Wireless PKI for Reducing Certificate Acquisition Time According to Authentication Path

Seung-Kwon Choi, Yong-Hwan Cho*
School of Electrical & Computer Engineering, Chungbuk National University
Cheongju, Korea

Seung-Soo Shin
Dept. of Information Security, Dongmyong University
Pusan, Korea

Yoon-Sik Jang
SK Telecom, Seoul, Korea

ABSTRACT

In this paper, we proposed an advanced authentication structure for reducing the certificate acquisition time which is one of the factors that should be improved in a conventional wireless PKI. A conventional key exchange method simply performs the key exchange setup step based on discrete algebraic subjects. But the mutual-authentication procedure of wireless PKI for reducing authentication time uses an elliptical curve for a key exchange setup step.
We simulated and compared the authentication structure proposed by Sufatrio, K. Lam[4] and proposed authentication structure in terms of the authentication time. Simulation results show that the proposed method reduces the authentication time compared to the conventional wireless PKI authentication method.

Keywords *: Wireless PKI, CA, SRP, OCSP, Certificate Acquisition Time*

1. INTRODUCTION

(A PKI(Public Key Infrastructure) based on authentication, which is adopting public key encryption method to acquire reliability and security of information transportation, is commonly used in many fields. In the PKI, for identifying the users' personal information and public key, all users must have a certification issued from CA(Certificate Authority) which is the disinterested party. However, due to frequent certification issuance, complicated problems may occur such as traffic increase, cost and time wastage, key management and so on. Therefore, in the communication among users, the disinterested third party is needed to maintain a secure and independent user certification and a key distribution without contact to the third party[1]. Conventional wireless PKI protocols still have technical and implemental problems such as routing optimization, Ingress filtering, wireless management of wireless nodes, and data transfer method. But, most of all, one of the problems that should be solved first is the mutual-authentication problem. The mutual-authentication might be solved in all communication systems. Surely, in wireless PKI, for providing electronic commerce, data communication, e-mail and so on, the mutual- authentication problem must be solved. Especially, much researches, that is strongly related with the co-existence of wireless PKI and various authentication structures used on the Internet, have been continuously done. Besides, for increasing a security of wireless PKI, the mutual- authentication for data protection and strict authentication procedure is needed. In wireless PKI, an authentication protocol suitable for the wireless environment should be constructed since it uses wireless environment for supporting the mobility of hosts. Chapter II shows the disadvantage of the current wireless PKI authentication based on private key which cannot be expanded. Also, it cannot provide non-repudiation, one of the important parts of e-commerce. Therefore, this chapter shows the authentication method based on public key proposed by Sufatrio and K. Lam[4] to solve this problem. Chapter III describes proposed wireless PKI authentication structure, and in chapter IV contains the simulation results between conventional algorithm and proposed algorithm related on certificate acquisition time according to traffic density and authentication path. Chapter V explains the conclusion and further studies.

2. RELATED WORKS

Current wireless PKI authentication based on private key has the main disadvantage that it cannot be expanded. Also, it cannot provide non-repudiation, one of the important parts of e-commerce. Therefore, to solve this problem, Sufatrio and K. Lam[4] proposed the authentication method based on public key. Table I shows the basic terminology to describe the

**Corresponding author. E-mail: yhcho@chungbuk.ac.kr*
Manuscript received Feb 3, 2005 ; accepted Mar 4, 2005

authentication structure based on public key of Sufatrio, K. Lam.

Table 1. Terminology

CA	Authentication Authority
K_{agent}, K_{server}, K_{CA}	Public key of CA, Agent, Server
K^{-1}_{agent}, K^{-1}_{server}, K^{-1}_{CA}	Private key of CA, Agent, Serve
$Cert_{agent}$, $Cert_{server}$	Certificate of Agent and Server
<<M>> K^{-1}_{A}	Digital Signature of Message M using private key of A
N_{agent}	nonce issued by Agent
N_{server}, N_{agent}, N_{MN}	nonce of Server, Agent and MN
MN_{HM}	Home address of MN
MN_{COA}	Care-Of-Address of MN
$Server_{ID}$, $Agent_{ID}$	IP address of Server and Agent
$S_{MN\text{-}server}$	Private key of MN and Server
Advertisement	Bit pattern of ad. message

Fig. 1 shows the conventional public key based algorithm.

