Performance Evaluation of Public Key Based Mechanisms for Mobile IPv4 Authentication in AAA Environments[*]

Jung-Muk Lim, Hyung-Jin Lim, and Tai-Myoung Chung

Internet Management Technology Laboratory,
Scool of Information and Communication Engineering,
SungKyunKwan University, Korea
{jmlim, hjlim, tmchung}@imtl.skku.ac.kr

Abstract. With the proliferation of mobile terminals, use of the Internet in mobile environments is becoming more common. In order to support mobility in these terminals, Mobile IPv4 was proposed, representing the standard in IPv4 environments. In this environment, authentication should be mandatory, because mobile terminals can utilize Internet services in all foreign domains. Mobile IPv4 provides symmetric key based authentication using the default HMAC-MD5. However, symmetric key based authentication creates a problem, when it comes to key distribution. In order to solve this problem, public key based authentication mechanisms were proposed. In this paper, the performance of each of these mechanisms is evaluated. The results demonstrate that, among these mechanisms, partial certificate based authentication results in superior performance, and certificate based authentication results in the worst performance. This paper creates the possibility of public key based authentication mechanisms being used for future mobile terminal authentication, although current public key based authentication mechanisms result in lower performance than symmetric key based authentication.

1 Introduction

Semiconductor and telecommunications technology has evolved steadily, the size of computers is continuously being reduced, and communications is progressing from wired environments to the wireless environments. These trends represent the foundation of mobile computers and new forms of communication. Therefore, it is natural for mobile terminals to continuously utilize Internet services, while in motion, and at any location. The current Internet network protocol standard, IPv4, does not support mobility for mobile terminals. Thus, Mobile IPv4 as an IPv4 extension must be implemented to support mobility.

[*] This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

I. Chong and K. Kawahara (Eds.): ICOIN 2006, LNCS 3961, pp. 62–71, 2006.

Within a mobile terminal, a user may request Internet services from a foreign domain instead of a home domain of which the user is registered. Therefore, terminal authentication is required, unlike wired networks in which a user is only connected to his/her domain. Authentication is classified into terminal authentication, granted by a service agent and service agent authentication granted by a terminal. The former represents preprocessing for authorization and accounting, and the latter represents processing for preventing attackers from masquerading as service agents.This mechanism is required for mobile terminals to interact with any other domain, because the terminals can request Internet services in any foreign domain. This is Authentication, Authorization, and Accounting (AAA), a framework to manage authentication, authorization, and accounting comprehensively. Consequently, Mobility of mobile terminals requires an AAA infrastructure.

Mobile IPv4 provides authentication, using HMAC-MD5 by default. However, this method suffers from the key distribution problem in which secret keys must be distributed in advance, due to the requirements of symmetric cryptography. Although a key may be distributed between a Mobile Node (MN) and a corresponding Home agent (HA), it is almost impossible for a key to be distributed between Foreign Agents (FAs) and MN, or between FAs and HA. Furthermore, performance is reduced be-tween domains. To solve this key distribution problem, certificated based authentication was proposed [4].

However, public key based mechanisms cannot be applied directly to mobile environments because this application results in noticeably slower operation over symmetric key based mechanisms. In addition, it suffers from the problem that mobile terminals do not have sufficient memory for certificates. To solve this public key based mechanism problem, a partial certificate based authentication mechanism was pro-posed [5]. The public key is used only between a FA and the HA, as both have high computation power. An identity based authentication mechanism was also proposed [6]. This mechanism does not require a certificate based infrastructure.

2 Mobile IPv4 Authentication Mechanisms

In this section, Mobile IPv4 authentication mechanisms are described. These mechanisms consist of default authentication, certificate based authentication, partial certificate based authentication, and identity based authentication.

2.1 Default Authentication

In order to use HMAC-MD5, the Mobile IPv4 default authentication mechanism requires that a Security Association (SA) between a MN and HA must be established in advance [1]. The registration process using default authentication is presented in [Figure 1].

