Security and Efficiency in Roaming Services for Wireless Networks: Challenges, Approaches, and Prospects

Daojing He, Chun Chen, and Jiajun Bu, Zhejiang University
Sammy Chan, City University of Hong Kong
Yan Zhang, Simula Research Laboratory, Norway

ABSTRACT

Seamless roaming over wireless networks is highly desirable to mobile users, but ensuring the security and efficiency of this process is challenging. Although the same may be said for all communication systems, roaming services have special requirements and vulnerabilities, and therefore deserve special attention. Over the years, we have seen a variety of authentication protocols emerging to address this issue. However, which protocol is the most effective is still debatable. In this article, we first identify the challenges unique to roaming services as a set of mandatory and optional requirements. Next, we provide a brief state-of-the-art survey of existing work and point out their limitations in securing roaming services, especially in resistance against denial of service attacks, efficient authentication, flexible roaming in mobile contexts, as well as backward and forward non-linkabilities. To complement the security provided by the existing work, we then propose some mechanisms that can meet the aforementioned security and efficiency requirements. Finally, we present challenges that need to be addressed in roaming authentication.

INTRODUCTION

With the advancement in various mobile and wireless networks, including universal mobile telecommunication systems, wireless local area networks, roadside-to-vehicle communication systems [1], and satellite networks, ubiquitous computing becomes a reality. Users can access network services anywhere and anytime, using their mobile devices (e.g., vehicle, smartphone, and tablet PC) even when they are out of the coverage of their subscribed networks. This is supported by roaming services, which allow connections to hand over from one network to another network, although the two networks may belong to different types.

A general roaming scenario for wireless networks is shown in Fig. 1. It involves three parties: a roaming user U, a visited foreign server V, and a home server H of which U is a subscriber. Normally, V and H have a roaming agreement, so U can access its subscribed services through V when U is in a foreign network administered by V. Before U can access resources provided by V, an appropriate authentication process between U and V must be carried out. Such a process is of great importance to all three involved parties because:

- The foreign network does not want its resources or services to be used by illegitimate users without payment.
- The home network does not want to be responsible for illegitimate usage of the foreign network's resources.
- U does not want to be charged by V for resource usage by someone else.

In this article, we first identify the characteristics of secure roaming services, and then present the mandatory and optional requirements for protocols of this kind. Then we review some existing work, providing an overview of these solutions and discussing what requirements they have met. This guides us to choose appropriate solution approaches when a roaming service is to be designed for a specific application scenario. We argue that no roaming technique is ideal for all scenarios where mobile networks are employed; thus, the techniques employed must depend on the requirements of target applications and careful choice of cryptographic techniques. We also point out some major limitations of previously reported studies on secure roaming and introduce a set of mechanisms to mitigate the limitations. Finally, we identify new challenges and suggest the directions of future work on secure roaming.

CHALLENGES

Many security and efficiency challenges exist in roaming services, mainly due to the resource constraints of mobile users, the authentication delay constraint, and the demanding security requirements of roaming applications. With the increasing use of cryptography to protect roaming services, it is important to have a clear understanding of the requirements that an effective roaming authentication protocol should meet. The mandatory requirements are listed and briefly described as follows [2–8]:

1 **Server authentication:** Roaming users should be allowed to authenticate the foreign server they visit to avoid potential deception and other malicious attacks.

2 **Subscription validation:** A visited foreign network must authenticate mobile users to ensure their legitimacy.

3 **Provision of user revocation:** Services to a roaming user should be terminated once its subscription period ends.

4 **Key establishment:** A session key should be established between a roaming user and a visited foreign server to protect subsequent data exchanged between them.

5 **Low computation complexity and communication cost:** A mobile user is generally constrained in terms of power, processing capability, and storage space. The degree of the resource limitation is different for various mobile devices (e.g., laptop PC, smart phone, PDA). Therefore, a roaming authentication process should be computationally efficient. At the same time, such a process should be fast enough to maintain persistent connectivity for mobile users.

6 **Basic user anonymity and non-traceability:** A user should be anonymous, and its activities must not be linkable by eavesdroppers. Non-linkability means that an adversary cannot link the communication activities of a particular user together and thus establish the user's profile.

7 **Attack resistance:** The roaming protocol should have the ability to resist various attacks in wireless networks (e.g., denial of service [DoS] attack, replay attack, deposit-case attack) such that it can be applied in the real world.

At the same time, besides the mandatory requirements, certain application scenarios may impose some optional requirements. They are listed and described briefly in Table 1. Note that some of them are numbered as sub-requirements of the related mandatory requirements. In summary, as depicted in Fig. 2, the main challenge in developing roaming authentication protocols is to provide robust security, that is, meet the mandatory security requirements 1–7 and customize optional security requirements (1.1)–(10) with high efficiency.

Brief Review of Existing Approaches

Existing roaming authentication protocols[1] (e.g., [2–8]) can be classified into two categories: three-party and two-party approaches. As shown in Fig. 3a, the three-party approach requires the involvement of all three parties. The simplest procedure is: Upon receiving a login request from a roaming user U, the foreign server V sends an authentication request to U's home server H. H checks whether U is its legitimate subscriber and V is a legitimate foreign server. After receiving a response from H, V uses the secret information provided by H to perform authentication and key establishment with U. Alternatively, as shown in Fig. 3b, the two-party approach does not involve the home network. That is, without the help of H, V performs mutual authentication and session key establishment with U.

