이동 센서 네트워크망에서의 인증 메카니즘 신호의 트래픽 분석

김정태

Analyses of a Signal Traffic for Authentication in Mobile Sensor Network

Jung-Tae Kim

ABSTRACT

In this paper, we analyses of a traffic for authentication signaling in third generation mobile sensor network. In universal mobile telecommunication system, authentication functions are utilized to identify and authentication a mobile station and validate the service request network services. The authenticating parties are the authentication the serving general packet radio service support node access the authentication center to obtain the authentication with the mobile station. In this paper, we propose that the automatic cost-effective solution size of the authentication vector array.

키워드
Security, Sensor Network, Authentication

Ⅰ. Introduction

Universal mobile telecommunication system(UMTS) is a third generation mobile service technology evolved from general packet radio service(GGPRS), which supports multimedia services to mobile users. In this UMTS, the packet data services of an mobile station(MS) are provided by the serving GPRS support node(SGSN) connecting to the UMTS terrestrial radio access network(UTRAN) that covers the MS. Mobility is a function that enables a user to move inside and around networks, and the network providing this function is called networks, and the network providing this function is called the mibility network. The mobility network includes the GSM AND PDC system. The UPT(univeraial personal mobility is also advancing dramatically. The FPLMTS(Future public land mobile telecommunication systems), based on intelligent network technology, are being studied energetically in order to provide personal communication service flexibility and effectively. an SGSN service area is partitioned into several routing areas. When the MS moves from one RA to another, a location update is performed, which informs the SGSN of the MSs current location. Note that a crossing of two RAs within SGSN area requires an intra-SGSN location update, while a crossing of two RAs of different SGSN areas requires an inter-SGSN location update.[1]

* 목원대학교 공과대학 정보전자영상공학부

접수일자 : 2005. 10. 28

Ⅱ. Security Requirements and Threats

Security network functional model and threats is presented. To study security in roaming service provision, it is required to extract the network functional entity and establish a network functional model to clarify security functional allocation. The treats in each functional entity to be studied are as follows.

a. treats on interworking between user and terminal:
b. treats on interworking between terminal and visited network
c. Threats on interworking within network
d. Threats on interworking between network
e. Threats on interworking between operator and database

From the point of authentication key management in roaming service provision, security threats can be categorized as follows:

a. illegal access by a fraudulent functional entity
- challenge/response interactive authentication using secret key cryptosystems
- one way authentication using a password
- one way authentication using synchronized data such as time stamps or counters
- one way authentication using public key cryptosystems

b. Eavesdropping of the signals between entities:
- the original authentication key Kh shared between the user and the home network
- the authentication key Kn used for mutual authentication of the network entities
- the authentication key Kv used for user authentication by visited network

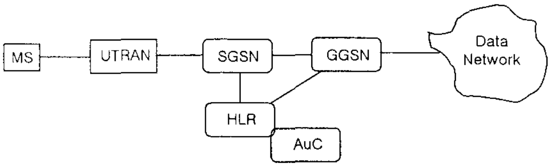
c. Leak of an authentication key shared by entities
- confidentiality of the original authentication key shared by the user and home network to the visited network
- confidentiality of the user authentication key in the key generating network to the other networks

Ⅲ. UMTS authentication procedure

In UMTS, authentication function identifies and authenticates an MS, and validates the service request type to ensure that the user is authorized to use the particular network services. Specially, authentication is performed for every location update, call origination, and call termination. UMTS authentication supports mutual authentication, authentication of the MS by the network and authentication of the network by the MS. The procedure also establishes a new UMTS cipher key(CK) and integrity key(IK) agreement between the SGSN and the MS.

In UMTS authentication, the authenticating parties are HLR/AuC in the home network and the user service identity module(USIM) in the user's MS/ Two major authentication procedures are described in this paper.

- ● Distribution of Authentication Vector: This procedure distributes authentication vector(AVs) from the HLR/AuC to the SGSN to engage in UMTS authentication and key agreement with a particular user.
- ● Authentication and Key Establishment: GSM only provides one way authentication. In UMTS, mutual authentication is achieved by sharing a secret key between the USIM and the HLR/AuC. This procedure follows a challenge/response protocol identical to the GSM subscriber authentication and key establishment protocol combined with a sequence number based one pass protocol for network authentication.



