통합된 WLAN/3G 네트워크의 증명 방법의 분석

Anish Prasad Shrestha* · 한경헌* · 조병록** · 한승조1*

*조선대학교

**순천대학교

Analysis of Authentication Architecture in Integrated WLAN/3G Networks

Anish Prasad Shrestha*, Kyong-heon Han*, Byung-Lok Cho**, Seung-jo Han1*

Department of Information and Communication Eng. Chosun University*

School of Mechanical & Automotive Eng. Sunchon University**

1*Corresponding author. E-mail : sjbhan@chosun.ac.kr

ABSTRACT

A number of wireless technologies have been implemented, but each technology has its limitation in terms of coverage and bandwidth. WLAN and 3G cellular network has emerged to be a complementary platform for wireless data communications. However, the mobility of roaming terminals in heterogeneous networks poses several risks. To maintain secure communications in universal roaming, the effective authentication must be implemented. The focus of this paper is on analysis of authentication architecture involved in integrated WLAN/3G networks.

Keywords

3G cellular system, Wireless LANs, authentication, security associations

I. Introduction

Increase in user demand for ubiquitous high speed wireless access is motivating the deployment of a wide array of wireless networks, ranging from Wi-Fi, Bluetooth, Wi-Max to cellular networks like CDMA and UMTS. However, each technology has itsown limits in terms of coverage and bandwidth. This led the idea of integrating different heterogeneous wireless networks. In recent years, the two technologies i.e. WLAN and 3G cellular networks have turned out to be complementary platform in making it truly ubiquitous - available anywhere, anytime.

A wireless LAN, which is very popular for hotspots such as airports, offices and hospitals, provides all the features of wired LANs, but without the wires. The most desirable aspect of WLAN is its data rates of 1 - 54 Mbps and flexibility in deployment. However, its service coverage is limited to the order of tens of meters. Furthermore, it operates in unlicensed ISM band resulting possible interference. On the other hand, the cellular networks offer greater coverage but with limited data rates. Even with the improvement in UMTS and WCDMA, the data rate is limited up to the range of 64Kbps to 2Mbps. As such ubiquitous high speed wireless access is viable by integration of WLAN and 3G cellular networks because of their strengths in different perspective [1]. A mobile user with dual radio interface supporting both WLAN and 3G cellular environment can enjoy high bandwidth in WLAN network and switch to cellular network in absence of WLAN for universal roaming.

Integrating 3G and WLAN network design efficiently is a complex and challenging task. Many issues should be considered, such as network architecture, consistent quality of service (QoS) and service provisioning, seamless mobility, unified accounting and billing mechanism, security management etc. However, the design of authentication architecture that serves universal roaming is a critical issue for both service providers and subscribers in the present context.

The verification of both the mobile user and alien network is obligatory prior to service delivery. Efficient authentication is the primary foundation which helps to achieve what are necessary elements in heterogeneous network security i.e. positively identifying visiting Mobile Nodes (MN); allowing them specific services; and holding them accountable for their actions or collectively known as AAA (Authentication Authorization and Accounting). The rest of paper is organized as follows. Section II introduces the background of authentication in 3G cellular network, WLAN and mobile IP. In section III, generic authentication architecture and drawbacks in such architecture is discussed. In section IV, improved authentication architecture is introduced along with establishment of security association and probable authentication process in such architecture. Section V focuses on possible improvement in such architecture. Finally the conclusion is drawn.

II. Authentication in different Networks

A. Authentication in 3G Cellular Network

UMTS and WCDMA are two emerging 3G cellular technologies. UMTS security builds on the security of GSM, inheriting the proven GSM security features [2]. UMTS consists of five security feature groups:

1) Network Access Security: provides users with secure access to UMTS services and protect against attacks on the radio access link. 2) Network Domain Security: protects against attacks on the wire line network and allows nodes in the provider domain to exchange signaling data securely. 3) User Domain Security: provides secure access to mobile stations. 4) Application Domain Security: allows the secure exchange of messages between applications in the user and in the provider domain. 5) Visibility and configurability of security allows the user to observe whether a security feature is currently in operation and if certain services depend on this security features

