This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings.

TTP Based Privacy Preserving Inter-WISP Roaming Architecture for Wireless Metropolitan Area Networks

Haojin Zhu, Xiaodong Lin, Pin-Han Ho, Xuemin (Sherman) Shen and Minghui Shi
Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada
{h9zhu,xdlin,pinhan,xshen,mshi}@bbcr.uwaterloo.ca

***Abstract*— We propose a novel inter-WISP roaming architecture based on Trusted Third Party (TTP) and partially blind signature technique in Wireless Metropolitan Area Networks (WMAN). The proposed architecture aims to not only greatly improve user privacy and identity anonymity even in the presence of cooperation between the Wireless Internet Service Provider (WISPs) and the TTP, but also dramatically reduce the required size of central database devised to minimize any possible service abuse. In addition, an efficient billing scheme among mobile users (MUs), WISPs and TTP, is introduced to address billing issues associated with roaming. Moreover, a localized inter-WISP authentication scheme is also proposed to support seamless handoff. Detailed analysis on a number of important performance metrics, such as computation time, handoff latency and power consumption, is conducted to verify the performance of the proposed schemes.**

I. Introduction

The advance and wide adoption of wireless communication and Internet technology have revolutionized the human's lifestyle by providing the best convenience and flexibility in accessing the Internet services. Nowadays, wireless hotspots, also known as public Wi-Fi, have been on an upswing, and the wireless Internet access has been readily available particularly in densely populated areas such as airports, restaurants, cafes, hotel and etc. Different from Wi-Fi, the introduction of broadband wireless WiMAX solution can provide a wide-area coverage and broadband access. It is expected that the future wireless metropolitan area networks (WMAN) will be supported by the integration of WIMAX and Wi-Fi. Nevertheless, thousands of subscribe stations (SS) and wireless hotspots must be built in order to provide a sufficiently wide Internet access coverage. Those hotspots could be operated by different operators and WISPs. Therefore, the inter-domain handover should be supported.

Currently, there are two kinds of roaming mechanisms which have been widely adopted by the carriers: peer-to-peer inter-WISP roaming architecture, and roaming broker based inter-WISP roaming architecture [1]. However, these two kinds of roaming architectures still face several challenges as follows. Firstly, the currently existing roaming mechanisms suffer from the overwhelming signaling overhead of authentication requests which go through the roaming broker to the home networks by the way of the visited network. Moreover, it also runs the risk of leaving the roaming broker to become the bottleneck in the inter-WISP roaming and authentication request processing. Secondly, the issues on user privacy are subject to more threats because, in addition to keep communication content private, users are also concerned with the commercial misuse of their personal data such that personal traveling preference and whereabouts [2].

This paper proposes a novel privacy preserving roaming and billing architecture based on a trusted third party (TTP). Different from the role of the roaming broker in the previous studies, the TTP additionally serves as a certificate authority (CA) and is responsible for qualification checking and tracking for the WISPs. The qualified WISPs will be issued with their corresponding certificates by which the their public keys are defined. Instead of using the traditional authentication mechanism based on user name and password, a user simply purchases a universal token (U-token) from the TTP as his authentication credential to gain access to the wireless internet service at any hotspot. Here, the U-token can preserve privacy of MUs through the partially blind digital signature technique, which is a cryptographic tool introduced in [3]. In addition, to avoid excessive involvement of the TTP in every inter-WISP handoff authentication, we propose to use a temporary token (T-token), which is essentially a digital signature designating the T-token receiver, to achieve localized authentication at visited WISP domain. With the proposed architecture, all the security mechanisms can be constructed with asymmetric key cryptography. In order to reduce the computational cost and energy consumption, we propose an efficient partially blind digital signature mechanism based on the improved Rabin's scheme [4] and we will show that the proposed architecture is highly energy- and computation-efficient.

The rest of the paper is organized as follows. In Section II, a brief overview of the related work is presented. In Section III, a privacy preserving roaming and billing architecture for WMANs is proposed. The security of the proposed architecture is analyzed and discussed in Section IV, followed by the efficiency analysis in Section V.

