5$ is the current timestamp.

(4) MR3 executes the following operations:

- Check the validity of Exp in OTK_M and the freshness of $t5$;
- Verify $\sigma 5$ with PK_{O2} and PK_{R2}: $\{\sigma 5\}_{\mathrm{IBPS\_Verify\_PK_{O2}\&PK_{R2}}}$;
- Compute $K_{R3-M} = \hat{e}(S_{R3} \cdot PS_M, PK_B + PK_{O1})$;
- Verify $\sigma 7$ with K_{R3-M}: $\{\sigma 7\}_{\mathrm{HMAC\_verify\_K_{R3\text{-}M}}}$;
- If all the above verifications hold, MR3 regards MC as a legitimate user.

(5) $\mathrm{R3} \rightarrow \mathrm{M} : \left[t6,\ \sigma 8 = \{t6\}_{\mathrm{HMAC\_Sign\_K_{R3\text{-}M}}}\right]$, where $t6$ is the current timestamp.

(6) MC executes the following operations:

- Check the freshness of t6;
- Verify $\sigma 8$ with $K_{M\text{ - }R3}$: $\{\sigma 8\}_{\mathrm{HMAC\_Verify\_K_{M\text{-}R3}}}$. If the verification success, MC regards MR3 as a legitimate MR.

When the intra-operator authentication finished, MC and MR3 are able to generate their session key $SEK_{M\text{-}R3}=H(K_{M\text{-}R3}||t5||t6)$ respectively to protect the subsequent communications.

OTK is effective within the operator domain. We can see from the above intra-operator authentication that the deposit and verification of OTK are based on HMAC and IBPS operations which are more efficient than the PBS process on CTK. Besides, MC may keep the pseudonym unchanged in the same operator domain in order to gain better user experience. However, from the unlinkability point of view, MC could also choose to show CTK and new generated pseudonym at accessing MR to allow frequent update of OTK.

Another issue should be considered is that MC handoffs across two cooperated operator domains. In our trust model, the OM of the two domains shares the trusted public keys (PK_O, PK_R) in the other domain through SLA. Theses public keys are further distributed to the managed MRs periodically by OM. For example, if operator2 and operator3 (in Fig.2) are cooperated, then OM3 will record the trusted PK_{O2}, PK_{R2}, PK_{R3} and broadcast them to MR4, vice versa. In light of this, OTK_M is still effective in operator3 domain though MC makes an inter-operator domain handover from MR3 to MR4, since MR4 is able to verify such OTK_M with PK_{O2} and PK_{R2} using the same operations in intra-operator authentication scheme.

4.5. MC-MC Authentication

There is no pre-established trust relationship between two MCs. As a consequence, privacy-preserving MC-MC authentication and key agreement are critical. Fortunately, with the help of the above proposed authentication schemes, MC-MC authentication can be easily implemented.

Suppose that two MCs (M1, M2) registered to different OMs (O1, O2) hold their CTKs (CTK_M1, CTK_M2) respectively. Mutual authentication between M1 and M2 is achieved as the inter-operator authentication scheme along with following steps.

(1) $\mathrm{M1} \to \mathrm{M2}: [\mathrm{PS_{M1}},\ \overrightarrow{\mathrm{SK_{M1}}} \cdot \mathrm{P},\ \mathrm{CTK\_M1} = <\mathrm{d},\ \mathrm{d1},\ \mathrm{d2},\ \omega\text{=Exp},\ \mathrm{O1_{INFO}} = <\mathrm{PK_B},\ \mathrm{PK_{O1}}>,\ \mathrm{S},\ \mathrm{C}>,$ $\mathrm{t7}, \sigma 9 = \{\mathrm{CTK\_M1} \,||\, \overrightarrow{\mathrm{SK_{M1}}} \cdot \mathrm{P} \,||\, \mathrm{t7}\}_{\mathrm{BLS\_Sign\_}\overline{\mathrm{SK_{M1}}}}]$, where t7 is the current timestamp.