The RRQ consists of M_1 and $< M_1 > K_{MN-HA}$. The M_1 is the RRQ's body including the MN's nonce and HA's previous nonce within the identification field. The $< M_1 > K_{MN-HA}$ is the Message Authentication Code (MAC) of the M_1 using HMAC-MD5 and a previously shared 128 bit secret key. The RRQ is

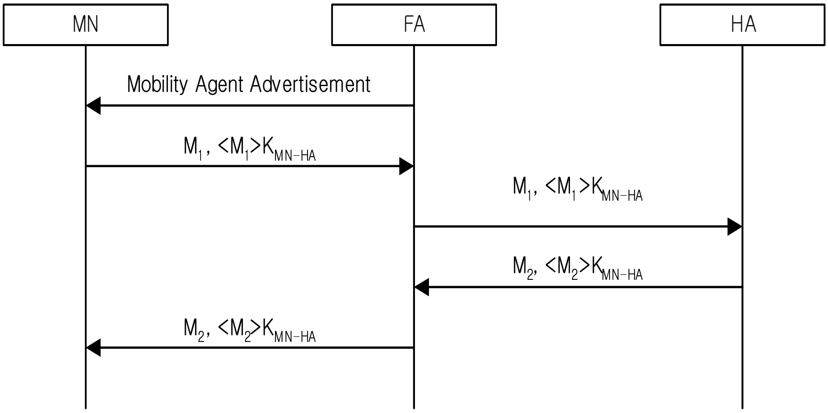


Fig. 1. Registration Process using Default Authentication

forwarded to the HA through the FA. The HA confirms whether its nonce in the RRQ is identical to the nonce previously sent to the MN. If they are not identical each other, the HA returns an error code in the RRP. If they are identical, the HA verifies the MAC. If the MAC is incorrect, the HA transmits an error code in the RRP to the MN, through the FA. If the MAC is correct, the HA updates its binding information and transmits a success code in the RRP to the MN, through the FA. Herein, the authentication between the FA and HA is omitted but authentication be-tween the FA and HA must be achieved if accounting is to be considered.

The RRP consists of M_2 and $< M_2 > K_{MN-HA}$. The M_2 is the RRP's body including the MN's nonce and HA's nonce within the identification field. The MN's nonce was in the RRQ and HA's nonce will be used for the next registration by the MN. The $< M_2 > K_{MN-HA}$ is the MAC of the M2 using HMAC-MD5 and the previously shared 128 bit secret key. Herein, the authentication between the FA and HA is omitted but authentication be-tween the FA and HA must be achieved if accounting is to be considered.

Default authentication assumes that previously shared secret keys exist between MN and HA, between MN and FA, and between FA and HA. It is slightly cumber-some, in that a MN and HA share a secret key between them in advance. Furthermore, it is almost impossible for a MN and FA, or a FA and HA, to share a secret key be-tween them in advance. To solve this problem, another mechanism is required. The requirement that secret key must be distributed in advance, can be solved by distributing keys dynamically. However, this solution is not suitable because of excessive overhead. Alternatively, this problem can be solved using public key cryptography.

2.2 Certificate Based Authentication

In order to solve the problem of the Mobile IPv4 default authentication mechanism being based on symmetric key, a public key based authentication mechanism was proposed [2][4]. This mechanism, which has a different basis to the Mobile IP default authentication mechanism, solves the key distribution problem by transmitting certificates, which include the public key, in the registration process. A registration process, using certificate based authentication, is presented in [Figure 2].

