Reducing Communication Overhead for Wireless Roaming Authentication: Methods and Performance Evaluation

Men Long[1], Chwan-Hwa "John" Wu[2], and J. David Irwin[2]
(Corresponding author: Chwan-Hwa Wu)

Communications Technology Lab, Intel Corporation[1]
2111 NE 25th Ave, Hillsboro, OR 97124, USA (Email: wu@eng.auburn.edu)
Department of Electrical and Computer Engineering, Auburn University, Auburn, AL 36849[2]

(Received June 12, 2006; revised and accepted Sept. 19, 2006 & Nov. 7, 2006)

Abstract

The protocol design for wireless roaming authentication is challenging because of the key management regarding users and home/visited networks. In this paper, we present two authentication methods that demonstrate better performance in terms of authentication latency and energy consumption of a mobile terminal, compared to the 3G cellular network approach of home network transporting authentication vector to visited network. The proposed Method I, referred to as Nonce-based Authentication, eliminates the sequence numbers used in the 3G roaming authentication and employs the key derivation and caching technique for mobile terminal and visited network. The proposed Method II, called Lightweight Localized Authentication, introduces the computation-efficient protocol based on a carefully designed public key certificate infrastructure. With the design goal of achieving security by lower cost, both methods significantly reduce the communication overhead between home and visited networks for roaming authentication, as indicated by analytical and experimental result.

Keywords: Authentication and key agreement (AKA), roaming authentication, security, wireless LAN, wireless roaming

1 Introduction

Wireless roaming authentication is an important component to achieve the ubiquitous computing paradigm-users can access the Internet anywhere and at any time. Due to the diversity of radio standards, we may observe roaming among the networks of same type or of different types. In this paper, we are mainly concerned about the roaming across different administrative domains. Thus, this paper focuses on the mutual authentication between a roaming user and a foreign wireless service provider domain. The protocol design difficulty lies in the fact that the authentication center of a visited network does not a priori share a secret with a roaming user. Thus, designing and deploying a scalable and efficient authentication protocol for various service providers and millions of users is quite challenging.

Authentication protocols for 3G roaming were finalized a few years ago [1, 2, 4]. Since the 3G authentication protocol is believed to be a viable approach for cellular networks, the AKA (Authentication and Key Agreement) protocol and the home/visited network authentication architecture, defined in the 3G specifications, might be reused for all other wireless roaming. However, given the evolution of networking technologies (such as the new networks of WiFi and WiMAX), it is worth asking the question: are there other computation/communication efficient roaming authentication approaches besides the AKA protocol defined in 3G?

Research community has been drawn attention to the communication overhead problem in roaming authentication. In 3G roaming authentication, when a roaming user makes authentication request, the home authentication server needs to transport authentication vectors to the visited authentication server. Lin and Chen [20] gave the method of adaptively adjusting the number of authentication vectors between home and visited networks per roaming authentication request. For generic wireless roaming, a number of research papers proposed various mechanisms for sharing an authentication key between a roaming user and a visited network, so the communication overhead between home and visited network can be significantly reduced. For instance, Chen *et al.* [9] proposed the scheme using public key certificate and mobile IP binding update to reduce the communication overhead between home and visited network authentication servers. Prasithsangaree and Krishnamurthy [26] investigated the dual digital signatures from 3G and WLAN operators for the localized authentication of 3G-WLAN integrated networks. Suzuki and Nakada [27] proposed that visited network generates a temporary authentication key, sends it to home network, and tunnels it back to user by home network. Hwang and Chang [14] studied the self-encryption method for achieving the authentication key agreement between user and visited network. Kambourakis *et al.* [16] introduced the EAP-TLS protocol for the authentication in client device, WLAN access point, and 3G authentication server. Long *et al.* [21] discussed a generic public key certificate infrastructure for the localized authentication.

This paper provides two alternative roaming authentication methods that exhibit superior performance in terms of reducing communication overhead between home and visited network without any security degradation. Compared to the existing methods, the proposed two protocols are simpler and more intuitive. In addition, several new features (on cryptographic key storage and defense against denial of services attacks) are introduced by the new methods in this paper.

The proposed Method I (called Nonce-based Authentication) employs the symmetric key based cryptography. We advocate a new notion in roaming authentication: a mobile terminal and its home network authentication center have different cryptographic random number seeds that generate the cryptographic nonces for authenticating each other. Another novelty of Method I is: after the initial authentication, a shared key is derived by utilizing the well-known cryptographic principle between the mobile terminal and the home network, and cached by the mobile terminal and the visited network for subsequent intra-network roaming authentication. Overall, the proposed Nonce-based Authentication eliminates the use of sequence numbers. In contrast, the synchronized authentication of 3G requires a mobile terminal and its home network to keep track of a sequence number, which accounts for authentication traffic overhead between home and visited networks.

The proposed Method II (called Lightweight Localized Authentication) utilizes public key-based cryptography. The authentication traffic is localized without any intervention of a user's home network. This method is robust against any possible failure of a home network authentication server or any of the networks along the path between home and visited network authentication servers. One design novelty of Method II is for the key storage scalability. We propose a practical public key certificate structure such that the number of public/private keys stored in a network authentication server is linear with the number of service providers rather than the much larger number of networks or users. Another new feature of the Lightweight Localized Authentication method is the protocol built-in defense against some forms of denial of service (DoS) attacks in which attackers try to exploit the intensive computation required by public key decryption.

The remainder of this paper is organized as follows. In Section 2, we introduce the related work in wireless roaming authentication. In Section 3, we discuss the proposed Method I in detail. The design rationale and the specific cryptographic primitive are described. In Section 4, we present the proposed Method II and its public key certificate structure. In Section 5, we outline the analytical model for roaming authentication transmission overhead between home and visited networks. In Section 6, we provide the measured data for the latency of roaming authentication. In Section 7, we measure and compare the energy consumption of mobile terminals under the various authentication methods. Conclusions appear in Section 8.