(2) M2 executes the following operations:

- Check the validity of *Exp* in CTK_M1 and the freshness of t7;
- Verify $\sigma 9$ with $PK_B,\ PK_{O1},\ PS_{M1}$: $\{\sigma 9\}_{\mathrm{BLS\_Verify\_PK_B\&PK_{O1}\&PS_{M1}}}$;
- Verify $<S,\ C>$ in CTK_M1 with $\mathrm{PK_B}$, $\mathrm{PK_{O1}}$: $\{\mathrm{S, C}\}_{\mathrm{PBS\_Verify\_PK_B\&PK_{O1}}}$;
- If all the verification success, M2 regards M1 as a legitimate MC;
- Compute $K_{M2-M1} = \hat{e}(\overrightarrow{\mathrm{SK_{M2}}} \cdot Q,\ \overrightarrow{\mathrm{SK_{M1}}} \cdot \mathrm{P})$.

(3) $\mathrm{M2} \to \mathrm{M1}: [\mathrm{PS_{M2}},\ \overrightarrow{\mathrm{SK_{M2}}} \cdot \mathrm{P},\ \mathrm{CTK\_M2} = <\mathrm{d}',\ \mathrm{d1}',\ \mathrm{d2}',\ \omega\text{=Exp}',\ \mathrm{O1_{INFO}} = <\mathrm{PK_B},\ \mathrm{PK_{O2}}>,\ \mathrm{S}',$ $\mathrm{C}'>,\ \mathrm{t8}, \sigma 10 = \{\mathrm{CTK\_M2} \,||\, \overrightarrow{\mathrm{SK_{M2}}} \cdot \mathrm{P} \,||\, \mathrm{t8}\}_{\mathrm{BLS\_Sign\_}\overline{\mathrm{SK_{M2}}}}]$, where t8 is the current timestamp.

(4) M1 executes the following operations:

- Check the validity of Exp' in CTK_M2 and the freshness of t8;
- Verify $\sigma 10$ with PK_B, PK_{O2}, PS_{M2}: $\{\sigma 10\}_{BLS\_Verify\_PK_B\&PK_{O2}\&PS_{M2}}$;
- Verify $< S', C' >$ in CTK_M2 with PK_B, PK_{O2}: $\{S', C'\}_{PBS\_Verify\_PK_B\&PK_{O2}}$;
- If all the verification success, M1 regards M2 as a legitimate MC;
- Compute $K_{M1-M2} = \hat{e}(\overrightarrow{SK_{M1}} \cdot Q, \overrightarrow{SK_{M2}} \cdot P)$.

It is obvious from the above operations that

$$K_{M1-M2} = \hat{e}(\overrightarrow{SK_{M1}} \cdot Q, \overrightarrow{SK_{M2}} \cdot P) = \hat{e}(Q,P)^{\overrightarrow{SK_{M1}} \cdot \overrightarrow{SK_{M2}}} = \hat{e}(\overrightarrow{SK_{M2}} \cdot Q, \overrightarrow{SK_{M1}} \cdot P) = K_{M2-M1}.$$

After the MC-MC authentication finished, M1 and M2 generate their session key $SEK_{M1\text{-}M2}$=H($K_{M1\text{-}M2}$||t7||t8) respectively to protect the subsequent communications.

4.6. User Accountability

PPS achieves fine user privacy through the combination of pseudonym and ticket, while still maintaining user accountability. In PPS, MC authenticates himself as a legitimate service subscriber to the OM (O_H) in the home operator domain. The real identity of MC (ID_M) and his account (A_M) are only known by himself and O_H. Neither the visiting OM (O_V) nor the broker has knowledge of MC's privacy information during his roaming. However, from the accountability point of view, it is necessary to detect malicious MCs. As described in our system model, MC's misbehavior is defined as his double depositing the CTKs at the same visiting mesh router (R_V).