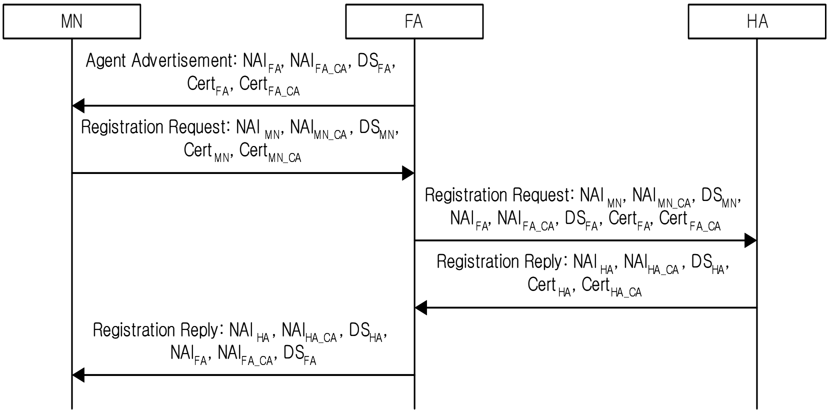

MN
FA
HA
Agent Advertisement: NAI_{FA}, NAI_{FA_CA}, DS_{FA}, $Cert_{FA}$, $Cert_{FA\_CA}$
Registration Request: NAI_{MN}, NAI_{MN_CA}, DS_{MN}, $Cert_{MN}$, $Cert_{MN\_CA}$
Registration Request: NAI_{MN}, NAI_{MN_CA}, DS_{MN}, NAI_{FA}, NAI_{FA_CA}, DS_{FA}, $Cert_{FA}$, $Cert_{FA\_CA}$
Registration Reply: NAI_{HA}, NAI_{HA_CA}, DS_{HA}, $Cert_{HA}$, $Cert_{HA\_CA}$
Registration Reply: NAI_{HA}, NAI_{HA_CA}, DS_{HA}, NAI_{FA}, NAI_{FA_CA}, DS_{FA}

Fig. 2. Registration Process using Certificate based Authentication

The FA transmits an Agent Advertisement message including its NAI, CA's NAI, signature, certificate, and CA's certificate to the MN. The MN authenticates the Agent Advertisement message by verifying the FA's signature using the FA's certificate and the CA's certificate of the FA. The MN transmits a RRQ, including its NAI, CA's NAI, signature, certificate, and CA's certificate to the FA. The FA authenticates the MN by verifying the MN's signa-ture using the MN's certificate and the CA's certificate of the MN.

The FA transmits the RRQ including the MN's NAI, MN's CA's NAI, MN's signature, its NAI, CA's NAI, certificate, and CA's certificate to the HA. The HA authenticates the MN by verifying the MN's signature using the MN's certificate and the CA's certificate of the MN, which are shared in advance. It also authenticates the FA by verifying the FA's signature using the FA's certificate and CA's certificate of the FA, in the RRQ received from the FA. The HA transmits a RRP including its NAI, CA's NAI, signature, certificate, and CA's certificate to the FA. The FA authenticates the HA by verifying the HA's signature using the HA's certificate and the CA's certificate of the HA.

The FA transmits the RRP including HA's NAI, the CA's NAI of the HA, HA's certificate, its NAI, and CA's NAI to the MN. The MN authenticates the HA by verifying the HA's signature using the HA's certificate and the CA's certificate of the HA which are shared in advance. It also authenticates the FA by verifying the FA's signature using the FA's certificate and the CA's certificate of the FA.

In these flows, mutual authentication between the MN and FA, between the MN and HA, and between the FA and HA are achieved. However, public key based authentication requires much more computation than symmetric key based authentication. Thus, it is not suitable to use in devices, which have low computation power such as mobile terminals. Furthermore, it has another problem where a MN must store certificates, despite the limited memory space of the MN.

2.3 Partial Certificate Based Authentication

Instead of protecting the entire registration process, a mechanism was proposed where certificate based authentication is used only in places where the MN does not require processing of the public key algorithm and does not require storage of the certificate [5]. The registration process using partial certificate based authentication is presented in [Figure 3].