II. Related Work

The issues of roaming, billing and authentication across different WISP domains have received extensive attentions due to the wide adoption of wireless Internet services. Baek et al. proposed an inter-WISP authentication, authorization and accounting protocol based on peer-to-peer inter-WISP roaming strategy [5]. In [6], an efficient localized authentication is introduced for inter-network roaming across wireless LANs based on public key certificate infrastructure. The scheme is efficient since the AAA communication overhead between the WISPs can be avoided and the authentication can be proceeded by WISPs without necessity to contact the roaming broker, which is also named *Localized Authentication*. However, it did not take the certificates revocation issue and billing issue into consideration, which may lead to service fraud.

Location privacy is another important issue related to roaming. Some of reported studies adopt the blind signature technique to provide privacy protection for MUs [2]. The blind signature means that the signature signer is unable to trace this signed message to the previous signing process. In other words, the WISPs cannot link an authentication event to the identity of a specific MU. However, to prevent double spending of the blind signature, the WISP has to maintain a database keeping all the spent blind signatures to check whether a specific blind signature has been spent before. Therefore, this database may grow unlimitedly, which motivated the development of partially blind signature scheme [3]. By embedding the information of expiration date into each blind signature, all the corresponding records of the expired blind signature in the database can thus be removed, which is referred to as the partial blindness property. Most of the existing wireless authentication systems providing privacy protection based on the blind signature mechanisms have never considered the partial blindness properties.

III. Proposed Privacy Preserving Roaming and Billing Architecture

A. Network Entities Definition

In this study, the proposed architecture can be composed of Wi-Fi hotspots and any other wireless access technology such as GPRS, UMTS, and IEEE 802.16. We consider an integrated architecture with Wi-Fi and WiMax systems, where WiMax serves as the wireless MAN backbone while Wi-Fi provides easy deployment and bulk data provisioning to hotspots operated by multiple WISPs. The three main entities involved in this architecture are: TTP, WISP and the MUs.

The core of the proposed architecture is the U-token, which should follow the same format:

d	ExpDate	PSign()	Issuer

Note that the notations for the proposed roaming and billing mechanisms are listed in Table I and *Issuer* stands for the party who issued this U-token, either TTP or WISPs.

However, due to the easy duplication property of the U-token mechanism, any U-token should still be ensured non-double-spent before it can be accepted by any WISP as a valid token. This may lead to significant overhead since the maintenance of a centralized database on all the spent U-tokens is required. To avoid searching the centralized database per every handoff, a temporal token (T-token) mechanism is employed, which should follow a uniform format:

MU	Issuer	Receiver	d	ExpDate	Sign()

where Issuer, and Receiver represent the identity of T-token issuer and T-token receiver, respectively. Since T-token includes the name of target WISP, which means that T-token is only valid for its intended receiver and therefore it can enure this T-token has not been spent before by searching its local server instead of requiring a centralized server.

TABLE I
NOTATIONS EXPLANATION

Notation	Cryptographic Operations
d	Denomination
$ExpDate$	Expiration date
$Sign()$	Digital signature
$PSign()$	Partially blind signature
$E_k(m)$	Symmetric encryption on message m with the key k
$E_k^{-1}(C)$	Symmetric decryption on ciphertext C with the key k
$\|\|$	Message concatenation operation

B. Proposed Privacy Preserving Roaming and Billing Architecture

The proposed architecture includes TTP initialization, WISP initialization, U-token purchase, authenticated key agreement (log in) phase, log off phase and roaming phase, which are detailed in the following subsections:

1) TTP initialization: The TTP randomly chooses two primes p_T and q_T, where $p_T, q_T \equiv 3(\mod 4)$. The triplet (a_0, n_T, a_0^{-1}) together with two hash functions H_0 and H_1 are published as the public key, and (p_T, q_T) is kept as the private key, where $n_T = p_T \cdot q_T$, and a_0 satisfies Jacobi symbol $(\frac{a_0}{n_T}) = -1$.

2) WISP initialization: A WISP A chooses its private key p_A, q_A and public key $n_A = p_A \cdot q_A$ following the same way as that by TTP. It also needs to establish the trust relationship with the TTP by having the TTP's signature on $< ID_A, n_A, ExpDate >$ as the certificate, where ID_A is the identity of the WISP, and $ExpDate$ is the validity period defined for the WISP. Furthermore, it has to be pre-loaded with the public key of the TTP.