Authentication in UMTS is defined as part of Network Access Security. Unlike GSM, which authenticates the user to the network only, UMTS uses mutual authentication which means the mobile user and the serving network authenticate each other, providing security against false base stations. This mutual authentication uses an authentication quintet. The authentication quintet consists of the user challenge (RAND), expected user response (X(RES)), the encryption key (CK), the integrity key (IK) and the authentication token for network authentication (AUTN). Also UMTS provides a new data integrity mechanism which protects the messages being signaled between the mobile station and the radio network controller (RNC). The user and network negotiate and agree on cipher and integrity algorithms. Both the integrity mechanism and enhanced authentication combine to provide protection against active attacks on the radio interface. This mutual authentication is referred as UMTS authentication and Key Agreement (AKA) which takes place between USIM and the SGSN/VLR.

On the other hand, the random number generation is standardized in WCDMA along with key generation algorithms and encryption and decryption algorithms. As such the authentication vectors for re authentication and tracking is influenced.

B. Authentication in WLAN

The evolution of WLAN security began with IEEE 802.11 standard. It helped launch practical wireless LANs suitable for hotspots, but security was not commercial grade from both the authentication and data privacy perspectives [3]. The solution for security services are provided largely by the Wired Equivalent Privacy (WEP) protocol. The authentication mechanisms both Open System authentication and Shared Key authentication as well as weak implementation of the RC4 algorithm made it less desirable. Soon, IEEE 802.1X was introduced to specifically address the WLAN authentication function which was based on port-level authentication. If a wireless user is authenticated via 802.1X for network access, a virtual port is opened on the access point allowing for communication. If not successfully authorized, the virtual port is not made available and communications are blocked. The client can be authenticated when it initially connects to a LAN before it gets an IP address (via DHCP) or other higher layer transport configuration tying a protocol called EAP (Extensible Authentication Protocol). EAP is simply an authentication protocol which supports multiple authentication mechanisms

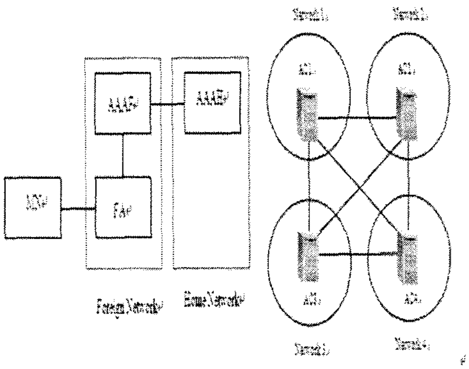
C. Authentication in Mobile IP

Mobile IP can be referred as basis for the integration of WLAN/ 3G cellular network as it involves complicated heterogeneous wireless environments. It allows users with mobile devices whose IP addresses are associated with one network to stay connected when moving to an alien network with a different IP address. Generally it defines an authentication extension by which a mobile node can authenticate itself to a foreign agent. Authentication based on Public key along with digital certificates and digital signatures can also be implemented [4]. To reduce latency in this design, key distribution center capable of generating the security contexts needed to authenticate Mobile IP control message is employed [5].

III. Generic Authentication Architecture

Since mobility amongst heterogeneous network environment is inevitably main stream in WLAN/3G interworking, the first objective is to provide network connectivity and resource necessary to mobile users at any time and in any location. A visiting mobile node needs the same level of service that it gets in home network so the foreign network must care about the service authorized and to it and the charging mechanism. This ultimately leads to the concept of Mobile IP with AAA extensions.

A generic authentication architecture implements AAA server in each network domain sharing security association amongst them so that it can share the credentials of MN in secured manner. Security association is simply a collection of connection-specific parameters which describes how two or more entities will utilize security services.



(a) AAA Servers with Mobile IP agents (b) Sharing of static SA amongst Authentication Centers

Figure 1 Conventional Authentication Architecture

The foreign agent (FA) advertises the challenge. The MN adds Network Access Identifier (NAI), Challenge Response etc to Mobile IP request. The FA invokes AAA protocol with its local AAA server (AAAF). The AAAF parses NAI, finds MN's home server address (AAAH) and invokes AAA protocol and awaits approval by AAAH. AAAH checks MN credentials and upon verification a home address for the mobile node is allocated.

