International Journal of Security and Its Applications
Vol.8, No.4 (2014), pp.123-138
http://dx.doi.org/10.14257/ijsia.2014.8.4.12

End-to-End Authentication Protocols for Personal/Portable Devices over Cognitive Radio Networks

Hyunsung Kim

Dept. of Cyber Security, Kyungil University
Kyungsan, Kyungbuk 712-701, Korea
kim@kiu.ac.kr

Abstract

Recent Federal Communications Commission rules promise a whole new set of possible applications, which allow unlicensed use on a secondary basis of the Television White Spaces (TVWS), called as cognitive radio technology. ECMA-International launched the first step towards realizing these applications by creating and adopting industry standards. This paper reviews the first industrial standards for personal/portable devices in the TVWS from ECMA-International focused on the security aspects. After that, we point out the lack of security facilities in the standard, which does support the link-to-link security but not for the end-to-end security, and then propose two location-based authentication protocols to cope up with the deficiencies over cognitive radio networks. We use location information as thesecurecredentialfor the authentications. The protocols can be support privacy issues of consumer premise equipments and integrated into the extensible authentication protocol.

Keywords: *Cognitive Radio Network, Location-based Authentication, Extensible Authentication Protocol*

1. Introduction

Withthe rapid growth of computer networks such as Internet, Wi-Fi, and TV broadcast, people tend to rely more and more on digital communications. Cognitive radio (CR) offers the promise of intelligent radios that can learn from and adapt to their environment [1-4]. Much research is currently underway developing various reasoning and learning algorithms that allow CRs to operate optimally in a large variety of different situations.IEEE 802.22 is the first wireless access standard based on CR technology, which is a standard for wireless regional area network (WRAN) that utilize TV bands between 54 and 862 MHz [6]. In addition, ECMA-International developed the first CR networking standard for personal/portable devices utilizing TV white spaces, namedECMA-392 [7-8]. The IEEE 802.22 standard addresses fixed access devices and targets rural area applications. However, the ECMA-392 addresses fixed and portable devices and targets in-home, in-building and neighborhood-area applications. TV band devices (TVBDs) are divided into two categories: fixed and personal/portable. Fixed TVBDs operate from a known, fixed location and can use a transmit power of up to 4 W EIRP [7]. They are required to have a geolocation capability, capability to retrieve list of available channels from an authorized database, and a spectrum sensing capability. TVBDs can only operate on channels that are not adjacent to an incumbent TV signal in any channel between 2 and 51 except channels 3, 4, and 37. Personal/portable devices are restricted to channels 21 – 51 (except Channel 37) and are allowed a maximum EIRP of 100 mW on non-adjacent channels and 40 mW on adjacent channels and are

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2014 SERSC

further divided into 2 types: Mode I and Mode II. Mode I devices do not need geolocation capability or access to a database but must have sensing capability. Mode II devices, like fixed devices, must have geolocation, database access and sensing ability.

Very little research has examined new security threats to CR due to their intelligent behavior [9-12]. Like conventional wireless networks, CR networks (CRNs) are also vulnerable to attacks such as denial of service (DoS), selfish misbehaviors, eavesdropping and so on. Some specific work has been conducted looking at attacks in dynamic spectrum access in [9, 10], and was broadened to look at a variety of denial of service attacks against policy radios in [11, 12]. The first edition of the ECMA-392is completed [8].As with the many new technologies, the initial standardization works have not been focused on the security aspects but the functionalities of CR. The authentication protocol in the ECMA-392provides security for link layer. But, it was not designed for protecting end-to-end traffic and data at upper layers in the network. End-to-end security will remain an important issue to the CR user in untrusted CRNs, but is most effective when used in combination with the link layer security [13]. For the end-to-end security, Kuroda et al. proposed a radio-independent authentication protocol for CRNs that is independent of the underlying radio protocols and able to support the extensible authentication protocol (EAP) [14]. The protocol uses a carousel, a data structure, as a shared secret between communication entities, which uses the concept that a list of location information is considered to be unique for each device. The protocol has good aspects which supports a light-weight mutual authentication and could be implemented on a mobile device that has small amount of memory with enough confidentiality. However, it does not consider privacy issue, especially focused on the identification of network and does not support the ECMA-392.

