無線ネットワークにおける新たなコミットメントベース認証プロトコルの提案

景 輝, 李 頡

筑波大学大学院 システム情報工学研究科 コンピュータサイエンス専攻

概要:

本論文では、新たに2-wayハンドシェイク認証プロトコルを提案する。提案プロトコルでは、認証、認可、アカウンティング (AAA) アーキテクチャーに基づいた無線ネットワークにおいて、ドメイン内を移動するユーザの局所的な認証を行うことで、効率化を実現する。また、認証において、コミットメント構造を利用した局所的なセキュリティアソシエーション (SAs) を設立する手順を考案する。さらに、モバイルユーザとそのホームAAAサーバーの間のメッセージ伝送時間だけでなく、モバイルユーザのトラフィックと移動パターンを考慮し、性能評価と比較を行い、提案したプロトコルが、従来の手法より優れていることを明らかにする。

A Novel Commitment-based Authentication Protocol for Wireless Networks

Hui Jing and Jie Li

Department of Computer Science, Graduate School of SIE, University of Tsukuba

Abstract:

In this paper, we present a novel 2-way handshake authentication protocol to locally authorize intra-domain roaming users for efficient authentication in wireless networks, which is based on authentication, authorization, accounting (AAA) architecture. We develop a detailed procedure to establish local security associations (SAs) for authentication using commitment schemes. By considering the traffic and mobility patterns of a mobile user (MU), as well as the message transmission time between the MU and its home AAA server, we provide a performance study comparing the authentication latency of existing authentication protocol and our approach. The result shows that our protocol outperforms the existing authentication protocol.

1 Introduction

The popularity of mobile systems such as PDAs, laptops, and mobile phones increases every day, whereas inducing more challenges to security. Wireless communication and mobility are considered to be at odds with security. Indeed, jamming or eavesdropping is easier on a wireless link than on a wired one, furthermore, a mobile device is more vulnerable to impersonation.

Mobile IP provides an efficient mechanism for mobility within the Internet [3]. Mobile IP is an open standard, defined by the Internet Engineering Task Force (IETF) that allows a user to keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP network domains. Mobile IP assigns each mobile user (MU) a permanent home address on its home network and a care-of address that identifies the current location of the device within a network domain and its subnets. To accurately deliver the call of an MU, the home agent (HA) should know the position of the MU. An MU will be registered at the HA when care-of address is changed. For successful registration, the home agent or the foreign agent (FA) should accept registration message of valid MUs. Moreover, when starting a communication session, an MU will use network resources provided by servers. At these times, the authentication server will authenticate the MU.

As one of the most widely used security mechanisms, authentication is a process to identify a mobile user, authorize resources to the MU, and negotiate secret credentials for protecting communications [1]. In an authentication process, an MU will submit secret materials, which will be verified with a security association (SA), a description on keys and encryption algorithms. After authenticated, the MU will be authorized access services within the network domain. And an accounting of the actual resources may be assembled. With the authentication, network resources are protected by only allowing legitimate users to obtain services. The information secrecy and data integrity are also guaranteed because session keys will be generated during the authentication process for data encryption and message authentication. Thus, the network security in terms of protection for network resources, information secrecy, and data integrity is affected greatly by the authentication service.

With public/private key based authentication mechanism, the computation complexity of encrypting/decrypting data consumes more time and power. Thus, in order to achieve efficient authentication, our authentication protocol is based on secret keys. Authentication delay affects the service quality of real-time applications of mobile users. During this authentication, no data for ongoing service can be transmitted. When the authentication time is greater than a threshold time, the connection will be broken.

In order to improve the security and efficiency during the authentication, many authentication schemes are proposed, focusing on the design of lightweight and secure authentication protocols. The challenge/response (C/R) authentication protocol is widely used in wireless networks. It requires a roaming MU to submit a response value for authentication each time, which is encrypted from a challenge value, a random number, with an SA shared between the MU and the authentication server. The authentication process is 4-way handshake which is proposed in [9].