The problem in using static SA lies on the fact that it causes the network to be unscalable because each AC must manage a huge amount of inter-domain SAs. The total number of inter-domain SAs in such architecture exhibits a tremendous growth when the number of ACs increases. Moreover, its lifetime is long and hence exposes more targets to be attacked.

However to cope up with the erratic growth in the number of AAA servers, hierarchical AAA brokers are used in between AAAF and AAAH to speed up the authentication. But the time taken to search upper AAA Brokers may last long especially if the roaming MN too far.

IV. Improved Architecture:

As static security association would be infeasible between mobile node and each visited domain in a scalable solution, the improved architecture is based on sharing of dynamic security association between authentication servers rather than static security association [7].

The architecture would basically comprise distributed or heterogeneous wireless network with an authentication server in each wireless network for authenticating MNs. The authentication server is referred as Home Authentication Server (HAS) for the MN which subscribes the service in its network and Local Authentication Server (LAS) for the MN roaming in foreign network. The intra-domain authentication can be processed using RADIUS or DIAMETER protocol since the MN would share static SA with home authentication server but for inter-domain, SA is established dynamically as shown in figure 2.

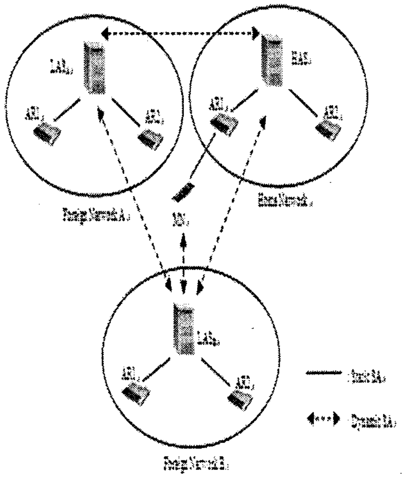
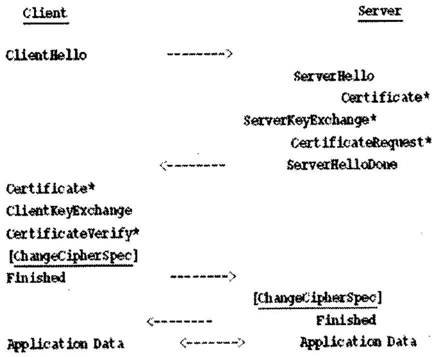


Figure 2: Improved authentication architecture

Basically, every access router (AR) in a wireless network shares a static SA with the Authentication server in its network. The MNs in its home network is intrusted by HAS through the static SA. However, the MN would dynamically establish SA with LASs in foreign network. The LASs are also connected to each other by dynamic SAs. During the authentication, if the SA exists MN is authenticated otherwise SA would be established dynamically and the credentials from MN are collected. It would also check if SA exists between LAC and HAS and transfer the credentials of MN to HAS for authentication. After the authentication of MN, a threshold time would be calculated for the expiration of set up security association.

A. Establishment of Dynamic SA

SA can be established dynamically by using four way handshake protocol in Transport Layer Security (TLS). The TLS consists of a suite of sub-protocols which are used to negotiate nodes for algorithm support and security parameters for the record layer, exchange keys and cipher encryption, instantiate negotiated security parameters and report error conditions to each other [8].



```
Client                                      Server

ClientHello           -------->
                                       ServerHello
                                      Certificate*
                                ServerKeyExchange*
                                CertificateRequest*
                      <--------     ServerHelloDone
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished              -------->
                                  [ChangeCipherSpec]
                      <--------           Finished
Application Data      <------->   Application Data
```

Fig.3 - Message flow for a full handshake

The first phase is to initiate a logical connection. At the second phase, a server sends a public key with its certificate to the client. The third phase is performed by the client to provide its public key and certificate to the server after successfully receiving and verifying the public key of the server. The fourth phase is to confirm cipher specification parameters, such as keys, algorithms, and lifetime of the SA, based on the shared secrets. After these steps, an SA is established between the client and the server.

B. Authentication in Foreign Network

During the authentication, the LAS would be administering three possible states of authentication:

Session Authentication in foreign network:

When an MN starts a communication session in a foreign network for the first time, a session authentication is initiated. The LAS establishes security associations with MN and then with HAS.