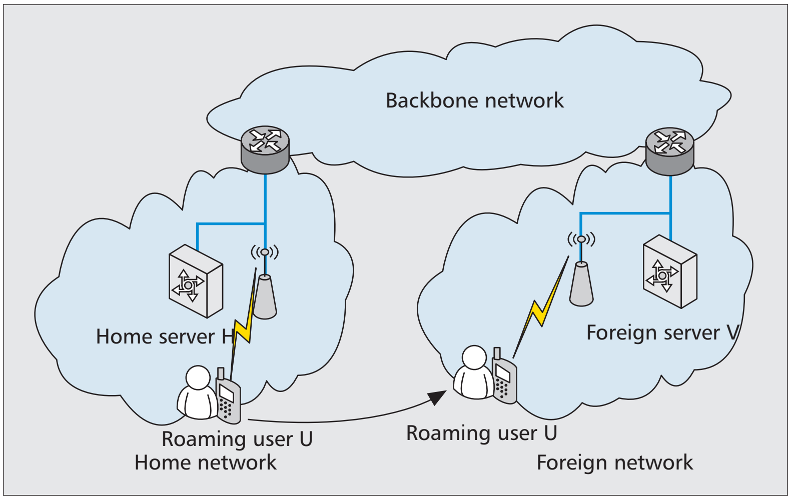

Figure 1. *Overview of roaming services.*

Three-Party Roaming Protocols

The conventional roaming authentication approaches [2, 3] follow the three-party structure. Simple cryptographic techniques (i.e., hash function operation, symmetric and public key cryptography) are usually used for this type of systems. The typical authentication procedures are as follows. A user U sends a login request ($\{ID, h(key||ID||nonce||\ldots)\}$, $\{ID, E_{key}(ID||nonce||\ldots)\}$, or $\{Cert, sign(nonce||\ldots)\}$) to the visited foreign server V, where the notations ID, $h(key||data)$, $E_{key}(.)$, and $sign(.)$ represent the user identity, keyed-hash-function with a session key, encryption with a symmetric key, and digital signature using public key cryptography, respectively. Additionally, $||$ denotes the bit concatenation operator. Also, *nonce* is a random number included in the *beacon messages*, which are periodically broadcast by V to declare service existence. Upon receiving this login request message, server V transmits the message to U's home server H for authentication. Since these approaches only require low-cost cryptographic operations on mobile users and network servers, they are suitable for resource-limited application scenarios. For example, our implementations show that Advanced Encryption Standard (AES) encryption (with a 128-bit plaintext and a 128-bit key) and an ECC-160 digital signature just take 0.6 μs and 102 μs on a 1.2-GHz laptop PC, respectively.

One example is wireless LAN (WLAN) secure roaming. The IEEE 802.1x standard provides an authentication framework that is based on the Extensible Authentication Protocol (EAP). In the EAP framework, some authentication methods including EAP-MD5 (Internet Engineering Task Force [IETF] RFC 1321), EAP-TLS, EAP-TTLS, and EAP-GPSK have

[1] *Disclaimer: To our knowledge, until now more than hundreds of roaming protocols have been proposed. Thus, the roaming authentication schemes covered in this article are not intended to be exhaustive. The choice is due partly to our (clearly subjective) decision about which existing roaming protocols are most eminent.*

(1.1) Local server validation	A user can be sure about the identity of the foreign server without the help of its home server.
(2.1) Local subscription validation	A foreign server can check whether a roaming user is a legitimate subscriber without consulting the user's home server.
(3.1) Local user revocation	Without the involvement of the home server, a foreign server can check whether a roaming user has been revoked.
(3.2) Provision of dynamic user revocation mechanism	To prevent misbehaving users from infiltrating the system, revocation of misbehaving users should take place at any time. Note that in contrast to Requirement (3), dynamic user revocation occurs before the subscription period of a user expires.
(3.3) Easily scheduled revocation	To be flexible, it should easily allow a scheduled revocation after which a user will resume the service. For example, a user may plan to suspend the service for a few months.
(4.1) Strong key establishment	If the session key is solely chosen by one of the two communication parties (i.e., roaming user and visited foreign server), the other party may be induced to force the use of an old key. Additionally, for personal privacy, the home server should not be allowed to obtain the session key.
(4.2) Key establishment with forward/ backward secrecy	Even if a long-term secret key is compromised at any point in time, all the preceding and subsequent session keys cannot be revealed.
(4.3) Update session key periodically	In order to ensure strong security, when a mobile user stays within the same foreign network (or its home network) for longer than a pre-defined threshold time, the session key needs to be updated periodically.
(6.1) The second level user anonymity and non-traceability	In addition to Requirement (6), any user is anonymous and its activities are not linkable by foreign servers. Unless user identity information is imperative in some emergency situations or special applications, the foreign server is only allowed to ensure the legitimacy, rather than the real identity and activity linkability of roaming users.
(6.2) The third level user anonymity and non-traceability	In addition to Requirement (6.1), relationship between roaming users and foreign servers should be anonymous to eavesdroppers.
(6.3) The fourth level user anonymity and non-traceability	In addition to Requirement (6.2), the home server is anonymous to foreign servers.
(6.4) The fifth level user anonymity and non-traceability	In addition to Requirement (6.3), any user is anonymous and its activities are not linkable by its home server.
(8) Non-repudiation	For purpose of billing, it is required that a user cannot deny its usage of network services.
(9) Universal authentication	The same protocol and signaling flows are used regardless of the domain (home or foreign) a user is visiting [5]. This helps reducing the system complexity in practice.
(10) Self-organization	Roaming authentication should not depend on the constant presence of a central authority which would cause scalability and accessibility problems.