3) U-token purchasing phase: A MU has to purchase U-tokens from the TTP or any WISP in order to gain wireless Internet access at any hotspot. This phase can be executed offline or in advance. Here, without loss of generality, we take TTP as an example. The U-token purchasing process is as follows:

Step 1: MU → TTP The MU sends a U-token purchase request to the TTP. This request includes (ID_{MU}, d), where ID_{MU} is the identity of the MU and d is the denomination of the request. Meanwhile, MU can send the payment information to TTP.

Step 2: TTP → MU After receiving the payment information and checking MU's corresponding payment, the TTP selects its randomizing factor $x \in Z_{n_T}^*$, and sends the duplet $(y, ExpDate)$ to the MU, where $y = x^{H_0(d||ExpDate)}(\mod n_T)$.

Step 3: MU→ TTP Assume that the MU intends to gain a blind signature signed on a randomly chosen message m. After receiving the commitment value y, the MU also selects its randomizing factor $u \in Z_{n_T}^*$ and computes $\beta \equiv u^{H_0(d||ExpDate)} y(\mod n_T)$. Then the MU selects the blinding factor $r \in Z_{n_T}^*$ for computing the blinded message submitted to the TTP: $\alpha \equiv r^2 u H_1(m||\beta)(\mod n_T)$.

Step 4: TTP→ MU After receiving α, the TTP injects its randomizing factor x into the blinded message α and compute (t, c_1, c_2), which satisfies the relationship $t^{-2} \equiv (-1)^{c_2} a_0^{c_1} x\alpha(\bmod n_T)$. Here, c_1 can be computed in the following fashion:

$$c_1 = \begin{cases} 0, & \text{if } (\frac{x\alpha}{n_T}) = 1, \\ 1, & \text{if } (\frac{x\alpha}{n_T}) = -1. \end{cases}$$

The TTP computes $\beta = a_0^{c_1} \cdot x\alpha(\bmod n_T)$, and derives c_2 such that

$$c_2 = \begin{cases} 0, & \text{if } (\frac{\beta}{p_T}) = (\frac{\beta}{q_T}) = 1, \\ 1, & \text{if } (\frac{\beta}{p_T}) = (\frac{\beta}{q_T}) = -1. \end{cases}$$

Then, the TTP can derive t such that $t^{-2} \equiv (-1)^{c_2} \cdot a_0^{c_1} \cdot x\alpha(\bmod n_T)$. The blinded signature (t, c_1, c_2) and the randomizing factor x are sent to the MU.

Step 5: Extracting U-token and Verification The MU computes $c \equiv ux(\bmod n_T)$ and $s \equiv rt(\bmod n_T)$. The triplet $(d, ExpDate, c_1, c_2, s, c, m, TTP)$ is a complete U-token for the MU to gain access to the wireless Internet service at hotspots.

The validation of $(d, ExpDate, c_1, c_2, s, c, m, TTP)$ can be examined by observing the following congruence:

$$s^2 H_1(m||c^{H_0(d||ExpDate)}(\bmod n_T))c \equiv (-1)^{c_2} a_0^{-c_1}(\bmod n_T) \qquad (1)$$

4) Authenticated Key Agreement Phase (log in): With the submission of U-token, the MU can gain access to the wireless Internet services at any available hotspot operated by the WISPs which accept the U-token as an effective payment method. Let AP_A denote the target access point. The access process is described as follows.

Step 1: MU→ AP_A Firstly, AP_A broadcasts its public key certificate along with service set identifier (SSID). Then, the MU can easily ensure the security of AP_A's public key n_A after validating the TTP's signature on n_A. To keep the freshness of agreed key, the MU chooses a random k-bit integer c_{MU} as the MU's key contribution and encrypts its temporary identity ID_{MU} and c_{MU} with AP_A's public key by using the relation:

$$Enc = (ID_{MU}||c_{MU})^2(\bmod n_A)$$

Then the MU sends Enc to AP_A.

Step 2: AP_A → MU AP_A decrypts Enc with its private key (p, q) and obtains $ID_{MU}||c_{MU}$. Then AP_A randomly chooses a k-bit integer c_{AP_A} as AP_A's key contribution and sends $Enc' = E_{c_{MU}}(ID_{AP_A}||c_{AP_A})$ back to MU.

