TUA: A Novel Compromise-Resilient Authentication Architecture for Wireless Mesh Networks

Xiaodong Lin, *Student Member, IEEE,* Rongxing Lu, Pin-Han Ho, *Member, IEEE,*
Xuemin (Sherman) Shen, *Senior Member, IEEE,* and Zhenfu Cao

***Abstract*— User authentication is essential in service-oriented communication networks to identify and reject any unauthorized network access. The state-of-the-art practice in securing wireless networks is based on the *authentication, authorization and accounting* (AAA) framework where one or multiple identical and duplicated AAA servers are adopted to authenticate *mobile users* (MUs), handle authorization requests, and collect accounting data. However, the conventional AAA framework cannot tolerate a server compromise event due to misuse, misconfiguration, and malicious access, etc., which may cause serious damages and resource abuses to the network operation. In this paper, we propose a novel design paradigm toward a compromise-resilient authentication architecture in service-oriented *wireless mesh networks* (WMNs) based on the (t, n) threshold signature technique, termed *Threshold User Authentication* (TUA) scheme. With the TUA scheme, only t or more out of n AAA servers in the WMN can cooperatively grant the network access to a MU, while any $t-1$ or less cannot. Detailed protocol-aspect design and implementations are presented. Extensive analysis on efficiency and reliability of authentication functionality is conducted to gain a deeper understanding on the parameter settings and optimization, which demonstrates the effectiveness of the TUA scheme. We conclude that the proposed authentication scheme can contribute to the WMN network design in metropolitan areas where numerous *mesh points* (MPs) coexist and are managed under a single control plane with multiple distributed AAA servers.**

***Index Terms*— Security, threshold authentication, wireless mesh networks.**

I. Introduction

With the intrinsic infrastructure-free and low-maintenance characteristics of wireless communication systems, *wireless mesh networks* (WMNs) based on IEEE 802.11 and/or IEEE 802.16 mesh mode technology is a promising alternative to the traditional wired *Digital Subscriber Line* (DSL) and Cable Modem services due to its flexibility, reliability, ease of deployment, and cost efficiency. The adoption of WMNs for supporting service-oriented metropolitan-area applications has attracted explosive attentions from both industry and academia recently. A WMN is mainly composed of a cloud of distributed *Mesh Points* (MPs) serving as the backhaul of the WMN. Each MP could be connected to all the other MPs in its transmission range, by which the network topology is formed. A data path with multiple hops could be created by performing MAC-layer forwarding for the launched traffic in each intermediate node. A routing table may be maintained at each intermediate node to facilitate the MAC layer hop-by-hop forwarding, where the MAC address of the next hop for each data path traversing through the node is kept. Each *mobile station* (MS) can gain access to the network by connecting with a MP.

User authentication is essential in any service-oriented communication network in order to identify and reject any access request of an unauthorized user. Currently, the best practice in securing wireless networks is based on the technique of *authentication, authorization and accounting* (AAA) framework, where an AAA server performs authentication for each MU, handle authorization requests, and collect accounting data [1]. Fig. 1 shows the AAA framework based on 802.1x with the *Extensible Authentication Protocol* (EAP) [2]. When a MS enters the radiation range of a MP and tries to associate with the MP, the MP inspects the MS's association and enables the MS's wireless connection. The MS then sends an *EAP-Start* message. The MP replies with an *EAP-Request Identity* message back to the MS to obtain the MS's identity. The MS's *EAP-Response* packet containing the MS's identity is then forwarded to the AAA server. The AAA server, e.g., RADIUS server [3], then issues a *RADIUS Access-Challenge* to the MP. After receiving the *Radius Access-Challenge*, the MP issues an authentication challenge to the MS, which is supposed to respond the challenge with its credentials. Then the MP forwards the user authentication credentials to the authentication server. At the end, an *ACCEPT* or *REJECT* notification is sent from the AAA server to the MP. If an *ACCEPT* is received, the MP transitions the MS's wireless network connection to an authorized state. Finally, the MS has the network access. Once the authentication is complete, a key agreement process is invoked such that the MS and MP possess the corresponding secret key at the end of procedure, respectively, where the confidentiality and integrity of communication between the MS and the MP are protected by the session key.

Manuscript received November 26, 2006; revised April 10, 2007; accepted June 17, 2007. The associate editor coordinating the review of this paper and approving it for publication was A. Sabharwal. This work was supported by research grants from the Provincial Centre of Excellence Communications and Information Technology Ontario (CITO), Canada.

X. Lin, P.-H. Ho, and X. Shen are with the Centre for Wireless Communications, Department of Electrical and Computer Engineering, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1 (e-mail: {xdlin,pinhan,xshen}@bbcr.uwaterloo.ca).

R. Lu and Z. Cao are with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai, P. R. China (e-mail: {rxlu, zfcao}@cs.sjtu.edu.cn).

Digital Object Identifier 10.1109/TWC.2008.060990.

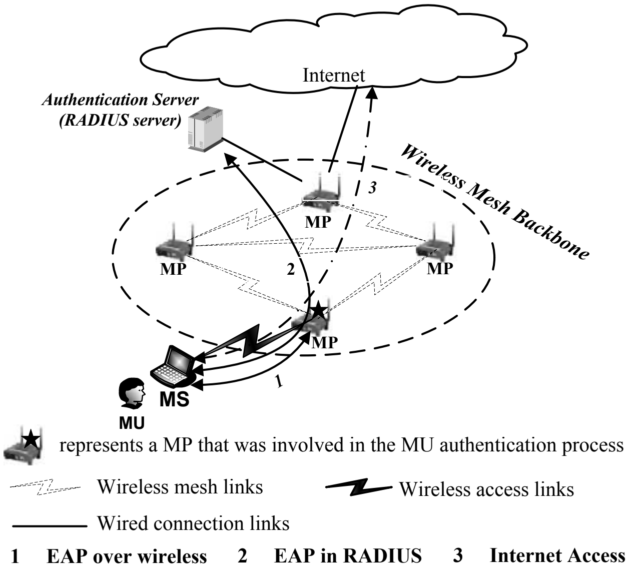


Fig. 1. Authentication process with 802.1x in wireless mesh networks.

Based on the AAA framework, several user authentication schemes for communication networks have been proposed in the past decades [4]–[9]. All the reported user authentication schemes were developed virtually over a single authentication server, and may suffer from two types of failures in the authentication functionality. The first type of failure occurs due to physical/protocol faults or a *Denial-of-service* (DoS) attack, which can disable the server normal function. More specifically, the physical/protocol failure and DoS attacks could be caused by any misuse, misconfiguration, and malicious access, which can simply make the server unavailable. In this case, the network becomes unavailable for performing authentication, which leads to revenue loss and service disruption. The impairment due to this type of failure can be well mitigated by allocating multiple redundant authentication servers working in a manner of distributed duplicated Database (DB) such that the unavailability of one or a subset of servers will not affect the whole network authentication operation. In this way, the availability of authentication functionality in the network (or termed *authenticability*) can be significantly improved in the presence of any physical/protocol failure and DoS attack.

The other type of failure is due to an authentication server compromise event by one or a group of malicious attackers, which may cause even more serious damages and, unfortunately, cannot be solved by equipping the network with multiple independent and identical authentication servers. Such a network status is termed *false-authenticative*, which is one of the worst situations that the network defense system is subject to. The problem lies in the fact that the false-authenticative status occurs as long as any one of the authentication servers is compromised. The compromised authentication server can be manipulated by the attackers and launch various vital attacks to the network operations such as allowing unauthorized network access, stealing of user credentials, and illegally updating billing information, etc. The solution to the problem, as far as we can see, is still open, and has been subject to little attention in the past.

As the growing demand on service-oriented WMNs in a metropolitan area, it will be highly desired to have a more resilient authentication architecture with multiple authentication servers cooperating with each other for assessing and evaluating the user access requests. In order to further guarantee the system security and authenticability, the user authentication architecture should be developed such that the system can survive from the situation where one or a subset of authentication servers are compromised by a malicious intruder. The characteristic of intrusion tolerance is expected to be critically demanded in the future WMN design, which allows the system to function well by performing authentication on each MU in a regular way.

