통합된 WLAN/3G 네트워크의 증명 방법의 분석

Anish Prasad Shrestha* · 이상덕** · 조병록*** · 한승조*†

Analysis of Authentication Architecture in Integrated WLAN/3G Networks

Anish Prasad Shrestha · Sang-duk Lee · Byung-Lok Cho · Seung-jo Han

이 논문은 2007년도 조선대학교 학술연구비의 지원을 받아 연구되었음.

요 약

많은 무선기술이 개발되었지만, 그 기술들은 적용사례와 대역폭에서 한계를 가지고 있다. WLAN과 3G 네트워크는 무선통신을 도와주기 위한 플랫폼으로 나왔다. 그러나 서로 다른 네트워크 터미널의 이동성은 여러 리스크를 발생시킨다. 통신 보안과 효과적인 증명이 실행되어야 한다. 이 논문의 주제는 통합된 WLAN/ 3G 네트워크에 관한 증명방법의 분석에 있다.

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.

키워드

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

Ⅰ. Introduction

A growing number of wide array of wireless networks technologies, ranging from Wi-Fi, Bluetooth, Wi-Max to cellular networks like WCDMA and UMTS, with increasing number of wireless service providers have truly created a heterogeneous wireless network with almost a global coverage. However, each technology has its own limitations in terms of coverage, bandwidth and delay. This led the idea of integrating different heterogeneous wireless networks so that mobile user can have seamless connectivity allowing inter-operation of the different technologies and providers.

* 조선대학교 정보통신학과
** 조선대학교 전자공학과
*** 순천대학교 전자공학과
† Corresponding author: Seung-jo Han

접수일자 2008. 05. 30

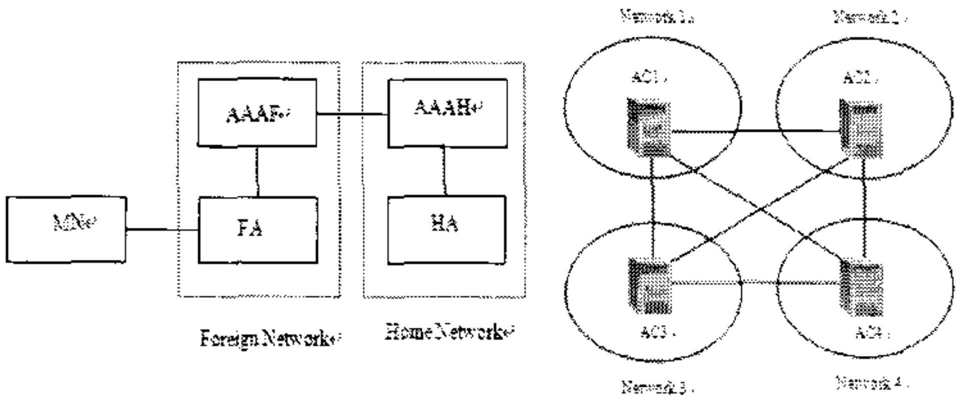
From a mobile user's viewpoint, it is highly desirable to have "Best Connection" available. For example, a cellular network user when enters a hotspot region supported by WLAN, it can switch to WLAN for higher data rates where as a WLAN user can switch to cellular network when it crosses hotspot region for higher mobility.

For a user visiting different foreign networks, hand-off mechanisms either horizontal or vertical is inevitable [1]. For a user to get seamless feeling, hand-off delay must be minimized. A key reason for a longer hand-off delay in the existing solutions for secure, seamless roaming across administrative domains is the delay introduced by the authentication process.

To accomplish secure and seamless communication in heterogeneous wireless networks, an authentication architecture that takes into account the mobility of users should be focused.

The rest of paper is organized as follows. Section II and section III introduces Authentication Architecture based on static security association and dynamic security association along with establishment of security association and probable authentication process in such architecture respectively. Section IV focuses on Integration of Mobility & Threshold Time and in section V, the benefits of such integration is analyzed. Finally, the conclusion is drawn.

Ⅱ. Authentication Architecture based on static security association



(a) AAA Servers with Mobile IP agents
(B) Sharing of static SA amongst Authentication Center
Figure 1. Conventional Authentication Architecture
(a) Mobile IP 에이전트가 있는 AAA 서버
(b) SA 증명 선터의 배분
그림 1. 증명 방법 형식

Mobile IP can be referred as basis for heterogeneous wireless environments as 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. The authentication architecture in implementing such techniques is proposed in [2]. 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 authentication centre (AAAF). The AAAF parses NAI, finds MN's home authentication centre 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 security association(SA) is maintained between two different networks which is normally static in nature.