Step 3: MU→ AP_A The MU decrypts Enc' by using symmetric-key decryption: $E^{-1}_{c_{MU}}(Enc') = ID_{AP_A}||c_{AP_A}$ and verifies ID_{AP_A}. Then a master key is obtained by:

$$K_{master} = H(ID_{MU}||ID_{AP_A}||c_{MU}||c_{AP_A})$$

The MU sends $z = E_{k_{master}}(U - token)$ to AP_A.

Step 4: AP_A After receiving z, AP_A can also derive the same master key by using the relation $K_{master} = H(ID_{MU}||ID_{AP_A}||c_{MU}||c_{AP_A})$ and obtain the U-Token by decrypting z. AP_A ensures the validity of the U-token by doing the following steps:

1) Verify the signature with the TTP's public key.
2) Check that this U-token doesn't expire.
3) Search the TTP's database to make sure that this U-token has not been spent before.

If these three conditions are satisfied, AP_A accepts the MU as a legitimate user and establishes a master key K_{master} with the MU. An entry of $(ID_{MU}, K_{master}, balance)$, called user information record (UIR), is kept in the AP_A's local database. Meanwhile, AP_A should deposit this U-token into the TTP's database to make sure that the MU cannot spend it again. Afterwards, the confidentiality and integrity of communication between the MU and AP_A is protected by K_{master}.

5) Log Off Phase: The MU that would like to log off and discontinue the existing services has to collect its left U-tokens. To keep identity information confidential, the MU is issued with a new U-token. The log off procedure is described as follows.

Step 1: MU→ AP_A The MU sends a *Leaving request* to the AP_A.

Step 2: AP_A → MU The AP_A summarizes the MU's remaining U-token based on the MU's communication time and the AP_A's billing policy. Let the remaining value of the U-token be d.

Step 3: MU Afterwards, MU and AP_A simply follows the standard U-token purchase protocol from step 2 to step 5 defined in section III-B.3 to obtain a new U-token $(d, ExpDate, c_1, c_2, s, c, m, WISP_A)$.

After obtaining this U-token, the MU can either use this U-token in the future or request for cash back from the TTP. However, because the issuer of this U-token is $WISP_A$ instead of the TTP, it is required that $WISP_B$ should check the certificate of $WISP_A$ first before verifying the validity of this U-token. If both criteria hold, $WISP_B$ could accept this U-Token and acknowledge the MU as a valid user.

6) Roaming Phase: In this section, we will show how to take advantage of T-token to realize the fast inter-WISP handoff authentication and payment. Let AP_A and AP_B denote the two hotspots belonging to different WISPs with public key n_A and n_B, respectively.

Step 1: MU→ AP_A The MU sends a handoff request to both AP_A and AP_B indicating that the MU intends to roam into AP_B. Due to roaming to a different network domain, the MU should ask for a T-token first, which represents the left credits of this MU and can be used in another designated WISP.

Step 2: $AP_A \rightarrow MU$ Upon receiving the handoff request from the MU, AP_A computes

$$\alpha = H(ID_{MU}||ID_{AP_A}||ID_{AP_B}||d||RAND||ExpDate)$$

where $RAND$ is a nonce.

Then, AP_A computes (t, c_1, c_2) which satisfies the relationship $t^2 \equiv (-1)^{c_2} a_0^{c_1} \alpha(\bmod n_A)$. Here, c_1 can be computed in the following fashion:

$$c_1 = \begin{cases} 0\,, & \text{if } (\frac{\alpha}{n_A}) = 1, \\ 1\,, & \text{if } (\frac{\alpha}{n_A}) = -1. \end{cases}$$

Assumed that $\beta = a_0^{c_1} \cdot x\alpha$, c_2 can be computed such that

$$c_2 = \begin{cases} 0\,, & \text{if } (\frac{\beta}{p_A}) = (\frac{\beta}{q_A}) = 1, \\ 1\,, & \text{if } (\frac{\beta}{p_A}) = (\frac{\beta}{q_A}) = -1. \end{cases}$$

Then, AP_A can derive t such that $t^2 \equiv (-1)^{c_2} \cdot a_0^{c_1} \cdot \alpha(\bmod n_A)$. Therefore, $(ID_{MU}, ID_{AP_A}, ID_{AP_B}, d, RAND, ExpDate, t, c_1, c_2)$ constitute a T-token and is sent to MU.

