Enhanced Authentication Protocol for Wibro Networks

Choonghun Lee and Hyunsu Chae

Samsung Advanced Institute of Technology (SAIT)

Summary
With the increasing the number of mobile users for the wireless networks that have been deployed, the security featured authentication protocol for accessing the network for the user service has been gaining the importance and playing the contributing role. In this paper, a enhanced authentication protocol with PKI-based-certificate scheme is proposed for the wireless networks such as wireless LAN, wireless MAN and Wibro. With the proposed authentication mechanism, user identity confidentiality would be kept private and also the time for authentication would be reduced to practically usable level in terms of authentication time and power consumption efficiency, effectively in the heterogeneous all IP network..

Key words:
authentication; PKI; wireless network; wireless security; Wibro.

1. Introduction

As the need for the user mobile device stupenduously has increased and wireless nework infrastructure has been deployed, one of the requirements for person who experences and enjoys benefits of the wireless is the security and privacy such as identity protection. That potential concern and regard has never became more serious than ever before, as in this widely and everywhere accessable internet information age.

Especially, Wibro(Wireless Broadband Network) service has been commercialized in many areas. This deployment is the commerization of IEEE 802.16e based wireless technology. This emerginig techonolgy provides high data rate for high speed moving enough for the multimedia as well as large access coverage range. Therefore, Wibro is the good and practical solution for interactive multimedia communication and heavy internet usage in the high speed moving environments. Although this techology provide mobility to the mobile users at high speed and users can get the enjoy of the internet connectivity while they are in the movement, the security problem such as privacy, identity and user information revelation threaten the prevailing mobility need and the promising with the variety of IP-based wireless internet services. In order to pass over this situation, the authentication mechanism would be tighten and more solid.

Manuscript received September 5, 2008
Manuscript revised September 20, 2008

With the commercialization, many various service provders would appear and want have own domain of service, authentication and security component. Thus, the requirement of security would need the more cross and inter domain technical features. Providing of the different service and security domain would have the sharp impact on the successful deployments of the all IP-based technology. Together with the inter-domain service, all IP-based network would support the heterogeneous wireless network such as WLAN, 3G, WPAN, etc. That means that the wireless service provides the mobile users the vertical and inter-domain handover, also based on the inter-domain authentication. All IP-network is the internet based open architecture, enabling plug&play of new IP-based at the system structural component level with easy insertion and removal.

User relevant information confidentiality is one of the requirement of security and privacy in this kind of inter-domain all IP-based network. User ID confidentiality could be considered together with the combination of user location confidentiality and user un-trace-ability. User ID confidentiality is the protection against a intruder trying to identify which subscriber is using a given resource on the radio path. User location confidentiality is the property that the presence or the arrival and leaving of a user in a certain area cannot be determined by eavesdropping on the radio acces link. User un-trace-ability is the property that an intruder cannot deduce if the different services are delivered to the same user by eavesdropping on the radio access link and the trace of service usage.

2. II. BACKGROUND AND RELATED WORKS

2.1 RSA overview

In this section, we overview the RSA basic mathematics, practical implementation and usage in terms of the performance and also practical performance.
From the RSA definition, n is chose such as, n = pq where p and q are distinct prime. Then e would be selected.

e<n such that GCD(e,phi) = 1 (phi, φ = (p-1)(q-1))
d = e^-1 mod phi
Encryption with public key would be
c = m^e mod n.

In this case, 17 bit(01000001) is usually the value of e.
Decryption with private key would be
m = c^d mod n.

In this case, d would be 1024 bit value.
And generally, the operation of asymmetric encryption take shorter time than that of symmetric encryption by two magnitude of 10.

The table 1 shows encryption/decryption operational time performance of the commercial crypto engine for RSA. The Encryption time is very different from the decryption time from the exponent value bit difference.

Table 1 Performance Advanced Crypto Engine

Operation	***Modulus***	***Exponent***	***Calculation Time***	
			15Mhz	33Mhz
Modular Exponentiation RSA Encrypt	1024bit	17bit	3ms	2ms
	2048bit	17bit	210ms	96ms
Modular exponentiation RSA Decrypt	1024 bit	1024 bit	273ms	124ms

2.2 X.509 certificate

The general purpose format of X.509 includes the subject unique identifier to identify each mobile end user. In case of 802.16e, the subject unique identifier would be the MAC address. From the fact that transferring the digital certificate which includes the MAC address in the air in the transparent form, there is the need of hiding the certificate for user id confidentiality. Some other practical features are discussed for the different certificate authorities(CA) usage of different ISP. It is true, in reality, that it is not easy to establish the required trust relationship of a hierarchy in the world.