This paper proposes a novel scheme of user authentication, which aims to significantly improve the system authenticability and minimize the probability of going into the false-authenticative state in the presence of authentication server compromise events. The proposed authentication scheme is based on a (t, n) threshold signature [10], where with the approval from t or more than t authentication servers out of the totally n authentication servers in the *Authentication Server Group* (ASG) can the corresponding login request from a MU be granted with network access. We will present detailed implementations of the proposed scheme, and demonstrate that such a *Threshold User Authentication* (TUA) scheme can perfectly work in the wireless communication scenario with stringent limitations on power and computation capacity on the MS of each MU. In addition, the proposed TUA scheme can well cooperate with the existing software artifacts, which can be recycled for saving much development effort. An analysis on the authenticability of the proposed TUA scheme is conducted at the end, which can serve as a guidance in the system parameter selection, i.e., finding n and the corresponding optimal value of t for the WMNs such that the targeted network authenticability can best be achieved with the good balance between authenticability and cost due to the deployment of multiple authentication servers. To the best of our knowledge, this is the first study that focuses on the improvement of authentication server compromise resilience in service-oriented WMNs in metropolitan areas.

The remainder of this paper is organized as follows. In Section II, related work is given. Section III provides some preliminaries and background knowledge. In Section IV, the proposed TUA scheme is presented, followed by the security analysis and performance evaluation in Section V-A and Section V-B, respectively. In Section V-C, the authenticability analysis is conducted. Finally, we draw our conclusions in Section VI.

II. Related Work

User authentication is one of the most important security mechanisms, which aims to grant services to legitimate users while avoiding any unauthorized access. Over the past years, many remote user authentication schemes have been proposed [4], [5], [11]–[15] based on the AAA framework. In 1981, Lamport [4] proposed a password based authentication scheme using a password table at the server side to achieve remote user authentication. However, the high hash overhead and the necessity for password reset, protection, and maintenance, have been reported to significantly decrease the feasibility and applicability of Lamport's scheme. To improve Lamport's scheme, several similar user authentication schemes were reported [11]–[13]. To avoid the password table maintained at server side, Hwang and Li [5] proposed a new remote user authentication scheme using a smart card. The scheme does not need to maintain the password table to check the validity of each login request while being able to resist the message replaying attack. However, Hwang-Li's scheme was identified insecure in the wireless network scenario [14], [15]. Later, a number of improved user authentication schemes dedicated for wireless communications were reported [16]–[19]. Those schemes have either focused on supporting multiple authentication factors, or emphasized on designing a secure authentication mechanism. A system-level design for improving compromise resilience is still an open issue.

Threshold cryptography was first proposed in [20], [21], and quickly became an important cryptographic primitive in many applications where a single entity in the system can't be trusted and the trust relationship has to be established with the involvement of a number of entities exceeding a threshold. In [22], Zhou and Hass proposed a distributed trust mechanism to distribute the trust to a set of nodes in wireless ad hoc networks. A valid certificate of any node can be only generated correctly if a number of nodes exceeding a threshold cooperate. In [23], Lee et al presented an efficient threshold password based authentication scheme using (k, n) threshold scheme, which allows a roaming user who accesses a network from different client terminals to get his private key from the servers, even if some of the servers are compromised under the multi-server roaming system. Recently, Chai et al [24] also presented an efficient threshold password authentication scheme against password guessing attacks in ad hoc networks. In this paper, we adopt threshold cryptography to design a compromise-resilient authentication architecture for *wireless mesh networks*.

III. Preliminaries

In this section, a brief review on the basis of bilinear pairing and related underlying problems is conducted, which serves as important background of the proposed TUA scheme. A brief introduction on threshold signature scheme is also given.

A. Bilinear Pairing

Bilinear pairing has caught tremendous interest and attention from the security community since the technique has been identified able to solve some problems that were previously well recognized as unsolvable, such as *ID-based cryptography* (IBC) [25]. IBC is a public-key cryptosystem where any string can be used to derive a valid public key such as user names, email addresses, IP addresses, MAC addresses, host or node names, etc. Compared with the traditional *public key infrastructure* (PKI) based on public key certificate, IBC simplifies the certificate management since the public key of any user could be any of its publicly known identity. Another good advantage of taking pairing-based schemes is that they can save communication bandwidth compared with traditional schemes such as RSA [26] and ElGamal [27] because pairing-based schemes feature a relatively small signature overhead when bilinear pairing is used for the design of signature schemes and/or secure protocols.

As the preliminaries of the proposed TUA scheme, bilinear pairing and the underlying problems are briefly reviewed in the following paragraphs.

Let $\mathbb{G}_1$, $\mathbb{G}_1'$ be two cyclic additive groups and $\mathbb{G}_2$ be a cyclic multiplicative group of the same prime order q, i.e., $|\mathbb{G}_1| = |\mathbb{G}_1'| = |\mathbb{G}_2| = q$. Let P be a generator of $\mathbb{G}_1$, P' be a generator of $\mathbb{G}_1'$, and ψ be an isomorphism from $\mathbb{G}_1'$ to $\mathbb{G}_1$, with $\psi(P') = P$. An efficient admissible bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1' \rightarrow \mathbb{G}_2$ with the following properties:

- Bilinear: for all $P_1 \in \mathbb{G}_1$, $Q_1 \in \mathbb{G}_1'$ and $a, b \in \mathbb{Z}_q^*$, $\hat{e}(aP_1, bQ_1) = \hat{e}(P_1, Q_1)^{ab}$.
- Non-degenerate: There exist $P_1 \in \mathbb{G}_1$ and $Q_1 \in \mathbb{G}_1'$ such that $\hat{e}(P_1, Q_1) \neq 1$.
- Computable: there is an efficient algorithm to compute $\hat{e}(P_1, Q_1)$ for any $P_1 \in \mathbb{G}_1$, $Q_1 \in \mathbb{G}_1'$.

Such an admissible bilinear map $\hat{e}$ can be constructed by Weil or Tate pairings on the elliptic curves. As mentioned in [28], [29], the Tate pairing on MNT curves [30] gives us the efficient implementation, where $\mathbb{G}_1 \neq \mathbb{G}_1'$, ψ can be implemented by the trace map, and the representations of $\mathbb{G}_1$ can be expressed in 171 bits when the order q is a 170-bit prime.

We assume the discrete logarithm problems in groups $\mathbb{G}_1$, $\mathbb{G}_1'$ and $\mathbb{G}_2$ are all hard, and define the Computational co-Diffie-Hellman (co-CDH) Problem and Decision co-Diffie-Hellman (co-DDH) Problem on $(\mathbb{G}_1, \mathbb{G}_1')$.

Definition 1 (co-CDH Problem). Given $P_1', aP_1' \in \mathbb{G}_1'$ and $Q \in \mathbb{G}_1$ for unknown $a \in \mathbb{Z}_q^*$, compute $aQ \in \mathbb{G}_1$. A (τ, ϵ)-co-CDH adversary in $(\mathbb{G}_1, \mathbb{G}_1')$ is a probabilistic machine $\mathcal{A}$ running in time τ such that

$$\mathbf{Adv}_{\mathbb{G}_1, \mathbb{G}_1'}^{\text{co}-\text{CDH}}(\mathcal{A}) = \Pr[\mathcal{A}(P_1', aP_1', Q) = aQ] \geq \epsilon$$

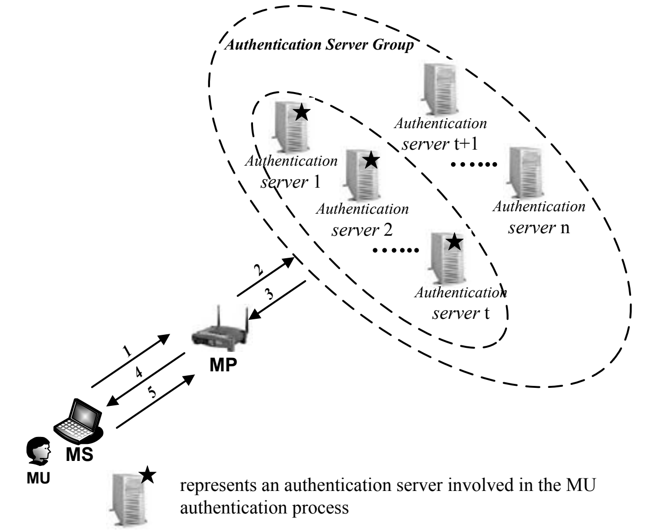
where the probability is taken over the random values a, Q. The co-CDH problem is (τ, ϵ)-intractable if there is no (τ, ϵ)-adversary in $(\mathbb{G}_1, \mathbb{G}_1')$. The co-CDH assumption states that is the case of all polynomial τ and any non-negligible ϵ.