Step 3: MU→ AP_B Afterwards, the MU simply follows the standard authenticated key agreement protocol defined in section III-B.4 to roam into AP_B with the U-token substituted by T-token.

IV. Security analysis

The security of the proposed scheme relies on the security of U-token, which is essentially a blind signature. The formal security proof on the security of U-token including correctness, untraceability and Unforgeability has been presented in [7]. Here, we only briefly analyze the unlinkability property of the U-tokens, which is highly related to the anonymity of MUs. After that, several possible attacks that could be launched by the attackers to the proposed architecture are analyzed.

A. Unlinkability of the U-token and Privacy Protection

Suppose that a U-token $(d, ExpDate, c_1, c_2, s, c, m, TTP)$ is the ith U-token issued by a TTP, the TTP can record (α_i, x_i, t_i) obtained from the U-token issuing process. The triplet (α_i, x_i, t_i) is referred as the *view* of the TTP upon the instance i. With the unlinkability property, the TTP cannot derive a link between the *view* and a valid U-token after the MU spends the U-token on a WISP, which remits this U-token to the TTP. In other words, TTP cannot trace the identity of MUs by linking a U-token to the U-token issuing phase. Here, we define five levels of privacy protection in WMANs as follows:

1) Hiding communication content.
2) Hiding identity information from the external attackers.
3) Hiding identity information from the WISP.
4) Hiding identity information from the TTP.
5) Hiding identity information under the cooperation of WISP and TTP.

With the proposed scheme, the identity of users can be well hidden even under the cooperation of WISP and TTP (Level 5) due to the employment of the partially blind signatures mechanism.

B. Impersonation of an AP Attack

A secure roaming scheme should provide a mutual authentication mechanism to prevent an impersonation attack upon an access point. For example, a malicious attacker could broadcast bogus beacons to attract the other legitimate users, which could possibly defraud the legitimate users for their authentication information. In the proposed access protocol, a highly efficient mutual authentication is devised to resist this attack, where a user has to send a challenge $x = (ID_{MU}||c_{MU})^2 \bmod n_A$ to the access point AP_A after verifying the certificates of the AP_A on its public key n_A. Only the real AP with the knowledge of factorization of n_A can factor x and obtain $ID_{MU}||c_{MU}$, and respond correctly with $y = E_{c_{MU}}(ID_{AP_A}||c_{AP_A})$.

TABLE II

Abbreviations of the Modular Operations Time

Notation	Modular Operation Category
T_{MUL}	Time for One modular multiplicative Operation
T_{EXP}	Time for One Modular Exponential Operation
T_{INV}	Time for One Modular Inverse Operation
T_{SQ}	Time for One Modular Square Operation
T_{SQR}	Time for One Modular Square Root Operation
T_{HASH}	Time for One Hash Operation
T_{SE}	Time for One Symmetric Encryption Operation

TABLE III

The computation for MU considering the pre-computation mechanism

Phase	Computation Cost
U-token Purchasing	$1T_{\text{EXP}} + 7T_{\text{MUL}} + 2T_{\text{SQ}} + 2T_{\text{hash}}$
Authenticated Key Agreement	$1T_{\text{SQ}} + 2T_{\text{SE}} + 1T_{\text{hash}}$
Intra-domain Roaming	$2T_{\text{SE}} + 1T_{\text{HASH}}$
Inter-domain Roaming	$1T_{\text{SQ}} + 2T_{\text{SE}} + 1T_{\text{HASH}}$
Log Off	$1T_{\text{EXP}} + 7T_{\text{MUL}} + 2T_{\text{SQ}} + 2T_{\text{HASH}}$

V. Efficiency Analysis

This section analyzes the computation complexity of the proposed scheme. Table II defines the abbreviations of the modular operations adopted in the discussions.

A. Summary of Computation Cost

We summarize the computation load for the MU during different phases in Table III. Note that, to reduce the computation in the blind signature process, we can adopt a pre-computation technique to speed up the U-token purchasing and log off process, where d and $ExpDate$ can be determined in advance since they are two public parameters. In addition, several random u can be chosen in advance, and the term $u^{H_0(d||ExpDate)}$ can be pre-computed and stored in the user's terminal equipment such that the user can make use of them in the purchasing and log off phase.