Assume that a MC accesses a foreign operator WMNs and double deposits his CTKs (CTK1, CTK2) to a R_V. Then two authentication records will be left at R_V according to the proposed inter-operator authentication scheme: Record1 <CTK1, e1, u1, v1> and Record2 <CTK2, e2, u2, v2>. In order to disclose the identity of such malicious MC, the following operations are executed with the collaboration of R_V, O_V, O_H, as well as broker.

(1) $R_V \rightarrow O_V \rightarrow B : [Record1, Record2]$.

(2) Broker deduces between Record1 and Record2 to compute $\beta = \frac{u2 \cdot e1 - u1 \cdot e2}{e1 - e2}$, broker further obtains $A_M = \beta^{-1} \cdot d$, where d is in MC's CTK.

(3) $B \rightarrow O_H : [A_M]$.

(4) O_H obtains $U_M = S_{O_H}{}^{-1} \cdot A_M$, thus to discolse ID_M through the binding relation <ID_M, A_M, k_M, U_M> stored during the pseudonym generation phase.

The implementation of the above user accountability function is due to the features of e-cash system based on PBS.

5. System Analysis

5.1. Security and privacy analysis

Authenticity. Mutual authentication is achieved in PPS to avert both free riders and bogus service providers. MC is equipped with pseudonym and ticket issued by OM under the delegation from broker. Owing such authentication credentials, MC is able to roam securely across multi-operator WMNs in light of the root trust to broker. In addition, the proposed inter-operator authentication scheme and intra-operator authentication scheme are implemented locally between MC and visiting MR for better efficiency.

Confidentiality. Communicating entities establish a shared symmetric key and the corresponding session key to secure their subsequent communications after authentication. In PPS, we adopt pairing-based key agreement approach to construct such keys between MC and the visiting MR. The symmetric key is also used in the mutual authentication protocols together with HMAC operations in order to mitigate the computation burden on both MC and MR sides.

Anonymity. MC takes pseudonym and CTK as the authentication credentials during the roaming procedure. While the pseudonym is composed of MC's own secret and the hash value of MC's identity information: $PS_M = S_M H_1(ID_M)$.

The $CTK =< d, d1, d2, \omega, O_{INFO}, S, C >$ contains some cryptographic results derived from MC's account (AM) and public keys of OM and broker, as well as the PBS signature on them. Neither pseudonym nor CTK comprises real identity of MC so that the anonymity is guaranteed during MC's roaming. Moreover, MC is also unable to know the real identity of the visiting MR since such information is not included in the $RTK =< E\text{xp}, PK_B, PK_O, PK_R, \sigma >$. Thus the anonymity is bidirectional.

Untraceability. Untraceability requires that the credential issuer can't trace MC's activity when he is roaming. On one hand, the pseudonym in PPS can be alerted by MC at his will to avoid the traceability from OM and broker. On the other hand, MC's CTK is also different between the insurance phase and the showing phase due to the non-key escrow feature of PBS. Consequently, OM cannot trace MC's activity through the CTK.

Sophisticated unlinkability. Sophisticated unlinkability is preferable in order to give consideration to both privacy-preserving and user experience. In PPS, when MC roaming across different operator WMNs, although the CTK remains unchanged, while the pseudonym is required to be alerted by MC. Thus the adversary is unable to link different communication sessions to the same user. In addition, MC will obtain a temporary OTK after the inter-operator authentication procedure. Owing such OTK and a constant pseudonym, MC can gain better user experience within the same operator WMNs.

User accountability. User accountability is so important in PPS for detecting malicious users. To achieve this, for a legitimate MC, none of the entities, including broker, OMs, as well as MRs, could disclose the real identity of MC in terms of the above anonymity and untraceability features. However, if MC double deposits his CTK at a visiting MR which is defined as misbehavior, upon the collusion of visiting OM, broker, and home OM, the real identity of malicious MC can be exposed with the help of the accountability function borrowed from PBS-based e-cash system.