Table 1. *Optional requirements for secure roaming protocols.*

been proposed. As one of the most popular EAP types, EAP-MD5 is primarily based on a one-way hash function. When using EAP-MD5, a subscriber computes the hash value with the password as input, and the hash value is transmitted through the visited server to the home server for subscriber validation. The main weakness is that EAP-MD5 cannot support user anonymity and non-traceability, and server authentication. Although the other EAP solutions (e.g., EAP-TLS, EAP-TTLS, and EAP-GPSK) can achieve mutual authentication between mobile users and the visited networks, recent studies [9] have shown that they cannot provide basic user anonymity and non-traceability, session key security, or attack resistance.

Two-Party Roaming Protocols

Compared with the three-party approach, the advantages of the two-party technique include the following. First, it avoids some problems such as the connection loss between the foreign server and the home server, and the single point of failure due to the home server, which are possible in the three-party structure. Second, one drawback of the three-party roaming structure is that these protocols require a foreign server to unconditionally forward any login request, valid or invalid, to the home server [2, 3]. Therefore, an adversary can easily launch DoS attacks on a home server through a foreign server. However, the two-party structure only requires the roam-

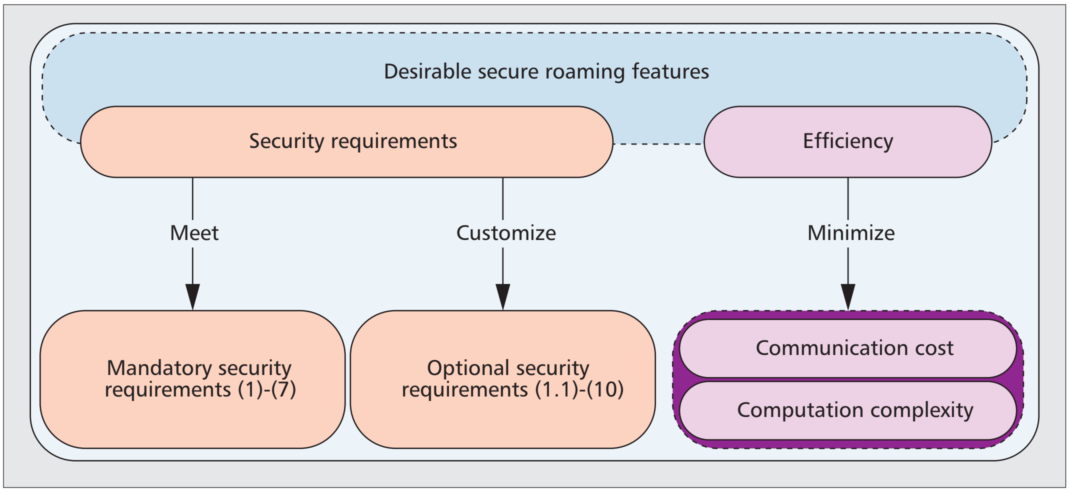
Desirable secure roaming features
Security requirements
Efficiency
Meet
Customize
Minimize
Mandatory security requirements (1)-(7)
Optional security requirements (1.1)-(10)
Communication cost
Computation complexity

Figure 2. *Desirable secure roaming features.*

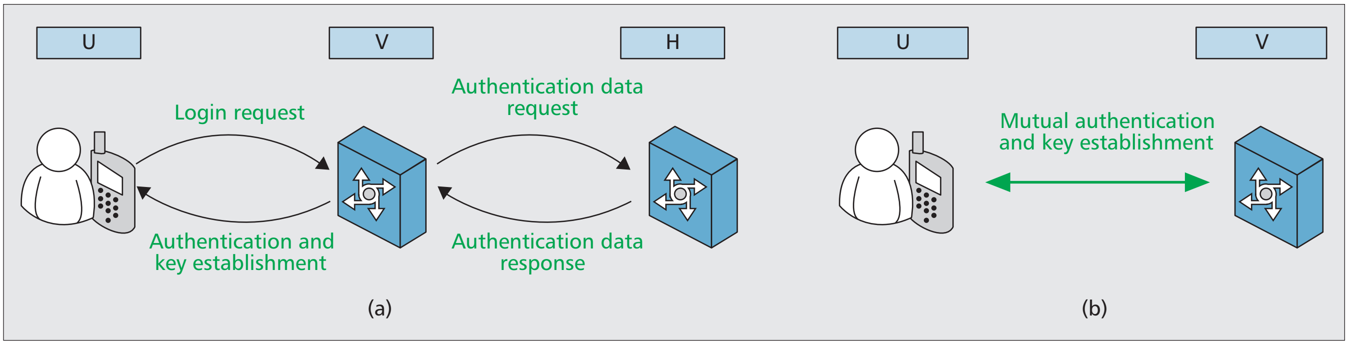
U
V
H
Login request
Authentication data request
Authentication and key establishment
Authentication data response
(a)
U
V
Mutual authentication and key establishment
(b)

Figure 3. *The structure of roaming authentication: a) the three-party roaming structure; b) the two-party roaming structure.*

ing user and the foreign server to be involved in each protocol run; the DoS attack on home servers is thus not applicable. Third, it requires fewer communication rounds. In the three-party roaming structure, a communication round between the foreign server and the home server is required. Especially when the home server is many network hops away from the foreign server, this communication delay becomes more crucial. These advantages together have led to the recent increasing popularity of the two-party roaming authentication [4–8].