Definition 2 (co-DDH Problem). Given $P_1', aP_1' \in \mathbb{G}_1'$ and $Q, bQ \in \mathbb{G}_1$ for unknown $a, b \in \mathbb{Z}_q^*$, decide whether $a = b \bmod q$. The co-DDH problem is easy here, since it is easy to compute $\hat{e}(bQ, P_1') = \hat{e}(Q, P_1')^b$ and decide whether or not $\hat{e}(Q, P_1')^b = \hat{e}(Q, aP_1') = \hat{e}(Q, P_1')^a$.

B. Threshold Signature Scheme

In [10], the concept of threshold signature is introduced. With a (t, n) threshold signature scheme, a valid signature can be generated only by t or more out of n participants, while any $t - 1$ or less cannot forge a valid signature. In this paper, the threshold signature technique is applied to design user authentication scheme in order to improve the security assurance and system authenticability.

As shown in Fig. 2, in the proposed TUA scheme, there are n authentication servers forming an ASG, and the ASG is in place of a single authentication server, which performs the authentication functionality on each MU. A MU initially shares a low-entropy password with the ASG. When a login request is received by a MP at a time segment, the MP


Authentication Server Group
Authentication server 1
Authentication server 2
Authentication server t+1
Authentication server n
Authentication server t
2
3
1
4
5
MP
MS
MU
represents an authentication server involved in the MU authentication process

1. **MU** login request.
2. **MP** sends **MU**'s login request to ***authentication server group***.
3. t authentication servers response to the **MU**'s login request
4. **MP** sends login response to the **MU**
5. **MU** has network access after successful authentication

Fig. 2. Threshold user authentication scheme.

forwards the request to all the servers in the ASG. Once t or more servers in the ASG agree to admit the MU, the MU can access to the network resource in the time segment.

IV. Threshold User Authentication Scheme

Based on the bilinear pairing stated above, the proposed *threshold user authentication* (TUA) scheme takes advantage of the BLS short signature [31], where only with the consent of t or more out of n authentication servers can a MU get the wireless network access. Similar to most previously reported authentication schemes, our TUA scheme consists of three phases: the setup phase, the registration phase, and the login and authentication phase. In the following, each phase is described in detail.

A. Setup Phase

Let $\mathcal{TA}$ be a trusted authority for the WMN, and a set $\mathcal{S} = \{S_1, S_2, \cdots, S_n\}$ represent the ASG of n members. In the proposed scheme, only with the consent of t or more authentication servers in the *authentication server group* $\mathcal{S}$, can the MU have network access. Prior to the network deployment, $\mathcal{TA}$ sets up the system parameters as follows:

Step 1: The $\mathcal{TA}$ randomly chooses two primes, p_0 and q_0, that satisfy $p_0 \equiv q_0 \equiv 3 \bmod 4$, along with a random number a_0, such that the Jacobi symbol $\left(\frac{a_0}{n_0}\right) = -1$ where $n_0 = p_0 \cdot q_0$. The duplet (a_0, n_0) is published as the public key, and (p_0, q_0) is kept as the private key. Furthermore, an one-way hash function $h() : \{0,1\}^* \rightarrow Z^*_{n_0}$ is also published.

Step 2: Let $\mathbb{G}_1$, $\mathbb{G}'_1$ be two cyclic additive groups, and $\mathbb{G}_2$ be a cyclic multiplicative group of the same prime order q, i.e., $|\mathbb{G}_1| = |\mathbb{G}'_1| = |\mathbb{G}_2| = q$. Let P be a generator of $\mathbb{G}_1$, P' be a generator of $\mathbb{G}'_1$, and ψ be an isomorphism from $\mathbb{G}'_1$ to $\mathbb{G}_1$ where $\psi(P') = P$. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}'_1 \rightarrow \mathbb{G}_2$ be an efficient admissible bilinear map. Then, the $\mathcal{TA}$ chooses a cryptographic hash function $H : \{0,1\}^* \rightarrow \mathbb{G}_1$.

Step 3: As an off-line effort, $\mathcal{TA}$ distributes the secret shares to all the authentication servers $S_1, S_2, \cdots, S_n$. For achieving this, $\mathcal{TA}$ first chooses a random number $x \in \mathbb{Z}^*_q$ as the *authentication server group* $\mathcal{S}$'s secret key and computes the corresponding public key $Y = xP' \in \mathbb{G}'_1$.

Step 4: $\mathcal{TA}$ randomly generates a secret polynomial function of $t-1$ degree as follows,

$$f(y) = x + a_1 y + \cdots + a_{t-1} y^{t-1} \bmod q \qquad (1)$$

and generates secret shadows $f(i)$ and corresponding public keys $Y_i = f(i)P' \in \mathbb{G}'_1$, where $i = 1, 2, \ldots, n$, for each server S_i. Clearly, it shows that $f(0) = x$.

Step 5: Each server S_i randomly chooses two primes, denoted as p_i and q_i, where $i = 1, 2, \ldots, n$, and keeps the duplet (p_i, q_i) as secret.

In addition to the initiation of $\mathcal{TA}$, each MP needs to be initiated by the $\mathcal{TA}$ before the MP can formally join the network domain and provide wireless Internet services to the MUs. The MP takes the following actions:

Step 1: The MP randomly chooses p_a, q_a that satisfy $p_a \equiv q_a \equiv 3 \bmod 4$, and sends its chosen service set identifier, *SSID*, to the $\mathcal{TA}$, while the duplet (p_a, q_a) is kept as the private key of the MP. The $\mathcal{TA}$ checks the legitimacy of the identity and ensures the uniqueness of the identity of the MP. If not, the MP has to choose another *SSID* that is legitimate and unique in order to further proceed. The $\mathcal{TA}$ is responsible for identity check of its managed MPs.

Step 2: The $\mathcal{TA}$ computes c_1 as follows:

$$c_1 = \begin{cases} 0, & \text{if } \left(\frac{h(SSID, n_a)}{n_0}\right) = 1 \\ 1, & \text{if } \left(\frac{h(SSID, n_a)}{n_0}\right) = -1 \end{cases}$$

where $n_a = p_a q_a$. Then the $\mathcal{TA}$ computes $t_0 = a_0^{c_1} \cdot h(SSID, n_a)$, and derives c_2 such that

$$c_2 = \begin{cases} 0, & \text{if } \left(\frac{t_0}{p_0}\right) = \left(\frac{t_0}{q_0}\right) = 1, \\ 1, & \text{if } \left(\frac{t_0}{p_0}\right) = \left(\frac{t_0}{q_0}\right) = -1. \end{cases}$$

Then, the $\mathcal{TA}$ computes $r_0 = (-1)^{c_2} \cdot a_0^{c_1} \cdot h(SSID, n_a)$, and derives s_0 such that $s_0^2 \equiv r_0 \bmod n_0$ since r_0 is a quadratic residue of n_0. The correctness can be demonstrated as follows:

If there is an integer $0 < x < n_0$ such that $x^2 \equiv a \bmod n_0$, then a is said to be a quadratic residue modulo n_0. Let QR_{n_0} denote the set of quadratic residue modulo n_0 and QNR_{n_0} denote the set of quadratic nonresidue modulo n_0. Furthermore, a is a quadratic residue modulo n_0 if and only if a is a quadratic residue modulo p_0 and modulo q_0 where $n_0 = p_0 q_0$ [32]. Then an integer a must belong to one of following four cases: 1) $Z_{(1,1)} = \{a \subseteq \mathbb{Z}^*_{n_0} | a \subseteq QR_{p_0} \cap a \subseteq QR_{q_0}\}$; 2) $Z_{(1,-1)} = \{a \subseteq \mathbb{Z}^*_{n_0} | a \subseteq QR_{p_0} \cap a \subseteq QNR_{q_0}\}$; 3) $Z_{(-1,1)} = \{a \subseteq \mathbb{Z}^*_{n_0} | a \subseteq QNR_{p_0} \cap a \subseteq QR_{q_0}\}$; and 4) $Z_{(-1,-1)} = \{a \subseteq \mathbb{Z}^*_{n_0} | a \subseteq QNR_{p_0} \cap a \subseteq QNR_{q_0}\}$. Obviously, $Z_{(1,1)}$ is QR_{n_0}. Note that $\left(\frac{1}{p_0}\right) = \left(\frac{1}{q_0}\right) = 1$, and $\left(\frac{-1}{p_0}\right) = \left(\frac{-1}{q_0}\right) = -1$ since $p_0 \equiv q_0 \equiv 3 \bmod 4$.