2.3 Initialization and Network entry

Authentication is the necessary step for the mobile end user to enter the network and is located usually in the initialization process for most network system. Authentication usually follows the physical layer detection, physical synchronization and ranging, and MAC layer capability protocol negotiations. After authentication and key exchange, logical registration and IP level connectivity goes on. From the general observation of the network entry, authentication process is between logical processes embedded in network entry procedure, not separate process.

2.4 Network Configuration

MS is the mobile station or mobile node which is the user domain terminal device. Home Network is the network domain where the maintainence of the user take place and it's involved with the responsibility of user subscriptions and billing, authorization and authenticaiton service. Vsisting network is the network which is defined as the different network service domain and has the different authentication authority and certificate authority. BS is the base station to which the user terminal has the immediate physical connection through the air interface. AAA server is responsible for the authentication, authorization and accounting, where Home AAA is the server from which the user subscriber has the regristration, and Foreign AAA is the server which user subscriber doesn't have the register with and is governed with different authorization policy. The visiting newtork is possibly the different ISP, heterogeneous wireless network and has the different CA for the PKI.

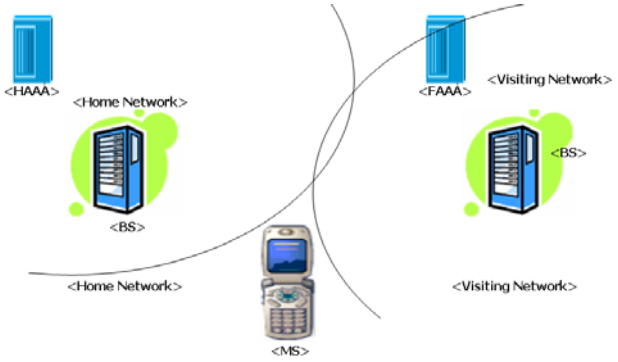

Fig. 1 Network Configuration

3. Authentication Scenario

The primary focus of this paper is the authentication process between user terminal and network for the network access entry. Typical authentication procedure is reviewed and compared with the proposed process. The scenarios and approaches are mainly focused upon the point of view for the user confidentiality and protocol handshake.

3.1 Typical Scenario

Fig.1 shows the general usage of the certificate for the entry of the wireless network.

flow (1) : user terminal → network

$Cert_{MS}, Cryptlist....$

flow (2) : network → user terminal

$E_{KU_{MS}(}(authkey, SSid), SN, LT$

$Cert_{MS}$ is the digital certificate for the user subscriber. $E_{KU_{MS}}$ is the encryption of public key of MS. In flow(1), user terminal sends the certificate and cryto capability list to negotiate and connect to the network for authentication info and authorization request message. The access network generates authentication key for MS and encrypts the authentication with MS public key. Then, reply back to MS, which forms the authorization reply message.

s

Above the scenario, in case that the ISP or authorization authority of the visiting network is different from that of the home network, the access for network entry is not considered as the network entry case and causes the extra time consumed. Even when the BS tries to connect to Home AAA, it has to get through other authentication procedure. On the wirelss path, when the MS tries to send out the physical wireless signal, as the contents of $Cert_{MS}$ is exposed to the outside, user identity confidentiality is not assured, and also that entry process is exposed to the replay attack.

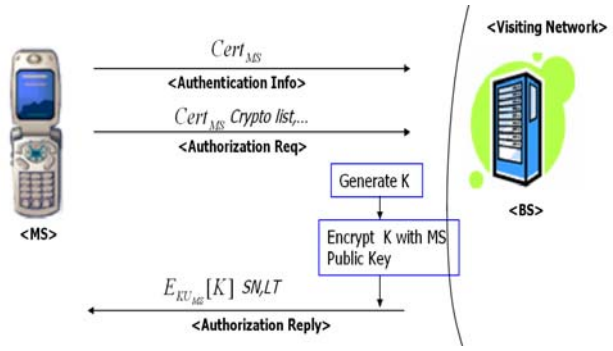

Fig. 2 Network Entry Procedure

3.2 Enhanced Scenario

Fig.2 shows the enhanced usage of the certificate for the network entry. That scenario consists of 3-way handshake. User's certificate is encrypted for the user confidentiality, since user certificate contains many user private information.