B. Seamless Mobility Support During inter-WISP handoff

To gurantee the real-time application connection and hence provide seamless mobility support in WMANs, it is crucial to reduce the authentication processing time.

In the proposed scheme, fast inter-WISP authentication can be achieved because: 1) The delay can be largely reduced due to the adoption of the proposed localized authentication strategy. 2) the proposed handoff authentication scheme can be executed in an extremely high speed. Note that the proposed Rabin-based handoff authentication scheme can be substituted by any other public key cryptosystems (PKCs) such as RSA and ECC. We evaluate the handoff signaling cost denoted as $C_{handoff}$ taken by the proposed authentication mechanism through the analytical model, where the unit $C_{handoff}$ can be defined as $signaling\ overhead * hops$.

For each session, two types of handoffs are defined: inter-WISP handoffs and intra-WISP handoffs. Let i be the total number of handoffs, j be the number of inter-WISP handoffs, and $(i-j)$ be the number of intra-WISP handoffs for each session. Then, the total authentication cost of the handoff can be expressed as:

$$C_{handoff}(i,j) = (i-j) * C_{intra-WISP} + j * C_{inter-WISP} \tag{2}$$

where $C_{intra-WISP}$ and $C_{inter-WISP}$ are the cost for each intra-WISP handoff and inter-WISP handoff, respectively. More specifically, $C_{intra-WISP}$ is determined by the size of authentication message denoted as $Size_{AM}$ and the average hop counts between access points and the corresponding WISP server D_1 denoted as D_1, i.e., $C_{intra-WISP} = Size_{AM} * 2 * D_1$. For $C_{inter-WISP}$, two scenarios are defined: one is with the proposed localized inter-WISP authentication, and the other is with non-localized inter-WISP authentication. The cost of each localized inter-WISP handoff authentication process can be obtained by $C^{local}_{inter-WISP} = 2 * Size_{T-token}$, where $Size_{T-token}$ is the size of the $T-token$. In comparison, each non-localized inter-WISP handoff authentication cost can be defined $C^{non_local}_{inter-WISP} = 2 * Size_{U-token} * D_2$, where D_2 is the average hop count from the visited access point to the TTP, and $Size_{U-token}$ is the size of the $U-token$.

In order to investigate the authentication cost, we compare the proposed localized authentication mechanism with the non-localized authentication [5]. Let the residence time of a MU in an AP (or the reciprocal of handoff frequency) follow a general distribution with a mean of $1/(\mu_{AP})$, whose probability density function (pdf) is $f_{AP}(t)$ and its Laplace transform is $f^*_{AP}(t)$. Let the WISP domain residence time of the MU also follow a general distribution with a mean of $1/(\mu_{WISP})$ whose PDF is $f_{WISP}(t)$ and its Laplace transform is $f^*_{WISP}(t)$. If MU arrival time follows an exponential distribution with a mean of $1/\lambda$, by the handoff model [5], the *pdf*s of i and j can be written as follows:

$$\alpha(i) = \begin{cases} 1 - 1/\rho_{AP}[1 - f^*_{AP}(\lambda)]\,, & \text{if } i = 0, \\ 1/\rho_{AP}[1 - f^*_{AP}(\lambda)]^2 * [f^*_{AP}(\lambda)]^{i-1}\,, & \text{if } i > 0 \end{cases}$$

$$\beta(j) = \begin{cases} 1 - 1/\rho_{WISP}[1 - f^*_{WISP}(\lambda)] \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } j = 0, \\ 1/\rho_{WISP}[1 - f^*_{WISP}(\lambda)]^2 * [f^*_{WISP}(\lambda)]^{j-1} \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } j > 0 \end{cases}$$

where $\rho_{AP} = \lambda/\mu_{AP}$ and $\rho_{WISP} = \lambda/\mu_{WISP}$.