5.2. Performance Analysis

In this section, the performance analysis of our scheme, PPS, in terms of communication and computation overhead is presented compared with the similar security approach of SAT [6] which also utilizes pseudonym and ticket as hybrid authentication credentials. Our analysis takes both inter-operator and intra-operator authentication scenarios into account. In addition, since the resource-constraint mesh client is the performance bottleneck of the whole system, our performance analysis is thus mainly focus on the mesh client side.

Without loss of generality, we borrow the parameters from [6] and [18] in the following analysis, resulting in the elements length in G_1 ($|G_1|$) and G_2 ($|G_2|$) to be roughly 171 bits and 1024 bits respectively. We also assume that SHA-1[19] is used in our HMAC operations, that yields a 160-bit output.

Communication Overhead. Communication overhead refers to the communication cost incurred by MC during the authentication procedure. The overhead is mainly composed of the pseudonym, ticket, signature, as well as HMAC result transmitted from MC side, where the shorter components are out of consideration compared with the above ones, such as the *Exp* and *TS*.

Inter-operator Communication Overhead. In SAT, a tree-based hierarchical security architecture and pseudonym approach is proposed. Both hierarchical pseudonym (PST_M) and client pseudonym (PS_M) should be transmitted by MC during inter-operator authentication. SAT introduces a ticket based on restrictive partially blind signature [20]. The total ticket length is $5|G_1|+2|G_2|$. In contrast, only one self-generated pseudonym is involved in inter-operator authentication in PPS contributed to our delegated trust model. Moreover, the CTK in PPS is signed with PBS, which makes the total ticket length $6|G_1|$. As a consequence, our ticket length is greatly reduced compared with SAT since $|G_2|$ is much longer than $|G_1|$. In light of the above analysis, we can observe from Table 2 that the inter-operator communication overhead of PPS outperforms SAT greatly over 59%.

Intra-operator Communication Overhead. There is no need of hierarchical pseudonym during the intra-operator authentication in SAT. However the same ticket ($5|G_1|+2|G_2|$) as in inter-operator authentication is still necessary. As described in section 4.4, an OTK ($6|G_1|$) is transmitted by MC instead of CTK ($6|G_1|$) plus pseudonym ($1|G_1|$) during intra-operator authentication in PPS, which will further reduces the communication overhead.

As shown in Table 3, the intra-operator communication overhead of PPS drops down almost 67% compared with that of SAT.

Table 2. Analysis results of inter-operator communication overhead

Scheme	Inter-operator communication overhead	Total bits
SAT	PST_M: 1|G_1| PS_M: 1|G_1| Key material: 1|G_1| σ_{HIBS}: 1|G_1| Ticket: 5|G_1|+2|G_2| σ_{HMAC}: 1|HMAC| **Total: 9|G_1|+2|G_2|+|HMAC|**	3747
PPS	PS_M: 1|G_1| CTK: 6|G_1| σ_{BLS}: 1|G_1| σ_{HMAC}: 1|HMAC| **Total: 8|G_1|+|HMAC|**	1528

Note: σ_{HIBS}, σ_{HMAC}, σ_{BLS} denote the signature results from HIBS [21], HMAC, and BLS respectively.

Table 3. Analysis results of intra-operator communication overhead.

Scheme	Intra-operator communication overhead	Total bits
SAT	PS_M: 1|G_1| 2σ_{BLS}: 2|G_1| Ticket: 5|G_1|+2|G_2| σ_{HMAC}: 1|HMAC| **Total: 8|G_1|+2|G_2|+|HMAC|**	3576
PPS	OTK: 6|G_1| σ_{HMAC}: 1|HMAC| **Total: 6|G_1|+|HMAC|**	1186

Table 4. Computational cost of the operations on MC side during authentication.