To the best of our knowledge, the design of efficient authentication for the end-to-end security focused on the ECMA-392has not been addressed yet, since designing an authentication protocol for CRNs is a difficult task. So, we will analyze state of the art in authentication mechanisms over the conventional wireless networks and the home networks. Authentication mechanisms have been extensively developed for wireless networks and password authentication is regarded as one of the simplest and the most convenient authentication mechanisms because it has the benefits of low implementation cost and convenient to users [15-20]. Also, the password-based authentication with smart cards is one of the convenient and effective remote user authentication mechanisms [16-18]. This technology has been widely deployed for various applications including remote host login, on-line banking, e-health service, and so on. Recently, two authentication protocols with smart cards are proposed by Vaidya, *et al.*, He, *et al.*, [19-20]. Vaidya, *et al.*, proposed a robust one-time password authentication protocol for digital home network environment [19]. They claimed that their protocol is designed not only to provide mutual authentication, to avoid time synchronization and to discard password-verifier at the remote server but also to thwart the stolen smart card attacks and provide forward secrecy with lost smart card. Furthermore, they have conducted formal verification of the protocol. Similar with them, He, *et al.*, proposes a secure and light-weight authentication protocol for better security strength while keeping the merits of the previous protocols in [15-18]. In their protocol, the required operations on mobile user are only symmetric encryption/decryption operation. Thereby, it is suitable for some lower bandwidth mobile communications. They claimed that their protocol could achieve user anonymity, single registration, user friendly, updating password securely and freely. However, the researches in [21] and [22] addressed that the existing smart cards are vulnerable as

 Copyright ⓒ 2014 SERSC

sensitive verifier and secret values stored in the smart cards could be extracted by monitoring their power consumption. For that reasons, most of the existing protocols using smart cards are still vulnerable to stolen smart card attacks even including the recent authentication protocol in [19], which will be analyzed briefly in the security analysis sub-section in this paper. Furthermore, these protocols are not focused on the CR features for the ECMA-392.

Hence, in order to overcome the shortfalls mentioned above, this paper proposes two new authentication protocols, named as $Auth_{MSN}$and $Auth_{PPN}$, to support end-to-end security for the ECMA-392by using the same notion as proposed by Kuroda, *et al.*, which can be integrated with EAP. $Auth_{MSN}$and $Auth_{PPN}$ use the same carousel in Kuroda, *et al.*, protocol as credential, which stores a series of node specific location related information. Theyare designed to support a set of requirements for EAP including generation of symmetric keying material, key strength, mutual authentication support, shared state equivalence, resistance to dictionary attacks, protection against man-in-the-middle attacks, and protected ciphersuits negotiation. Additionally, they provide privacy issues of consumer premise equipments (CPEs), mainly focused on identity privacy and location privacy.The proposed protocols keep the merits from Kuroda et al.'s protocol but solve the problems in their protocol.

This paper is organized as follows. Section 2 reviews the network architecture for the ECMA-392 and the security mechanism in link layer. Two new authentication protocolsare proposed to solve the problems in the ECMA-392 in Section 3. Some analyses for security, performance and functionality and conclusion are given in Sections 4 and 5, respectively.

2. Overview of ECMA-392 Standard

The ECMA-392 standard aims to serve a broad range of applications including high speed video streaming and Internet access on personal/portable electronics, home electronics equipment, and computers and peripherals. For that, the standard specifies a medium access control (MAC) sub-layer and a physical (PHY) layer for personal/portable cognitive wireless networks operating in TV bands [8]. It also specifies a MUX sub-layer for higher layer protocols. This section briefs the ECMA-392focused on the network architecture and the security.