Moreover, the localized C/R (LC/R) authentication protocol is proposed for efficient authentication in [2]. But based on C/R authentication protocol, the authentication process is 4-way handshake. So, it may cause a long authentication time.

In order to deliver the authentication messages between networks, in our paper, we consider the authentication, authorization, and accounting (AAA) architecture, which is initially proposed by IETF for Mobile IP networks and is being deployed in 3G systems [4]. An AAA architecture is composed of local AAA servers (LASs), home AAA servers (HASs). An LAS is only takes charge of authentication for visiting MUs from foreign network domains. An HAS is an authentication server to identify the MU who subscribes the service in its network domain. All of these AAA servers are organized hierarchically with shared SAs between the AAA server in lower layer. Within the Mobile IP network, an MU belonging to one home network domain often needs to use resources provided by foreign network domain. If the LAS has no information to verify the MU, it contacts the HAS of the MU through an authentication architecture. If the distance between the LAS and the HAS is long, the authentication efficiency in terms of signaling cost and encryption/decryption cost for authentication should be considered. To consider the efficiency and security with different mobility and traffic patterns, we propose a local authentication protocol with local SA control, which can be implemented based on the AAA architecture. Therefore, it can be applied in various mobile environments including 3G, such as CDMA-2000 and UMTS, and 802.11 networks because AAA architecture has been deployed in these networks.

A commitment scheme [7] is an important cryptographic buildings block that we will be using in our protocols. It is a method by which a sender can commit to a value to a receiver. And the commitment can be revealed later by the sender. The properties of a commitment scheme are on the following:

▶ Binding: A user who commits to a certain value cannot change this value afterwards;

▶ Hiding: The commitment is hidden from its receiver until the sender allows receiver to open it.

A useful way to visualize a commitment scheme is to think of sender as putting the message in a box, securing the box with a lock to which only he has the key, and giving the box to receiver. A commitment scheme transforms a value m into a commitment/opening pair (c, d), where c reveals no information about m, but (c, d) together reveal m, and it is infeasible to find $\widehat{d}$ such that $(c, \widehat{d})$ reveals $\widehat{m} \neq m$. We denote with $\widehat{x}$ the message at the receiver's side when message x is sent over a public (unauthentic) channel. Now, if Alice wants to commit a value m to Bob, she first generates the commitment/opening pair $(c_A, d_A) \leftarrow commit(m)$, and sends c_A to Bob. For Bob to open m, Alice sends d_A to him, who runs $\widehat{m} \leftarrow open(\widehat{c_A}, \widehat{d_A})$. If the employed commitment scheme is correct, at the end of the protocol we must have $m = \widehat{m}$. In our research, we assume an ideal commitment scheme is used.

The rest of our paper is organized as follows. In Section 2, a system is defined for authentication based on AAA architecture. In order to minimize authentication latency, we propose a local authentication protocol in Section 3. And a system model is introduced to analysis the impact of authentication in Section 4. We analyze the mean authentication time per call as metrics with the concern of the message transmission time between the MU and its home AAA server, mobility and traffic patterns in Section 5. Finally, we draw conclusions in Section 6.