	SM	PA	BP	MG	MTP	Hash
BLS_s	1	N/A	N/A	N/A	1	N/A
BLS_v	N/A	N/A	2	N/A	1	N/A
$HIBS_s$	1	1	N/A	N/A	1	N/A
$HIBS_v$	N/A	N/A	3	2	1	N/A
$IBPS_s$	2	N/A	N/A	N/A	N/A	1
$IBPS_v$	1	2	2	N/A	N/A	1
$HMAC_s$	N/A	N/A	N/A	N/A	N/A	1
$HMAC_v$	N/A	N/A	N/A	N/A	N/A	1
KA	N/A	N/A	1	N/A	N/A	N/A

Note: $BLS_{s/v}$, $HIBS_{s/v}$, $IBPS_{s/v}$ denote the signing and verifying operations of each schemes respectively. KA denotes the key generation operation.

Computation Overhead. Communication overhead refers to the computation cost experienced at MC side during the authentication procedure, which mainly caused by the signing, verifying, as well as key generating operations. The involved operations consist of bilinear pairing (BP), scale multiplication (SM), point addition (PA), multiplication in group (MG), map to point function (MTP), and hash function (Hash). We first report the cost of these operations in Table 4 for the consequent analysis.

Inter-operator Computation Overhead. Table 5 shows the computation operations involved in the inter-operator authentication of SAT and PPS. With the correlated observation from Tab.4 and Table 5, we can draw the following conclusions:

$$IRCO_{SAT}=4BP+2MTP+1SM+1PA+2MG+1Hash \qquad (1)$$

$$IRCO_{PPS}=3BP+1MTP+2SM+2PA+3Hash \qquad (2)$$

where $IRCO_{SAT}$ and $IRCO_{PPS}$ represent the inter-operator computation overhead of SAT and PPS respectively.

Table 5. Analysis results of inter-operator computation overhead.

Scheme	BLS_s	$HIBS_s$	$HIBS_v$	$IBPS_v$	$HMAC_s$	$HMAC_v$	KA
SAT	N/A	1	1	N/A	1	N/A	1
PPS	1	N/A	N/A	1	1	1	1

Let t_x denote the computational cost of operation x. According to [22-23], t_{PA}, t_{MG}, and t_{Hash} are negligible compared with t_{BP} ,t_{MTP}, and t_{SM}. In addition, based on the analysis results in [24], we also get the following conclusions:

$$t_{BP} =2\ t_{MTP} =3t_{SM} \qquad (3)$$

Through equations (1)-(3), we obtain that $IRCO_{PPS}$ is about 78% of $IRCO_{SAT}$ since less BP operations are involved in PPS than in SAT.

Intra-operator Computation Overhead. The computation operations deal with the intra-operator authentication of SAT and PPS are shown as Table 6. The following conclusions are able to be obtained through the combination of Table 4 and Table 6.

$$IACO_{SAT}=4BP+2MTP+1SM+2MG+1Hash \qquad (4)$$

$$IACO_{PPS}=3BP+1SM+2PA+3Hash \qquad (5)$$

where $IACO_{SAT}$ and $IACO_{PPS}$ represent the intra-operator computation overhead of SAT and PPS respectively.

Table 6. Analysis results of intra-operator computation overhead

Scheme	$\mathbf{BLS_s}$	$\mathbf{HIBS_s}$	$\mathbf{HIBS_v}$	$\mathbf{IBPS_v}$	$\mathbf{HMAC_s}$	$\mathbf{HMAC_v}$	KA
SAT	1	N/A	1	N/A	1	N/A	1
PPS	N/A	N/A	N/A	1	1	1	1

Through equations (3)-(5), $IACO_{PPS}$ is only 62.5% of $IACO_{SAT}$ as the computation consuming operations in PPS are further mitigated during intra-operator authentication.

Though PPS owes better computation overhead compared with SAT from the above analysis. We can still see some computation intensive BP operations in PPS. However, many literature efforts have been made to speedup BP computation either by software or hardware means. For example, in [32], the authors propose a set of software optimizations for BP computation and demonstrate the feasibility of integrating BP-based security approaches into wireless network. The performance results show that it only take 0.14s for BP computation even on Imote2 embedded platform [33]. The authors of [34] also present the FPGA implementation of BP on mobile device which only needs 1.07ms for the computation. Such realizations are able to make PPS more practical in multi-operator WMNs against the heavy computation overhead.