2 Background and Related Work

In future, a few wireless Internet service providers may appear in a network scale comparable to that of cellular networks. Roaming supports the goal of connecting to the Internet anywhere and at any time. Users are able to receive only one bill from their service provider when they travel across different networks. Figure 1 depicts this concept. A mobile terminal, belonging to home network A, shares a secret with A's authentication center. When the mobile terminal travels into visited network B, the authentication center of network B does not have a shared secret with the mobile terminal. If the mobile terminal makes an association request, a mutual authentication will be required between the authentication center of network B and the mobile terminal. If the mobile terminal subsequently moves from one cluster of access points to another within network B, or is periodically reauthenticated by network B during the residence, intra-network roaming authentications occurs.

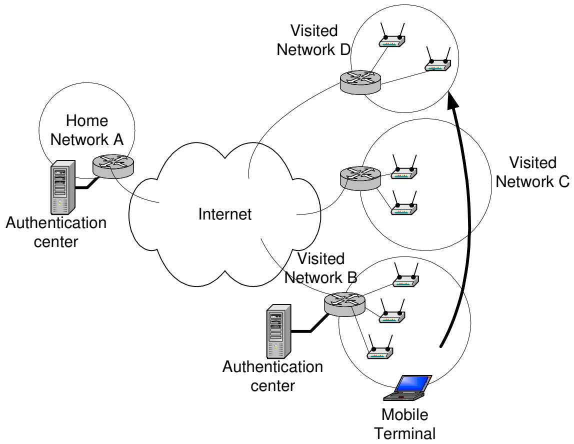

Figure 1: Roaming from a network to another requires the initial roaming authentication. Moving across access points within a network requires intra-network roaming authentication.

Roaming across different administrative domains of the same type of wireless networks are illustrated in Figure 1. Note that there is an active research and standardization field on the roaming between networks of different types (e.g. roaming from cellular to WiFi networks). For instance, IEEE formed the 802.21 group to work on the roaming standardization. Arkko and Haverinen [7] proposed an EAP method in RFC 4187 that uses the algorithm of 3G authentication and key agreement for wireless LAN. The group of 3GPP also published the corresponding technical specification [3]. Among the research literature, Yang *et al.* [30] gave a comprehensive review on the 3G and WLAN interworking security. Koien and Haslestad [19] presented the security architectures for the WLAN-UMTS and elaborated on the issue of identity privacy. Salkintzis *et al.* [28] compared various interworking architectures for the WLAN-GPRS integration and discussed the authentication under tight and loose WLAN-GPRS coupling. Kim and Afifi [18] introduced the new architecture combining the AAA framework with the 3G AKA. Cheng and Tsao [10] proposed a novel access control mechanism that reuses the existing 3G authentication procedures to obtain wireless LAN access with or without IEEE 802.1x. Dutta *et al.* [13] used standard virtual private network technologies to support authentication for seamless mobility across heterogeneous radio systems. Ouyang and Chu [24] introduced public-key encryption based one-time session key generation protocol for handover security between UMTS and WLAN.

It is conceivable that mutual authentication between roaming user and visited network needs to be bootstrapped by the trust of home network (by either public key certificate infrastructure or the communication between home and visited network). The technical challenge is how to perform the mutual authentication efficiently when a roaming user makes multiple authentication requests in a visited network. Most existing methods rely on the continuous authentication credential communication between home and visited networks. Some previous work introduced the mechanisms of visited network/roaming user caching authentication key. Alternatively public key methods are used for the localized authentication, which requires a proper public key certificate infrastructure. Nevertheless, those existing protocols are rather complex. Therefore, both achieving the security and the performance in terms of communication/computation overhead are the desirable goals for the roaming authentication protocols.

2.1 AKA in 3G Roaming Authentication Protocol

In the 3G authentication protocol [1, 2, 4], a mobile terminal and its home network authentication center share a key. In addition, both entities keep track of a sequence number. Upon receiving the authentication request, the authentication center of the home network performs the cryptographic algorithm to calculate AV (Authentication Vector), using the shared secret and sequence number. Each AV is good for one authentication and key agreement (AKA) between the mobile terminal and the visited network. The roaming mobile terminal uses its key and the synchronized sequence number to verify part of AV in order to validate the visited network. The visited network compares the received response from the mobile terminal with the expected response in AV to authenticate the roaming mobile terminal.

The sequence number defends against replay attacks. Nevertheless, since the visited network cannot derive AV, every intra-network roaming authentication requires one transmission of AV between the home and the visited networks. Because this kind of transmission is usually expensive, increasing the number L of AVs in one transmission to reduce the number of transmissions is desirable. On the other hand, if L is too large, the AVs may be wasted if a mobile terminal does not make many authentication attempts within the visited network. In the 3G standard, L is fixed at an empirical number 5. An adaptive algorithm on L was proposed by Lin and Chen [20], which achieved better performance on transmission overhead at the cost of increasing implementation complexity.

In summary, under the 3G authentication protocol, the initial and intra-network roaming authentication relies on home networks to generate the authentication vectors. This characteristic determines that a visited network needs to frequently communicate with a home network to fetch the authentication vectors.

2.2 SSL/TLS-based Methods

The password-based method leveraging TLS [12] or SSL was proposed by Anton *et al.* [6]. A user has a password and the authentication center of its home network stores the cryptographic hash of the password. An encrypted channel will be established by the SSL or TLS protocol between the mobile terminal and the visited network. Then the user enters his/her credentials, such as name@domain and password, into the authentication portal of the visited network through the encrypted channel. Next, the visited network sends the user's credentials to its home network through a pre-established secure channel between networks. Only the home network is capable of verifying the user's credentials and thus sends the decision ("accept" or "reject") back to the visited network. The network-to-user authentication is achieved during the execution of the SSL handshake. One potential drawback of this method is that the password, presumably a secret only shared by the mobile terminal and its home network, is now released to visited networks. A single sign-on authentication architecture that confederates wireless LAN service providers through trusted identity providers was proposed by Matsunaga *et al.* [22]. Tseng *et al.* [29] presented a one-time password protocol to enhance the security of [6]. Another protocol based on public key scheme in [29] provides the non-repudiation for roaming authentication in the integration of WLAN and 3G networks.

3 Proposed Method I: Nonce-based Authentication

In Method I, a user's mobile terminal and its home network share a key, but have different cryptographic random number seeds. During the initial roaming authentication, a user and its home network authentication center will challenge each other using the nonce generated by the random number seed. Another feature of the scheme is that an authentication key K_{auth} is derived by the nonces and the shared key during the protocol execution, which is then cached by the visited network authentication center and the mobile terminal. The derived K_{auth} is used for subsequent intra-network roaming authentication.