flow (1) : user terminal → network

$R_{MS}, Cert_{HAAA}$: <HN Info>

flow (2) : network → user terminal

$R_{MS}, R_{BS}, Cert_{BS}$: <HN Info Reply>

flow (3) : user terminal → network

$E_{KU_{BS}}(K), \{Cert_{MS}\}_K, SN, LT$: <MS Info>

R_{MS} is the random number generated for the service subscriber of the user terminal, which would prevent a replay attack and R_{BS} is the random number generated for base station. $Cert_{BS}$ is the digital certificate for the base station of the network to which subscriber is trying to attach and used for the mutual authentication between user subscriber and base station. K is the authentication key that is generated by the user subscriber terminal. $E_{KU_{BS}}$ is the encryption process with the public key of BS. $\{Cert_{MS}\}_K$ is the certification of MS encrypted with K. $E_{KU_{BS}}(K)$ is the K encrypted with public key of BS. SN is the sequence number. LT is the life time.

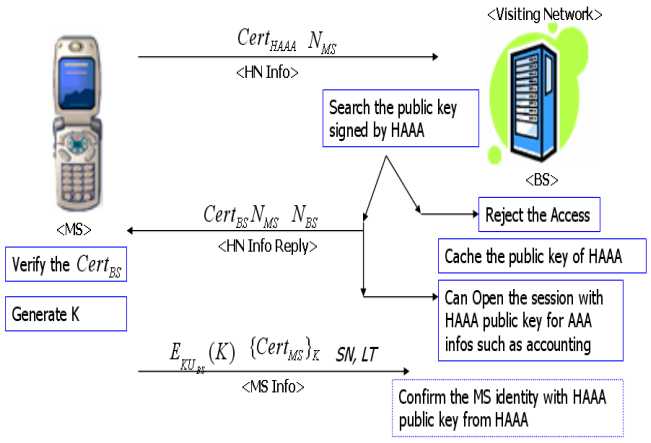

Fig. 3 Enhanced Network Entry Procedure

Each flow(1), flow(2), flow(3) corresponds to the "authentication request", "authentication reply" and "authentication acknowledge" message in the negotiation process.

In flow (1), when user subscriber tries to enter the network, it sends <HN Info> message which contains the certification of its HAAA together with random number.

The network searches for the public key signed by HAAA. If failed, the network would reject the network entry access. Or, the network would open the session with HAAA for AAA informations such as accounting. And also, the network could cache the public key of HAAA for later use in the case of the uses for same HAAA. If the BS caches the public key of HAAA, it is not ncecssary to contact to the same HAAA server for another request of authention and would contribute to time saving at the network side.

In flow (2), then, BS sends back the <HN Info Reply> message to the user subscriber terminal. The user subscriber terminal verifies the certification of BS, and generate the key . This verification of BS certification gets rid of the possibility of rogue base station.

In flow (3), after verification of base station, the user terminal encrypts the key with the public key of base station and together encrypts the certificate of user terminal, enhancing the privacy of user identity in the user certificate. Then, user subscriber terminal sends them along with sequence number and for <MS Info> message. At the other side then, base station would confirm ths identity of user subscriber terminal with HAAA public key from HAAA.

From above scenario, it is achieved that the avoidance of rouge base station through verification of base station's certificate and easy access to other domain visiting network through HAAA certificate. And also, other advanages of this scheme are the protection of user subscriber terminal identity as well as the prevention of replay attack.