• AuC: Authentication Center
• CGSN: Gateway GPRS Support Node
• HLR: Home Location Register
• MS: Mobile Station
• SGSN: Serving GPRS Support Node
• UTRAN: UMTS Terrestrial Radio Access Network

Fig 1. UMTS architecture

Signaling flows of above two procedure are described in the following steps.

Step 1) When an MS moves into a new SGSN area, the SGSN does not have previously stored authentication information. The SGSN invokesthe distribution of authentication vector procedure by sending the Authentication Data Request message to the HLR/AuC. This message includes the international mobile subscriber identity(IMSI) that uniquely the MS.

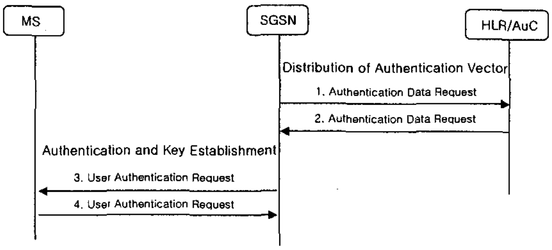

MS
SGSN
HLR/AuC
Distribution of Authentication Vector
1. Authentication Data Request
2. Authentication Data Request
Authentication and Key Establishment
3. User Authentication Request
4. User Authentication Request

Fig 2. UMTS authentication procedure

Step 2) Upon recept of a request from the SGSN, the IMSI is used to identify the HLR/AuC record of the MS, and the HLR/AuC sends an ordered array of K AVs to the SGSN through the Authentication Data Response message. An AV consists of a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK, and an authentication token AUTN. Each AV is good for one authentication nd key agreement between the SGSN and the USIM.

Step 3) When the SGSN initiates an authentication and key agreement, it selects the next unused authentication vector from the ordered AV array and sends the parameters RAND and AUTN(from the selected unauthentication) to the USIM through User Authentication Response message

Step 4) The USIM checks whether AUTN (from the selected authentication vector) can be accepted and, if so, produces a response RES which is sent back to the SGSN through the User Authentication Response message. The SGSN compares the received RES with XRES. If they match, then the authetication and key aagreement exchange is successfully completed. Note that in this mutual authentication procedure, AUTN is used by the USIM to authenticate the network, and RES/XRES is used by the network to authenticate the USIM.

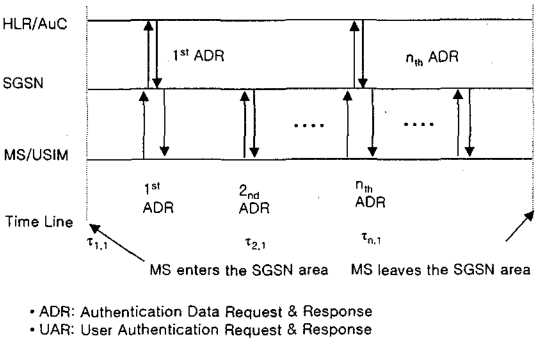


Fig. 3. Timing diagram

Consider the timing diagram in Fig.3. Suppose that an MS enters a new SGSN area at time τ1.1. The MS sends a registration message to the SGSN. Since the SGSN does not have authentication information, the distribution of authentication vector procedure is exxecuted through an ADR, where the number of AVs obtained the AV array from the HLR/AuC is K. After the SGSN has obtained the AV array from the HLR/AuC, mutual authentication is performed between the SGSN and the MS/USIM through a User Authentication Request and Response(UAR) message pair exchange by using the first AV. After τ1.1, the second authentication event(a call request or an inter-SGSN RA update) occurs at time τ1.2. The MS/USIM initiates the second UAR, and the SGSN uses the second AV in the array for mutual authentication. At time τ1.k, the last AV in the array is used for the UAR of the Kth authentication event. After τ1.k, the next authentication event occurs a τ2.1. The SGSN realizes that no AV is available, which issues the second ADR to obtain the next AV array from the HLR/AuC and then performs a UAR. For the next incomming authentication events, ADRs and UARs are executed accordingly as described above.