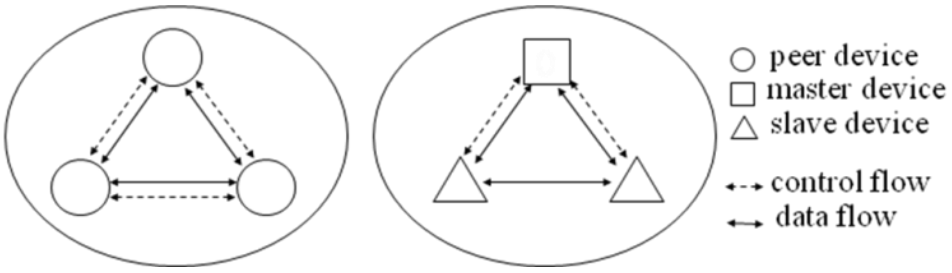
2.1. Network Architecture

The standard supports flexible network formation with three types of devices: master devices, slave devices, and peer devices. The device type of a device is preconfigured. The autonomous transition of device type is not supported in thestandard.A network can be formed as master-slave or peer-to-peer, as illustrated in Figure 1, or as a mesh-network. In a master-slave network, a device is designated as master and others are associated as slaves to the master. The master coordinates communication channel related configurations on behalf of slave devices. A peer-to-peer network comprises of peer devices. Peer devices coordinate the communication channel related configurations in a distributed fashion. A peer device is able to directly communicate with any other peer device as long as it is within the range of the other peer device. In other words, a peer-to-peer network can be ad hoc, self-organizing, and self-healing.

The interoperability of the three device types is built-in due to the fact that all devices follow the same beaconing and channel access protocols. Two or more networks can share the same channel and are also able to communicate with each other.

Copyright ⓒ 2014 SERSC

As a result, a number of networks may form a large-scale network such as a mesh-network or a cluster-tree network using a single channel or multiple channels. While not addressed by the standard, additional support from higher layer will be necessary to allow multi-hop routing of messages from any device to any other device in the extended network.



(a) Peer-to-Peer Network **(b) Master-Slave Network**

Figure 1. Network Topology [8]

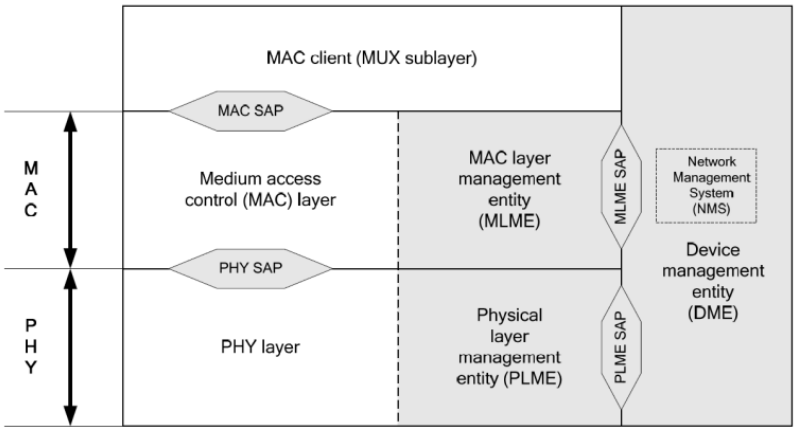


Figure 2. The Reference Model [8]

The standard specifies a PHY layer and a MAC sub-layer. Service access points (SAPs) interaction with PHY and MAC sub-layers are illustrated in Figure 2. As a reference, SAPs are provided for both data transfer as well as management of the MAC sub-layer. The MAC service specified in the standard provides many CR specific services, especially secure communication with data authentication and encryption using cryptographic algorithms.

2.2. Security Mechanism for Link Layer

The security mechanisms specified in the ECMA-392control the security operation of devices by setting appropriate security modes [8]. They allow devices to authenticate each other, to derive pair-wise master keys (PTKs), and to establish secure relationships. The security mechanisms specify the parameters needed in applying the AES-128 CCM to protect the privacy and integrity of traffic. Privacy is protected by encrypting the secure payload, while integrity is protected by including a message integrity code (MIC). This sub-section only focuses on the authentication. Table 1 defines notations used in this paper.

 Copyright ⓒ 2014 SERSC

Table 1. Notations

Symbol	Description
PE_i	A consumer premise equipment *i*
AuC	A home authentication center
ID_i	The identity of an entity *i*
PID_i	The privacy identity of an entity *i*
PMK	The master key
$h(\cdot)$	A secure one-way hash function
$PRF_i(\cdot)$	A pseudo random function with *i* bits result
Loc	A location information
R	A 128 bits random number
R_j	An*i*-th generated 128 bits random number
L	A registered hashed value
CR_i	The carousel ofan entity *i*
KCK_i	An *i*-th generated key confirmation key
PTK_i	An *i*-th generated pair-wise temporal key
MAC_i	A message authentication code
$\{\}K$	A symmetric-key based encryption with a key *K*
$\|\|$	A string concatenation operation
$\rightarrow$	A message transmission

The standard provides a 4-way handshake to provide mutual authentication and PTK generation for two devices sharing a master key. To perform a 4-way handshake, the two devices assume the roles of initiator PE_i, the first message sender and responder PE_j, the other device, respectively. The details of the link layer authentication protocol, named as $Auth_{link}$, are as follows.