3.1 Initial Roaming Authentication Scheme

Figure 2 shows the message flows of the proposed Method I. In contrast to the 3G authentication protocol, a cryptographic nonce $Nonce_{MT}$ generated by the mobile terminal is included in the first message flow. Accordingly, the authentication center of the home network performs the cryptographic algorithm over the mobile terminal $Nonce_{MT}$ and its own $Nonce_{HN}$. Assume that the mobile terminal and its home network authentication center share a key k. The construction of the authentication vector AV is expressed as:

$$\begin{aligned} XRES &= HMAC_k(Nonce_{MT}, Nonce_{HN}) && (1)\\ AUTN &= HMAC_k(Nonce_{HN}, Nonce_{MT}) && (2)\\ K_{auth} &= HMAC_k(Nonce_{MT}, Nonce_{HN}, ID_{MT}, \\ &\quad ID_{HN}) && (3)\\ CK &= HMAC_k(Nonce_{MT}, Nonce_{HN}, padding_A) && (4)\\ IK &= HMAC_k(Nonce_{MT}, Nonce_{HN}, padding_B) && (5) \end{aligned}$$

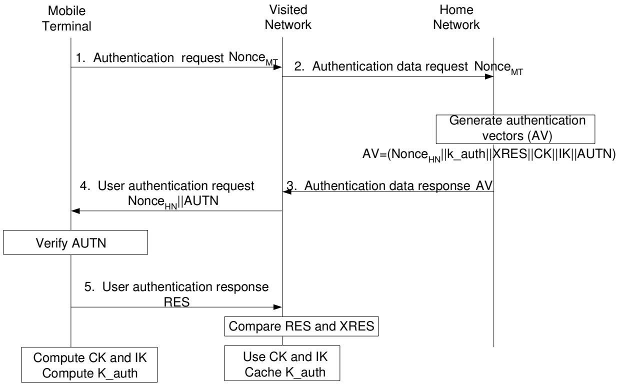
Mobile Terminal
Visited Network
Home Network
1. Authentication request Nonce$_{MT}$
2. Authentication data request Nonce$_{MT}$
Generate authentication vectors (AV)
AV=(Nonce$_{HN}$||k_auth||XRES||CK||IK||AUTN)
3. Authentication data response AV
4. User authentication request Nonce$_{HN}$||AUTN
Verify AUTN
5. User authentication response RES
Compare RES and XRES
Compute CK and IK
Compute K_auth
Use CK and IK
Cache K_auth

Figure 2: Message flows in the proposed Method I (Nonce-based Authentication). The characteristic of Method I lies in the fields of Nonce, AUTH, and K_{auth}.

Where HMAC is the standard keyed message authentication code [23], IDs are the identifiers or names, and *paddings* are the prescribed publicly known character strings. $XRES$ is the expected response used by the visited network to authenticate the mobile terminal. $AUTN$ is the authentication token used by the mobile terminal to authenticate the visited network. Notice that we assume *a priori* secured channel between home and visited networks, which is typically true in current operations of cellular networks. In other words, at Step 3, the home network sends the authentication credentials to the visited network through the secured channel.

At Step 4 in Figure 2, the visited network passes $AUTN$ and $Nonce_{HN}$ to the mobile terminal. Because the mobile terminal knows shared key k and $Nonce_{MT}$, it can verify the authenticity of $AUTN$ by computing Equation (2). If transmitted value of $AUTN$ does not match the computed one, the mobile terminal will drop the session. Otherwise, the mobile terminal will calculate the response RES according to Equation (1) and send it to the visited network. The visited network, by comparing RES with $XRES$, determines if the mobile terminal is authentic or not. CK and IK are the cipher and integrity keys for the data protection of the initial session after the handshake. The padding is used to ensure that CK and IK are distinct and independent.

For the AKA protocol in the 3G, the home network sends the sequence number via the visited network to the mobile terminal. In order to keep the synchronization of the sequence for the freshness of the authentication, the visited network needs to communicate with the home network. In the proposed Nonce-based Authentication, $Nonce_{MT}$ and $Nonce_{HN}$ can ensure the freshness of the authentication handshake, which eliminates the sequence number and thus reduces the communication overhead between home and visited network. Overall, the design of the proposed Nonce-based Authentication protocol follows the well-understood key exchange and authentication principles in [5, 8].

3.2 Intra-Network Roaming Authentication

The number of AV (or authentication vector shown at Step 3 in Figure 2 in the proposed method is one. After the inital roaming authentication, the visited network authentication center caches K_{auth}, which is derived by both nonces, identifiers, and the shared key between the home network and the user. For instance, K_{auth} will be cached from the time of creation to 23:59:59 of the same day or even longer. Similarly, the client program in the user's terminal also caches K_{auth}. During the cache valid period, K_{auth} will be used for all intra-network roaming authentications. The authentication protocol for this two-party intra-network authentication can use the well-known ones such as the 802.11i 4-way handshake or the TLS handshake under session reuse. Consequently, no authentication transmission between the home and visited networks is required for intra-network roaming authentications.

3.3 Security Analysis

The authentication request includes $Nonce_{MT}$ generated by the mobile terminal, which is an unpredictable random number. The home network also produces $Nonce_{HN}$. Both nonces appearing in the HMAC function can ensure freshness of the AV components including K_{auth}. In addition, both sides contribute to the input of the HMAC function, which can defend against chosen text attacks. Without both nonces, the malicious protocol participant may perform many handshakes with a legitimate participant and use the legitimate one as the oracle to obtain the pairs of plain/cipher text or message/signature for cryptanalysis. Furthermore, these random nonces $Nonce_{MT}$ and $Nonce_{HN}$ make the synchronized sequence number between a roaming user and its home network unnecessary.

The mobile terminal can use the nonce and the shared key to verify the authenticity of the message at Step 4. The correctness of the message implies that it is from the home network. Subsequently, the mobile terminal believes that the home network trusts the visited network, and is convinced that the visited network is authentic. The visited network compares the message at Step 5 with the expected response. Only the party that possesses the correct key can compute a valid message of Step 5; therefore, the visited network believes that the mobile terminal is the legitimate one from the corresponding home network.