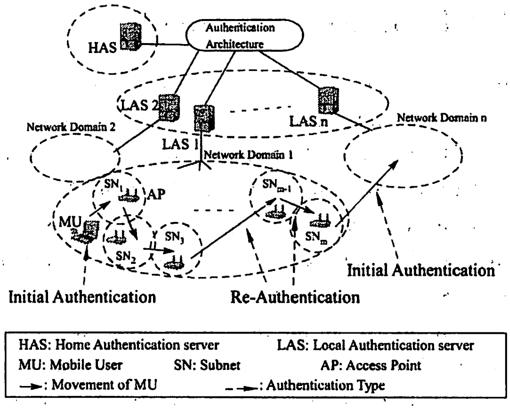

Figure 1: System Model of Authentication

2 System Description

We consider a system for the authentication within wireless networks which is shown in Fig.1. The generic system in our paper is consistent with many practical wireless networks such as the authentication, authorization, and accounting (AAA) architecture in Mobile IP networks and wireless local area networks (WLAN). In this system there are a number of n autonomous wireless network domains. Each network domain has an LAS and an HAS, which are central authentication servers in a network domain. In our research, An LAS only takes charge of authentication for visiting MUs, while an HAS is only responsible for authentication of the MUs that subscribe services in current network domain. These LASs and HASs are connected through the Internet. It is assume that the HAS and LAS are integrated together.

We further assume that a network domain is composed of M subnets of equal size, and each subnet is controlled by an access point (AP). Here, an AP is a function unit that can transmit data for MUs with established SAs. An LAS controls the authentication in the network domain with M subnets in it, and shares SAs with M APs.

3 Proposed Protocol

In our research, we define the authentication value as a secret information that only be known by the MU and the HAS. The authentication message is delivered to LAS by the HAS or the MU for local authentication. In our research, we assume that the HAS and LAS are secure authentication servers in wireless networks.

To minimize authentication latency, our proposal is based on a new technique that uses local authentication in the LAS independent of reauthentication in the HAS. To enhance the security and improve the efficiency of authentication, we propose the new authentication protocol by commitment schemes.

3.1 Basic idea

The basic idea of **Commitment-based authentication protocol** is that an HAS delegates the authentication to an LAS for local authentication. Also, in our proposal, one authentication process is 2-way handshake. To enhance the security, an HAS does not directly send the authentication value to LAS for the local authentication. In our proposal, the LAS will use the authentication message which is transformed by authentication value to authenticate the MU.

In our proposal, the LAS just stores one part of authentication messages (c) for local authentication which will be sent by the HAS. For successful authentication, the LAS should receive another part of the authentication messages (d) which will be sent by the MU. The two different parts of the authentication messages (c, d) together reveal the information for authentication.

3.2 Commitment-based authentication protocol

3.2.1 Initial authentication (Type 1)

When an MU starts the authentication at an LAS, an initial authentication procedure shown in Fig.2 is performed. However, at this time, there is no authentication message for the MU in the LAS. With this procedure, the MU first sends the authentication request to the LAS. Then the LAS replies the message including a random number R_1 for generating authentication message. Next, the MU calculates commitment pair (c_1, d_1) for concatenation the MU's ID encrypted with the authentication value and R_1. Here authentication value is only known by the MU and the HAS. The MU sends (c_1, d_1) to the LAS, encrypted with the key between the MU and the HAS. The LAS forwards this message adding R_1 to the HAS. The HAS decrypts this message and gets the $(\widehat{c_1}, \widehat{d_1})$. Then the HAS transforms the commitment pair into commitment value, gets $\widehat{R_1}$ and verifies it with R_1. If they are matched, the authentication is successful. Then, the HAS sends c_1 to the FA, encrypted with the $K_{LAS-HAS}$. The LAS decrypts this message and generates a random number R_2 used to prevent a replay attack for the next authentication. Then the LAS sends R_2 to the MU, encrypted with the key between the MU and the LAS (K_{MU-LAS}). It is assumed that the K_{MU-LAS} is equal to c_1. Finally, the MU can use network resources in the foreign network domain.