Step 1) $PE_i \rightarrow PE_j$:Handshake Message_1(*MKID*, *TKID*, R_1);

PE_ispecifies the master key identifier *MKID*, proposes a temporal key identifier *TKID* for the pair-wise temporal key, *PTK*, to be derived, and includes a unique 128 bits cryptographic random number R_1. The *TKID* shall be different from any *TKID* currently installed in the initiator's local entity. PE_isends a handshake message 1 to PE_j.

Step 2) $PE_j \rightarrow PE_i$:HandshakeMessage_2(*SC*,R_2, MAC_1);

PE_jverifies that the requested *TKID* is unique. Only if it is unique, PE_j generates a new 128 bits cryptographic random number R_2 and derives a key stream *KS*by using the predefined key derivation functions $KS=PRF_{256}(TKID||PMK||R_1||R_2)$ in [8]. The *KS* is then split to form the desired pair-wise temporal key*PTK* and key confirmation key*KCK*. The least significant 16 octets of *KS* become *KCK* while the most significant 16 octets become *PTK*. After that,PE_j computes $MAC_1= PRF_{64}(KCK||R_1||R_2)$.$PE_j$ responds to PE_i with the message 2.

Step 3) $PE_i \rightarrow PE_j$:HandshakeMessage_3(R_1, MAC_2);

First of all, PE_iderives *PTK′* and *KCK′* in the same way as PE_j, checks *SC*, and verifies MAC_1. MAC_1 is verified by comparing it with PE_i's own computation of $PRF_{64}(KCK′||R_1||R_2)$. If the check or verification is failed, PE_i aborts the process. Otherwise, PE_i computes $MAC_2=PRF_{64}(KCK′||R_1)$ for the message integrity.PE_i sends the message 3 back to the responder PE_j.

Step 4) $PE_j \rightarrow PE_i$:HandshakeMessage_4(R_2, MAC_3);

PE_jverifies MAC_2 by comparing it with PE_j's own computation of $PRF_{64}(KCK||R_1)$. Only if the verification is successful, PE_j answers back to $PE_i$by forming the response message 4 after the computation of $MAC_3=PRF_{64}(KCK||R_2)$.

Step 5) PE_i ;

Copyright ⓒ 2014 SERSC

On reception of the message 4, PE_i verifies MAC_3 by comparing it with PE_i's own computation of $PRF_{64}(KCK \| R_2)$. Only if the verification is successful, mutual authentication is successful.

The link layer authentication provided by the ECMA-392 is an essential component for the CRN security. While the authentication protocol supported by the standard provides a base line of security between directly connected network devices, it was not specifically designed for protecting end-to-end traffic and data at upper layers in the network.

End-to-end security will remain an important issue to the CR user in untrusted CRNs, but is most effective when used in combination with link layer security. Link layer security used in conjunction with the upper layer security provides a double layer of security to meet the needs of the most security conscious organizations [13]. Next section will consider the end-to-end security for the ECMA-392.

3. End-to-End Authentication Protocol

In this section, we propose two new authentication protocols, named as $Auth_{MSN}$and $Auth_{PPN}$, to support end-to-end security for personal/portable devices and home networks to provide radio agility by using TV white spaces. Since location information for the device is one of the very important factors in the CRNs due to the primary user protection, our protocols use the information as the secret credential between entities. For that, it is assumed in our protocols that each entity in the CRNs is equipped with GPS to gather the location related information as the same as in the IEEE 802.22 WRAN [5]. $Auth_{MSN}$and $Auth_{PPN}$are designed to support a set of requirements for EAP that are suitable for wireless LAN authentication. First of all, this section describes location-based credential, which is a basic security building block for authentication and then proposes two end-to-end authentication protocols based on the credential.