Since $\left(\frac{t_0}{n_0}\right) = \left(\frac{a_0^{c_1}\cdot h(SSID,n_a)}{n_0}\right) = \left(\frac{a_0^{c_1}}{n_0}\right)\left(\frac{h(SSID,n_a)}{n_0}\right) = 1$, we know $t_0 = a_0^{c_1}\cdot h(SSID,n_a)$ belongs to either $Z_{(1,1)}$ or $Z_{(-1,-1)}$. Then $\left(\frac{(-1)^{c_2}\cdot a_0^{c_1}\cdot h(SSID,n_a)}{n_0}\right) = \left(\frac{(-1)^{c_2}}{n_0}\right)\left(\frac{t_0}{n_0}\right) = 1$. Thus, we can be assured that $r_0 = (-1)^{c_2}\cdot a_0^{c_1}\cdot h(SSID,n_a)$ is a quadratic residue of n_0.

Step 3: Finally, the signature signed on MP's public key as well as the linkage between the public key and the MP's identity can be derived as a duple (s_0, c_1, c_2). Then the $\mathcal{TA}$ sends $(a_0, n_0, n_a, SSID, s_0, c_1, c_2)$ to the MP.

B. Registration Phase

In this phase, the MU randomly chooses a low-entropy password PW and calculates $h(PW)$, where $h(.)$ is a collision-resistant hash function. Afterwards, the MU submits its identity ID and $h(PW)$ to the $\mathcal{TA}$ in a secure way, for example, through SSL [33]. The $\mathcal{TA}$ is responsible for identity check of the MU. After checking the validity of the identity ID, the duple $(ID, h(PW))$ will be securely distributed among of the *authentication server group* $\mathcal{S}$ by the $\mathcal{TA}$. In the end, each server $S_i \in \mathcal{S}$ takes the following actions:

1) Each server S_i calculates V_i as follows:

$$\begin{cases} V_i = ID \mod p_i \\ V_i = h(PW) \mod q_i \end{cases} \tag{2}$$

Then using Chinese remainder theorem (*CRT*) [32], we can solve (2) for V_i. Thus, the server S_i can obtain

$$V_i = ID \cdot b_1 \cdot q_i + h(PW)\cdot b_2 \cdot p_i \bmod \ n_i \tag{3}$$

where $n_i = p_i q_i$, and the b_1 and b_2 are determined from $b_1 \cdot q_i \equiv 1 \mod p_i$ and $b_2 \cdot p_i \equiv 1 \mod q_i$, respectively.

2) The server S_i then stores V_i into its verification table, called $\mathcal{V}$ table. It is worth pointing out that $\mathcal{V}$ table resists dictionary attack even if an attacker compromises an authentication server and learns with the $\mathcal{V}$ table. Without the knowledge of the p_i and q_i, it is infeasible to obtain the MU's *ID* and the hash value of the password from the $\mathcal{V}$ table. In reality, if an attacker can learn with the hash value of a MU's password, an attacker can easily launch an off-line dictionary attack to figure out the MU's authentication credentials.

C. Login and Authentication Phase

In this phase, the MU authenticates itself to a MP whenever the MU tries to gain wireless Internet access from the MP at time T. The MP is called the *serving MP* (sMP) of the MU when the request is permitted. Let the sMP be equipped with a *service set identifier* denoted as *SSID*. The access process to the sMP from the MU is described as follows.

Step 1: ***sMP→MU*** Consider that the sMP broadcasts its public parameters, $(a_0, n_0, n_a, SSID, s_0, c_1, c_2)$, in its beacon frames. In this case, the MU can easily ensure the security of the sMP's public key n_a after validating the $\mathcal{TA}$'s signature on it by the following relation:

$$s_0^2 = (-1)^{c_2}\cdot a_0^{c_1}\cdot h(SSID,n_a) \bmod n_0$$

If the validation fails, the MU aborts the login process since the MU could be subject to impersonation by the sMP.

Step 2: ***MU→sMP*** The MU calculates $h(PW)$, and randomly selects two random numbers k_1 and r where k_1 is a l-bit number as the MU's key contribution, and encrypts its identity ID, k_1, r , $h(PW)$ and T by using the following relation:

$$c = (ID||k_1||r||h(PW)||T)^2 \bmod n_a$$

where T is the current date and time of the MS. Then, the MU sends a login request c to the sMP.

Step 3: ***sMP*→ASG** Upon receiving a login request, the sMP decrypts c with its private key (p_a, q_a), and obtains $(ID, h(PW), k_1, r, T)$. Then, the sMP takes the following actions:

1) The sMP checks the format of ID, and will reject this login request if the ID is not a valid user identity.
2) The sMP checks if the timestamp T is a valid of timestamp, and if so continue. Otherwise, it stops.
3) Then, the sMP sends an authentication request $(ID, h(PW), r)$ to the ASG $\mathcal{S}$ through a preestablished secure channel between the sMP and ASG.

Step 4: **ASG→*sMP*** Without loss of generality, we assume that there are t servers in the sub-group $\mathcal{T} = (S_1, S_2, \cdots, S_t)$ from the ASG $\mathcal{S}$ agree to accept MU's login request after a successful user password verification procedure, which is illustrated in Fig. 3. Then, the t servers in the sub-group $\mathcal{T}$ begin to execute the following steps to generate a signature on message r.

1) Each $S_i \in \mathcal{T}$ uses his secret shadow $f(i)$ to compute

$$\sigma_i = f(i)H(r) \in \mathbb{G}_1 \tag{4}$$

and sends it to the sMP, a designated clerk.

2) After receiving t partial signatures $\sigma_1, \sigma_2, \cdots, \sigma_t$, the sMP combines them as a whole signature σ on message r as follows,

$$\sigma = \sum_{i=1}^{t}\left(\left(\prod_{j=1, j\neq i}^{t}\frac{0-i}{j-i}\right)\cdot \sigma_i\right) \in \mathbb{G}_1 \tag{5}$$

4) In the end, the signature of message r is σ.

Step 5: ***sMP→MU*** The sMP then can verify the validity of signature σ by the following equation

$$\hat{e}(\sigma, P') = \hat{e}(H(r), Y) \tag{6}$$

If it holds, the signature σ can be accepted, and the sMP accepts the login request; otherwise, the login request is rejected. The verification is performed based on the

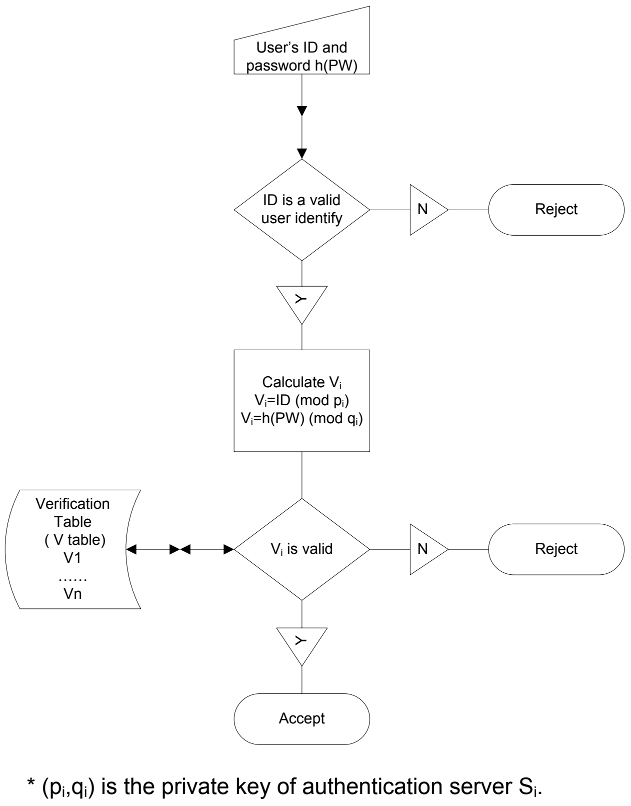

User's ID and password h(PW)
ID is a valid user identify
N
Reject
Y
Calculate V$_i$
V$_i$=ID (mod p$_i$)
V$_i$=h(PW) (mod q$_i$)
Verification Table (V table) V1 ...... Vn
V$_i$ is valid
N
Reject
Y
Accept
* (p$_i$,q$_i$) is the private key of authentication server S$_i$.

