한국산업정보학회논문지 제6권 제1호 (2001. 3)

A Proposal of the Authentication Protocol for Wireless Mobile Communication Systems Using Keyed Hash Function

Young-Ho Park*

요 약 본 논문에서는 무선이동 통신시스템을 위한 인증 프로토콜을 제안한다. 제안한 프로토콜은 상호 인증과 세션 키 분배를 제공하기 위해서 키 해쉬 함수를 사용한다. 본 프로토콜은 이동국에서의 계산량이 적다. 또한, 중간 전송 네트워크에서의 최소 보호설정을 제공하기 위하여 고정망에서의 보호 설정을 하지 않았다.

Abstract An authentication protocol for wireless mobile communication systems is proposed. The protocol employs the keyed hash function to provide mutual authentication and session key distribution. This makes the low computation power of mobile stations. To provide the security architecture with minimal assumption about the security of intermediate transport networks, this protocol has no assumptions about the security of the intermediate, fixed networks.

1. Introduction

Recently, the rapid progress of wireless mobile communication technology has prompted new security problems. Since the mobility of users and wireless access to the network exasperate potential security threats such as eavesdropping and illegal access, security services for mobile communication should be provided. Authentication and confidentiality are essential security services to control fraud and to protect private communication against unauthorized eavesdropping, respectively. Authentication protocol is to provide the communicating parties with some assurance that they know each other's true identities. Hence, a mobile user should be authenticated to the network mobile center before access to the mobile network is allowed. The message transmitted through the wireless network can be concealed by encrypting them. To apply the encryption techniques, both parties involved in secure communication should share a common session key before communication session begins[1].

Authentication protocols proposed by standard bodies include GSM(global system for mobile communication)[2], USDC(U.S. digital cellular)[3], CDPD(cellular digital packet data)[4], and etc. Independent researchers have also proposed their own protocols for similar environments. With modern digital and cryptographic techniques, some protocols aim to provide secure services to mobile subscribers which are at least as secure as comparable services provided by traditional wired network. But, the security architecture with minimal assumption about the security of intermediate transport networks is needed. Several security-related protocols for wireless mobile communication systems have been on the symmetric key or public key cryptosystem[5,6]. However, in

* 상주대학교 전자전기공학부 조교수

mobile communication systems, the low computation power of mobile stations should be considered[1]. That means a security system requiring heavy computation on the mobile stations is not adequate.

In this paper, an authentication protocol for wireless mobile communication systems is proposed. This protocol employs the keyed hash function to provide mutual authentication and session key distribution. This makes the low computation power of mobile stations. To provide the security architecture with minimal assumption about the security of intermediate transport networks, this protocol has no assumptions about the security of the intermediate, fixed networks. The confidentiality between VLR(visiting location resister) and HLR(home location resister) is compromised.

2. Authentication Protocols

GSM is the first mobile digital cellular network architecture to provide security services such as user authentication, traffic confidentiality and key distribution. The main concern with the GSM authentication approach is its reliance on the security of the internetwork that is traversed between VLR and HLR. Even if this was a reasonable assumption for the signalling networks of today's mobile telephone systems, the same cannot be guaranteed in a large or global scale, administratively heterogeneous, network environment. Another point of contention with GSM has to do with the use of the unpublished algorithms to obtain authentication and secrecy. Hiding the algorithm is certainly contrary to the open-system philosophy. The time-tried, security-by-obscurity principle has not proven to be effective in preventing hostile attacks.

<Figure 1> shows the MS(mobile station) authentication protocol in GSM. Message flows between HLR and VLR perform the export of the subscriber's credentials from the home domain to the remote domain while the interaction between MS and VLR consists of challenge-based authentication of MS by VLR. Security services in CDPD are composed of data confidentiality, key distribution and mobile unit authentication. CDPD requires a logically distinct entity,

MS VLR HLR

ID_m (MS → VLR)

ID_m, ID_v (VLR → HLR)

r, s, K_c (HLR → VLR)

r (VLR → MS)

s (MS → VLR)

ID_m : MS identifier
ID_v : VLR identifier
r : random number
s = A3(K_i, r)
K_c = A8(K_i, r)

o f

<Figure 1>. The MS authentication protocol in GSM.

MS Serving MD-IS Home MD-IS

D-H key exchange (MS ↔ Serving MD-IS)

compute K_s compute K_s

R4(Ks(NEI, ARN, ASN)) (MS → Serving MD-IS)

(NEI, ARN, ASN) (Serving MD-IS → Home MD-IS)

(NEI, ARN', ASN') (Home MD-IS → Serving MD-IS)

R4(Ks(NEI, ARN', ASN')) (Serving MD-IS → MS)

NEI : Network equipment identifier
ARN : Authentication random number
ASN : Authentication sequence number
ARN' : New ARN
ASN' : New ASN
R4( ) : Encryption function

<Figure 2>. The MS authentication protocol in CDPD.

an authentication server(AS), to be present in every CDPD domain. An AS is typically co-located with the MD-IS(mobile data intermediate system) in a service provider's domain. MS authentication always involves contacting the AS in the home domain.