3.1. Location-based Credential

Our protocols use carousel as the basic credential for the authentication, which stores a series of location related information.

a) Carousel

A carousel is a circular list of cells that contains location information and has an entry, named rear, which points the input position of the list [14]. A conceptual image of the carousel is shown in Figure 3. A cell pointed by the entry is updated whenever a new location is put into the carousel. The movement of the entry is considered as rotation of the carousel and the rotation is performed by only predefined direction. Each registered device in the network has a carousel synchronized with the home network authentication center. Synchronization refers to arrange two carousels so that they have their cells in the same order. As one carousel rotates and location information is written to the entry cell, two carousels become unsynchronized. Therefore, resynchronization is necessary by which the second entity rotates and updates its carousel to the same configuration as the first one. That's why it is necessary for the carousels to be synchronized between two communication entities before establishing shared keys.

Each entity in the CRN needs to have a function to derive a secret key from the carousel. Pseudo random function the same as in [8] is used so that it creates the same key from the same carousel if the carousels on entities are synchronized.

 Copyright ⓒ 2014 SERSC

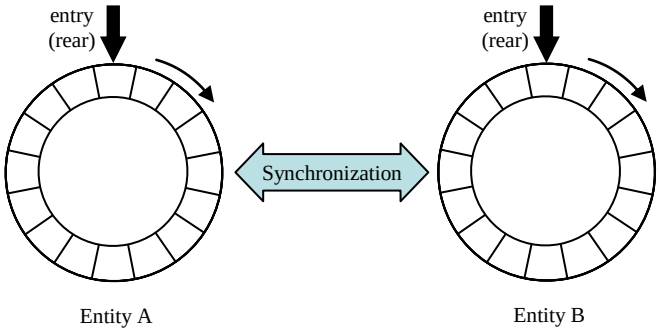


Figure 3. Carousel Structure

b) Initial Setup

It is assumed that when a newdevice tries to be registered into aCRN,a carousel is initialized between the device and the home server, also called as authentication center (*AuC*), by offline via a secure channel. This initial setup is performed by filling each cell into $h(Loc, R_i)$ of the carousel, where *Loc* is the current location information for the device and R_i is a random number at the cell *i*. At the same time of the carousel initialization, the device also registers it's privacy identity $PID_{PEi}=h(ID_{PEi}, R_i)$ to the *AuC*. It is optional that the *AuC* asks and keeps the real identity of the device for the future usage. Theprivacy identity is updated regularly by computing $PID_{i+1}=h(PID_i, R_j)$ in each session*j* after the successful authentication between the device and the *AuC*, which is to support the message unlinkability in each session.

3.2. End-to-End Authentication Protocol

This subsection proposes two new authentication protocols, $Auth_{MSN}$and $Auth_{PPN}$, which support EAP and use the shared keying properties from the carousel for the mutual authentication. Figure 4 and Figure 5 show the overview of the protocols.

a) Authentication Protocol for Master-Slave Network

It is assumed that one party is master and the other is slave in this network formation. Thesteps for $Auth_{MSN}$are as follows:

Step 1) $AuC \rightarrow PE_i$:HandshakeMessage_1();
*AuC*sends a handshake message 1 to a device PE_i.

Step 2) $PE_i \rightarrow AuC$:HandshakeMessage_2(PID_{PEi}, R_1);
PE_i generates a random numberR_1 and responds to*AuC*with the handshake message 2, which triggers a mutual authentication between PE_i and *AuC* using carousels.

Step 3) $AuC \rightarrow PE_i$:HandshakeMessage_3(R_2,MAC_1);
AuC generates a random numberR_2 and derives the desired PTK_1 and $KCK_1$for PE_i by using PID_{PEi}, $h(Loc, R_i)$,R_1, and R_2, where $h(Loc, R_i)$ is PE_i's carousel informationat the cell *i* pointed by the entry.*AuC*, then, sends the handshake message 3 to PE_i after it computes MAC_1 from $MAC_1=PRF_{64}(KCK_1||R_1||R_2)$.