Fig. 3. The flowchart for password verification procedure

following derivation:

$$
\begin{aligned}
&\hat{e}(\sigma, P') \\
= \;& \hat{e}\left(\sum_{i=1}^{t}\left(\left(\prod_{j=1,j\neq i}^{t}\frac{0-i}{j-i}\right)\cdot\sigma_i\right), P'\right) \\
= \;& \hat{e}\left(\sum_{i=1}^{t}\left(\left(\prod_{j=1,j\neq i}^{t}\frac{0-i}{j-i}\right)\cdot f(i)H(r)\right), P'\right) \\
= \;& \hat{e}\left(H(r), \sum_{i=1}^{t}\left(\left(\prod_{j=1,j\neq i}^{t}\frac{0-i}{j-i}\right)\cdot f(i)P'\right)\right) \\
= \;& \hat{e}\left(H(r), f(0)P'\right) \\
= \;& \hat{e}\left(H(r), xP'\right) \\
= \;& \hat{e}\left(H(r), Y\right)
\end{aligned}
$$

It is well recognized that the signature technique is the only currently available approach that can ensure data authenticity, integrity, and non-repudiation, which are three most important characteristics mandatory to the authentication process. However, a digital signature serves as extra information and obviously becomes overhead on top of the original message to be transmitted through communication channels. With most of the previously reported threshold signature schemes, causing large signature overhead is always a serious concern when the schemes are applied in a practical environment. Note that the heavier the signature overhead is, the larger the transmitting and receiving energy is consumed, which impairs the service availability on those battery-powered MSs. Therefore, minimizing the signature overhead is one of the major efforts in the design of our scheme.

With TUA, the overhead can be kept minimum since the size of signature σ is as short as the BLS short signature [31] (roughly 171 bits, when using the MNT curves [30]). In case the authentication process succeeds, the sMP randomly chooses a l-bit number k_2 as the sMP's key contribution, and computes $d = E_{k_1}(SSID||k_2)$. Then, the sMP sends d back to the MU.

Step 6: ***MU*** After the MU receives d, the MU decrypts d by using symmetric-key decryption: $E_{k_1}^{-1}(d) = SSID||k_2$, and verifies *SSID*. Afterwards, both the MU and the sMP generate a session key k by the following:

$$k = H(ID||SSID||k_1||k_2)$$

The confidentiality and integrity of communication between the MU and the sMP are protected by the session key k.

V. Performance Analysis

A. Security Analysis

In the section, we evaluate the security of the proposed TUA scheme in the following four aspects.

1) All private keys are secure in the proposed TUA scheme.

Based on the hardness of the discrete logarithm problem in $\mathbb{G}_1'$, it is computationally infeasible to find a given aP' where $a \in \mathbb{Z}_q^*$ and $P' \in \mathbb{G}_1$. Therefore, it is very difficult to derive the ASG $\mathcal{S}$'s private key $f(0) \in \mathbb{Z}_q^*$ from $Y = f(0)P'$ and each server S_i's private key $f(i) \in \mathbb{Z}_q^*$ from $Y_i = f(i)P'$.

2) A MU's low-entropy password PW is secure in the proposed TUA scheme.

Because the large integer factorization problem is considered as NP complete under some given security level, it is hard for an adversary to directly derive the MU's low-entropy password PW from $c = (ID||k_1||r||h(PW)||T)^2 \bmod n_a$ without knowing the private key (p_a, q_a) of the sMP. At the same time, the low-entropy password PW is protected by introducing a high-entropy random number r in $c = (ID||k_1||r||h(PW)||T)^2 \bmod n_a$. Therefore, the proposed TUA scheme can resist an off-line password guessing attack.

3) The proposed TUA scheme can resist the replay attack.

Let an adversary $\mathcal{A}$ attempt to replay the intercepted login request message from a legitimate MU and impersonate the MU as a legitimate one. Obviously, the replay of an intercepted $c = (ID||k_1||r||h(PW)||T)^2 \bmod n_a$ does not work due to the device of the time segment T in the login message, where the sMP will reject the request if the time interval for transmission of the login message is larger than a pre-defined threshold. Therefore, the proposed TUA scheme can resist the replay attack.

4) The signature σ signed by the server group $\mathcal{S}$ is a secure (t, n) threshold signature, provided that the co-CDH assumption holds in $\mathbb{G}_1$.

Suppose that $t-1$ authentication servers in group $\mathcal{S}$ can produce a valid signature σ such that $\hat{e}(\sigma, P') = \hat{e}(H(r), Y)$. Without loss of generality, we assume that the $t-1$ servers are $(S_1, S_2, \cdots, S_{t-1})$, and the corresponding $t-1$ sub-signatures are $\sigma_1, \sigma_2, \cdots, \sigma_{t-1}$. Thus, according to the relation

$$\sigma = \sum_{i=1}^{t} \left(\left(\prod_{j=1, j\neq i}^{t} \frac{0-i}{j-i} \right) \cdot \sigma_i \right)$$

we can compute the sub-signature of S_t

$$\sigma_t = \left(\prod_{j=1}^{t-1} \frac{0-t}{j-t} \right)^{-1} \cdot \left(\sigma - \sum_{i=1}^{t-1} \left(\left(\prod_{j=1, j\neq i}^{t} \frac{0-i}{j-i} \right) \cdot \sigma_i \right) \right)$$

Since $\sigma_t = f(t)H(r) \in \mathbb{G}_1$, the co-CDH problem *"Given $H(r) \in \mathbb{G}_1, P', Y_t = f(t)P' \in \mathbb{G}_1'$, compute $f(t)H(r) \in \mathbb{G}_1$"* is resolved, which nonetheless contradicts with the co-CDH assumption.

On the other hand, when totally t servers $(S_1, S_2, \cdots, S_t)$ cooperate, the signature σ clearly can be constructed from $\sigma_1, \sigma_2, \cdots, \sigma_t$ according to the relation,

$$\sigma = \sum_{i=1}^{t} \left(\left(\prod_{j=1, j\neq i}^{t} \frac{0-i}{j-i} \right) \cdot \sigma_i \right)$$

Thus, the MU can be granted with the service. In summary, σ is actually a secure (t, n) threshold signature in the proposed TUA scheme.

B. Authentication Latency Analysis

In this subsection, we provide a comprehensive evaluation of the authentication delay encountered in the login and authentication phase for the proposed TUA scheme. Here we do not consider the overhead in the setup phase and the registration phase since they involve only very few heavy operations in the signing process while leaving most of the computation extensive operations performed off-line. Furthermore, it has been fully demonstrated that the implementation of the cryptographic mechanisms adopted in TUA can minimize the real-time computation workload by deriving some intermediate values in an off-line manner. For example, in Eq. 3, the two intermediate values b_1 and b_2 can be precomputed in order to speed up authentication procedure.

According to [34], the authentication delay can be defined as the time period between the instant when a MU launches an authentication request and the instant when it receives the authentication reply. Therefore, the delay per each authentication procedure $\mathbb{T}_{\textsf{Auth-Latency}}$ can be expressed as:

$$\mathbb{T}_{\textsf{Auth-Latency}} = \vec{d} \cdot \vec{t}^{T} + \mathbb{T}_{\textsf{TD}}$$

where $\vec{d}$ is the vector denoting the number of time variables for an authentication procedure and defined as $\vec{d} = (4, 1, 2, t+1, t-1, 2)$, $\mathbb{T}_{\textsf{TD}}$ stands for the transmission delay of authentication messages, $\vec{t}$ is a vector referred to as the cryptographic operations which contribute to the overall authentication latency, and are defined as $\vec{t} = (T_{\textsf{mul}}, T_{\textsf{exp}}, T_{\textsf{mhash}}, T_{\textsf{pmul}}, T_{\textsf{padd}}, T_{\textsf{pair}})$. The time components are defined in Table I along with the corresponding values. Note that we do not take the symmetric key processing time and cryptographic hash operation time into consideration since they are negligible compared with that of the other operations. We evaluate the delay of cryptographic operations on an Intel Pentium 4 3.0 GHz machine with 1GB RAM running Fedora Core 4 based on cryptographic library MIRACL [35].

TABLE I

DEFINITION OF NOTATIONS

Notation	Description	Execution Time
$T_{\textsf{TR}}$	Message transmission time on one hop	0.0049 ms/byte†
$T_{\textsf{mul}}$	The time for a multiplication operation	0.015 ms
$T_{\textsf{exp}}$	The time for an exponentiation operation	2.26 ms
$T_{\textsf{mhash}}$	The speed for map-to-point hash operation	3.91 ms
$T_{\textsf{pmul}}$	The time for a point multiplication operation	1.51 ms
$T_{\textsf{padd}}$	The time for an addition in $\mathbb{G}_1$ operation	0.0076 ms
$T_{\textsf{pair}}$	The time for a pairing operation	8.2 ms

† IEEE 802.1x, when the maximum authentication message is 4096 bytes [34], the transmission delay per hop is about 20 milliseconds with the assumption of 2 Mbps link capacity [36].