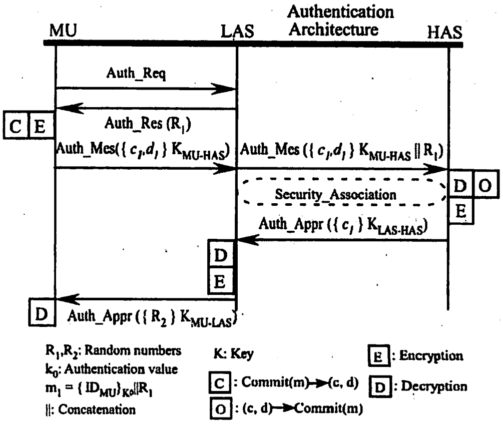

Figure 2: Initial Authentication

3.2.2 Re-authentication (Type 2)

Re-authentication is composed of re-session authentication and intra-domain authentication. When an MU restarts a session, a re-session au-

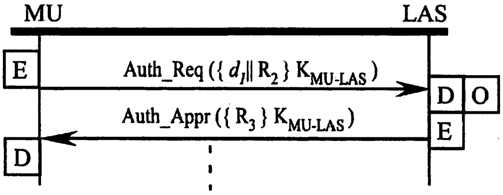
MU
LAS
E
Auth_Req ({ d_l|| R$_2$ } K$_{MU-LAS}$)
D
O
Auth_Appr ({ R$_3$ } K$_{MU-LAS}$)
E
D

Figure 3: Re-authentication

thentication occurs. When an MU crosses the boundary of different subnets in the same network domain, an intra-domain authentication is initiated. With this procedure, the authentication message c_1 for local authentication has already existed in the LAS. Therefore, it is unnecessary to contact the HAS with the MU for authentication. In the case shown in Fig.3, the MU sends d_1 and R_2 to the LAS, encrypted with the K_{MU-LAS}, through the access point. After decrypting this message, the LAS opens the commitment pair (c_1, d_1) and verifies the R_1. If the verification is successful, the LAS sends the authentication appropriation message to the MU, including a random number R_3 which is encrypted with the K_{MU-LAS} for the next authentication.

4 System Model

In this section, we introduce a system model to analyze the impact of authentication in wireless networks. We assume that an MU is roaming into foreign network domains. In order to evaluate the performance of authentication, we need to further describe specific conditions such as mobility and traffic patterns with which the impact of authentication can be evaluated clearly.

Mobility pattern: The mobility pattern of an MU is represented with residence time of the MU in one subnet, denoted as T_r. We assume that T_r is a random variable and the probability density function (PDF) of T_r, denoted as $f_{T_r}(t)$, is Gamma distribution with mean $1/\mu$ and variance V. Then, the Laplace transform of $f_{T_r}(t)$, $F_r(s)$, is:

$$F_r(s) = (\frac{\mu\gamma}{s+\mu\gamma})^{\gamma}, \text{ where } \gamma = \frac{1}{V\mu^2}. \quad (1)$$

Furthermore, if the number of subnets passed by an MU is assumed to be uniformly distributed between [1,M], the PDF of the residence time in a network domain, denoted as $f_{T_M}(t)$, can be expressed with Laplace transform $F_M(s)$ as follows:

$$F_M(s) = \frac{1}{M}\sum_{n=1}^{M}(\frac{\mu\gamma}{s+\mu\gamma})^{n\gamma}. \quad (2)$$

Then, the mean value of residence time in this network domain, denoted as $\overline{T}_M$, can be expressed as:

$$\overline{T}_M = -\frac{\partial F_M(s)}{\partial s}|_{s=0} = \frac{M+1}{2\mu}. \quad (3)$$

Traffic pattern: In our proposal, we consider the call rate and call duration time of the MU as the traffic patterns of the MU. We assume that the number of calls, which includes the incoming calls and outgoing calls, has a Poisson distribution with average rate λ, and a call duration time, denoted as T_D, has an exponential distribution with mean $1/\eta$. Then, the PDFs of the call inter time and call duration time, denoted as $f_{T_A}(t)$ and $f_{T_D}(t)$, respectively, become:

$$f_{T_A}(t) = \lambda e^{-\lambda t}, \text{ and } f_{T_D}(t) = \eta e^{-\eta t}. \quad (4)$$

Based on these assumptions on the mobility and traffic patterns of the MU, we evaluate the mean authentication time per call when the MU is roaming in our generic system model.