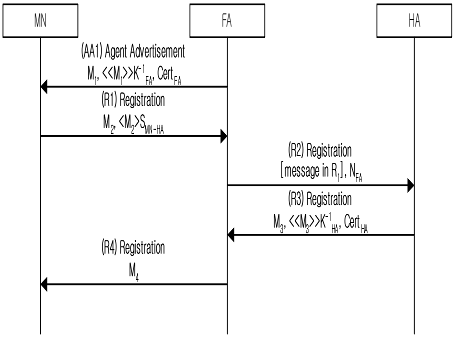

MN
FA
HA
(AA1) Agent Advertisement
$M_1, <<M_1>>K^{-1}_{FA}, Cert_{FA}$
(R1) Registration
$M_2, <M_2>S_{MN-HA}$
(R2) Registration
$[message in R_1], N_{FA}$
(R3) Registration
$M_3, <<M_3>>K^{-1}_{HA}, Cert_{HA}$
(R4) Registration
M_4

Fig. 3. Registration Process using Partial Certificate based Authentication

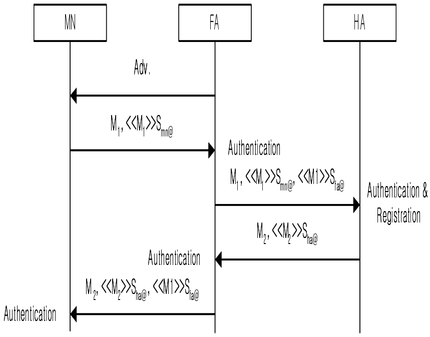


Fig. 4. Registration Process using Identity based Authentication

The FA transmits an Agent Advertisement including M_1 and signature of the M_1, its certificate to the MN. The M_1 includes its id and the MN's CoA. Without any authentication process to the FA, the MN transmits a RRQ including the FA's id, HA's id, its home address, its CoA, previous HA's nonce, its nonce, M_2, and the MAC of the M_2 using the secret key shared with the HA to the FA. M_2 represents the Agent Advertisement message received from the FA. The FA appends its nonce to the RRQ received from the MN and transmits it to the HA. The HA prevents a malicious person from deploying a replay attack, by confirming its previous nonce. It authenticates the FA by verifying the FA's signature using the FA's certificate, and authenticates the MN by verifying the MN's MAC, using the previously shared secret key. Thus, the FA and MN are authenticated by the HA.

The HA transmits a RRP, which includes M_3, signature of the M_3, and its certificate to the FA. The M_3 includes M_4, MAC of the M_4 using the secret key, which is shared with the MN, and FA's nonce. The M_4 includes the FA's id, its id, the MN's home address, its next nonce, and the MN's nonce. The FA prevents malicious individuals from deploying a replay attack by confirming its nonce in the RRP received from the HA. It authenticates the HA by verifying the HA's signature using the HA's certificate and authenticates the MN by confirming the registration result in the RRP received from the HA. The FA transmits the M_4 to the MN. The MN authenticates the HA by verifying the HA's MAC using the secret key which is shared with the HA, and authenticates the FA by confirming the registration result in the RRP received from the FA. Thus, the MN and HA are authenticated by the FA, and the FA and HA are authenticated by the MN.

This mechanism requires that a MN and HA must have a previously shared secret key and a public key infrastructure must exist for the FA and HA.

2.4 Identity Based Authentication

To solve the problem of storing certificates by the MN, and reducing network over-head by transmitting certificates, identity based authentication was proposed [3][6]. The registration process using identity based authentication is presented in [Figure 4].

The MN receives an Agent Advertisement message from the FA and then transmits M1, which is the RRQ's body, and its signature of the M_1 to the FA. The FA authenticates the MN by verifying the MN's signature using the MN's identity, appends its signature to the RRQ, and then transmits it. The HA authenticates the MN by verify-ing the MN's signature using the MN's identity and authenticates the FA by verifying the FA's signature using the FA's identity.