TABLE II

COMPUTATION OVERHEAD OF THE PROPOSED TUA SCHEME

	Login and Authentication phase
MU	$2T_{\textsf{mul}}$
sMP	$T_{\textsf{exp}} + tT_{\textsf{pmul}} + 2T_{\textsf{pair}} + T_{\textsf{mhash}} + (t-1)T_{\textsf{padd}}$
$S_i \in \mathcal{S}$	$2T_{\textsf{mul}} + T_{\textsf{pmul}} + T_{\textsf{mhash}}$

For simplicity, we assume all authentication servers are located at the same distance to the sMP of the MU. Also, authentication servers can simultaneously process MU authentication requests. The authentication request is transmitted to the authentication servers via *N* hops and the authentication servers will send the authentication result back via another *N* hops. Without loss of generality, we assume *N* is 3. Thus, we can obtain the authentication delay as follows:

$$\begin{aligned} & \mathbb{T}_{\textsf{Auth-Latency}} \\ = \; & \vec{d} \cdot \vec{t}^{T} + \mathbb{T}_{\textsf{TD}} \\ = \; & (4, 1, 2, t+1, t-1, 2) \\ & \cdot (T_{\textsf{mul}}, T_{\textsf{exp}}, T_{\textsf{mhash}}, T_{\textsf{pmul}}, T_{\textsf{padd}}, T_{\textsf{pair}})^{T} + \mathbb{T}_{\textsf{TD}} \\ = \; & 32.23 + 1.52t \; ms \end{aligned}$$

It is observed that t plays important role in the authentication delay in the proposed TUA scheme. The smaller the t is, the shorter authentication delay the MU may experience at the expense of less improved authenticability. Therefore, a tradeoff between the security assurance and authentication latency must be initiated. We will demonstrate in the next section that the proposed TUA scheme can achieve a very high authenticability with a small number of authentication servers even in the presence of relatively high server compromise and physical/protocol failure probabilities. In this case, the authentication latency can be well constrained to meet the stringent requirement in a handoff event for real-time services while a high authenticability, such as six-nine and seven-nine, can be achieved.

Furthermore, the breakdowns of the authentication delay at the MU's side, at the sMP's side, and at the authentication servers' side, are investigated and summarized in Table II.

Based on Table II, it is observed that the delay at the MU's side remains static no matter how many authentication servers are adopted in the proposed TUA scheme, which is a critical feature to meet the design requirement in WMNs where the resources at different network entities are asymmetric. Note that the MU side is supposed subject to a stringent limitation on power consumption and computation capacity. On the other hand, the MPs and authentication servers are physically stationary with unlimited power and sufficiently strong computation capacity.

C. Authenticability Analysis

The proposed TUA scheme can significantly improve the system security guarantee by achieving high availability of network authentication functionality (or referred to as *authenticability*). Let each AAA server possibly be subject to two types of failures: one is the *compromise failure* due to a malicious attack with a probability v, and the other is the physical/protocol failure that causes a *DoS failure* on the server with a probability of u. Note that a DoS event could be due to not only hardware/protocol problems, but also any malicious DoS attack that makes the AAA server unavailable for performing authentication function. We are interested in deriving the network *authenticability* under the TUA scheme.

The following discussion simply assumes that each failure event hits the AAA servers independently. Let V and U be two random variables representing the number of AAA servers that are subject to compromise failure and unintended authentication server failure at a specific time moment, respectively. Note that an unintended failure event could be due to not only hardware problems, but also any protocol and software failure that makes the AAA server unavailable for performing authentication function. Three states in terms of whether the network can well perform the authentication functionality are defined as follows: (i) authenticative, (ii) unauthenticative, (iii) false-authenticative. The first state happens when the total number of unavailable servers and compromised servers is less than or equal to $n - t$ such that at least t servers can authenticate a legitimate user login request. Besides, the number of compromised servers must be less than t such that there is no possibility for the event of false-authenticative to occur. Thus we have Eq. 7 which describes state (i):

$$\begin{cases} U + V \leq n - t \\ V < t \end{cases} \tag{7}$$

The second state happens when the number of unavailable and compromised servers is larger than $n - t$ such that there are not sufficient available servers to authenticate a legitimate user. We have Eq. 8 to describe state (ii):

$$\begin{cases} U + V > n - t \\ V < t \end{cases} \tag{8}$$

The last state occurs when at least t among all the n AAA servers are compromised. We have:

$$V \geq t \tag{9}$$

U and V basically follow a binomial distribution, i.e.,

$$\begin{cases} Pr\{U = i\} = \binom{n}{i} u^i (1-u)^{n-i} \\ Pr\{V = j | U = i\} = \binom{n-i}{j} v^j (1-v)^{n-i-j}, \end{cases} \tag{10}$$

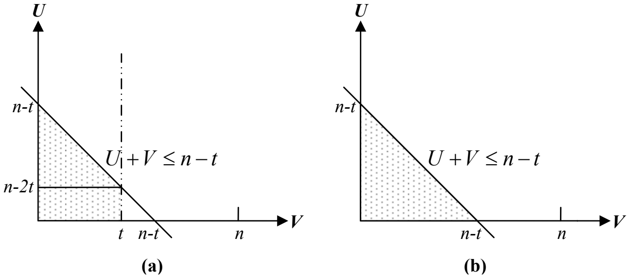


Fig. 4. The region on the $U - V$ plane corresponding to $n \geq 2t$ and $n < 2t$ in (a) and (b), respectively.

Based on Eqs. 10, we can derive the network *authenticability* in case $n \geq 2t$:

$$\begin{aligned} & Pr\{U + V \leq n - t, V < t\} \\ = & \sum_{i=0}^{n-2t-1} \sum_{j=0}^{t-1} Pr\{U = i\} Pr\{V = j | U = i\} \\ & + \sum_{i=n-2t}^{n-t} \sum_{j=0}^{n-t-i} Pr\{U = i\} Pr\{V = j | U = i\} \\ = & \sum_{i=0}^{n-2t-1} \sum_{j=0}^{t-1} \binom{n}{i}\binom{n-i}{j} u^i (1-u)^{n-i} v^j (1-v)^{n-i-j} \\ & + \sum_{i=n-2t}^{n-t} \sum_{j=0}^{n-t-i} \binom{n}{i}\binom{n-i}{j} u^i (1-u)^{n-i} v^j (1-v)^{n-i-j} \end{aligned} \tag{11}$$

The upper bounds of the summations in Eq. 11 can be derived by observing Fig. 4(a). In case $n < 2t$ such that the condition $\{V < t\} \supset \{U + V \leq n - t\}$ holds, the covered area is shown in Fig. 4(b), where the network authenticability can be expressed as the following:

$$\begin{aligned} & Pr\{U + V \leq n - t, V < t\} \\ = & Pr\{U + V \leq n - t\} \\ = & \sum_{i=0}^{n-t} \sum_{j=0}^{n-t-i} Pr\{U = i\} Pr\{V = j | U = i\} \\ = & \sum_{i=0}^{n-t} \sum_{j=0}^{n-t-i} \binom{n}{i} \binom{n-i}{j} u^i (1-u)^{n-i} v^j (1-v)^{n-i-j} \end{aligned} \tag{12}$$

Obviously, the network *authenticability* is determined by t and n, where the value of t is bounded by n. With more AAA servers (or a larger n), the *authenticability* can be further improved. We define the *un-authenticability* of the network (denoted as Q_{ac}) to include both the unauthenticative and false-authenticative, which is $1 - Pr\{U + V \leq n - t, V < t\}$. We simulated different combinations of u, v, t, and n. The values of 0.01, 0.001, and 0.0001 are tested for u and v, while the values of $4 - 8$ for n are tested. The results are shown in Figs. 5, 6, and 7.