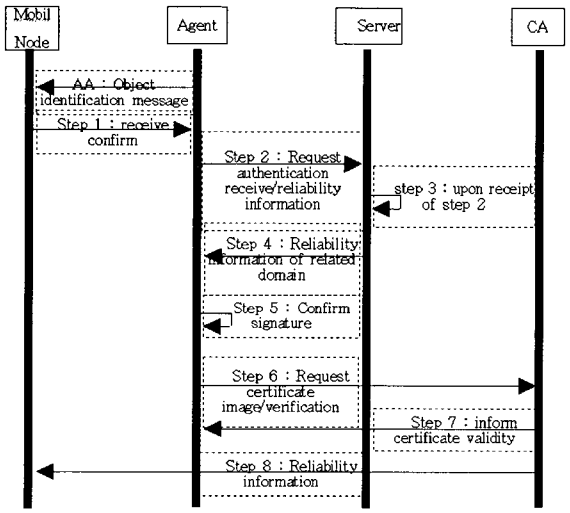

Fig. 1. Flow chart of conventional algorithm

3. WIRELESS PKI DESIGN FOR REDUCING AUTHENTICATION TIME

In this chapter, we propose a wireless PKI based authentication structure for reducing the authentication time to implement mutual- authentication. The proposed wireless PKI authentication structure consisted of a CA, servers, agents, and mobile nodes. The agents perform as a CA after acquiring the needed information from a CA. Especially, in wireless PKI authentication structure for reducing authentication time, the mutual-authentication performs on a SRP(Secure Remote Password) protocol[2]. The SRP protocol is based on the Diffie-Hellman key exchange method. It is constructed by discrete algebraic subjects in a key exchange setup step between server and agent, and the mutual-authentication between server and agent is constructed by hash function.

In a conventional key exchange method, the key exchange setup step performs on discrete algebraic subjects. But in mutual-authentication procedure of wireless PKI for reducing authentication time, an elliptical curve for key exchange setup step is used. The mutual- authentication consists of a setup step and an execution step.

3.1 Certificate request method

We assume that the relationship between server and CA in a sub-network is always reliable. A request procedure for certificate of mobile node is as follows.

MN ⇒ Agent ⇒ Server ⇒ CA

An issuance procedure of certificate of CA is as follows.

CA ⇒ Server ⇒ Agent ⇒ MN

If CA performs a response, the certificate information among the information of mobile nodes which is stored in CA is transferred to the mobile node via servers and agents, At this time, agents and servers keep a certificate issued by the higher organization. If a mobile node re-requests the certificate which is under the validity, the certificate will not be transferred to CA and the agent issues a copy of certificate. A server or an agent can performs as a CA during the valid period of an issued certificate.

3.2 Mutual-authentication procedure

The Mutual authentication procedure performs on SRP[2] Protocol. The SRP protocol is based on the Diffie-Hellman key exchange method. It is constructed by the discrete algebraic subjects in key exchange setup step between server and agent, and mutual-authentication between a server and an agent is constructed by a hash function. The conventional key exchange method performs a key exchange setup step based on discrete algebraic subjects. But our mutual- authentication procedure of wireless PKI for reducing certificate acquisition time uses an elliptical curve for key exchange setup step. The mutual-authentication consists of a setup step and an execution step as Fig. 2 and Fig. 3.