The SAs are unidirectional, so that peer 1 will offer peer 2 a policy. If peer 2 accepts this policy, it will send that policy back to peer 1. This establishes two one-way SAs between the peers. Two-way communication consists of two SAs, one for each direction.

For a distributed as shown in figure network with NAC number of ACs, the total number of inter-domain SAs denoted as NSA, can be expressed as

$$NSA = NAC\ (NAC - 1)$$

The total number of inter-domain SAs for distributed network with varying LACs is shown below:

Table 1. Increase in no of SAs with increase in NO. of LACs
표 1. SAs의 증가량과 LACs의 증가량

No. of LACs	Number of inter-domain SAs
3	6
4	12
5	20
6	30

As can be seen from the above table, the total number of inter-domain SAs in such architecture exhibits a tremendous growth with unit increase in number of LACs. This leads the network to be unscalable because each AC must manage a huge amount of inter-domain SAs. Moreover, its lifetime is long and hence exposes more targets to be attacked.

Ⅲ. Authentication Architecture based on dynamic security association:

As static security association would be infeasible in a scalable solution, the authentication architecture is based on sharing of dynamic security association rather than static security association is proposed in [3].

The architecture would basically comprise distributed 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. SA is established dynamically during authentication in foreign network as shown in figure 2.

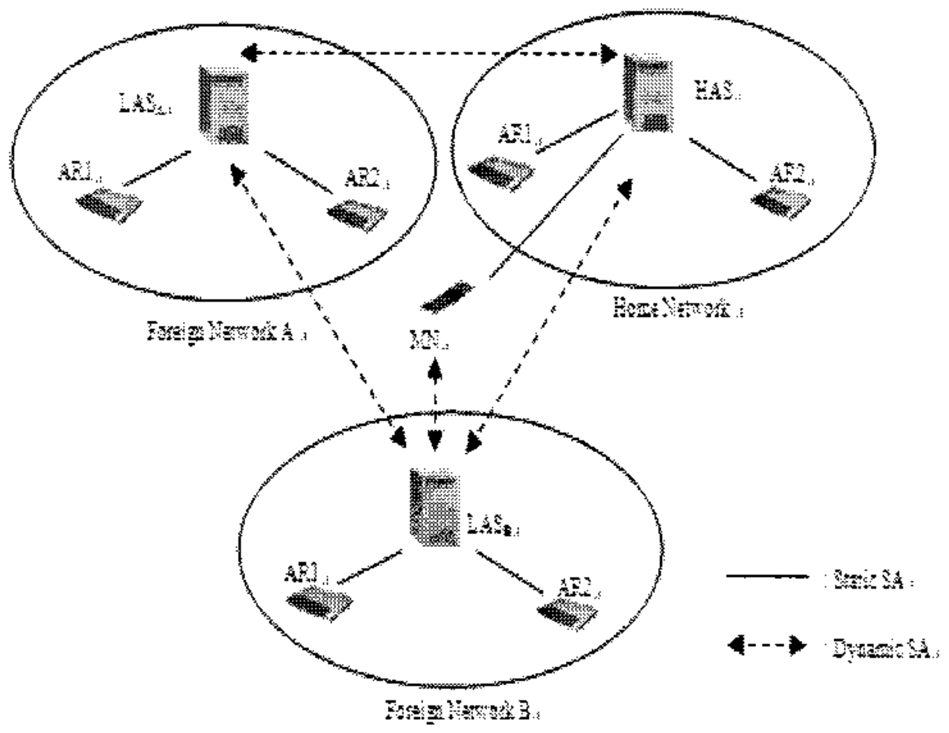


Figure 2. Authentication architecture based on dynamic security association
그림 2. 동적인 보안 단체에 기초를 둔 증명 방법

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 [4].

```
      Client                                    Server

Client Hello          -------->
                                          Server Hello
                                         Certificate*
                                     Server Key Exchange*
                                      Certificate Request*
                      <--------          Server Hello Done
Certificate*
Client Key Exchange
Certificate Verify*
[Change Cipher Spec]
Finished              -------->
                                      [Change Cipher Spec]
                      <--------             Finished
Application Data      <------->         Application Data
```

Initially, client and server exchange two messages in which they tell each other which cryptography and compression features they support, along with "pseudo"-nounces and a session ID. The server decides upon the list of cryptography and compression algorithms sent by the client whethe rto continue or cancel the session. There must be at least one match in both lists, otherwise the session will fail.