The authenticability by employing the conventional authentication architecture with a single AAA server can be simply derived by setting $n = t = 1$ in Eq. 12. Therefore, the TUA scheme can achieve a significant improvement against the conventional authentication architecture in terms of authenticability, where the un-authenticability of the conventional one

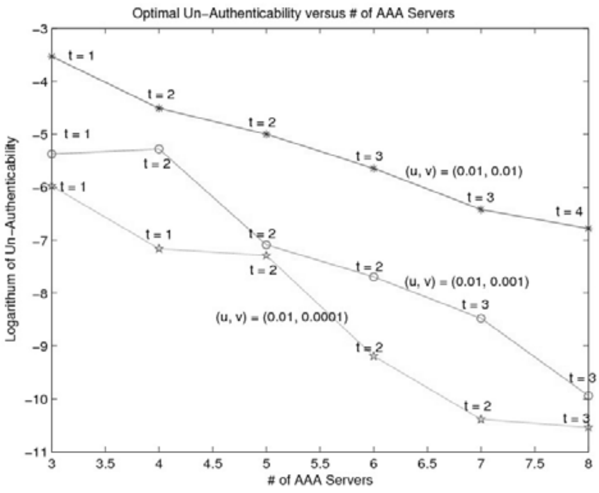


Fig. 5. The logarithm of the optimal network un-authenticability $Q_{ac}^{optimal}$ versus the number of AAA servers with $(u, v) = (0.01, 0.01)$, $(0.01, 0.001)$, and $(0.01, 0.0001)$, respectively, where $t_{optimal}$ is shown beside the data.

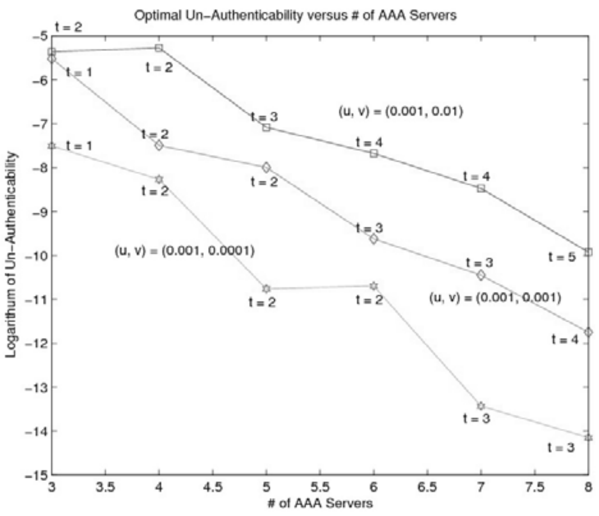


Fig. 6. The logarithm of the optimal network un-authenticability $Q_{ac}^{optimal}$ versus the number of AAA servers with $(u, v) = (0.001, 0.01)$, $(0.001, 0.001)$, and $(0.001, 0.0001)$, respectively, where $t_{optimal}$ is shown beside the data.

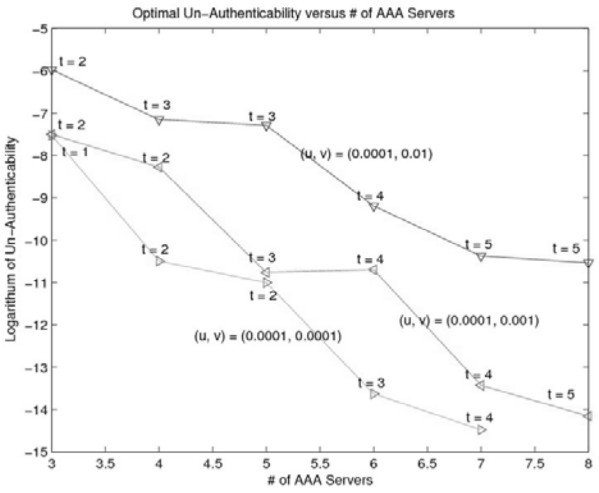


Fig. 7. The logarithm of the optimal network un-authenticability $Q_{ac}^{optimal}$ versus the number of AAA servers with $(u, v) = (0.0001, 0.01)$, $(0.0001, 0.001)$, and $(0.0001, 0.0001)$, respectively, where $t_{optimal}$ is shown beside the data.

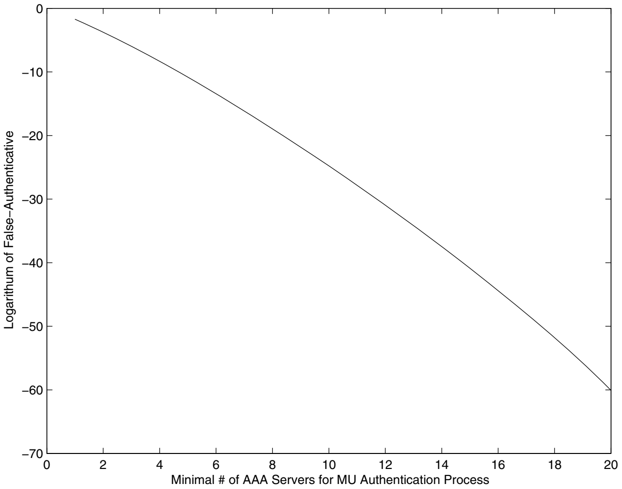


Fig. 8. The logarithm of the network *false-authenticative* versus the minimal number of AAA servers for MU authentication process with $(u, v) = (0.01, 0.001)$ and n=20.

is in the same order as u. It is also verified that n does not need to be very large to achieve high network authenticability. From our analysis, the authenticability can be as high as "10 nines", i.e., $1 - 10^{-10}$, with $(u, v) = (0.001, 0.001)$, where $(n, t) = (7, 3)$.

The network *false-authenticative* is

$$\begin{aligned} & Pr\{V \geq t\} \\ = & \sum_{i=t}^{n}\sum_{j=0}^{n-i} Pr\{U = j\}Pr\{V = i|U = j\} \\ = & \sum_{i=t}^{n}\sum_{j=0}^{n-i} \binom{n}{j}\binom{n-j}{i} u^j(1-u)^{n-j}v^i(1-v)^{n-i-j} \end{aligned} \tag{13}$$

It is worth noting that the network *false-authenticative* of the conventional one is in the same order as v. However, as shown in Fig. 8, with increase of t, the network *false-authenticative* of the TUA scheme decreases significantly.

VI. Conclusions

In this paper, we have proposed a novel *threshold user authentication* (TUA) scheme based on the bilinear pairing, where only t or more out of n servers in the *Authentication Server Group* (ASG) can cooperatively grant the Internet services to a *Mobile User* (MU). Therefore, compared with the conventional AAA framework, the proposed scheme can achieve much better security guarantee and can be very suitable for the wireless environments with highly distributed-controlled *Mesh Points* (MPs) and multiple cooperative authentication servers. The paper has presented detailed implementations on the proposed TUA scheme along with comprehensive illustrations. We have conducted extensive analysis on the proposed scheme, where the security guarantee under a number of typical attack models and the resultant computational efficiency of the proposed authentication mechanism are discussed. To demonstrate the effectiveness, we evaluate the resultant system *authenticability* of the TUA scheme, where the availabilities of authentication functionality due to authentication server compromise and physical/protocol failures are jointly considered. The result shows that the proposed TUA scheme can achieve a very high authenticability and is suitable for the application scenario considered in the study, where a "10-nine", i.e., $1-10^{-10}$, authenticability can be achieved with 7 authentication servers even in the presence of relatively high server compromise and physical/protocol failure probabilities (i.e., 0.001).

ACKNOWLEDGMENT

The research is financially supported by Provincial Centre of Excellence Communications and Information Technology Ontario (CITO), Canada.

REFERENCES

[1] C. d. Laat, G. Gross, and L. Gommans, “Generic AAA architecture,” IETF RFC 2903, Mar. 2000.

[2] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, “Extensible authentication protocol (EAP),” IETF RFC 3748, June 2004.

[3] B. Aboba and P. Calhoun, “RADIUS (remote authentication dial in user service) support for extensible authentication protocol (EAP),” IETF RFC 3579, Sep. 2003.

[4] L. Lamport, “Password authentication with insecure communication,” *Commun. ACM*, vol. 24, no. 11, pp. 770-772, 1981.

[5] M. S. Hwang and L. H. Li, “A new remote user authentication scheme using smart cards,” *IEEE Trans. Consumer Electron.*, vol. 46, no. 1, pp. 28-30, 2000.

[6] A. K. Awasthi and S. Lal, “A remote user authentication scheme using smart cards with forward secrecy,” *IEEE Trans. Consumer Electron.*, vol. 49, no. 4, pp. 1246-1248, 2003.

[7] M. L. Das, A. Saxena, and V. P. Gulati, “A dynamic ID-based remote user authentication scheme,” *IEEE Trans. Consumer Electron.*, vol. 50, no. 2, pp. 629-631, 2004.

[8] R. Lu and Z. Cao, “Efficient remote user authentication scheme using smart card,” *Computer Networks*, vol. 49, no. 4, pp. 535-540, 2005.