Finally, we can calculate the average authentication cost of the proposed localized authentication mechanism as follows:

$$C_{handoff} = \sum_j \sum_i C_{handoff}(i,j) \cdot \alpha(i) \cdot \beta(j) \tag{3}$$

TABLE IV

PARAMETERS USED IN NUMERICAL RESULTS (BITS)

RAND	t	Mu	Receiver	c_1	c_2
64	1024	64	64	1	1
Issuer	d	ExpDate	c	s	m
64	8	64	1024	1024	64

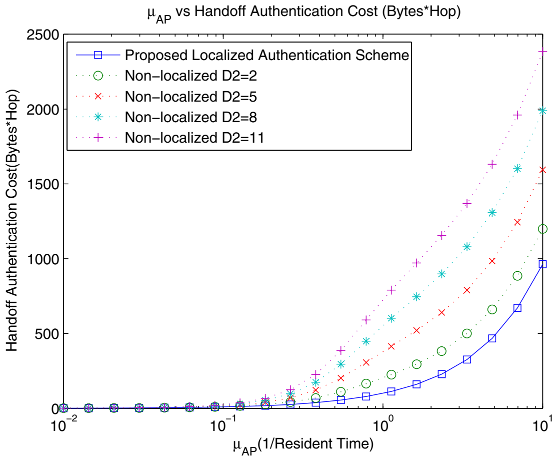

Fig. 1. Average Authentication Signaling Cost due to Handoffs

Assume that the data length of parameters related to intra- and inter-WISP handoff authentication is set as shown in Table IV. Also let the number of access points in a WISP domain be 36 and D_1 be 2, λ and μ_{AP} be normalized to 1.0 and μ_{WISP} be $\mu_{AP}/\sqrt{N}$. We first investigate the effect by varying the access point residence time of each MU upon the authentication cost of the MU, where D_2 is set to 2, 5, 8 and 11 for the non-localized authentication scheme. Based on [8], we can obtain the result shown in Figure 2. It is observed the authentication cost for the proposed localized authentication and the non-localized authentication mechanisms are very close to each other when handoff frequency is low. Further, the authentication cost due to the handoffs keep on increasing as the handoff frequency μ_{AP} increases. We do not vary D_1 because of the WiMAX PMP-mode adopted in the network architecture where each SS directly connects to the BS with a single hop.

When the non-localized authentication mechanism is applied, the authentication cost is significantly large compared with the proposed localized authentication. The authentication cost of non-localized authentication method becomes much larger than that of the proposed localized authentication mechanism as the handoff frequency increases. The reason is that there exists the large authentication signaling overhead as MUs frequently perform intra- and inter-domain handoffs.

It is also observed that the average hop counts between the visited access point and the TTP (D_2) play an important role in the authentication cost when a non-localized authentication method is in place. On the other hand, the hop counts have little impact on the authentication cost by the proposed localized authentication mechanism. This further demonstrates that achieving localized authentication could be very critical to the overall success of seamless mobility support.

C. Energy Efficiency

Energy consumption has become a critical issue in wireless networks where network nodes are battery-powered devices such as cell phones, handheld computers, etc. Let E denote the total energy consumption of a single handoff procedure for inter-domain roaming, which can be represented as follows:

$$E_{inter} = E_{cost}(V) + E_{cost}(pe) + E_{cost}(se) + E_{cost}(T) + E_{cost}(R) \tag{4}$$

where V, pe, se, T, R stand for a verification operation, an asymmetric encryption operation, the symmetric decryption operations, the total transmitting operations, and the total receiving operations, respectively.

The energy consumption of an intra-WISP handoff procedure can obtained as follows:

$$E_{intra-WISP} = E_{cost}(se) + E_{cost}(T) + E_{cost}(R) \tag{5}$$

Let i be the total number of handoffs and j be the number of inter-WISP handoffs, the total energy consumption taken by authentication can be obtained as follows.

$$E_{handoff}(i, j) = (i - j) * E_{intra-WISP} + j * E_{inter-WISP} \tag{6}$$

Then, we can calculate the average energy consumption of the proposed localized authentication mechanism based on various PKCs as follows:

$$E_{handoff} = \sum_{j} \sum_{i} E_{handoff}(i, j) \cdot \alpha(i) \cdot \beta(j) \tag{7}$$