Ⅳ. Analytical Modeling with Fixed K

Let N be the total number of ADRs performed when the MS resides in an SGSN area. For each ADR, the number of AVs obtained ffrom HLR/AuC is K. Suppose that the aggregate incoming/outgoing call and registration arrivals form a poisson process with rate λ. As we mentioned earlier, for every incoming/outgoing call and registration, a UAR is performed. Let C(K) be the total message transmission cost for ADRs when an MS resides in an SGSN area.[2] Then

$$C(K) = E(N) \times (K + 2\alpha) \qquad (1)$$

Where α represents the cost for an SS7 message overhead normalized by the cost an AV transmission and the processing time for generating the AV through the authentication procedure. In the right-hand side of equation, this overhead is considered for the Request and Response message pair exchanged in an ADR. The total ADR transmission cost for exponential SGSN residence times is expressed as [3]

$$C(K) = \frac{k + 2\alpha}{1 - \left(\frac{\lambda}{\lambda + \nu}\right)^{K}} \qquad (2)$$

Ⅴ. Simulation Result

Figure 4 shows how the expected number E[N] and cost C(K) of ADR are affected by the AV array size K. We say that the AV array are affected by the AV array size K. We say that the AV array size is selected by the fixed-K mechanism if the selected K value is fixed throughtout an MS's lifetime. Our analytic mode can be used to compute E[N] and C(K) for the fixed mechanism. The analytic results are compared with simulation. Fig. 4. plots E[N] against K with the simulation UAR arrival rates λ . The SGSN residence times are assumed to be exponentially distributed with mean 1/μ.

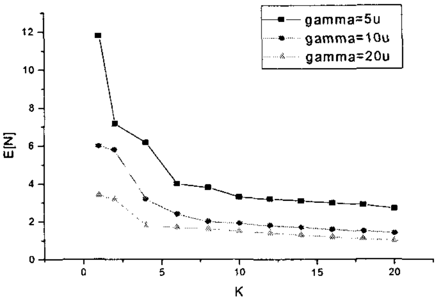


Fig. 4. Effect of the UAR arrival rate

Figure 5. shows the effect of the variance υ for the gamma SGSN residence time distribution. The mean SGSN residence time is 1/μ. and the UAR arrival rate λ =10μ. The figure shows that as υ increases, more short SGSN residence times and more long SGSN residence times are observed.

Ⅵ. Conclusion

In the mobile network, authentication is exercised for every location update and every call event. In UMTS, mutual authentication is performed between the MS and the SGSN. In order to carry out authentication, the SGSN obtains authentication data from the HLR/AuC. Since the cost for accessing AuC is expensive, the SGSN may obtain an array of AVs at a time so that the number of accesses can be reduced. We observed the following results.

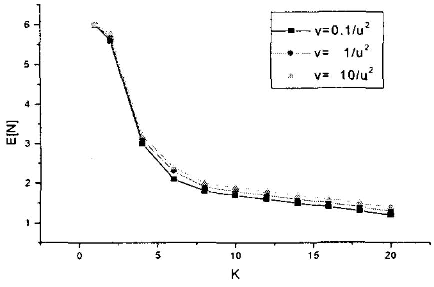


Fig. 5. Effect of the time variance υ for gamma SGSN residence times

- Increasing K will decrease the expected number E[N] of accesses from the SGSN to the HLR/AuC. However, when K is large, increasing K only insignificantly reduces E[N].
- When the variance of the SGSN residence times increase, E[N] increases.
- Let C(K) be the cost for the SGSN to acess the authentication data of HLR/AuC. C[K] is a concavecurve, and there exists an optimal K value that minimizes C[K].
- The optimal K value increases as the authentication event rate λ increases.

REFERENCES

[1] Y.Fang and I.Chlamtac, "Teletraffic analysis and mobility modeling for PCS networks," IEEE Trans. Commun., vol.47, pp.1062-1072, July, 1999

[2] Y.B.Lin, "Wireless and Mobile Network Architectuals". New York,2001.

[3] I.F. Akyildiz, "Mobility management in next generation wireless systems," Proc. IEEE, vol.87, pp.1347-1384, Aug.1999

저자소개

Jung-Tae Kim

Jung-Tae Kim received his B.S. degree in Electronic Engineering from Yeungnam University in 1989 and M.S. and Ph.D. degrees in Electrical and Electronic Engineering from the Yonsei University in 1991 and 1996, respectively. From 1991 to 1996, he joined at ETRI, where he worked as Senior Member of Technical Staff. In 2002, he joined the department of Electronic and Information security Engineering, Mokwon University, Korea, where he is presently a professor. His research interest is in the area of Optical security technology that includes Information security system design, Network security and crypto-processor design.