Notice that the bogus network cannot establish itself as the man-in-the-middle because it cannot setup the security association with an actual home network. In practice, different networks will typically use out-of-band channel to distribute keys to establish their security association. Hence, the bogus network is not able to generate the correct message at Step 4, and the authentication protocol will abort upon the invalidity of message in Step 4. In addition, the use of nonces can thwart the replay attacks by the adversaries.

4 Method II: Lightweight Localized Authentication

Method II, Lightweight Localized Authentication, is based on public key cryptography. The nodes involved in the system, i.e. authentication centers and mobile terminals, have their public/private key pairs. Since this is a closed system comprised of wireless Internet service providers (WISP) and their subscribers, we advocate that the service providers are the key issuer or certification authority. Thus, the operation cost of the scheme can be reduced, as third-party certificate authority charges a fee per certificate. If all users and networks had a certificate, a considerable amount of money would be spent on certificates by third-parties. Another noticeable feature of the proposed public key certificate structure is the significant reduction in key storage.

4.1 Public Key Certificate Structure

Figure 3 illustrates the public key certificate structure. For simplicity of presentation, we assume an imaginary user Bob, subscribing to WISP I. His home network is network I. Under the proposed public key certificate structure, service providers are in the top of the hierarchy and have the master public/private key pairs. In the example, WISPs I and II have the public/private key pairs PK_1/SK_1 and PK_2/SK_2, respectively. The valid period for these keys may be relatively long (e.g. half year or more). Service providers in the roaming agreement will also cross-certify each other's public key, as is shown by $SK_1 \ll PK_2 \gg$ (WISP I certifying the public key of WISP II) in the notation of X.509 [15].

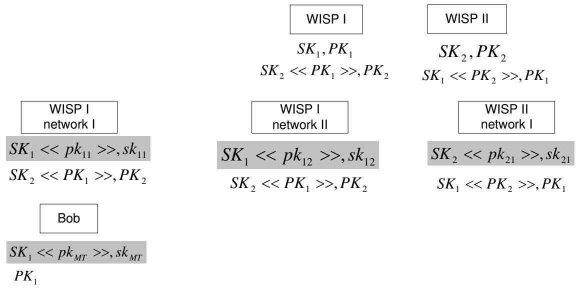

Figure 3: Proposed public key certificate structure for Method II (Lightweight Localized Authentication). Three-level hierarchy is shown: service providers, their networks, and end-users. The notation of public key certificate is from X.509. SK/PK denote private/public keys, respectively.

Each network of a service provider will have a public/private key pair, e.g. $SK_1 \ll PK_{11} \gg /SK_{11}$ in the case of network I of WISP I. The network's private/public key pair may have a shorter valid period (e.g. one month). Additionally, the service provider distributes its public key as well as other service providers' public keys to its networks.

A subscriber (such as Bob) of WISP I has their public/private key pair certified by the service provider, as denoted by $SK_1 \ll PK_{MT} \gg /SK_{MT}$. The user also obtains the public key of its service provider. The valid period of the public/private key pair of the user may be short (e.g. one month). We have chosen a short valid period for user's and network's public key so that the certificate revocation issue may be avoided in our scheme.

We use the following example to illustrate the correctness of the proposed public key certificate structure. When Bob moves to network II of WISP I, Bob is able to verify the visited network's public key $SK_1 \ll pk_{12} \gg$via PK_1. Meanwhile, the visited network can verify Bob's public key $SK_1 \ll PK_{MT} \gg$through PK_1. If Bob moves to network I of WISP II, Bob can chain-verify the visited network's public key $SK_2 \ll pk_{21} \gg$ and $SK_1 \ll PK_2 \gg$ via PK_1, and the visited network can verify Bob's public key $SK_1 \ll PK_{MT} \gg$ through PK_1.

In addition to the advantage of reducing costs, the above public key certificate structure renders a scalable solution not only to the service providers but also to users. Suppose there are a service providers, b networks and c subscribers in the roaming agreement. One estimate is that a, b, and c equal to 6, 2000, and 1,000,000, respectively. Under our scheme, as depicted in Figure 3, each user stores 3 keys (its public/private key pair and the service provider's public key); each network stores $2(a-1)+2$ keys (its public/private key pair of 2 keys plus other service providers public keys of the number $(a-1)$ plus its service provider public key cross-certified by other service providers of the number $(a-1)$); By the same token, each service provider stores $2(a-1)+2$ keys. As a result, the number of keys stored is linear with the number a of service providers, which is relatively a small number.

4.2 Protocol Details

Figure 4 shows the message flows of the authentication protocol, which is inspired by the SSL or TLS handshake. After verifying the authenticity of the visited network's public key, the mobile terminal will encrypt a secret random number *premaster_key* using the visited network's public key PK_{VN}. Since only the visited network has the corresponding private key, the visited network can decrypt the cipher text to obtain the *premaster_key.* Thus, both sides establish a shared secret of *premaster_key.*

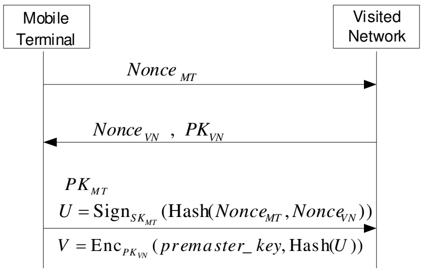
Mobile Terminal
Visited Network
$Nonce_{MT}$
$Nonce_{VN}$, PK_{VN}
PK_{MT}
$U = \mathrm{Sign}_{SK_{MT}}(\mathrm{Hash}(Nonce_{MT}, Nonce_{VN}))$
$V = \mathrm{Enc}_{PK_{VN}}(premaster\_key, \mathrm{Hash}(U))$

Figure 4: Message flows in Method II (Lightweight Localized Authentication). The main features of Method II lie in the construction of U and V