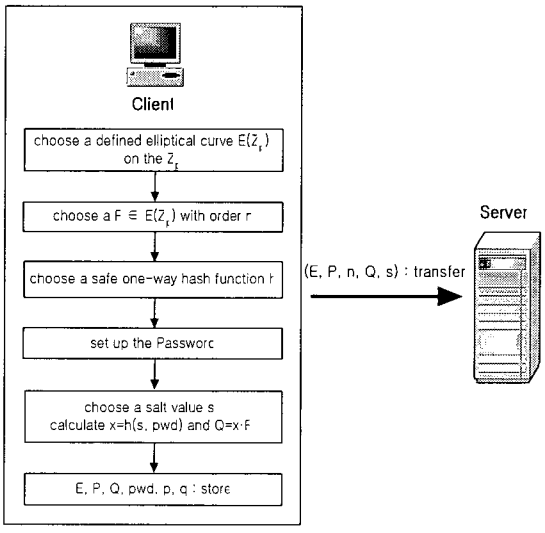

Fig. 2. Setup step between client and server

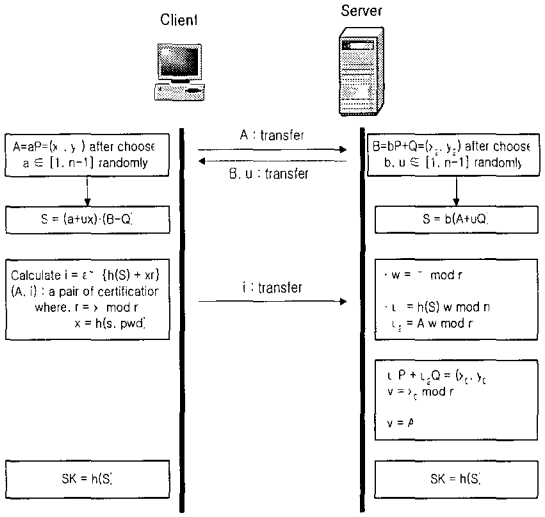

Fig. 3. Execution step between client and server

3.3 Process of certificate renewal using OCSP

OCSP(Online Certificate Status Protocol), a method of verifying certificate status, which was proposed to solve the problem that CRL-based certificate verification method cannot solve as a realtime verification of certificate status, was announced by document IETF RFC2560 in July 1999[3].

In the OCSP-based certificate verification method, an OCSP client verifies the current state of a certificate without requesting CRL, so the realtime certificate status verification is possible but it causes overload on the network by generating heavy traffics and the length of time taken for verification is different depending on the network condition.

In the OCSP-based certificate status verification method, a client requests a certificate verification from the URL where the certificate is stored and receives the result. A certificate received by the client is sent to the OCSP server to determine if the certificate is accurate or not. Then the OCSP server performs the verification of the corresponding certificate and informs the client of the accuracy of the certificate.

In the process of certificate renewal, after a mobile node issues a certificate from CA, it requests an electronic signature from the OCSP client in a predefined form. Then the OCSP client requests the OCSP server to look up the certificate status information and to perform an electronic signature, and the OCSP server delivers the result of the performance to the OCSP client. In this way, the realtime certificate verification is performed.

4. EXPERIMENT ON THE PROPOSED WIRELESS PKI AND THE RESULTS

4.1 Certificate Acquisition according to Authentication Path

In order to evaluate the performance of the mobile PKI structure, which was proposed to reduce the verification time, this study carried out an experiment and compared the proposed structure with the existing Sufatrio, K. Lam[4] verification structure. For the experiment on certificate acquisition time according to the length of the Authentication path, parameters were defined as in Table 2.

Table 2. Definition of used parameters

Symbol	Definition	Value
BW_w	Bandwidth of wired link	1Gbps
BW_{wl}	Bandwidth of wireless link	1Mbps
L_w	Delay of wired link	0.5ms
L_{wl}	Delay of wireless link	7ms
S_{data}	Max. size of data packet	1024byte
S_{reg}	Size of registration request packet	50byte
T_{acq}	Time for acquiring wireless channel for MN	20ms
T_{Int}	Packet transfer time between nodes on the Internet	3ms
T_{prot}	Registration packet processing time of protocol	3ms
T_{reg}	Registration generation time of current agent	5ms
T_{tun}	Packet tunneling time of protocol	7ms
T_{wait}	Average packet authentication time during hand-over	400ms

Packet transmission time between two nodes on the Internet is assumed to be uniformly $3ms$ in case the server is placed on the next node.

In the experiment environment as shown in Fig. 4, $P(X_0)$, $P(X_1)$ and $P(X_2)$ indicate respectively the probability that the mobile node is located in the agent, the probability that the mobile node moves from the agent to another agent, and the probability that the mobile node moves from the server to another server.

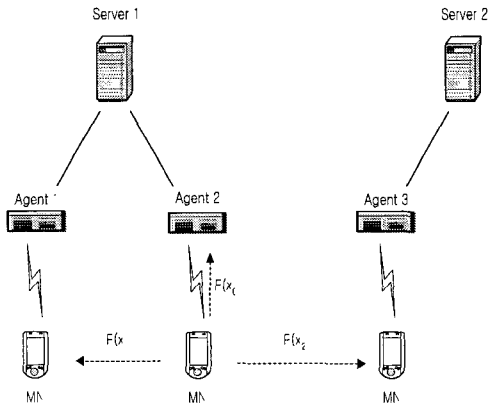

Fig. 4. Movement of mobile node

In the X509-based verification system which has a hierarchical certificate verification structure, if the certification

path is very long, the delay of certification path verification has a very important meaning.