The typical authentication procedure of the two-party technique is: A user U sends a login request $\{alias, sign_{key}(alias || nonce || ...)\}$ to the visited foreign server V, where the notations $alias$ and $sign_{key}(.)$ represent a pseudo-ID (i.e., unused pseudonym) and digital signature using some complex cryptographic techniques (e.g., group signature), respectively. With public key materials, V checks whether U is a legitimate subscriber of the claimed server H.

While the two-party structure ensures more robust and fault-tolerant roaming authentication, such a structure also poses some security challenges. First, in order to enable the foreign server to locally check the validity of roaming users, some complex cryptographic techniques (e.g., identity-based signature, group signature) must be used, which usually result in high computation overhead on mobile users and the foreign server. For example, our implementations show that as a common operation of these techniques, pairing computation takes 3.8 ms on a 1.2-GHz laptop PC.

Limitations of Existing Work

Existing work has some limitations in securing roaming services.

Resistance against DoS Attacks

With DoS attacks, adversaries flood a large number of illegal access request messages to network servers in order to exhaust their resources and render them less capable of serving legitimate users. A practical authentication mechanism should maintain service availability even in the presence of DoS attacks. Such attacks can be classified into three categories [10].

First, as described earlier, the three-party roaming approach suffers from the DoS attack on a home server through a foreign server. Second, in order to satisfy some design requirements (e.g., establishing a session key or recording a cookie), some roaming protocols (e.g., [4, 5]) based on the two-party structure require each foreign server to use a challenge-response approach with a roaming user before the foreign server authenticates the user. An adversary can easily send a large volume of forged access requests to exhaust the storage, processing, and bandwidth resources of foreign servers. Third, in most roaming authentication techniques (e.g., [3–6]), for each access request message, a foreign server needs to perform expensive cryptographic

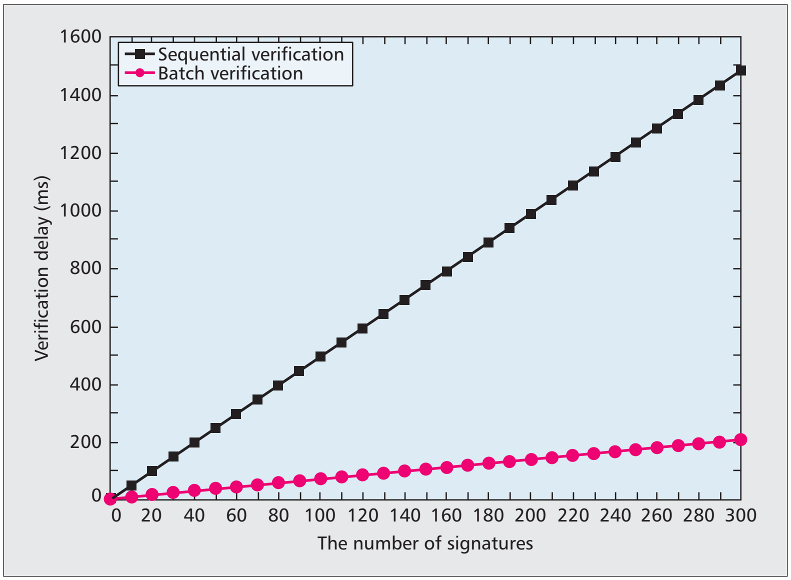

Figure 4. *Verification delay comparison.*

operations (e.g., pairing computation in [4–6]) to check the validity of the sender. This limitation can easily be exploited by the adversary. Accordingly, some mechanisms for resisting the second and third categories of DoS attacks are needed to overcome this limitation.

Efficient Authentication

A roaming authentication process should be fast enough to maintain persistent connectivity for roaming users. Otherwise, packet loss during the handover process becomes serious. For example, the IEEE is considering a 50-ms limit on handover time, of which the authentication module should ideally take less than 20 ms. However, in most existing work (e.g., [2–6]), a foreign server verifies each signature individually. Such an approach is not scalable since the foreign server does not have sufficient time to verify each received signature if the arrival rate of signatures is high. For example, in vehicular ad hoc networks (VANETs), each stationary roadside unit (RSU) (i.e., each visited foreign server in this article) could possibly communicate with hundreds of wireless onboard units equipped in vehicles, each sending a safety related message to the RSU every 100–300 ms. Hence, there is a necessity for mechanisms that can accelerate the authentication in roaming services.