One salient difference of the proposed scheme from the SSL/TLS protocol is the mechanism of signature verification independent from public key decryption in message flow 3 from the mobile terminal to the visited network, which has the characteristic for performance efficiency. We reiterate message flow 3 as follows:

$$U = Sign_{SK_{MT}}(Hash(Nonce_{MT}, Nonce_{VN})) \quad (6)$$
$$V = Enc_{PK_{VN}}(premaster\_key, Hash(U))), \quad (7)$$

where the mobile terminal uses its private key SK_{MT} to sign over the hash result of two nonces in Equation (6) and encrypts using the public key PK_{VN} of visited network in Equation (7). For the verification, the visited network validates the user's signature first using the public key PK_{MT}. If the signature is authentic, the visited network then decrypts the cipher text. If the signature of the mobile terminal is invalid, the visited network simply drops the handshake. Given a bogus handshake message, the computational cost saved by our scheme is the public key decryption that is usually expensive in cryptographic protocols. We did the benchmark using the well-regarded Crypto++ library [11] on a Pentium 4 machine with 1.9GHz CPU and 256 MB memory. The result is shown in Table I, where public key decryption timing is an order of magnitude higher than signature verification. In Equation (7), we add Hash(U) in the plaintext so that U and V are interleaved. If adversaries change V, the visited network can detect such modifications by comparing the hashes Hash(U). Note that, in SSL and TLS, U and V are mixed by keyed hash in Equation (6). Thus a server has to do the decryption first in SSL/TLS, which increases the computation cost. The proposed scheme also derives K_{auth}, which is used for all subsequent intra-network roaming authentication. A secure yet convenient way to derive K_{auth} is

$$K_{auth} = HMAC_{premaster\_key}(Nonce_{VN}, PK_{VN}, Nonce_{MT}, PK_{MT}).$$

Table 1: Computational time of crypto operations on a 1.9 GHz Intel Pentium 4 with 256 MB memory (RSA: 1024 bits, HMAC: 160 bits using SHA-1)

	Computational time (ms)
RSA encryption (e=17)	0.19
RSA decryption	4.65
RSA signature generation	4.65
RSA signature verification (e=17)	0.19
HMAC	0.002

In a concrete example, assume that an attacker, who does not have the legitimate public/private key pair, sends an authentication request. Under our scheme, the visited network consumes 0.19ms of CPU time to verify the signature, while in the original SSL protocol the visited network has to consume 4.65ms+0.19ms to determine that the message is invalid. As a result, the effect of flooding authentication requests to overwhelm the authentication center of a visited network can be mitigated by our scheme.

4.3 Security Analysis

The proposed Localized Lightweight Authentication protocol requires public/private keys. We assume that SK_{MT} is only known by the mobile terminal. Also, the mobile terminal has the correct public key of the user's home network. In addition, the private key of the visited network is only known by the visited network itself. For the implementation matter, we also assume that the pseudo-random number generator is secure, i.e. the random nonce is unpredictable for any party except the mobile terminal or the visited network. Based on the above assumptions, we analyze the security of the proposed protocol against replay attacks and impersonation attacks.

Messages 1 and 2 exchange the nonces of the mobile terminal and the visited network. Based on the proposed public key certificate infrastructure, the roaming user's device can verify the authenticity of the public key of the visited network. The bogus network does not have the private key of a legitimate network, so it cannot decrypt the message 3 to obtain the proper *premaster_key*. Consequently, it will not able to establish the security association with the mobile terminal.

In the other case, a malicious client does not have the appropriate public key certified by a wireless Internet service provider. Thus the malicious client cannot generate valid signature over the two nonces. Therefore, the visited network will surely reject the message 3 and the authentication request upon the invalid signature in message 3. It can be seen that the nonces can ensure that the client signature is fresh and the attacker cannot succeed in replay attacks.

Attacker, as a middle-man between the mobile terminal and visited network, cannot derive the correct *premaster_key*. Thus the malicious middle-man cannot establish the secure association on behalf of the legitimate network or the legitimate user. Notice that the hash of the signature in message 3 is included in the public key encryption, which guarantees that the signature U and the ciphertext V are bounded together for a particular session. In other words, the attackers cannot pick U and V individually from different authentication sessions and combine them to construct a valid message 3 in one authentication session.

5 Analytical Model: Authentication Transmission Overhead

BETWEEN HOME AND VISITED NETWORKS

It is folklore in the wireless networking community that, for roaming authentication purposes, transmission between the home and visited networks might be expensive [20]. In this section, we evaluate the performance of Method I, the 3G authentication protocol, and the adaptive scheme for 3G authentication (method of Lin and Chen) [20] in terms of the number of authentication transmissions between the home and visited networks. The evaluation methodology is the average-case analysis drawn from [20].

Let the transmission overhead between home and visited networks per user be defined $J = nC$, where n is the number of transmissions between home and visited networks and C is the normalized cost per transmission. Assume that a roaming user makes a number of authentication requests that satisfy the Poisson distribution with mean λ in a unit time. According to the probability mass function of the Poisson distribution,

$$\Theta(n,\tau) = \sum_{i=1}^{L}\{\frac{(\lambda\tau^{(n-1)L+i})}{[(n-1)L+i!]}\}e^{-\lambda\tau},$$

where $\Theta(n,\tau)$ is the probability that there are n transmissions between the visited and home networks in a specific period τ, and L is the number of AVs during each transmission. The residence time period is assumed to be exponentially distributed with mean $1/\mu$, and the probability density function is

$$f(t) = \mu e^{-\mu t}.$$

Then the probability that there are n authentication transmissions between the visited and home networks during the mobile terminal's residence in the visited network is

$$p(n) = \int_{t=0}^{\infty}\Theta(n,t)f(t)dt = (\frac{\lambda}{\lambda+\mu})^{(n-1)L}[1-(\frac{\lambda}{\lambda+\mu})^{L}].$$

Thus the average number of transmissions is

$$E[n] = \sum_{n-1}^{\infty} np(n) = 1/(1-(\frac{\lambda}{\lambda+\mu})^{L}).$$

Define transmitting one AV is a unit cost. Therefore, the normalized transmission overhead per user in its residence at a visited network for both the 3G method and the method of Lin and Chen is

$$J_0(L) = E[n](L+2\alpha),$$

where 2α is the fixed cost of a round-trip transmission from the home network to the visited network, and L represents the transmission cost of L AVs from the home network to the visited network. The 3G standard fixes $L = 5$, whereas L is adaptive in the method of Lin and Chen. The transmission cost of the proposed Method I (Nonce-based Authentication) is

$$J_1(L) = 1 \times (1+2\alpha).$$

In the Method I, only one transmission and one authentication vector are required so that we have $E[n] = 1$ and $L = 1$.