In fig. 5, T_1 shows the time for an agent to wait for acquiring a certificate through a mobile channel.

The total length of time consumed to acquire a certificate is the sum of the time consumed in the mobile section including the processing time inside the mobile node and the time consumed the time in the wired section on upper layers including the gent. The in the mobile section is composed of the time for mobile channel acquisition by the mobile node (T_{acq}) the time for the

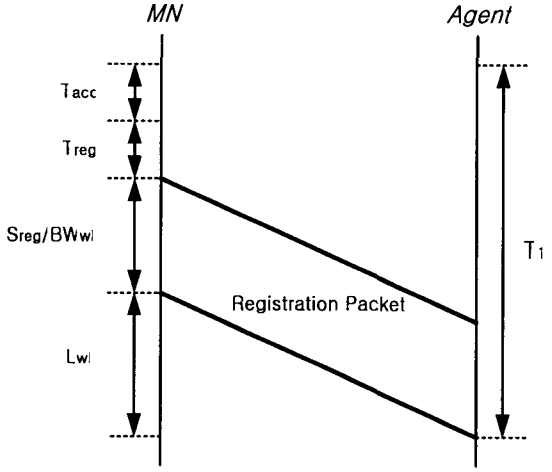

Fig. 5. Waiting time for certificate acquisition

registration packet generation by the mobile node (T_{reg}), the time for transmitting the registration time (S_{reg}/B_{wl}) and the delay in mobile link (L_{wl}).

Based on these elements, let the time for an agent to wait for acquiring a certificate through a mobile channel be T_1, which can then be expressed as follows.

$$T_1 = T_{acq} + (S_{reg}/BW_{wl}) + L_{wl} + T_{reg} \quad (3\text{-}1)$$

Waiting time for packet transmission in the mobile section is as follows.

$$T_2 = (S_{data}/BW_w) + L_{wl} \quad (3\text{-}2)$$

Waiting time for packet processing in order to acquire a certificate between agents interconnected through a wire is as follows.

$$T_3 = ((S_{reg}/BW_w) + L_w) \times number\ of\ nodes + T_{prot} \quad (3\text{-}3)$$

Packet transmission time between agents interconnected through a wire is as follows (time for tunneling).

$$T_4 = ((S_{data}/BW_w) + L_w) \times number\ of\ nodes + T_{tun} \quad (3\text{-}4)$$

where, the time for ACK of the packet to acquire a certificate is not considered. Certificate acquisition time is as follows. T_{old} is the certificate acquisition time under the existing structure and T_{new} is the certificate acquisition time under the proposed structure.

$$T_{old} = (P(X_0)\times(T_1 + T_3 m + 2D)) + (P(X_1)\times(T_1 + T_3 l + 4D)) + (P(X_2)\times(T_1 + 2\times T_3 m + 4D + k\times D\times T_{Int})) \quad (3\text{-}5)$$

$$T_{new} = (P(X_0)\times(T_1 + T_3 s + D)) + (P X_1)\times(T_1 + T_3 m + 2D)) + (P(X_2)\times(T_1 + T_3 m + 2D + k\times D\times T_{Int})) \quad (3\text{-}6)$$

where, $0 < P(X_i) \leq 1$, $i = 0, 1, 2$ and $\sum_{i=0}^{2} P(X_i) = 1$. In addition, $P(X_0) \geq P(X_1) \geq P(X_2)$ and $0.3 \leq P(X_0) \leq 1.0$. $P(X_0)$, $P(X_1)$ and $P(X_2)$ indicate respectively the probability that the mobile node is located in the agent, the probability that the mobile node moves from the agent to another agent, and the probability that the mobile node moves from the server to another server. D means the average waiting time for a certification on hand-over in each node. k is the number of nodes between sub-networks, and its value is between $1 \leq k \leq 10$.