The HA transmits M_2, which is RRP's body, and its signature of the M_2 to the FA. The FA authenticates the HA by verifying the HA's signature using the HA's identity, appends its signature to the RRP, and then transmits it. The MN authenticates the HA by verifying the HA's signature using the HA's identity and authenticates the FA by verifying the FA's signature using the FA's identity.

3 Performance Evaluation

In this section, the previously described mechanisms are modeled, and their performance is evaluated.

3.1 Modeling

To evaluate each authentication mechanism, this model is as follows. There is only one AAA server in one domain. A handoff is classified into two types, a handoff in the same domain, and a handoff between different domains. The former is called intra-handoff, and the latter is called inter-handoff. Authentication during the intra-handoff process occurs in a local AAA server and authentication during the inter-handoff process occurs in the home AAA server [7]. The network topology for modeling is presented in [Figure 5].

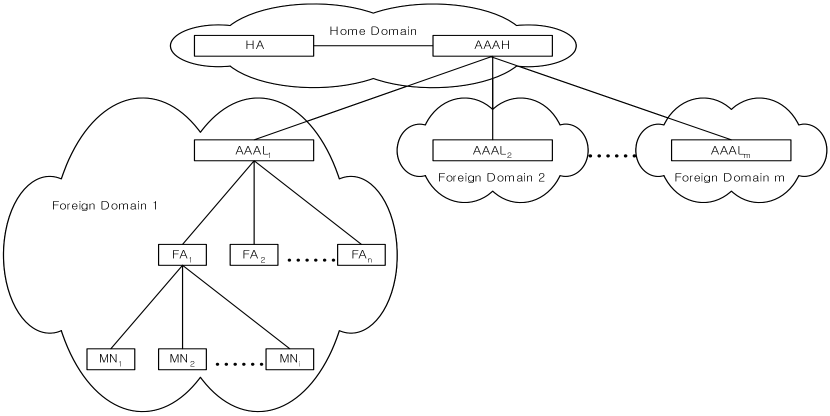


Fig. 5. Network Topology for Modeling

If ND_i^{RRQ} represents the network delay in each link, when each node transmits RRQ and ND_i^{RRP} represents network delay in each link when each node transmits RRP, total network delay ND is expressed using the following equation:

$$ND = \sum ND_i^{RRQ} + \sum ND_i^{RRP} \tag{1}$$

Herein, network delay of the same link is calculated separately in each direction because the size of RRQ and the size of RRP can be different from each other and the size of the packet affects network delay.

If PD_i^{RRQ} represents the general processing delay occurring by routing and register-ing the RRQ in each node, and PD_i^{RRP} is a general processing delay, occurring through routing and registering the RRP in each node, total routing and registration processing delay PD is expressed using the following equation:

$$PD = \sum PD_i^{RRQ} + \sum PD_i^{RRP} \tag{2}$$

If AD_i^{RRQ} is the RRQ authentication processing delay in each node and AD_i^{RRP} represents the authentication processing delay of RRP in each node, total authentication processing delay AD is expressed using the following equation:

$$AD = \sum AD_i^{RRQ} + \sum AD_i^{RRP} \tag{3}$$

During inter-handoff, the total delay D_{INTER} is expressed using the following equation:

$$D_{INTER} = ND + PD + AD \tag{4}$$

Similarly, during intra-handoff, total delay D_{INTER} is expressed by the following equation:

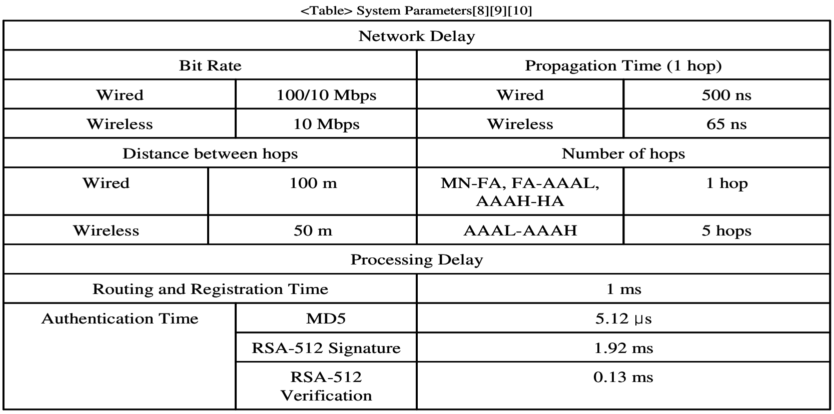
$$D_{INTER} = L_{ND} + L_{PD} + L_{AD} \tag{5}$$

If N networks exist, and the average number of networks in one domain is k, M which represents the average amount of MN movement during inter-handoff, is ex-pressed using the following equation:

$$D_{INTER} = D_{INTER} * M + D_{INTER} \tag{6}$$

3.2 Results

The cumulative handoff delay is calculated using the previously derived equations and system parameters in Table 1.



<Table> System Parameters[8][9][10]

Network Delay			
Bit Rate		Propagation Time (1 hop)	
Wired	100/10 Mbps	Wired	500 ns
Wireless	10 Mbps	Wireless	65 ns
Distance between hops		Number of hops	
Wired	100 m	MN-FA, FA-AAAL, AAAH-HA	1 hop
Wireless	50 m	AAAL-AAAH	5 hops
Processing Delay			
Routing and Registration Time		1 ms	
Authentication Time	MD5	5.12 μs	
	RSA-512 Signature	1.92 ms	
	RSA-512 Verification	0.13 ms	

Fig. 6. System parameter [8][9][10]

The wireless environment parameters are based on 11Mbps, semi-open office using 802.11b wireless LAN standard. In wired environments, the propagation speed is between $2.0{*}10^8$ and $3.0{*}10^8$, and in this paper, $2.0{*}10^8$ is used. Network delay includes transmission delay and propagation delay. Based on bit rates, transmission delay of wired and wireless is 10/100ns, and 100ns respectively. In wired environments, the distance between hops is assumed to be 100m while in wireless environments, the distance between hops is assumed to be 50m. In the same domain, the number of hops between nodes is assumed to be 1 hop while in different domains, the number of hops between nodes is assumed to be 5 hops.

In 100Mbps wired environments, the relationship between the number of handoffs and cumulative handoff delay is presented in [Figure 7, Left]. The performance rank is ordered as default authentication, partial certificate based authentication, identity based authentication, and certificate based authentication. Partial certificate based authentication reduces authentication processing delay and network delay to transmit certificates using partial symmetric key based authentication. Identity based authentication eliminates network delay when transmitting certificates, by eliminating the requirement for a certificate. The reason partial certificate based authentication is superior over identity based

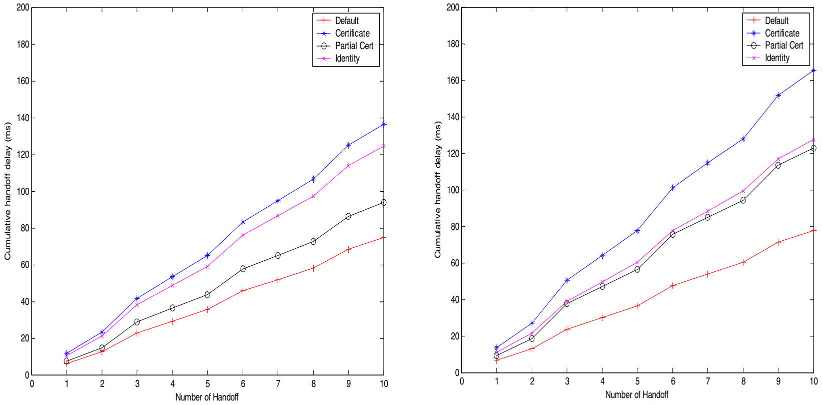


Fig. 7. Relationship between the Number of Handoffs and Cumulative Handoff Delay (Left: 100Mbps Wired Environments, Right: 10Mbps Wired Environments)

authentication, is that the network delay used to send certificates is mitigated due to the high speed wired environments.