In the baseline result of the analysis, we assume that transmission of one AV from the home network to the visited network is 1. Thus, to extrapolate the results of J_0 and J_1, we can adjust the parameter 2α (the ratio of fixed cost to one AV transmission cost) and L (number of AVs). Figure 5 shows the results of the normalized overhead per user under the three methods with different values of α and ratio λ/μ. A larger α means the fixed transmission has a higher share of the transmission cost; and a larger λ/μ indicates a roaming user makes more frequent authentication requests during its residence in a visited network. For the 3G method, $E[n]$ can be obtained by dividing λ/μ with L. The method of Lin and Chen basically estimates the number of authentication requests in current visited network based on the number in the previous visited network. The simulation of their algorithm is based on the assumption of the exponential distribution of the residence time at a visited network.

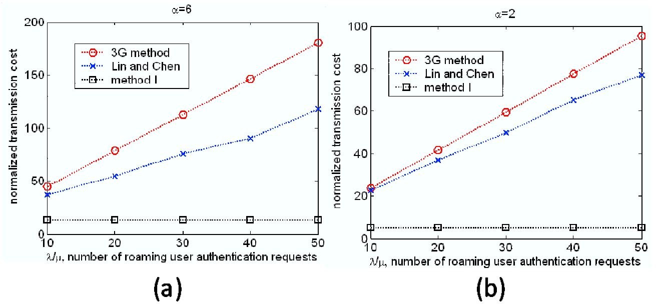

Figure 5: Normalized cost (traffic overhead) between visited and home networks under different authentication protocols. (a) $\alpha = 6$, (b) $\alpha = 2$. α is the ratio of fixed transmission cost to authentication vector transmission cost.

For 3G authentication and the method of Lin and Chen, the transmission cost between the home and visited networks increases with the number of authentication requests, whereas the cost curve remains flat in Method I. For example, when $\lambda/\mu = 50$ and $\alpha = 6$, the cost of Method I is 1/14 of that in 3G authentication and 1/9.5 of that in the method of Lin and Chen. When $\lambda/\mu = 50$ and $\alpha = 2$, the cost of Method I is 1/19 of that in 3G authentication and 1/13.6 of that in the method of Lin and Chen.

6 Measured Authentication Latency

Method II does not contain the transmission cost between the home and visited networks for authentication; however, the cryptographic computation involved in Method II is more expensive than that in Method I and the 3G authentication protocol. In this section, we use the measured data to compare the authentication latency of methods I, II and the 3G authentication protocol.

A laptop in the authors' lab within Auburn University sent requests to three SSL or TLS-enabled Webmail servers: Auburn University or AU (https://tigermail.auburn.edu/), The Georgia Institute of Technology or GT (https://webmail.mail.gatech.edu/), and The University of Washington at Seattle or UW (https://weblogin.washington.edu/). The rationale for performing this study is contained in the fact that the cost of a single roaming transmission for the 3G authentication protocol and Method I is comparable to the SSL session reuse case while the computational cost of Method II is comparable to that of the SSL handshake protocol. The laptop made repeated connections within the first five-minute span of every hour from 8:00 until 22:00 (US central time) on February 17, 2004. The `tcpdump` tool records the time of transmission from the authentication request (or `client hello`) leaving the laptop Ethernet interface to the Web servers' authentication response (or `Finished message from the server`) coming back to the Ethernet interface.

The session reuse case between the laptop and the Auburn Webmail server (labelled "AU" in Figure 6) estimates the cost of intra-network roaming authentication. The other session reuse cases (labelled "GT" and "UW" in Figure 6) approximate the latency of authentication transmission between home and visited networks. The SSL handshake protocol of Auburn University's Webmail server (labelled "AU public key" in Figure 6) estimates the latency of Method II. Notice that this cost will be a slight underestimate since the implementation of the SSL handshake protocol does not include client signature (computational time of signature generation listed in Table 1).

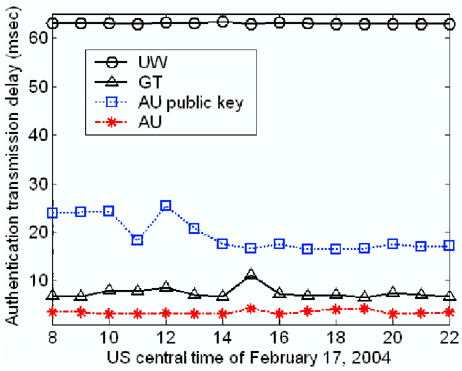

Figure 6: Measured data of authentication transmission delay. "UW" and "GT": transmission between home and visited networks, "AU": intra-network authentication, "AU public key": latency of Method II.

The average transmission delays from UW and GT are 62ms and 8 ms, respectively. The data clearly demonstrate the effect of different geographic distances. GT is about 169 km away from Auburn whereas UW is at a distance of about 6400 km. The AU case is roughly 3 ms, which shows that intra-network authentication can be quite cheap because there is no round-trip between the home and visited networks. All in all, these data indicate that for roaming authentication purposes the transmission between the home and visited networks is expensive, especially if they are far apart. Therefore, a roaming authentication protocol should reduce transmission between the home and visited networks as much as possible.

An average of 20ms is observed for the SSL handshake protocol in Figure 6. If a home network is far away from a visited network (as is the case with the UW), Method II will probably have the lowest latency. In all cases, Method I is better than the 3G authentication method because there is only one transmission between the home and visited networks in Method I but possibly many transmissions in the 3G approach.

7 Energy Consumption Measurement

Energy consumption is an important issue in wireless roaming authentication because of the nature of battery-powered mobile terminals. Previous work investigating energy consumption of cryptographic protocols appeared in [17]. The methodology for energy measurement is derived from the experimental setup reported in [25]. A PDA (266 MHz CPU), through an IEEE 802.11b interface, connects to an access point, which in turn connects through a hub to an authentication server (Pentium 4, 1.9 GHz CPU, 512 MB memory). The experimental setup is shown in Figure 7. The results are obtained by measuring the current drawn from the power supply (connecting a sense resistor in series between the PDA and the external energy supply) during authentication handshake.