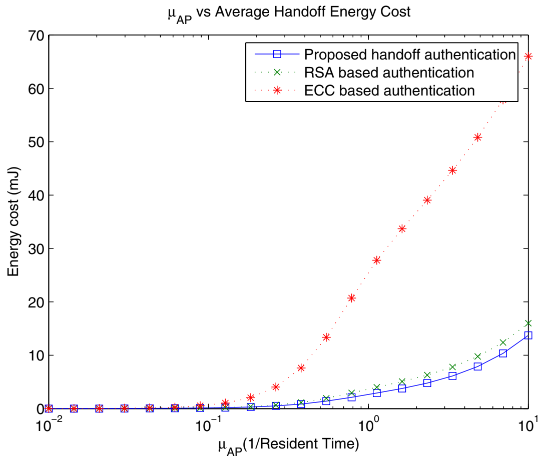

Fig. 2. Average Energy Cost for Handoff Authentication Based On Various PKCs

We evaluate the effect by varying the residence time of a MU in an AP. We assume that except MUs, all devices in the network including access points and TTP have no power constraint. Thus, we are only interested in investigating the energy consumption of the MUs caused by the handoffs while various PKCs are applied. Here, all the energy consumption cost for various cryptographic operations comes from [9].

From Fig. 2, it is observed that the energy consumption of different PKCs is very close to each other when handoffs frequency is low. Further, the energy consumption due to the handoffs increases as μ_{AP} increases. It is also observed that the energy consumption of ECC scheme increases significantlyt compared with RSA and the proposed handoff authentication schemes when μ_{AP} increases. The reason is that the verification procedures of RSA and the proposed handoff scheme are very efficient compared with ECC based method.

VI. Conclusion

In this paper, a novel roaming and billing architecture based on a trusted third party (TTP) has been proposed for Wireless MANs. The proposed architecture not only eliminates the need for mutual roaming agreement between WISPs, but also guarantees the user privacy and identity anonymity. Most importantly, it is complementary to and can co-exist with the existing heterogeneous wireless service billing systems for roaming among different WISPs. We have demonstrated with detailed explanation that the proposed scheme can achieve localized authentication under different roaming scenarios. We have also verified the security levels, computation efforts, and power consumption.

References

[1] J. Leu, R. Lai, H. Lin and W. Shih, "Running Cellular/PWLAN Services: Practical Considerations for Cellular/PWLAN Architecture Supporting Interoperator Roaming," *IEEE Communications Magazine*, vol. 44, no. 2, pp. 73-84, Feb. 2006.

[2] Y. Tsiounis, A. Kiayias and A. Karygiannis, "A Solution for Wireless Privacy and Payments based on E-cash," in *IEEE SecureComm 2005*, Athens, Greece, September 2005.

[3] M. Abe and E. Fujisaki, "How to date blind signatures," in *Proc. ASIACRYPT '96*, ser. LNCS, vol.1163. Springer-Verlag, 1996, pp. 244-251.

[4] M. O. Rabin, "Digitized signatures and public-key functions as intractable as factorization," *MIT Lab. Comput. Sci.*, Cambridge, MA, Tech. Rep. LCS/TR-212, 1979.

[5] S. Baek, S. Pack, T. Kwon, and Y. Choi, "A Localized Authentication, Authorization, and Accounting (AAA) protocol for mobile hotspots," to apear in *WONS 2006 : Third Annual Conference on Wireless On-demand Network Systems and Services* , 2006.

[6] Y. Zhang and Y. Fang, "ARSA: an attack-resilient security architecture for multi-hop wireless mesh networks," in *IEEE JSAC*, vol.24, no.10, pp. 1916-1928, October 2006.

[7] H. Zhu, X. Lin, P. Ho, X. Shen and M. Shi, "A Privacy Preserving Roaming and Billing Architecture for Wireless Metropolitan Networks," bbcr technical report 2006-09.

[8] P. Prasithsangaree and P. Krishnamurthy, "A Variation of the WTLS authentication protocol for reducing energy consumption in wireless devices," In *Proc. of 7th IEEE HSNMC'04*, Toulouse, France, pp. 696-706, 2004.

[9] N. R. Potlapally, S. Ravi, A. Raghunathan and N. K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols," *IEEE Trans. on Mobile Computing*, vol. 5, no. 2, pp. 128-143, March-April 2006.