Step 4) $PE_i \rightarrow AuC$:HandshakeMessage_4(MAC_2, $\{Loc\}_{PTK1'}$, MAC_3);
PE_irotates the carousel once, computes $PRF_{64}(KCK_1'||R_1||R_2)$ after the derivation of the desired PTK_1' and $KCK_1'$by using the location related information from the carousel and the other information PID_{PEi}, R_1, and R_2, and checks if the equation $MAC_1=PRF_{64}(KCK_1'||R_1||R_2)$ holds. If the verification fails, PE_i rotates the carousel once again and verifies MAC_1 until it is successful. PE_i derives the current location information *Loc*, computes$L=h(Loc, R_1)$, which uses thelocation information, *Loc* and the session

dependent randomR_1.PE_icomputes $MAC_2=PRF_{64}(KCK_1'||R_1)$ and $MAC_3=PRF_{64}(KCK_2||R_2)$ after the derivation of the desired PTK_2 and $KCK_2$by using the location related information L and the other information PID_{PEi}, R_1, and R_2, encryptsLoc by using PTK_1' and answers back toAuC with the handshake message 4.

Step 5) $AuC \rightarrow PE_i$:HandshakeMessage_5(MAC_4);

AuC derives PE_i's location information Loc by decrypting $\{Loc\}_{PTK1}'$ with the previously derived key PTK_1 and verifies MAC_2. Only if the verification is successful, AuC computes PTK_2' and $KCK_2'$by using the location related information L and the other information PID_{PEi}, R_1, and R_2, and verifies MAC_3 from the received message by using KCK_2'. If it is necessary to check the validity of Loc received from PE_i, AuCverifies the real location of PE_i by estimating the position of a given source based on the received signal strength by using methods in [23, 24]. Only if these verifications are successful, AuCupdates the entry cell of the carousel with L, the new location related information of PE_i,and sends the handshake message 5 with $MAC_4=PRF_{64}(KCK_2'||R_1)$ to PE_i.

Step 6) PE_i;

PE_iverifies MAC_4 by using the previously derived KCK_2 and R_1. Only if theverification is successful, PE_iupdates the entry cell of the carousel with L.

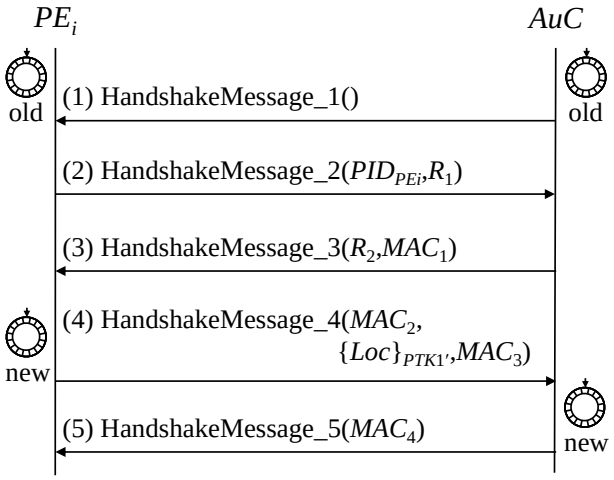


Figure 4. Authentication Protocol for Master-Slave Network ($Auth_{MSN}$)

After the successful mutual authentication, PE_i and AuC generate the required keys by using the key derivation algorithms suggested in [8] and [14], such as a master session key (MSK) and an extended master session key (EMSK) for EAP, an authentication key (AK), and a traffic encryption key (TEK) for the security control management (SCM) key hierarchy in CRNs, and so on, from the carousel. These keys are used as the keys to secure the communications. For the consequent session, both of PE_i and AuC updates the privacy identity $PID_{PEi}=h(PID_{PEi}, R_1)$.

b) Authentication Protocol for Peer-to-Peer Network

It is assumed that sender and receiver are peer devices in this network. The steps for $Auth_{PPN}$are as follows;

Step 1) $PE_1 \rightarrow PE_2$:HandshakeMessage_1();

PE_1sends the handshake message 1 to PE_2 as an identity request.

 Copyright ⓒ 2014 SERSC

Step 2) $PE_2 \rightarrow PE_1$:HandshakeMessage_2(PID_{PE2}, R_1);

PE_2generates a new 128-bits cryptographic random number R_1 and sends an authentication requestcomposed of the privacy identification PID_{PE2} and $R_1$to PE_1.