<Figure 2> shows the MS authentication protocol in CDPD. The authentication protocol begin with the D-H key exchange protocol[7]. As a result, the MS and the serving MD-IS come to share a secret key, K_s. Like GSM, CDPD makes an assumption that the fixed network is secure. Therefore, communication between the serving MD-IS and the home MD-IS is conducted in the clear. CDPD, like GSM, uses unpublished encryption function.

Researchers at Bellcore proposed several authentication protocols for PCS environment. The most notable one is the so-called MSR+DH protocol[5]. This protocol incorporates both the private-key and public-key technique for the authentication. The RCE(radio control equipment) broadcasts its identity ID_n, public key y_n, and certificate $cert_n$. After validating $cert_n$, MS chooses a random number r and sends it to the RCE encrypted under the RCE's public key. The MS also sends to the RCE its identity and certificate encrypted under r. With D-H key distribution scheme, both sides can derive a common key η. The session key K_s is then determined as $K_s = f(\eta, r)$. Figure 3 shows the MSR+DH authentication protocol. This protocol requires the mobile station to do much more computation than those in GSM and CDPD.

MS　　　　　　　　　　RCE

y_n, $cert_n$
<------------------------

$E(y_n, r), E(r,(ID_m, cert_m)$
------------------------>

Exchange known message using K_s
<------------------------>

ID_m : MS identifier
y_n : RCE public key
$cert_n$: RCE certificate
$cert_m$: MS certificate
E( ) : Encrption function

<Figure 3>. The MSR+DH authentication protocol.

3. Proposed Authentication Protocol

<Figure 4> shows the authentication protocol for wireless mobile communication systems. This protocol employs the keyed hash function to provide mutual authentication and session key distribution. The keyed hash function may be implemented using encryption if required. This protocol makes the low computation power of mobile stations. The distributed session key is used to encrypt messages over the traffic channel between the MS and the VLR. In this paper, to avoid the drawbacks of GSM and CDPD, we make no assumptions about the security of the intermediate, fixed networks. The confidentiality between VLR and HLR is compromised.

MS　　　　　　　　　　VLR　　　　　　　　　　HLR

$ID_m, r_m, t_m, Hk_{mh}(ID_m, r_m, t_m)$
------------------------>

$ID_v, r_v, x, Hk_{vh}(ID_v, r_v, x)$
------------------------>

$ID_h, k_s \oplus Hk_{vh}(ID_h, r_v), y,$
$Hk_{vh}(ID_h, k_s \oplus Hk_{vh}(ID_h, r_v), y)$
<------------------------

$ID_h, k_s \oplus Hk_{mh}(ID_h, r_m),$
$Hk_{mh}(ID_h, k_s \oplus Hk_{mh}(ID_h, r_m))$
<------------------------

ID_m : MS identifier
ID_v : VLR identifier
ID_h : HLR identifier
r_a : random number generated by a
t_a : time stamp generated by a
k_s : session key between MS and VLR
k_{ab} : key shared between a and b
Hk( ) : keyed hash function
$x = ID_m, r_m, t_m, Hk_{mh}(ID_m, r_m, t_m)$

$y = ID_h, k_s \oplus Hk_{mh}(ID_h, r_m), Hk_{mh}(ID_h, k_s \oplus Hk_{mh}(ID_h, r_m))$

<Figure 4>. The proposed authentication protocol for wireless communication systems.

The following is the procedure of the authentication protocol.

1. MS begins by generating a random challenge r_m and a timestamp t_m and by computing the corresponding authenticator to VLR. The authenticator, $Hk_{mh}(ID_m, r_m, t_m)$ is a keyed hash function, where k_{mh} is the secret key shared between MS and HLR.
2. VLR generates a random challenge r_v and computes the corresponding authenticator, $Hk_{vh}(ID_v, r_v, x)$ to HLR. where x is the message transmitted from MS. k_{vh} is the secret key shared between VLR and HLR.
3. HLR validates t_m by comparing it to the current clock reading. If the new timestamp is not greater than the last timestamp recorded, the request is rejected. HLR checks authenticators from MS and VLR. If authenticators match, HLR generates k_s and computes $k_s \oplus Hk_{vh}(ID_h, r_v)$ and $k_s \oplus Hk_{mh}(ID_h, r_m)$. HLR computes the corresponding authenticators to VLR and MS.
4. VLR checks the authenticator, $Hk_{vh}(ID_h, r_v, k_s \oplus Hk_{vh}(ID_h, r_v), y)$ by using k_{vh}, where y is the message to HLR. If the authenticator matches, VLR computes the authenticator, $Hk_{vh}(ID_h, r_v)$ and the session key, k_s.
5. MS checks the authenticator, $Hk_{mh}(ID_h, r_m, k_s \oplus Hk_{mh}(ID_h, r_m))$. If the authenticator matches, MS computes the authenticator, $Hk_{mh}(ID_h, r_m)$ and the session key, k_s.