The next stage of handshake involves authentication and key exchange between both parties. Authentication and key exchange are both done by sending certificates, as long as both sides can provide them. If not, it is possible to transfer public keys without transferring certificates. Depending on if there were certificates send, and depending on the type of these certificates, both sides may be able to verify each other's identity by checking the validity of these certificates.

The change cipher specmessage simply tells the other side to set up the cipher suite agreed on in the first stage one for data encryption and one for subsequent key exchanges. The notification at the end marks the completion of the handshake. It is already encrypted using the agreed-on algorithms. After these steps, an SA is established between the client and the serverand a threshold time to expire the SA is also set.

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 handoff 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 MN and the LAS in the visiting network domain. Therefore, it is unnecessary to contact the HAS for authentication. The hand-off is normally horizontal hand-off.

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. The hand-off can either be vertical or horizontal hand-off.

Ⅳ. Integrating Mobility & Threshold Time

A user in heterogeneous network is expected to exhibit some kind of mobility patterns which we categorize into high mobility and low mobility. A mobile node with high mobility (MNHM) is likely to contribute more inter-domain handoff authentication request in a given duration than a mobile node with low mobility (MNLM) which is likely to cover less area and hence contributing less inter-domain handoff authentication and more of intra-domain handoff authentication. As such, dynamically established SA can be reused by MNLM where as MNHM has to frequently visit new foreign networks and set up new SA.

The total lifetime of SA can be calculated as

Lifetime of SA = T_{au} + T_s + T_{th}

T_{au} = Time taken for authentication

T_s = Time of service

T_{th} = Threshold time for expiration of dynamic SA

We propose to set high threshold time for MN_{LM} and low for MN_{HM}. As such the lifetime of SA for the earlier becomes longer and for latter one becomes shorter.

Ⅴ. Consequences

To assess the efficiency of authentication architecture, four parameters are considered namely: average number of security association, authentication latency, bandwidth efficiency and risk of SA being revealed. Minimization of average number of security association, authentication latency and risk and maximization of bandwidth efficiency improves the architecture. Decrease of T_{th} minimizes average number of security association and risk while increase of T_{th} maximizes bandwidth efficiency and authentication latency. As T th is set high for MN_{LM} and low for MNHM, the overall scenario can be summarized as shown in table below:

Table 2. Analyzed parameters
표 2. 분석된 파라미터

Parameters	Objective	Threshold Time	Low Mobility	High Mobility
No. of SA	Minimize	Decrease	Tth increased	Tth decreased
Authentication Latency	Minimize	Increase		
Bandwidth Efficiency	Maximize	Increase		
Risk	Minimize	Decrease		

The effect of such integration of mobility and threshold time is analyzed below

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 dispersed wireless networks. Huge number of SA can impose great management effort to authentication server which can degrade the performance of the entire network.

The average number of SA is relative to the lifetime of SA. Since the lifetime of SA is decreased for MN_{HM}, number of SA is decreased. On the other hand, MN_{LM} which has increased lifetime results increase in number of SA. However, it helps to improve authentication latency and bandwidth efficiency.

Authentication latency:

The delay caused by authentication not only induces the degradation in network performance but at times could result the loss in connection. Therefore, a roaming authentication should be aimed at decreasing time taken for authentication.

As the threshold time is maintained before expiration of dynamically established SA, it could be reused for authentication. Therefore

$$Tau = \begin{cases} Tsa_{au} & \text{if Tth exists} \\ Tna_{au} & \text{if Tth expires} \end{cases}$$

Tsa_{au} = Time taken for authentication with reuse of SA

Tsa_{au} = Time taken for authentication with establishment of new SA

The time taken for establishing new SA is very time consuming as it has to carry on four way handshake protocol in TLS protocol all over again, so

$$Tsa_{au} < Tnaau$$

As the lifetime of MNLM is increased, Tau = Tsa_{au} and hence it improves authentication latency. However, in case of high mobility nodes, irrespective of lifetime of SA, Tau = Tna_{au} as it has to establish new SA most of the times so authentication latency is independent of threshold time resulting constant authentication latency.