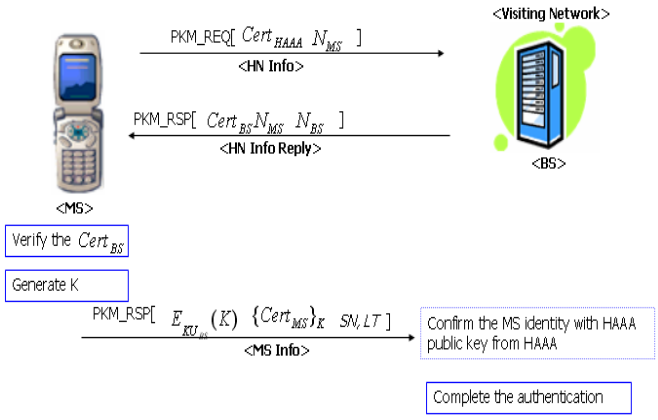

Fig. 4 Enhanced Network Entry for Wibro

3.3 Wibro Scenario

Proposed Enhanced network entry authentication process would be applied to the Wibro system. Contents of the message from the Enhanced network entry authentication would be wrapped within the Wibro authentication messages. And the number and back-and-forth direction of the handshake is well matched with that of Wibro authenticaiton process, resulting to the easy adaptability and implementation without heavy modifications.

From point view of operation number and time consuming efficiency, In flow (1), after receiving the <HN Info> message as the authentication request, BS verifies the certificate using RSA signature verification operation with public key, which amounts to 1 operation of RSA encryption. And also, in flow (2), MS verifies BS certificate with 1 operation RSA encryption. And user terminal encrypts the generation key with base station public key for 1 RSA operation. Totally, at this point of time, 1 RSA encryption operation and 1 RSA decryption operation took place in MS and 2 RSA encryption operations in BS of network.

Other advantages are the power consumed and the computation time for lean mobile terminal device compared with heavy installed equipment such as BS from this proposed authentication scheme. Power consumption and computation capability usually give the restrictions on the mobile device size, cpu selection, price and in result the usage time for mobility. Enhanced authentication scheme assigns the jobs which cost heavy computation and power consuming to the base station side for which those restrictions are not serious problems and tolerant.

Encryption with public key takes place at the user terminal and decryption with private key is executed at the base station side. From the table 1., the time discrepancy would be the two order of magnitude. That amount of time would be practically the critical factor for the real deployment. Usually, time and computation complexity depends up the length of key. Considering the difference of length of the key, it is appropriate for the use of private key to happen in the base station. That asymmetric assignment of encryption and decryption save the power and make the network entry authenticaton time short at the user subscriber terminal.

4. Conclusions

In this paper, the enhanced authentication machanism is proposed for the wireless network with the certificate based MS. In the authentication process, as the certificate

of home server is submitted, home server information and public key information are given to the target access network, being enable to enter easily the heterogeneous network or network that has the different CA and is the different ISP. Through the symmetric encryption of the MS certificate with user generated key, the user identity confidentiality is accomplished without any load and the replay attack through air interface is prevented. The proper handshake processes has achieved the critical reduction of authentication time in the practical network entry, together with taking off the user terminal the burden of the power consumption and complex computation. It is expressed that the BS would cache the certificate of home server. And the propsed authentication mechanism is applicable to the Wibro without any technical restriction and glitch.

Consequently, certificate based enhanced authentication scheme leads to the satisfying results for the all IP wireless network.Acknowledgments

References

[1] Wenhui Zhang, “Interworking security in heterogenous wireless IP networks”, WCNC 2004

[2] Kim,P.: Fast Handover for Mobile Ipv6 Based IEEE802.16e Wireless Netowrks.(June 2006)

[3] IEEE Std802.16e.

[4] 3GPP,3G TS 33.102 “Security architecture”.

[5] D.Johnson,C.Perkeins, and J. Arkko,”Mobility Support in Ipv6”.IETF

[6] H.Wang, A.R. Prasad, P. Schoo, “Research issues for fast authentication in inter-domain handover”, in Proc. Of Wireless World Research Forum(WWRF), 2004

[7] M.Zhang and Y. Fang. “Security analysis and enhancements of 3GPP authentication and key agreement protocol”. IEEE Transations on wireless communication,2005

[8] RFC 3748,”Extensible authentication protocol(EAP)” June, 2004

[9] Wenbo Mao,Modern Cryptography: Theory and Practice, Prentice Hall PTR,2003

[10] C.M.Huang and J.W.Li. “Authentication and Key Agreement Protocol for UMTS with Low Bandwidth Consumption” AINA 2005

[11] S.Burnett and S. Paine,”RSA Security’s Official Guide to Cryptographu”, The McGraw-Hill companies

[12] S.Kent and R. Atkinson. “Security Architecture for the Internet Protocol”, RFC2401