Fig. 6 shows the result of comparing the certificate acquisition time between the existing structure and the proposed structure depending on the number of nodes, assuming that the probability that the mobile node is located in Agent 2 is $P(X_0)$=0.5, the probability that the mobile node is located in Agent 1 is $P(X_1)$=0.3 and the probability that the mobile node is located in another server is $P(X_2)$=0.2.

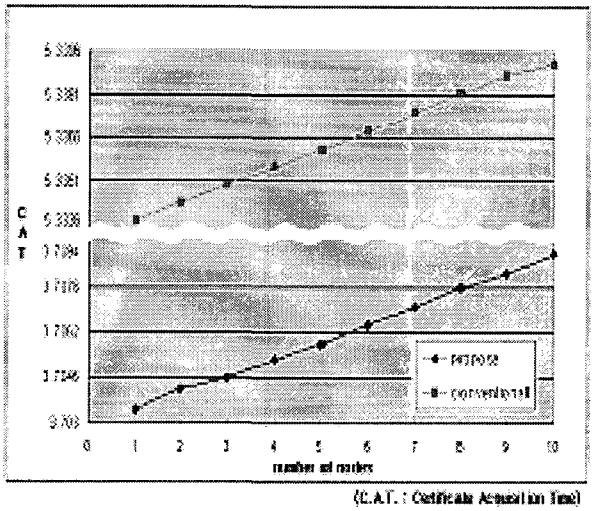

Fig. 6. Certificate acquisition time

Fig. 7 shows the result of comparing certificate acquisition time according to the number of nodes between the existing structure and the proposed structure when the probability that the mobile node is located in Agent 2 is $P(X_0)$=0.8, the probability that the mobile node is located in Agent 1 is $P(X_1)$=0.1 and the probability that the mobile node is located in another server is $P(X_2)$=0.1.

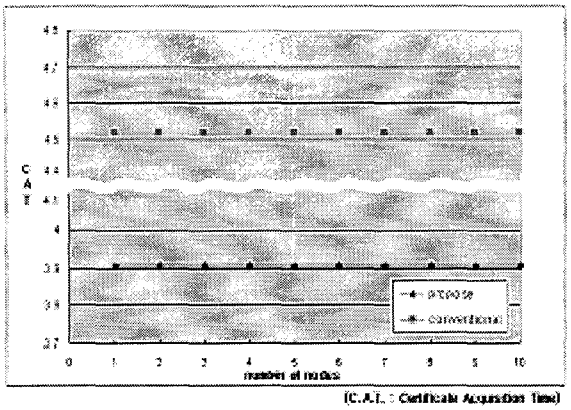

Fig. 7. Certificate acquisition time

Fig. 8 shows the result of comparing certificate acquisition time according to the number of nodes between the existing structure and the proposed structure when the probability that the mobile node is located in Agent 2 is $P(X_0)$=1.0, the probability that the mobile node is located in Agent 1 is $P(X_1)$=0.0 and the probability that the mobile node is located in another server is $P(X_2)$=0.0.

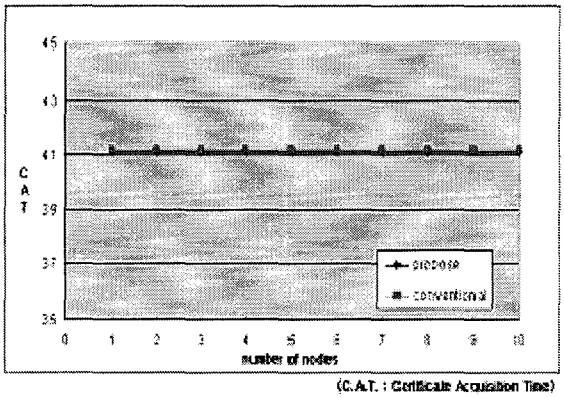

Fig. 8. Certificate acquisition time

4.2. Certificate Acquisition according to Traffic Density

For simulation, TAIL method that is used in [5] was used for performance analysis of certificate acquisition according to traffic density.

Besides, buffer management method for acquiring certificate acquisition time according to traffic density is assumed FIFO(First-In-First-Out).

The notations and definitions for analyzing are as follows.

- λ : Packet arrival rate of queue(Poisson distribution)
- μ : Service rate of output packet (Exponential distribution)
- traffic density ρ to the system

$$\rho = \lambda / \mu$$

In the mobile environment using (PKI), CLR is increased according to the increment of mobile node users, and that means increment of certificate acquisition time. Therefore, CRL retrieval in certificate process at handover of MN consumed much time, this cannot provide the effective mobile service. However, the CRL retrieval processing time in certificate process of MN is the key for providing effective service.