[9] H. M. Sun, “An efficient remote user authentication scheme using smart cards,” *IEEE Trans. Consumer Electron.*, vol. 46, no. 4, pp. 958-961, 2000.

[10] Y. Desmedt and Y. Frankel, “Shared generation of authentication and signatures,” in *Proc. Advances Cryptology*, ser. LNCS, vol. 576. Springer-Verlag, pp. 457-469, 1991.

[11] R. E. Lennon, S. M. Matyas, and C. H. Mayer, “Cryptographic authentication of time-variant quantities,” *IEEE Trans. Commun.*, vol. 29, no. 6, pp. 773-777, 1981.

[12] S. M. Yen and K.H. Liao, “Shared authentication token secure against replay and weak key attack,” *IEEE Inform. Processing Lett.*, vol. 62, no. 2, pp. 78-80, 1997.

[13] S. J. Wang, “Yet another login authentication using N-dimensional construction based on circle property,” *IEEE Trans. Consumer Electron.*, vol. 49, no. 2, pp. 337-341, 2003.

[14] C. K. Chan and L. M. Cheng, “Cryptanalysis of a remote user authentication scheme using smart cards,” *IEEE Trans. Consumer Electron.*, vol. 46, no. 4, pp. 992-993, 2000.

[15] J. J. Shen, C. W. Lin, and M. S. Hwang, “A modified remote user authentication scheme using smart cards,” *IEEE Trans. Consumer Electron.*, vol. 49, no. 2, pp. 414-416, 2003.

[16] G. Horn and B. Preneel, “Authentication and payment in future mobile systems,” in *Proc. Computer Security - ESORICS’98*, ser. LNCS, vol. 1485. Springer-Verlag, pp. 277-293, 1998.

[17] Z. J. Tzeng and W. G. Tzeng, “Authentication of mobile users in third generation mobile System,” *Wireless Pers. Commun.*, vol. 16, no. 1, pp. 35-50, 2001.

[18] X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “Two-factor localized authentication scheme for WLAN roaming,” in *Proc. IEEE ICC*, June 2007, pp. 1172-1178.

[19] J. M. Zhu and J. F. Ma, “A new authentication scheme with anonymous for wireless environments,” *IEEE Trans. Consumer Electron.*, vol. 50, no. 1, pp. 231-235, 2004.

[20] Y. Desmedt and Y. Frankel, “Threshold cryptosystems,” in *Proc. Advances Cryptology*, ser. LNCS, vol. 435. Springer-Verlag, pp. 307-315, 1990.

[21] Y. Desmedt, “Threshold cryptography,” *European Trans. Telecommun.*, vol. 5, no. 4, pp. 449-457, 1994.

[22] L. Zhou and Z. J. Haas, “Securing Ad Hoc Networks,” *IEEE Networks*, vol. 13, no. 6, pp. 24-30, 1999.

[23] S. Lee, K. Han, S. Kang, K. Kim, and S. Ine, “Threshold password-based authentication using bilinear pairings,” in *Proc. Public Key Infrastructure - EuroPKI 2004*, ser. LNCS, vol. 3093. Springer-Verlag, pp. 350-363, 2004.

[24] Z. Chai, Z. Cao, and R. Lu, “Threshold password authentication against guessing attacks in Ad hoc networks,” to be published.

[25] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” in *Proc. Advances in Cryptology*, ser. LNCS, vol. 2139. Springer-Verlag, pp. 213-229, 2001.

[26] R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[27] T. ElGamal, “A public-key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE Trans. Inform. Theory,* vol. 31, no. 4, pp. 469-472, 1985.

[28] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in *Proc. Advances Crytology*, ser. LNCS, vol. 3152. Springer-Verlag, pp. 41-55, 2004.

[29] T. Nakanishi and N. Funabiki, “A short verifier-local revocation group signature scheme with backward unlinkability,” in *Proc. IWSEC*, ser. LNCS, vol. 4266. Springer-Verlag, pp. 17-32, 2006.

[30] A. Miyaji, M. Nakabayashi, and S. Takano, “New explicit conditions of elliptic curve traces for FR-reduction,” *IEICE Trans. Fundamentals*, vol. E84-A, no. 5, pp. 1234-123, 2001.

[31] D. Boneh, B. Lynn, and H. Shacham, “ Short signatures from the Weil pairing,” in *Proc. Advances in Cryptology*, ser. LNCS, vol. 2248. Springer-Verlag, pp. 514-532, 2001.

[32] W. Mao, *Modern Cryptography: Theory and Practice*, Upper Saddle River, NJ: Prentice Hall PTR, 2003.

[33] K. E. B. Hickman, “SSL 2.0 protocol specification,” Feb. 1995. [Online]. Available: http://www.netscape.com/eng/security/SSL_2.html

[34] W. Liang and W. Wang, “A quantitative study of authentication and QoS in wireless IP networks,” in *Proc. IEEE INFOCOM*, Mar. 2005, pp. 1478-1489.

[35] Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL). [Online]. Available: http://indigo.ie/ mscott/

[36] A. Hess and G. Schafer, “Performance evaluation of AAA / mobile IP authentication,” [Online]. Available: http://www-tkn.ee.tuberlin.de/publications/papers/pgts2002.pdf

Xiaodong Lin (S’07) is currently working toward his Ph.D. degree in the Department of Electrical and Computer Engineering at the University of Waterloo, Ontario, Canada, where he is a Research Assistant in the Broadband Communications Research (BBCR) Group. His research interests include wireless network security, applied cryptography, and anomaly-based intrusion detection.

Rongxing Lu received the B.Sc. and M.Sc. degrees in computer science from Tongji University, Shanghai, China, in 2000 and 2003, respectively. In 2006, he received the Ph.D degree in computer science from Shanghai Jiao Tong University, Shanghai, China. Currently, he is a Post-doctoral fellow at the University of Waterloo, Waterloo, Canada. His current research interests include wireless network security and cryptography. He is the co-recipient of the IEEE ICC 2007 - Computer and Communications Secuity Symposium Best Paper Award.

Pin-Han Ho (M'04) received his B.Sc. and M.Sc. Degree from the Electrical and Computer Engineering department at National Taiwan University in 1993 and 1995, respectively. He started his Ph.D. study in the year 2000 at Queen's University, Kingston, Canada, focusing on optical communications systems, survivable networking, and QoS routing problems. He finished his Ph.D. in 2002, and joined the Electrical and Computer Engineering department at the University of Waterloo, Waterloo, Canada, as an assistant professor in the same year. Professor Pin-Han Ho is the author/coauthor of more than 100 refereed technical papers and book chapters, and the co-author of a book on optical networking and survivability. He is the recipient of the Distinguished Research Excellence Award in the ECE department of the University of Waterloo, the Early Researcher Award (Premier Research Excellence Award) in 2005, the Best Paper Award in SPECTS'02, ICC'05 Optical Networking Symposium, and ICC'07 Security and Wireless Communications symposium, and the Outstanding Paper Award in HPSR'02.

Xuemin (Sherman) Shen (M'97-SM'02) received the B.Sc. (1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a Professor and University Research Chair, and the Associate Chair for Graduate Studies, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research focuses on mobility and resource management in interconnected wireless/wireline networks, UWB wireless communications systems, wireless security, and ad hoc and sensor networks. He is a co-author of three books, and has published more than 300 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen served as the Technical Program Committee Chair for IEEE Globecom'07, General Co-Chair for Chinacom'07 and QShine'06, and the Founding Chair for the IEEE Communications Society Technical Committee on P2P Communications and Networking. He also serves as a Founding Area Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS; Editor-in-Chief for *Peer-to-Peer Networking and Application*; Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the *KICS/IEEE Journal of Communications and Networks*, *Computer Networks*, *ACM/Wireless Networks*, and *Wireless Communications and Mobile Computing (Wiley)*, etc. He has also served as Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS, and *IEEE Communications Magazine*. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada.

Zhenfu Cao received his B.S. degree in computer science and technology from Harbin Institute of Technology, China, in 1983, and his Ph.D. degree in mathematics from the same university. Currently, he is a professor and a doctoral supervisor at the Department of Computer Science and Engineering of Shanghai Jiao Tong University. His main research areas are number theory, cryptography, trusted computing, trusted network, and information security, etc. He has published more than 300 academic papers and four monographs, and more than 30 academic research projects have been completed. He received the first prize award for science and technology from the Chinese University in 2001, and the National Outstanding Youth Fund award in 2002.