Bandwidth efficiency:

The establishment of dynamic SA is time-consuming and will degrade the bandwidth efficiency due to bandwidth idle for authentication waiting time. The bandwidth efficiency of a visiting MN as proposed in [5] is

$$\eta_{B.W.} = \frac{Bs \times Ts}{Bau \times Tau + Bs \times Ts}$$

Bs = Required bandwidth for the service of MN

Bau = Bandwidth idle during the authentication of MN

For MN_{LM} as SAs can be reused due to its higher lifetime, T_{au} = Ts_{au}. Therefore the bandwidth efficiency is improved for MN_{LM}. However, for MN_{HM} irrespective of T_{th}, T_{au} = Tn_{au}. Therefore the B.W. remains constant.

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 up to certain extent. The risk of being exposed remains higher in foreign network than in home network.

Since the mobile nodes with high mobility are repeatedly visiting new foreign networks the risk rises more in such nodes than in mobile node with low mobility. Therefore decrease in lifetime of SA in high mobility nodes will help to reduce such risks whereas once again the increase in lifetime of SA in low mobility nodes has to be overlooked for improvement in authentication latency and bandwidth efficiency.

Ⅵ. Conclusion

In this paper, we analyzed the incorporation of user mobility with authentication architecture based on dynamic establishment of security association. We propose the varying threshold time for expiration of SA based on user mobility to improve the authentication latency and bandwidth efficiency in low mobility nodes and minimize number of SAs and risk in high mobility nodes with constant authentication latency and bandwidth efficiency.

※ This study was supported by research funds from chosun university, 2007.

References

[1] M. Cappiello, A. Floris, L. Veltri Mobiility amongst heterogeneous Nettworks with AAA Support

[2] S. Glass, S. Jacobs, C. Perkins, Mobile IP Authentication, Authorization, and Accounting Requirements draft-ietf-mobileip-aaa-reqs-00.txt

[3] 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

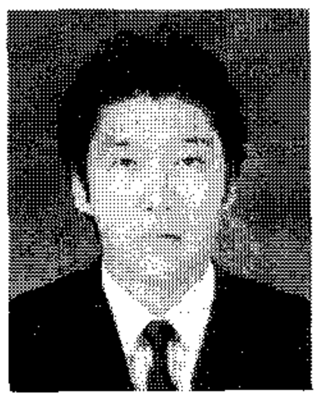
[4] T. Dierks and C. Allen. The TLS Protocol. RFC2246, January 1999

[5] Wei Liang Wenye Wang, A Dynamic Security Association Control Scheme for Efficient Authentication in Wireless Networks

저자소개

Anish Prasad Shrestha

2007년 Tribhuvan University electronics and communication (학사)
2008년 조선대학교 정보통신학과 (석사 입학)
※관심분야 : 무선 인증 프로토콜, 무선 보안



이상덕 (Sang-duk Lee)

1997년 조선대학교 전자공학과 (학사)
1999년 조선대학교 전자공학과 (공학 석사)
2008년 조선대학교 전자공학과 (공학 박사)
※관심분야 : 네트워크 보안, 임베디드

조병록 (Byung-Lok Cho)

1987년 성균관대학교 전자공학과 (학사)
1990년 성균관대학교 대학원 전자공학과 (공학 석사)
1994년 성균관대학교 대학원 전자공학과 (공학 박사)
1987년 1월~1988년 3월 삼성전자(주) 종합연구소
1994년 3월 ~현재 순천대학교 전자공학과 교수
※관심분야 : 디지털 통신이론, ASIC 설계, 무선망 성능분석

한승조 (Seung-jo Han)

1980년 조선대학교 전자공학과 (학사)
1982년 조선대학교 전자공학과 (공학 석사)
1994년 충북대학교 전자계산학과 (공학 박사)
1986년 6월~1987년 3월 뉴올리언즈대학 객원교수
1995년 2월~1996년 1월 택사스대학 객원교수
2000년 12월~2002년 3월 버클리대학 객원교수
1998년 3월~현재 조선대학교 전자정보통신공학부 교수
※관심분야 : 통신보안시스템설계, S/W 불법복제 방지시스템, ASIC 설계