In 10Mbps wired environments, the relationship between the number of handoffs and cumulative handoff delay is presented in [Figure 7, Right]. Similarly, performance rank is ordered as default authentication, partial certificate based authentication, identity based authentication, and certificate based authentication. However, performance difference between partial certificate based authentication and identity based authentication is smaller than that in 100Mbps wired environments, because network delay when sending certificates increases. If the bit rate of a wired environment is much less than 10Mbps, identity based authentication is expected to provide superior performance over partial certificate based authentication.

4 Conclusion

Symmetric key based authentication, using HMAC-MD5 provided in Mobile IPv4 standard is fast but suffers from the key distribution problem. Key distribution between a MN and HA is slightly cumbersome, but possible, however, key distribution between a MN and FA or between a HA and FA is impossible because a MN can move to any network in any domain. To solve this problem, public key based authentication mechanisms were proposed. The previously proposed pure certificate based authentication is not suitable for a mobile terminal suffering from low network band-width and low computation power, because large network overhead is created when sending certificates and a large processing overhead is required when processing the public key algorithm. To solve these problems, partial certificate based authentication and identity based authentication are proposed. However, they still create more over-head over symmetric key based authentication. This paper evaluates these public key based authentication mechanisms, presenting the current direction of public key based authentication mechanisms, providing an indication of future mechanisms.

In the future, advantages from the previously proposed public key based authentica-tion mechanisms will be extracted, and disadvantages will be eliminated, creating a new authentication mechanism.

References

1. C. Perkins, 'IP Mobility Support for IPv4', RFC 3344, August 2002.
2. U.S. DEPARTMENT OF COMMERCE / National Institute of Standards and Technology, 'ENTITY AUTHENTICATION USING PUBLIC KEY CRYPTOCRAPHY', February 1997.
3. A. Shamir, 'IDENTITY-BASED CRYPTOSYSTEMS AND SIGNATURE SCHEMES', in Proc. of Crypto '84, LNCS, vol. 196, pp. 47-53, Springer-Verlag 1985.
4. S. Jacobs, S. Belgard, 'Mobile IP Public Key Based Authentication', INTERNET DRAFT, draft-jacobs-mobileip-pki-auth-03.txt, July 2001.
5. Sufatrio, Kwok Yan Lam, 'Registration Protocol: A Security Attack and New Secure Mini-mal Public-Key Based Authentication', ISPAN'99, June 1999.
6. Byung-Gil Lee, Doo-Ho Choi, Hyun-Gon Kim, Seung-Won Sohn, Kil-Houm Park, 'Mobile IP and WLAN with AAA Authentication Protocol using Identity-based Cryptography', ICT 2004, February 2003.
7. A. Hess, G. Schaefer, 'Performance Evaluation of AAA / Mobile IP Authentication', Tech-nical Report TKN-01-012, Telecommunication Networks Group, Technische Universit?t Berlin, August 2001.
8. Hoseong Jeon, Hyunseung Choo, Jai-Ho Oh, 'Identification Key Based AAA Mechanism in Mobile IP Networks', Springer-Verlag Lecture Notes in Computer Science, vol. 3043, pp. 765-775, May 2004.
9. C. L. Beaver, D. R. Gallup, W. D. NeuMann, M. D. Torgerson, 'Key Management for SCADA', SAND2001-3252, March 2002.
10. Proxim Corporation, 'ORiNOCO AP-2500 Access Point User Guide', Sofeware v2, March 2004.