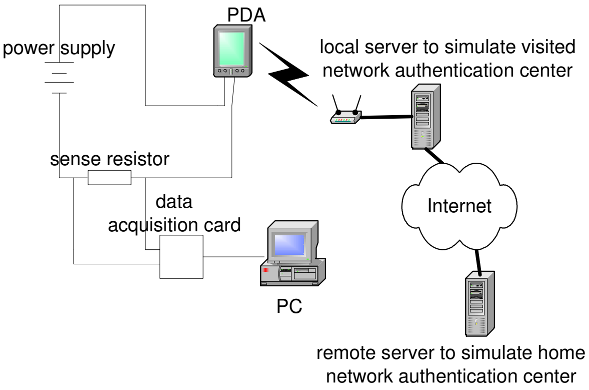
PDA
power supply
local server to simulate visited
network authentication center
sense resistor
data
acquisition card
Internet
PC
remote server to simulate home
network authentication center

Figure 7: Energy measurement tested

Three tests were performed: the first test is the SSL protocol with client authentication (local authentication server); the second test is the implementation of a shared-key protocol (local authentication server); and the third test is a shared-key protocol implementation (remote authentication server, 169 km away). The first one approximates the energy consumption of Method II; the second one approximates the energy consumption for intra-network roaming authentication; and the third one approximates the energy consumption for roaming authentication with home network intervention.

We let the equipment make repeated authentication handshakes for each method. Dividing the total energy expenditure by the number of repetitions, we obtain the average energy cost per authentication. The results are: the SSL protocol costs 710 mJ, the second test 67 mJ, and the third test 117 mJ. The difference between the last two can be explained by the transmission between the remote and local servers, which increases the energy consumption of the wireless transceiver in PDA by elongating the duration of authentication. To quantitatively compare the energy consumption of a mobile terminal for 3G, the proposed nonce-based, lightweight localization authentication methods, we extrapolate the above data and plot the results in Figure 8. Assume that a user makes z authentication requests during its residence in a visited network. Under the 3G method, the energy cost is $117\times(\lfloor z/5\rfloor+1)+67\times(z-\lfloor z/5\rfloor-1)$ (mJ); under the proposed Method II, the energy cost is $710+67(z-1)$ (mJ); under the proposed Method I, the energy cost is $117+67(z-1)$ (mJ). Note that $\lfloor x\rfloor$denotes the largest integer that does not exceed x.

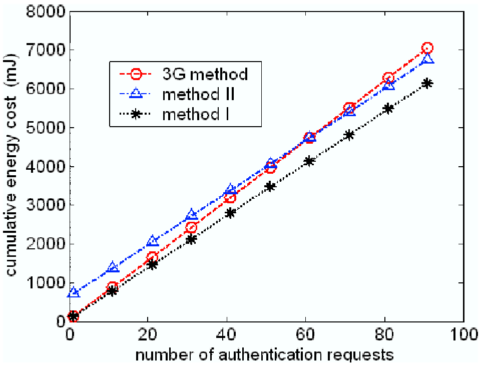

Figure 8: Extrapolated energy consumption results of the mobile terminal under three authentication methods under the specific energy measurement tested described in this paper.

In terms of energy consumption, the proposed Method I generally has the best performance in that it only incurs one transmission between the home and visited networks. If a roaming user has many authentication requests during residence (larger than 60 in our test platform), both proposed methods have lower energy consumption than the 3G authentication protocol.

8 Conclusions

In this paper, two authentication methods are proposed for wireless roaming authentication. The design goal is to reduce the number of transmissions between the home and visited networks for roaming authentication. Experimental results demonstrate that the proposed methods can reduce the authentication traffic overhead for the network operators, the authentication latency experienced by an end user, and the energy consumption for a mobile terminal. Method I, Nonce-based Authentication, generally has the best overall performance in terms of authentication delay and energy consumption for a mobile terminal. Method II, Lightweight Localized Authentication, is suitable in the situation in which a home network is far away or there may be a failure along the path between home/visited network authentication centers.

References

[1] 3GPP, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements (Release 4)*, TS 33.105 V4.1.0, June 2001.

[2] 3GPP, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 6)*, TS 33.102 V6.3.0, Dec. 2004.

[3] 3GPP, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Wireless Local Area Network (WLAN) Interwoking Security (Release 6)*, TS 33.234 V6.5.1, June 2005.

[4] 3GPP2, *Enhanced Cryptographic Algorithm*, S. S0055, V1.0, Jan. 2002.

[5] M. Abadi, and R. Needham, "Prudent engineering practice for cryptographic protocols," *IEEE Transactions on Software Engineering*, vol. 22, no. 1, pp. 6-15, Jan. 1996.

[6] B. Anton, B. Bullock, and J. Short, *Best Current Practices for Wireless Internet Service Provider (WISP) Roaming*, Wi-Fi Alliance, Feb. 2003. (http://www.weca.net/OpenSection/wispr.asp)

[7] J. Arkko and H. Haverinen, *Extensible Authentication Protocol Method For 3rd Generation Authentication And Key Agreement (EAP-AKA)*, RFC 4187, Jan. 2006.

[8] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, and M. Yung, "Systematic design of two-party authentication protocols," in *Proceedings of Crypto'91*, pp. 44-61, Aug. 1991.

[9] C. W. Chen, M. C. Chuang, and C. S. Tsai, "An efficient authentication scheme between MANET and WLAN based on mobile IPv6," *International Journal of Network Security*, vol. 1, no. 1, pp. 14-23, July 2005.

[10] R. G. Cheng and S. L. Tsao, "3G-based access control for 3GPP-WLAN interworking," in *Proceedings of 2004 IEEE 59th Spring Vehicular Technology Conference*, vol. 5, pp. 2967-2971, 2004.

[11] W. Dai, *Crypto++ Library 5.1.* (http://www.eskimo.com/ weidai/cryptlib.html)

[12] T. Dierks and C. Allen, *The TLS Protocol Version 1.0*, RFC 2246, Jan. 1999.

[13] A. Dutta, T. Zhang, S. Madhani, K. Taniuchi, K. Fujimoto, Y. katsube, Y. Ohba, and H. Schulzrinne, "Secure universal mobility for wireless Internet," in *Proceedings of ACM 2nd International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots*, pp. 71-80, Oct. 2004.