5 Performance Evaluation

We use mean authentication time per call as metrics which is mostly used of analyzing the performance of authentication protocols. We define the mean authentication time per call as the mean time per call from when the MU sends out authentication requests to when the MU receives the authentication replies. The mean authentication time per call, $T_{Au\_percall}$, can be written as:

$$T_{Au\_percall} = \frac{\sum_{i=1}^{2} N_i T_i}{N_{Call}}. \quad (5)$$

Where i is the index of authentication type. $i = 1$ represents an initial authentication, and $i = 2$

means a re-authentication. T_i is the authentication time per operation for authentication type i, and N_i is the number of authentication requests with type i. N_{Call} is the number of calls.

For our evaluation, we assume that an MU first starts a call in the FA. And in one network domain, the number of calls can be obtained by

$$N_{Call\_E} = \lambda T_M. \tag{6}$$

The mean authentication time per call can be written as

$$T_{Au\_percall\_E} = \frac{T_1 + (N_{Call\_E} - 1 + \frac{M+1}{2} - 1) \cdot T_2}{N_{Call\_E}} \tag{7}$$

To calculate the time for different types of authentications, we define a set of time parameters shown in Table1 for convenient description.

Then, T_i can be expressed as

$$T_i = \overrightarrow{d}_i \cdot \overrightarrow{x}, \quad \forall i = 1, 2. \tag{8}$$

Here, $\overrightarrow{x}$ is a vector defined as

$$\overrightarrow{x}^T = [T_{MU-LAS}, T_{LAS-HAS}, T_{ed}, T_c, T_o]. \tag{9}$$

And, $\overrightarrow{d}_i$ are the vectors defines as follows:

$$\begin{aligned} \overrightarrow{d}_1 &= [4, 2, 6, 1, 1], \\ \overrightarrow{d}_2 &= [2, 0, 4, 0, 1]. \end{aligned} \tag{10}$$

Table 1: Authentication time parameters

Symbol	Description
T_{MU-LAS}	Message transmission time between MU and LAS
$T_{LAS-HAS}$	Message transmission time between LAS and HAS
T_{ed}	Message encryption/decryption time
T_c	Commitment pair generation time
T_o	Opening commitment pair time

5.1 Evaluation

In this section, we firstly introduce the parameters for evaluation. Then, the mean authentication time per call is evaluated and compared to the localized C/R authentication protocol based on different conditions.

Table 2: Parameters for evaluation

Parameters for authentication time			
T_{MU-FA}	T_{FA-HA}	T_{ed}	T_c, T_o
$20ms$	$20 - 100ms$	$2ms$	$5ms$
Parameters for random variables			
λ	η	$1/\mu$	M
$0.05 - 0.14min^{-1}$	$0.3min^{-1}$	$5 - 30min$	120

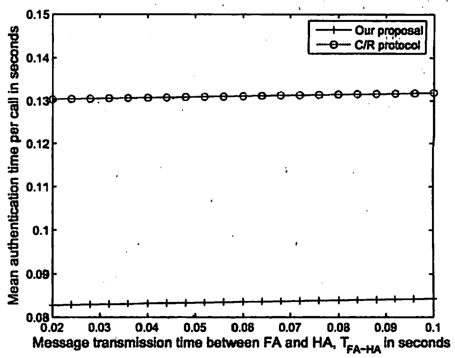

Figure 4: Mean authentication time per call in one domain at $\lambda = 0.1min^{-1}$, $1/\mu = 18min$

The parameters to evaluate the mean authentication time per call are shown in Table2. The values of T_{MU-LAS}, $T_{LAS-HAS}$, T_{ed}, are obtained from the existing research [8]. In one network domain, we assume that the number of subnets (M) is 120. Just one network domain is evaluated.

The effect of message transmission time between LAS and HAS of the mean authentication time per call is shown in Fig.4. In this figure, both in the localized C/R authentication protocol and in our proposed protocol, the mean authentication time per call time is almost not effected by the message transmission time between LAS and HAS. And it will be reduced up to 36.1%.