6. Related work

Security and privacy issues in WMNs have gained considerable research focus in the literature. Most of these efforts fall in the scope of addressing the general security and privacy issues or establishing cross-domain security architecture.

Some efforts depend on identity manipulation approaches to satisfy the security and privacy requirements in WMNs. [18] organizes mobile users into different groups, the identity information is only known to the user and the group manager. The anonymity and unlikability are achieved through the variant short group signature [25] and late binding scheme. In terms of the feature of group signature, user accountability is also implemented with the collusion of domain manager and group manager. However, the key escrow problem is still existed and high computation cost is obligatory on user side. Ahmet Onur Durahim et al. [26-27] introduce an authority that is responsible of issuing pseudonym for mobile user as authentication credential. They utilize DAA [28] to achieve the anonymity and untraceability during user's roaming. Furthermore, the malicious users can be tracked by the collusion of the authority and domain manager. While the scheme suffers from the public key management problem inherited from PKI.

Other efforts take cross-domain authentication issues into account. Wang Z. et al. [29] propose a security architecture and trust model regards to cross-domain scenarios. The hierarchical credential is designed for user anonymity and cross-domain authentication. In addition, the certificateless cryptographic approach [30] is adopted in the authentication procedure to avert the key-escrow problem. Unfortunately, the other privacy requirements beyond anonymity, such as unlinkability, untraceability, accountability, are not involved in the scheme. [6] brings another cross-domain hierarchical security architecture for WMNs based on HIBS scheme. Most of the privacy requirements are also satisfied due to the usage of partially blind signature scheme. However, some drawbacks in accountability procedure of [6] have been pointed out by [31].

In summary, the literature research are mainly focus on the security and privacy issues of WMNs, few of them take multi-operator scenarios and user experience into the design account. These are the motivations for us to provide our privacy-preserving security scheme with fine user experience for multi-operator WMNs.

7. Conclusion

In this paper, we propose PPS, a privacy-preserving security scheme for multi-operator WMNs, which addresses the conflicting privacy requirement of unlinkability and fine user experience. By hybrid utilization of the tri-lateral variable pseudonym approach and different kinds of tickets under identity-based proxy signature (IBPS) and proxy blind signature (PBS), anonymity, untraceability, as well as sophisticated unlinkability are satisfied during MC's roaming. User accountability is also achieved through PBS-based e-cash system that is incorporated into our mutual authentication protocols equipped with key agreement features. Our analysis shows that PPS is able to implement desired security objectives and high efficiency.

As a future work, intensive simulations of PPS, e.g. on NS3 [35], should be made to further demonstrate its feasibility. We also plan to develop location privacy approach and anonymous routing scheme for multi-operator WMNs upon our hierarchical security architecture.

Acknowledgements. This work was supported by Major National Scientific & Technological Projects of China under Grant No. 2013ZX03002006.

References

1. Jaydip Sen: Secure and Privacy-Preserving Authentication Protocols for Wireless Mesh Networks. Book Chapter in Applied Cryptography and Network Security, 3-34. (2012)
2. Ze Wang, Maode Ma, Wenju Liu, Xixi Wei: A Unified Security Framework for Multi-domain Wireless Mesh Networks, Lecture Notes in Computer Science, Vol. 7043, 319-329. (2011)
3. Yanchao Zhang, Yuguang Fang: ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks. IEEE journal on selected areas in communications, 24(10): 1916-1928. (2006)
4. Tianhan Gao, Nan Guo, Kangbin Yim: LEAS: Localized Efficient Authentication Scheme for Multi-operator Wireless Mesh Network with Identity-based Proxy Signature. Mathematical and Computer Modeling, Volume 58, Issues 5–6, 1427-1440. (2013)
5. Bo Gyeong Kang, Je Hong Park, Sang Geun Hahn: A Certificate-Based Signature Scheme. In Proceedings of The Cryptographer's Track at RSA Conference - CT-RSA, 99-111. (2004)
6. Jinyuan Sun, Chi Zhang, Yanchao Zhang: SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks. IEEE Transactions on Dependable and Secure Computing, Vol. 8, No. 2, 295-307. (2011)
7. When Privacy and Enhanced User Experience Collide Online. [Online]. Available: http://inklingmedia.net/2013/01/10/when-privacy-and-enhanced-user-experience-collide-online/(current July 2014)