Flexible Roaming in Mobile Contexts

The proliferation of mobile devices has given rise to novel user-centric applications and services. However, existing roaming authentication solutions do not involve mobile contexts of each user as input. More specifically, once a roaming protocol is employed, each step of the authentication process has already been fixed. Addressing this challenge requires roaming authentication that allows mobile users to flexibly choose their desired security and efficiency levels of a roaming service, based on the roaming agreement between foreign servers and the corresponding home server. With such a flexible roaming system, a roaming user can balance security and efficiency of roaming services according to mobile contexts. The following scenarios, which involve a visited server operating in the application layer, illustrate the requirements for a flexible roaming system in mobile contexts.

When Brown is in vacation and visits, for example, Disney Wonderland, s/he will let the wonderland management track him/her for safety and management purposes, but s/he does not want this information correlated with his/her identity. However, Brown sometimes may want to know whether s/he is near one of his/her friends (e.g., whether s/he and one of his/her friends are in the same network cell) through a find-a-friend service. In this case, Brown has to disclose his/her identity to the visited server. Thus, it is desirable for Brown to be able to flexibly choose whether his/her identity is exposed to the visited server.

Furthermore, regarding roaming services, Brown prefers efficiency to security for delay-constrained applications such as VoIP in many private places such as homes and offices. On the other hand, s/he hopes to choose a more secure roaming service in many public places such as shopping malls.

Provision of User Revocation with Backward and Forward Non-Linkabilities

When user revocation is supported in roaming protocols based on the two-party roaming structure, achieving user non-traceability becomes an challenging issue. This is because sufficient information needs to be provided to foreign servers to identify revoked users, and yet such information should not be enough to enable foreign servers to link other protocol runs of the revoked users. That is, as described in Requirement (6.1), the protocol runs of a revoked user should be both backward and forward non-linkable. Backward non-linkability means that the protocol runs of a revoked user before its revocation should remain anonymous and non-linkable. Forward non-linkability means that for a time-limited revocation due to, for example, suspension of service for a period of time, the anonymity and non-linkability of the revoked user's protocol runs after the revocation period should also be maintained. Unfortunately, even recently proposed roaming protocols do not address this issue. For example, based on the group signature technique, a novel roaming protocol [5] has been proposed to achieve strong user anonymity that protects users' identities against both eavesdroppers and foreign servers (i.e., part of Requirement (6.1)). This protocol only lets the foreign server know the identity of the group to which a user belongs (i.e., the corresponding home server), but not the real identity of the user, thus achieving user anonymity. However, it fails to provide user revocation with backward and forward non-linkabilities because once a particular user exists in the revocation list sent to a foreign server, the foreign server is able to identify all (including past and future) protocol runs in which the user has been and will be involved. In reality, the revocation list is large and updated very frequently, which means that a

The parameter l	12	14	16	18	20	22	24	26
The execution time (s)	0.013	0.046	0.182	0.565	2.769	12.779	34.98	240.203

Table 2. *The execution time for solving a message-specific puzzle.*

The proliferation of mobile devices has given rise to novel user-centric applications and services. However, existing roaming authentication solutions do not involve mobile contexts of each user as input. More specifically, once a roaming protocol is employed, each step of the authentication process has already been fixed.

foreign server can obtain many users' trace keys. Thus, this weakness is serious, and existing work should be amended to support user revocation with backward and forward non-linkabilities.

Mechanisms to Mitigate the Limitations

Resistance against DoS Attacks

To thwart the second DoS attack, a feasible approach is that upon receiving an access request message, each foreign server first verifies this message.

To prevent the third DoS attack, in [10], we have suggested that the message-specific puzzles (also referred to as client puzzles) of [11] can be incorporated into current roaming authentication protocols (e.g., [3–8]) in the following way. When a foreign server finds no evidence of the attack (e.g., the arrival rate of bogus access requests is less than a predefined threshold), it processes access requests normally (i.e., indiscriminately). However, when it suspects itself of being attacked, it only performs expensive verification on access requests selectively. In particular, the server attaches a unique puzzle into the beacon messages and requires the solution of the puzzle to be attached to each access request message. The server commits resources to process an access request only when the solution is correct. In general, solving a puzzle requires a brute force search in the solution space, while solution verification is very fast. Additionally, puzzles are deployed in conjunction with conventional time-outs on server resources. Thus, in order to create an interruption in services, an adversary must have abundant resources to be able to promptly compute a large enough number of puzzle solutions in line with its sending rate of illegal access requests. In contrast, although puzzles slightly increase legitimate users' computational load when the server is under attack, they are still able to obtain network access regardless of the existence of the attack. The detailed description is as follows.

If a network server, say V, is not under attack, it attaches "No" into the beacon messages. It indicates to the roaming users that no puzzles are being distributed, and the roaming protocol is executed normally. On the other hand, if V is under attack, it adds "Yes" and a puzzle (i.e., a random number a and an integer l) into the beacon messages. In order to initiate a connection with V, a roaming user must solve the puzzle within a specified time interval. A valid solution L is such a value that after applying the hash function $h()$ to {Access request$||a||L$}, the first l bits of the result are all 0. The parameter l determines the strength of the puzzle. Before transmitting the access request message, a user first tries to solve the puzzle by finding the puzzle solution L. Subsequently, the user sends the final access request message {Access request$||a||L$} to V. The puzzle solution in every access request can be efficiently verified by V via a hash function operation and comparison. Only if this verification is successful does V perform expensive verification on the access request.