The effect of call rate on the mean authentication time per call is demonstrated in Fig.5. It shows that the mean authentication time per call declines while the call rate increases. It is because the sum of intra-domain authentication time in one domain is not variable. When the call rate increases, the number of calls increases. Compar-

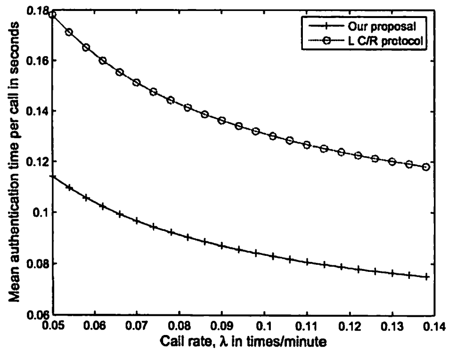

Figure 5: Mean authentication time per call in one domain at $T_{FA-HA} = 0.06s$, $1/\mu = 18min$

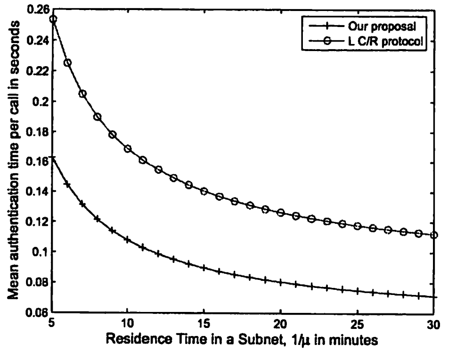

Figure 6: Mean authentication time per call in one domain at $T_{FA-HA} = 0.06s$, $\lambda = 0.1min^{-1}$

ing with localized C/R authentication protocol, our proposal shows a improvement around 0.05s. That is to say, the mean authentication time per call can be reduced up to 35.9% at least. Fig.6 reveals the effect of residence time on the mean authentication time per call. As we can see, authentication time decreases with the increase of the residence time of an MU in a subnet. The improvement of mean authentication time comparing with localized C/R authentication protocol is around 35.7%.

6 Conclusion

In this paper, a novel local authentication protocol to reduce authentication latency and securely produce a key for communication has been proposed. Compared to the localized C/R authentication protocol, our protocol reduces the re-authentication time, and enables the LAS to authenticate the MU accurately.

References

[1] W. Liang and W. Wang, "On performance analysis of challenge/response based authentication in wireless networks," *Computer Network*, vol. 48, no. 2, pp. 267-288, 2005.

[2] W. Liang and W. Wang, "A Local Authentication Control Scheme Based on AAA Architecture in Wireless Networks," *in Proc. of the 60th IEEE Vehicular Technology Conference*, Los Angeles, September 2004.

[3] C. Perkins, Ed. "IP Mobility Support for IPv4," *RFC3344*, August 2002.

[4] C. Perkins, P. Calhoun, "Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4," *RFC3957*, March 2005.

[5] S. Glass, T. Hiller, S. Jacobs, C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements," *RFC2977*, October 2000.

[6] A. Diab, A. Mitschele-Thiel and J. Xu, "Cellular networks: Performance analysis of the mobile IP fast authentication protocol ," *in Proc. of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems* , Venezia, Italy, October 2004.

[7] M. Cagalj, S. Capkun and J. Hubaux, "Key agreement in peer-to-peer wireless networks," *in Proc. of the IEEE, Special Issue on Security and Cryptography*, 2006.

[8] A. Hess, G. Schafer, "Performance evaluation of AAA/mobile IP authentication," *in Proc. of 2nd Polish-German Teletraffic Symposium*,September,2002.

[9] C. He, "Effects of Security Features on the Performance of Voice Over WLAN," *Available from http://theory.stanford.edu/~changhua/ee384c_reports_he.pdf*, 2004.