8. Zuowen Tan: An E-Cash Scheme Based on Proxy Blind Signature from Bilinear Pairings. Journal of Computers, Vol.5, No. 11, 1638-1645. (2010)
9. Joseph H. Silverman: The Arithmetic of Elliptic Curves. Springer. (2009)
10. Antoine Joux: The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems Survey. In Proceedings of the 5th International Symposium on Algorithmic Number Theory (ANTS-V), LNCS 2369, 11-18. (2002)
11. Dan Boneh, Ben Lynn, Hovav Shacham: Short Signatures from the Weil Pairing. In Proceedings of ASIACRYPT - ASIACRYPT , 514-532. (2001)
12. M. Mambo, K. Usuda, E. Okamoto. Proxy signatures: delegation of the power to sign messages. Transactions on Fundamentals of Electronic Communications and Computer Science, vol. E79-A, 1338-1354. (1996)
13. Craig Gentry: Certificate-Based Encryption and the Certificate Revocation Problem. In Proceedings of Theory and Application of Cryptographic Techniques - EUROCRYPT , 272-293. (2003)
14. C. Adams, S. Farrell, T. Kause, T. Mononen: Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP). RFC4210. (2005)
15. M. Raya, J-P. Hubaux: Securing Vehicular Ad Hoc Networks,Journal of Computer Security. special issue on security of ad hoc and sensor networks, Vol. 15, No. 1, 39-68. (2007)
16. G. Ateniese, A. Herzberg, H. Krawczyk, G. Tsudik: Untraceable Mobility or How to Travel Incognito. Computer Networks,Vol. 31, No. 8, 871-884. (1999)
17. H. Krawczyk, M. Bellare, R. Canetti: HMAC: Keyed-Hashing for Message Authentication. RFC2104. (1997)
18. Kui Ren, Shucheng Yu, Wenjing Lou, Yanchao Zhang: PEACE: A Novel Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks. IEEE Transactions on Parallel and Distributed Systems, Vol. 21, No. 2, 203-215. (2010)
19. D. Eastlake, P. Jones: US Secure Hash Algorithm 1 (SHA1). RFC3174. (2001)
20. X. Chen, F. Zhang, and S. Liu: ID-Based Restrictive Partially Blind Signatures and Applications. Journal of Systems and Software, vol. 80(2), 164-171. (2007)
21. Craig G, Alice S: Hierarchical ID-based cryptography. In: Proc. of the 8th Int'l Conf. on the Theory and Application of Cryptology and Information Security. LNCS 2501, 548-566. (2002)
22. Sandip Vijay, Subhash C. Sharma: Threshold signature cryptography scheme in wireless ad-hoc computing. Contemporary Computing, 40 (7), 327–335. (2009)
23. Mohamed Abid, Songbo Song, Hassnaa Moustafa, Hossam Afifi: Integrating identity-based cryptography in IMS service authentication. International Journal of Network Security and Its Applications, 1–13. (2010)
24. Tianhan Gao, Nan Guo, Kangbin Yim: A Hybrid Approach to Secure Hierarchical Mobile IPv6 Networks. Computer Science and Information Systems, Vol. 10 No. 2, 913-938. (2013)
25. D. Boneh and H. Shacham: Group Signatures with Verifier-Local Revocation. In Proc. ACM Conf. Computer and Comm. Security (CCS), 168-177. (2004)
26 Ahmet Onur Durahim, Erkay Savas: A-MAKE: An Efficient, Anonymous and Accountable Authentication Framework for WMNs. In Proceedings of Fifth International Conference on Internet Monitoring and Protection, 54-59. (2010)
27. Ahmet Onur Durahim, Erkay Savas: A2-MAKE: An efficient anonymous and accountable mutual authentication and key agreement protocol for WMNs. Ad Hoc Networks 9(7): 1202-1220. (2011)
28. E. F. Brickell, J. Camenisch, and L. Chen: Direct anonymous attestation. In Proc. of ACM CCS 04, 132–145. (2004)
29. Ze Wang, Maode Ma, Wenju Liu, Xixi Wei: A Unified Security Framework for Multi-domain Wireless Mesh Networks, Lecture Notes in Computer Science, Vol. 7043, 319-329. (2011)
30. Al-Riyami, S.S., Paterson, K.G: Certificateless Public Key Cryptography. In: Laih, C.-S.(ed.) ASIACRYPT 2003, LNCS, vol. 2894, 452–473. (2003)