Fig. 9 shows the certificate acquisition time according to the traffic density ρ of conventional algorithm and proposed algorithm at buffer size=10.

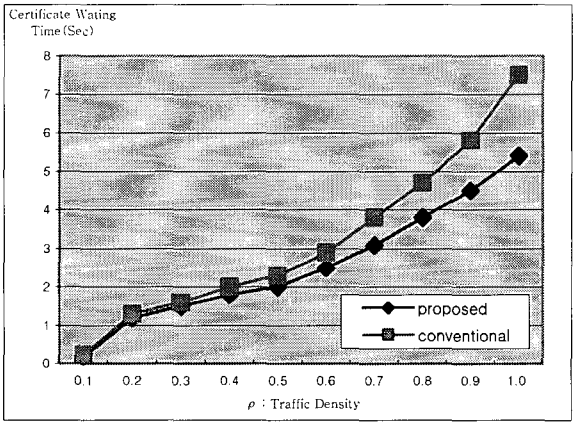

Fig. 9. Certificate wating time according to the traffic density ρ

From the graph of the conventional algorithm in Fig. 9, certificate acquisition time is increased according to the increment of traffic density. In contrast to this, the case that using the proposed method, certificate acquisition time differs from conventional algorithm in the intervals of traffic density = 0.5 or higher.

5. CONCLUSION

In order to evaluate the performance of the wireless PKI certification structure which we proposed in this study, we simulated the proposed structure and the existing Sufatrio, K. Lam certification structure and compared both structures in terms of the certificate acquisition time depending on the length of certification path. The result of the simulation showed that the proposed wireless PKI structure is superior to the existing certification structure in the certificate acquisition time. For the efficient mobile Internet service diminishing the time for a mobile node to look up the certificate which is used in the wireless PKI certification structure, it is necessary in the future to research the certification structure supporting a wireless hand-over.

* This research was sponsored by IITA

REFERENCES

[1] R. Anderson and T. Lomas, "Fortifying Key negotiation schemes with poorly chosen passwords," **Electronics Letters**, 1994, Vol. 30, No. 13.

[2] Thomas Wu, "The Secure Remote Password Protocol", Internet Society Symp., **Network and Distributed Systems Security Symposium**, pp. 97-111, 1998,

[3] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, Internet X.509 Public Key Infrastructure On-line Certificate Status Protocol-OCSP," **RFC2560**, 1999.

[4] Sufatrio, K. Lam, "Mobile IP Registration Protocol : A Security Attack and New Secure Minimal Public-Key Based Authentication," **I-SPAN'99**, June 1999.
[5] S. Bellovin and M. Merritt, Augmented Encrypted Key Exchange", in **Proceedings of the First ACM Conference on Computer and Communication Security**, pp. 244-250, 1993.
[6] 은유진, "X.509 인증서 및 인증서 폐지 목록 프로파일 분석", 전자서명인증관리센터, 1996. 6.
[7] 고병수, 장재혁, 최용락, "디지털 콘텐츠 유통 및 보호를 위한 인증 시스템 설계 및 구현", OA 학회, 제 8 권 3 호, 2003.

Seung-Kwon Choi received the BS, MS, and Ph.D degrees in computer engineering from Chungbuk national university, Cheongju, Korea in 1995, 1997 and 2001, respectively. His research interests include multimedia contents and multimedia communications. Currently, he is in a faculty position in the Chungbuk national university, Korea, sponsored by IT NURI.

Seung-Soo Shin received the BS and MS degrees in mathematics from Chungbuk national university, Cheongju, Korea, and the Ph.D in mathematics and computer engineering from Chungbuk national university, Cheongju, Korea in 2001 and 2004, respectively. He is now in a faculty position in the Dongmyong University, Korea

Yoon-Sik Jang received the BS and MS degrees in electronical engineering from Kwangwoon university, Seoul, Korea. He is currently the director of the SK Telecom, Korea.

Yong-Hwan Cho received the BS, MS and Ph.D degrees in mathematics and statistics from Korea university, Seoul, Korea, respectively, He is currently the president of the Korea Contents Association. He is a professor of the Chungbuk national university, Korea, also.