We implemented the proposed approach and added it into the roaming authentication protocol of [6] to show its efficiency in practice. Table 2 gives the time required to solve a message-specific puzzle on a 1.6-GHz laptop PC (using the OpenSSL library) when the parameter l varies. For example, the time required to solve a message-specific puzzle is 0.182 s when the parameter l is set to 16. As described above, this time consumption is enough to defeat the DoS attack.

Note that in some application scenarios, the adversary may have much higher computation power than a legal mobile user. To prevent a powerful adversary, the parameter l should be considerably large; however, this would bring an extra burden to the low-power mobile devices in a normal authentication process. To solve this issue, instead of the message-specific approach, we have proposed a polynomial-based lightweight verification scheme to enhance the resistance to DoS attacks by imposing more computational load to adversaries as follows [7].

This scheme requires that in the system initiation phase of current roaming protocols, each server randomly generates a bivariate t-degree polynomial $f(x, y) = \Sigma_{i,j=0}^{t} a_{ij}x^iy^j$ over a finite field F_q, where q is a large prime number, such that it has the property of $f(x, y) = f(y, x)$. When a user U registers to its home server H, H chooses a family of non-linkable pseudo-IDs. For each pseudo-ID *alias*, H computes a polynomial share of $f(x, y)$, that is, $f(alias, y)$, and then delivers them to U using a secure transmission protocol (e.g., wired transport layer security protocol). Also, H securely transmits $\mathrm{f}(ID_V, y)$ to foreign server V, where ID_V is the identity of V. When U wants to access the network via V, it computes the common key $f(alias, ID_V)$ by evaluating $f(alias, y)$ at point ID_V, and V can compute the same key $f(alias, ID_V) = f(ID_V, alias)$ by evaluating $f(ID_V, y)$ at point *alias*. Then V can use key $f(ID_V, alias)$ to verify the access request message of U through a message authentication code. Experimental results in [7] show that evaluation of the polynomial is very fast, and hence V can efficiently verify the access request messages before performing expensive verification to mitigate the DoS attack. Compared to the message-specific puzzles, this lightweight verification scheme can more effectively mitigate DoS attacks because an authorized user has a clear advantage over the adversary due to its prior knowledge of the communication key with each server. On the other hand, the adversary has to guess the communication key first, before gener-

An important first step in achieving flexible roaming is notifying mobile users to specify the security and efficiency levels of roaming services. To become truly ubiquitous, this step should be merged into the background processes such that it becomes a part of the fabric of everyday life.

ating a valid access request. Thus, this scheme would not bring much of a burden to the low-power mobile devices and, at the same time, can resist a DoS attack from a powerful adversary. Note that this scheme is unconditionally secure and t-collusion resistant, which means that only when $t + 1$ network identities are compromised is the secret polynomial f of server H disclosed.

Batch Verification for Low-Delay Authentication

In order to speed up the process of verification for a foreign server, we have proposed to use batch verification on roaming services [7], in which a foreign server can simultaneously verify multiple received signatures to dramatically reduce the total verification time. For example, two pairing operations are required to verify a single signature. With the batch verification scheme of [7], verifying n signatures also takes two pairing operations instead of $2 \times n$ pairing operations. In other words, the running time of the dominant operation (i.e., pairing) of the verification process is independent of the number of signatures to verify. Therefore, the batch verification can dramatically decrease the time spent on verifying a large number of signatures. The verification delay of a foreign server against the number of received messages is plotted in Fig. 4. In this experiment, server side programs have been implemented in C and executed in a 2-GHz laptop PC. The maximum number of signatures that can be verified simultaneously in 200 ms are 40 and 291 for sequential verification and batch verification, respectively. In the context of the secure VANET application discussed earlier, it means that with batch verification, an RSU can verify 291 safety related messages every 200 ms.

Flexible Roaming in Mobile Contexts

An important first step in achieving flexible roaming is notifying mobile users to specify the security and efficiency levels of roaming services. To become truly ubiquitous, this step should be merged into the background processes such that it becomes a part of the fabric of everyday life. Users want a flexible roaming system that "just works" according to mobility context with little or no action on their part; otherwise, users are reluctant to accept such a roaming service because they view it as inconvenient. Therefore, the goal is to minimize technology's intrusiveness, and the demands of users and network providers. Here, we suggest a feasible approach as follows.

As depicted in Fig. 2, the goal is to allow each roaming user to configure its security and efficiency properties as policies and to have user-friendly operations that result in minimal disruption while satisfying the user's security and efficiency policy. For example, a user configures the security and efficiency of a roaming service using a Boolean flag (e.g., a checkbox) indicating whether the user desires the requirement or not. Before each user makes such a decision, the network providers are responsible for providing full information about different policies, and the corresponding security and efficiency levels. For example, this information is built into the web browsers of each user or included in the beacon messages.

Provision of User Revocation with Backward and Forward Non-Linkabilities

We have proposed Priauth, a privacy-preserving universal authentication protocol, in [6]. It is built on the verifier-local revocation group signature with backward non-linkability technique (VLR-GS-BU). Compared to a basic group signature technique, the VLR-GS-BU algorithm can provide a way to trace users' signatures in an individual period defined by H. More specifically, once the revocation token (i.e., trace key) of a user at time interval j is transmitted to a foreign server, the foreign server only has ability to trace the user's signatures at time interval j, but not at any other interval k, where $k \uparrow j$. Thus, Priauth can preserve backward and forward non-linkabilities in roaming services.