[14] K. Hwang and C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," *IEEE Transactions on Wireless Communications*, vol. 2, no. 2, pp. 400-407, 2003.

[15] ITU-T, *Information Technology - Open Systems Interconnection - The Directory: Public-Key And Attribute Certificate Frameworks; Recommendation X.509*, Mar. 2000.

[16] G. Kambourakis, A. Rouskas, G. Kormentzas, and S. Gritzalis, "Advanced SSL/TLS-based authentication for secure WLAN-3G interworking," *IEE Proceedings of Communications,* vol. 151, no. 5, pp. 501-506, Oct. 2004.

[17] R. Karri and P. Mishra, "Minimizing energy consumption of secure wireless session with QoS constraints," in *Proceedings of IEEE ICC'02,* vol. 4, pp. 2053-2057, 2002.

[18] H. Kim and H. Afifi, "Improving mobile authentication with new AAA protocols," in *Proceedings of IEEE Conference on Communications (ICC'03),* vol. 1, pp. 497-501, May 2003.

[19] G. Koien and T. Haslestad, "Security aspects of 3G-WLAN interworking," *IEEE Communications Magazine,* vol. 41, no. 11, pp. 82-88, Nov. 2003.

[20] Y. B. Lin and Y. K. Chen, "Reducing authentication signaling traffic in third-generation mobile network," *IEEE Transactions on Wireless Communications,* vol. 2, no. 3, pp. 493-501, 2003.

[21] M. Long, C. H. Wu, and J. D. Irwin, "Localized authentication for wireless LAN inter-network roaming," in *Proceedings of IEEE Wireless Communications and Networking (WCNC'04),* pp. 264-267, Mar. 2004.

[22] Y. Matsunaga, A. Merino, T. Suzuki, and R. Katz, "Secure authentication system for public WLAN roaming," in *Proceedings of ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots*, pp. 113-121, Sep. 2003.

[23] NIST, *The Keyed-Hash Message Authentication Code (HMAC)*, FIPS PUB 198, Mar. 2002.

[24] Y. C. Ouyang and C. H. Chu, "A secure context transfer scheme for integration of UMTS and 802.11 WLANs," in *Proceedings of 2004 IEEE International Conference on Networking, Sensing and Control*, vol. 1, pp. 559-564, Mar. 2004.

[25] N. Potlapally, S. Ravi, A. Raghunathan, and N. Jha, "Analyzing the energy consumption of security protocols," in *Proceedings of ACM International Symposium on Low Power Electronics and Design*, pp. 30-35, 2003.

[26] P. Prasithsangaree and P. Krishnamurthy, "A new authentication mechanism for loosely coupled 3G-WLAN integrated networks," in *Proceedings of 2004 IEEE 59th Spring Vehicular Technology Conference*, vol. 5, pp. 2998-3003, May 2004.

[27] S. Suzuki and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," *IEEE Journal of Selected Areas in Communications*, vol. 15, no. 8, pp. 1608-1617, 1997.

[28] A. K. Salkintzis, C. Fors, and R. Pazhyannur, "WLAN-GPRS integration for next-generation mobile data networks," *IEEE Wireless Communications,* pp. 112-124, Oct. 2002.

[29] Y. M. Tseng, C. C. Yang, and J. H. Su, "Authentication and billing protocols for the integration of WLAN and 3G networks," *Wireless Personal Communications*, vol. 29, pp. 351-366, June 2004.

[30] C. C. Yang, K. H. Chu, and Y. W. Yang, "3G and WLAN interworking security: current status and key issues," *International Journal of Network Security*, vol. 2, no. 1, pp. 1-13, Jan. 2006.

Men Long was born in Chongqing, China, in 1978. He received the B.E. degree (Honors) from Chongqing University in 2000, and the Ph.D. degree from Auburn University, Auburn, AL, USA, in 2005, both in Electrical Engineering. Men Long joined the Communications Technology Lab of Intel Corporation as a network software engineer at Hillsboro, OR, USA, in 2005. He is working on various projects on computer and network security. Dr. Long has published dozens of transactions and conference papers in the areas of network security, wireless networking, and image processing.

Chwan-Hwa "John" Wu is currently a Professor of Electrical and Computer Engineering at Auburn University. He has been the principal investigator on research projects funded by DoD, NSF, NASA, US Marshals Service, USDA, and Cray Research, Inc and many other companies. His current research interests include information security and computer networks. Dr. Wu is an author and co-author of over 50 journal papers in IEEE Transactions, International Journal of Network Security, Physical Reviews, Applied Physics Letters, Applied Optics, Journal of Parallel and Distributed Computing and the like, and over 110 conference publications, as well as holding a U. S. patent. His first book, entitled merging Technologies in Multimedia Computer Communications, was published by Prentice Hall in 1997. He has served as committee members and referees for numerous conferences and journals, Guest Editors for IEEE Transactions on Plasma Science and IEEE Transactions on Industrial Electronics, an Associate Editor of IEEE Transactions on Industrial Electronics, a member of Steering Committee of IEEE Transactions on Mobile Computing and an editorial board member of International Journal of Information and Computer Security. He received IEEE Transactions on Industrial Electronics 1997 Outstanding Paper Award. He is an IEEE Fellow.

J. David Irwin (F) was born in Minneapolis MN on August 9, 1939. He received the B.E.E. degree from Auburn University in 1961 and the M.S. and Ph.D. degrees from the University of Tennessee at Knoxville in 1962 and 1967, respectively. In 1967 he joined Bell Telephone Laboratories, Inc., Holmdel, NJ, as a Member of the Technical Staff and was made a Supervisor in 1968. He joined Auburn University in 1969 as an Assistant Professor of Electrical Engineering. He was made an Associate Professor in 1972, Associate Professor and Head in 1973, and Professor and Head in 1976. He has been Earle C. Williams Eminent Scholar and Head since 1993. He has held a number of positions with IEEE including President of both the Industrial Electronics and Education Societies and Editor of the IEEE Transactions on Industrial Electronics. He is the author or co-author of numerous books and papers including Basic Engineering Circuit Analysis, currently in the eighth edition. He is also a Series Editor for Academic Press and CRC Press. He has received a number of awards including an IEEE Third Millennium Medal and the 2000 IEEE Richard M. Emberson Award.