31. Huaqun Wang,Yuqing Zhang: On the Security of a Ticket-Based Anonymity System with Traceability Property in Wireless Mesh Networks. IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 3, 443-446. (2012)
32. Leonardo B. Oliveira, Diego F. Aranha, Conrado P.L. Gouvêa, Michael Scott, Danilo F. Câmara, Julio López , Ricardo Dahab: TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks, Computer Communications, Vol. 34, No. 3, 485–493. (2011)
33. L. Nachman, R. Kling, R. Adler, J. Huang, V. Hummel: The intel mote platform: abluetooth-based sensor network for industrial monitoring. In Proceedings of Fourth International Symposium on Information Processing in Sensor Networks, 437–442. (2005)
34. Sylvain D, Nicolas G: A FPGA pairing implementation using the residue number system. Cryptology ePrint Archive. (2011). [Online]. Available: http://eprint.iacr.org/2011/176 (current July 2014)
35. George F. Riley, Thomas R. Henderson: The ns-3 Network Simulator, Modeling and Tools for Network Simulation, 15-34. (2010)

Tianhan Gao received the BE in Computer Science & Technology, the ME and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2006, respectively. He joined Northeastern University in April 2006 as a lecture of Software College. He obtained an early promotion to an associate professor in January 2010. He has been a visiting scholar at department of Computer Science, Purdue, from February 2011 to February 2012. He is the author or co-author of more than 30 research publications. His primary research interests are next generation network security, MIPv6/HMIPv6 security, wireless mesh network security, Internet security, as well as security and privacy in ubiquitous computing.

Nan Guo received the BE in Computer Science & Technology, the ME and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2005, respectively. She joined Northeastern University in September 2005. She has been an associate professor since 2008. She has been a visiting scholar at department of Computer Science, Purdue, from August 2010 to August 2011. She is the author or co-author of more than 20 research publications. Her primary research interests are security and privacy in service computing and digital identity management.

Kangbin Yim received his B.S., M.S., and Ph.D. from Ajou University, Suwon, Korea in 1992, 1994 and 2001, respectively. He is currently an associate professor in the Department of Information Security Engineering, Soonchunhyang University. He has served as an executive board member of Korea Institute of Information Security and Cryptology, Korean Society for Internet Information and The Institute of Electronics Engineers of Korea. He also has served as a committee chair of the international conferences and workshops and the guest editor of the journals such as JIT, MIS, JISIS and JoWUA. His research interests include vulnerability assessment, code obfuscation, malware analysis, leakage protection, secure hardware, and systems security. Related to these topics, he has worked on more than fifty research projects and published more than a hundred research papers.

Qianyi Wang received her B.S. from Troy University, U.S.A in 2012, and working on her M.S in university of Malaya, Malaysia. She is currently a research student of Department of Economics and Administration, Faculty of Economics and Administration, University of Malaya. Her primary research interest is rural land consolidation in China. She is also involved in researches of China rural economy development, spatial planning as well as technology development.

Received: September 17, 2013; Accepted: January 16, 2014.