4. Analysis

Without proper protection, data transmitted on the wireless communication channel can suffer from unauthorized exposure and modification. To counteract the threats, several security features should be provided in the authentication protocol. The following show security features.

· Message confidentiality

Messages transmitted over the radio link are susceptible to eavesdropping. To protect communication over the wireless network, messages should be sent in ciphertext over the air. The key used for encryption/decryption is typically established during the authentication process.

· Subscriber authentication

Fraudulent use of the wireless service is one of the major concerns because there is no physical association between the subscriber and the network. Therefore, subscriber authentication is necessary to prevent impersonators from using services.

· Session independence

It is always possible that a session key used in a secret conversation can be compromised under some attacks. This should not lead to the compromise of the next session key. This property is called forward privacy. It is also desired that security parameters used in one session not be used again for impersonation or other misuse. That is, authentication protocols should be strong enough to sustain a replayed attack.

· Computation power of mobile stations

The computation power of mobile stations should be considered, which means a security protocol requiring heavy computation on the mobile station is not adequate.

· Security between HLR and VLR

Some protocols aim to provide secure services to mobile subscribers which are at least as secure as comparable services provided by traditional wired network. But, signals transmitted over the wired networks are susceptible to eavesdropping. With the help of cryptographic techniques, secure communications on the wired network should be considered.

<Table 1> Security features of authentication protocols.

Security features \ Authentication Protocols	GSM	CDPD	MSR+DH	Proposed protocol
Message confidentiality	yes	yes	yes	yes
Subscriber authentication	yes	yes	yes	yes
Session independence	no	no	no	yes
Computation power of mobile stations	low	high	high	low
Security between HLR and VLR	no	no	implicit	yes

<Table 1> shows security features provided by the GSM, CDPD, MSR+DH, and the proposed authentication protocols. GSM, CDPD, MSR+DH, and the proposed authentication protocols provide message confidentiality and subscriber authentication. The content of messages transmitted through the wireless network can be concealed by encrypting them. To apply the encryption techniques, both parties involved in secure communication should share a common session key before a communication session begins. In the proposed protocol, the security parameters used in one session are not used to the compromise of the next session key. The session independence is provide. The proposed protocol employs the keyed hash function to provide mutual authentication and session key distribution. The keyed hash function may be implemented using encryption if required. This protocol makes the low computation power of mobile stations. Unlike GSM and CDPD, the proposed protocol makes no assumptions about the security of the intermediate, fixed networks. The confidentiality between VLR and HLR is compromised.

5. Conclusions

Security is one of the most important requirements in wireless mobile communication systems. This paper proposed an authentication protocol for wireless mobile communication systems. This protocol employs the keyed hash function to provide mutual authentication and session key distribution. This protocol makes the low computation power of mobile stations. The distributed session key is used to encrypt messages over the traffic channel between the MS and the VLR. In this paper, to avoid the drawbacks of GSM and CDPD, we make no assumptions about the security of the intermediate, fixed networks. The confidentiality between VLR and HLR is compromised.

References

[1] C. S. Park, On certificate-based security protocols for wireless mobile communication systems, IEEE Network, pp.50-55, September/October 1997.

[2] ETSI GSM Tech. Spec. GSM 03.20, Security Related Network Function, 1992.

[3] TIA/EIA/IS-95, Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System, 1993.

[4] CDPD Forum, Cellular Digital Packet Data(CDPD) System Specification, 1995.

[5] M. J. Beller, L. Cheng, and Y. Yacobi, Privacy and authentication on a portable communication system, IEEE JSAC, vol.11, no. 6, pp.821-829, August 1993.

[6] A. Aziz and W. Diffie, Privacy and authentication for wireless local area network, IEEE Personal Commun., pp.25-31, First Quarter 1994.

[7] W. Diffie and M. E. Hellman, New directions in cryptology, IEEE Trans. on Information Theory, vol.IT-22, no.6, pp.644-654, November 1976.

박 영 호 (Park Young-Ho)

1989년 경북대학교 공과대학 전자공학과 (공학사)

1991년 경북대학교 대학원 전자공학과 (공학석사)

1995년 경북대학교 대학원 전자공학과 (공학박사)

1996년 3월 - 현재 상주대학교 전자전기공학부 조교수

관심분야: 정보보호, 컴퓨터 네트워크