Intra domain hand-off authentication within same foreign network:

When an MN crosses the boundary of subnets in the foreign network domain with an on-going service, an intra-domain hand-off authentication takes place. Since there is an on-going communication session between the MN and an AR, one session SA exists between the MNand the LAS in the visiting network domain. Therefore, it is unnecessary to contact the HAS for authentication.

Inter domain hand-off authentication in new foreign network:

When an MN is crossing the boundaries of different foreign network domains with an on-going service, an inter-domain hand-off authentication occurs. Since no session SA exists between the MN and the new AR, and it is necessary to contact the HAS of the MN for authentication.

V. Prospective improvements

Authentication introduces delay and traffic overhead into the network operators which is unavoidable by any means. So it is necessary to consider certain factors while developing authentication design to reduce setback caused by it. Four important factors can be taken up into consideration in this design i.e. average number of security associations, risk evaluation of DSA, bandwidth efficiency and finally authentication latency.

Average Number of security association:

Our main objective should be maintaining minimum number of SA between the nodes as possible. Reducing the number of SAs can be beneficial to authentication server in managing these SAs and thus improving the manageability of networks, which is of particular interest to large-scale and distributed wireless networks. Huge number of SA can impose great management effort to authentication server which can degrade the performance of the entire network.

Risk Evaluation:

Due to open environment in wireless network, transmitted data are in constant threat of being exposed. As such longer an SA exists, more vulnerable it becomes. Thus, a decrease of the threshold time to keep a dynamic SA will reduce the risk that an SA is hacked. The risk of being exposed remains higher in foreign network than in home network. There also remains risk of denial of service due to incompatibility in a foreign network that MN may face in foreign network.

Bandwidth efficiency:

The minimization of threshold time to retain less number of SAs and minimum risk can increase the number of establishment of dynamic SA which is time-consuming and will degrade the bandwidth efficiency due to bandwidth idle for authentication waiting time. Therefore the threshold time should be adjusted for the expiration of DSA as per the roaming pattern. The roaming pattern from one network to another is usually different in different time periods. For example, during peak hours, there is normally high mobility as people may be moving from home to work place and vice versa whereas lower mobility may be the case after business hours for the same group of people in the same area. Therefore, the threshold time can be set up to adapt such roaming patterns.

Authentication latency:

The delay caused by authentication induces the probability of loss in connection. Therefore, a roaming authentication should be aimed at reducing number of transmissions between the home and visited networks as much as possible. Moreover, the longer threshold time allows the reuse of dynamic SA during authentication which subsequently reduces the authentication latency.

VI. Conclusion

In summary, this paper analyzed the authentication in 3G cellular network, WLAN and in Mobile IP. After that, improved authentication architecture in 3G/WLAN integration is explored based on establishing security associations on demand instead of using static security association. Although the use of dynamic SA has strong benefits over use of static SA, a proper computation of threshold time while deploying dynamic SA would further enhance the overall network performance. In future, a pioneering effort for the calculation of threshold time is expected to be carried out with proper trade off between number of SAs, risk evaluation, bandwidth efficiency and authentication latency as per the roaming patterns and traffic volume of the heterogeneous network.

References

1. Geir M. Køien and Thomas Haslestad, Telenor R&D, Norway, Security Aspects of 3G-WLAN Interworking

2 . http://www.umtsworld.com/technology/security.htm

3. Jim Burns, John Hill, Evolution of WLAN Security 10/4/03

4. Jacobs S. Mobile IP public key based authentication. draftjacobs-mobileip-pki-auth-02.txt, March 1999

5. Sanchez L, Troxel G. Rapid authentication for mobile IP.draft-ietf-mobileip-ra-00.txt (expired), November 1997.

6. S. Glass, T. Hiller, S. Jacobs, C Perkins Mobile IP Authentication, Authorization, and Accounting Requirements, October 2000

7. Wenye Wang, Wei Liang and Avesh K. Agarwal, Integration of authentication and mobility management in third generation and WLAN data networks, Wirel. Commun. Mob. Comput. 2005; 5:665 - 678

8. T. Dierks and C. Allen. The TLS Protocol. RFC2246, January 1999

※ This work was supported in part by MIC & IITA <08-Infra-13, IT Research Infrastructure Program>