Remark

Since a roaming system is deployed in a wide variety of wireless networks, the requirements (i.e., optional security requirements (1.1)–(10) and efficiency requirement) for a roaming protocol vary in different application scenarios. Of course, the roaming authentication technique must minimally satisfy the mandatory requirements. At the same time, different applications may need to satisfy different optional requirements. This is illustrated by the following example. In general, it is desirable to provide user anonymity and non-traceability. However, in some application scenarios, it is the responsibility of the corresponding home server to reveal the related private information (e.g., identity, position) of a roaming user in case of emergency (e.g., enhanced 911 location service mandated by the U.S. Federal Communications Commission). We call this feature conditional privacy preservation. Therefore, any roaming system with the feature that a user is completely anonymous such that its activities are not linkable by its home server would not be adequate here. That is, any roaming protocol that meets Requirement (6.4) is not applicable here. We can see that no roaming technique is ideal in all mobile scenarios; thus, the techniques employed must depend on the requirements of target applications and careful choice of cryptographic techniques.

Prospects

Although the research field of roaming authentication has received significant attention, there are still many challenging issues that need to be addressed. Here, we list some important ones.

Cross-Layer Protocol Design for Roaming Authentication

Most of the existing work in roaming authentication (e.g., [2–7]) only focuses on network layer protocol design. We exemplify the need for cross-layer design in the following.

In the physical layer, the adversary can analyze the overheard wireless traffic to obtain useful information, such as the network usage pattern. However, all existing roaming techniques do not consider such an attack; thus, a physical-layer solution must be incorporated into the current techniques to address the traffic analysis attack.

In the medium access control (MAC) layer, the standards of current wireless technologies (e.g., IEEE 802.11 and Bluetooth) commonly require manufacturers to assign an identification number (i.e., MAC address) to every mobile device. Regarding security, the MAC address is like an annoying tag attached to a mobile device anytime and anywhere. Such a practice exposes the ID of a mobile device at the MAC layer. As a result, without considering this security issue, all existing roaming authentication approaches cannot protect user anonymity and non-traceability against eavesdroppers (i.e., Requirement (6)).

Designing authentication protocols that can handle attacks from different layers is a challenging issue. Currently, only preliminary solutions are available [8]. Future work on roaming systems should be based on a cross-layer approach that is no longer limited by the firm boundary currently existing between different layers of the network protocol stack.

Roaming Authentication in Emerging Networks

Recent advances in wireless communication technology have motivated new application domains for wireless networks. For example, body area networks (BANs) revolutionize the way to seek healthcare at home, at a hospital, or in large medical facilities. Another example is that future wireless sensor networks will follow a two-tiered architecture, where the lower tier comprises a large number of resource-constrained sensor nodes, while the upper tier contains fewer relatively resource-rich master nodes. In general, wireless networking is in the process of transition from conventional infrastructure-based last-hop-wireless networks to more dynamic self-forming autonomous peer-to-peer networks. This transition has significant implications for both security and efficiency of roaming services. Although the roaming services of other types of wireless networks have the same or similar requirements, traditional network roaming approaches do not generally apply to these emerging networks mainly because they assume unlimited resource of foreign servers and non-stringent roaming delay requirements.

For example, a registered user (e.g., healthcare staff, researchers, insurance companies) may roam over multiple BANs and use a handheld device (e.g., smartphone) to access the health-related parameters through contacting a biosensor node of a BSN (i.e., the foreign server in this article). A key design objective is to limit delays introduced by the roaming mechanism in order to comply with BAN latency requirements, especially when a medical emergency happens. On the other hand, a biosensor node has very limited resources compared to a traditional foreign server. Thus, future work on roaming services should focus on these emerging networks.

Non-Cryptographic Roaming Authentication Technique

All existing roaming authentication approaches resort to cryptography. However, cryptographic exchange mechanisms are complex and therefore induce potential vulnerabilities in themselves. As reported in [12], lower/physical layer characteristics (e.g., MAC behavior, clock skew, signal strength) have been considered as potential alternatives/complements to provide security in wireless networks. We expect that some progress can be made by using these non-cryptographic techniques to achieve an effective roaming authentication. Here, we use clock skew and Requirement (1) (i.e., server authentication) as an example. Clock skews are the inherent tiny drifts in the clocks of hardware devices due to variations in the manufacturing process. It has been demonstrated that the measurement of clock skews can provide the fingerprints of the devices (e.g., access points). To meet Requirement (1), a feasible approach is that each mobile user gets the clock skews of the foreign servers from the corresponding home network and uses this information to establish the first point of trust with a legitimate foreign server. This method does not require any additional hardware to realize as it exploits the already existing defects in the clock crystals.

Conclusion

Roaming services in wireless networks provide people with attractive flexibility and convenience. This process should be fast enough to support demanding applications such as multimedia content delivery, but also be secure enough. In this article, we have presented a state-of-the-art survey and conclusion on some recent prominent work in secure roaming services. We have proposed a set of mechanisms to complement existing work for defending against DoS attacks, efficient authentication, flexible roaming in mobile contexts, as well as backward and forward non-linkabilities. We encourage more research in roaming protocols to address the challenges that are still outstanding.

We have proposed a set of mechanisms to complement existing work for defending against DoS attacks, efficient authentication, flexible roaming in mobile contexts, as well as backward and forward non-linkabilities. We encourage more research in roaming protocols to address the challenges that are still outstanding.

Acknowledgment

This work was supported by the National Science Foundation of China (Grant No. 61070155), Program for New Century Excellent Talents in University (NCET-09-0685), the Fundamental Research Funds for the Central Universities (2012FZA5017), and a grant from the Research Grants Council of the Hong Kong SAR, China [Project No. CityU 111208]. Also, we are grateful to the anonymous reviewers for their valuable comments to improve the quality of the manuscript.

References

[1] D. Huang, X. Hong, and M. Gerla, "Situation-Aware Trust Architecture for Vehicular Networks," *IEEE Commun. Mag.*, vol. 48, no. 11, 2010, pp. 128–35.

[2] D. Samfat, R. Molva, and N. Asokan, "Non-Traceability in Mobile Networks," *Proc. MobiCom '95*, 1995, pp. 26–36.

[3] G. Yang, D. S. Wong, and X. Deng, "Anonymous and Authenticated Key Exchange for Roaming Networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, Sept. 2007, pp. 3461–72.

[4] Z. Wan, K. Ren, and B. Preneel, "A Secure Privacy-Preserving Roaming Protocol based on Hierarchical Identity-based Encryption for Mobile Networks," *Proc. ACM WiSec '08*, 2008, pp. 62–67.
[5] G. Yang *et al.*, "Universal Authentication Protocols for Anonymous Wireless Communications," *IEEE Trans. Wireless Commun.*, vol. 9, no. 1, Jan. 2010, pp. 168–74.
[6] D. He *et al.*, "Privacy-Preserving Universal Authentication Protocol for Wireless Communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, Feb. 2011, pp. 431–36.
[7] D. He *et al.*, "Secure and Efficient Handover Authentication based on Bilinear Pairing Functions," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, Jan. 2012, pp. 48–53.
[8] D. He *et al.*, "Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks," *IEEE Trans. Computers*, published online 27 Dec. 2011.
[9] K. Hoeper and L. Chen, "Where EAP Security Claims Fail," *Proc. Qshine '07*, 2007.
[10] D. He *et al.*, "Strong Roaming Authentication Technique for Wireless and Mobile Networks," *Int'l. J. Commun. Systems*, published online 4 Jan. 2012.
[11] A. Juels and J. Brainard, "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks," *Proc. NDSS '99*, 1999, pp. 151–65.
[12] K. Zeng, K. Govindan, and P. Mohapatra, "Non-Cryptographic Authentication and Identification in Wireless Networks," *IEEE Wireless Commun.*, vol. 17, no. 5, Oct. 2010, pp. 56–62.

Biographies

DAOJING HE (hedaojinghit@gmail.com) received his B.Eng. and M.Eng. degrees in computer science from Harbin Institute of Technology in 2007 and 2009, respectively, and a Ph.D. degree in computer science from Zhejiang University, P.R. China, in 2012. He is an associate editor or on the editorial board of some international journals such as Wiley's *Wireless Communications and Mobile Computing Journal*, Wiley's *Security and Communication Networks Journal*, and *KSII Transactions on Internet and Information Systems*. His research interests include network and systems security. He has been a Technical Program Committee member of many international conferences.

CHUN CHEN (chenc@cs.zju.edu.cn) received his Bachelor's degree in mathematics from Xiamen University, China, in 1981, and his Master's and Ph.D. degrees in computer science from Zhejiang University, China, in 1984 and 1990, respectively. He is a professor in the College of Computer Science and the director of the Institute of Computer Software at Zhejiang University. His research activity is in image processing, computer vision, and embedded system.

SAMMY CHAN (eeschan@cityu.edu.hk) received his B.E. and M.Eng.Sc. degrees in electrical engineering from the University of Melbourne, Australia, in 1988 and 1990, respectively, and a Ph.D. degree in communication engineering from the Royal Melbourne Institute of Technology, Australia, in 1995. From 1989 to 1994 he was with Telecom Australia Research Laboratories, first as a research engineer, and between 1992 and 1994 as a senior research engineer and project leader. Since December 1994 he has been with the Department of Electronic Engineering, City University of Hong Kong, where he is currently an associate professor.

JIAJUN BU (bjj@zju.edu.cn) received his B.S. and Ph.D. degrees in computer science from Zhejiang University, China, in 1995 and 2000, respectively. He is a professor in the College of Computer Science and the deputy director of the Institute of Computer Software at Zhejiang University. His research interests include embedded systems, mobile multimedia, and data mining.

YAN ZHANG (yanzhang@ieee.org) received a Ph.D. degree from Nanyang Technological University, Singapore. He is working with Simula Research Laboratory, Norway, and is an adjunct associate professor at the University of Oslo. He has been an associate editor or guest editor of a number of international journals. He has served as an organizing committee chair for many international conferences. His research interests include resource, mobility, spectrum, energy, and data management in communication networks.