Step 3) $PE_1 \rightarrow AuC$:HandshakeMessage_3(PID_{PE1}, PID_{PE2}, R_1, R_2);

PE_1generates a new 128-bits cryptographic random number R_2 and sends the handshake message 3 composed of two communication parties' privacy identifiers, PID_{PE1} and PID_{PE2},and random numbers, R_1 and R_2, to *AuC*.

Step 4) $AuC \rightarrow PE_1$:HandshakeMessage_4(R_3, MAC_1, $\{h(Loc, R_j)\}_{PTK1}$);

AuC generates a 128-bits cryptographic random numberR_3, rotates carousels once shared with PE_1 and PE_2, respectively. After that, *AuC*derives the desired PTK_1 and $KCK_1$for PE_1 by using PID_{PE1}, $h(Loc, R_i)$,R_2, and R_3, where $h(Loc, R_i)$ is PE_1's carousel information at the cell i pointed by the entry.*AuC*also derives the desired PTK_2 and $KCK_2$for $PE_2$for the later usage in the same way for PE_1.Then, *AuC*computes $MAC_1=PRF_{64}(KCK_1||R_2||R_3)$, encrypts $h(Loc, R_j)$ by using PTK_1, where $h(Loc, R_j)$ is PE_2's carousel information at the cell j pointed by the entry, and sends the handshake message 4 to PE_1.

Step 5) $PE_1 \rightarrow PE_2$:HandshakeMessage_5(R_2,MAC_2);

PE_1 rotates the carousel once, computes $PRF_{64}(KCK_1'|R_2||R_3)$after the derivation of the desired PTK_1' and KCK_1' by using the location related information from the carousel and the other information PID_{PE1}, R_2, and R_3, and checks if the equation $MAC_1=PRF_{64}(KCK_1'||R_2||R_3)$ holds. If the verification fails, PE_1 rotates the carousel once again and verifies MAC_1 until it is successful. Then, PE_1decrypts the received $\{h(Loc, R_j)\}_{PTK1}$ by using PTK_1' and computes $MAC_2=PRF_{64}(KCK_2||R_1||R_2)$after the derivation of the desired PTK_2 and KCK_2 by using the decrypted location related information for PE_2 the other information, and answers back to PE_2 with the handshake message 5.

Step 6) $PE_2 \rightarrow PE_1$:HandshakeMessage_6(R_1, MAC_3, $\{Loc_2\}_{PTK2'}$);

PE_2 rotates the carousel once, computes $PRF_{64}(KCK_2'||R_1||R_2)$after the derivation of the desired PTK_2' and KCK_2' by using the carousel information and the other information, and checks if the equation $MAC_2=PRF_{64}(KCK_2'||R_1||R_2)$ holds. If the verification fails, PE_2 rotates the carousel once again and verifies MAC_2 until it is successful. After that, PE_2 derives the current location information Loc_2, computes $L_2=h(Loc_2, R_1)$, and stores L_2into a new cellfor the carousel update. PE_2encrypts Loc_2 by using PTK_2', computes $MAC_3=PRF_{64}(KCK_2'||R_1)$ and answers back to PE_1 with the handshake message 6.

Step 7) $PE_1 \rightarrow AuC$:HandshakeMessage_7(MAC_3, $\{Loc_2\}_{PTK2'}$, MAC_4, $\{Loc_1\}_{PTK1'}$);

PE_1verifies MAC_3 by checking whether it matches with it's own computation of $PRF_{64}(KCK_2||R_1)$. If the verification is successful, PE_1 derives PE_2's location information Loc_2 by decrypting $\{Loc_2\}_{PTK2'}$ with the previously derived key PTK_2. If it is necessary to check the validity of Loc_2 received from PE_2, PE_1 verifies the real location of PE_2 by estimating the position of a given source based on the received signal strength by using methods in [23, 24]. Only if theverifications are successful, PE_1 derives the current location information Loc_1, computes $L_1=h(Loc_1, R_2)$, and stores L_1into the current cell for the carousel update. PE_1encrypts Loc_1 by using PTK_1', computes $MAC_4=PRF_{64}(KCK_1'||R_2)$, and sends back to *AuC* with the handshake message 7.

Step 8) *AuC* ;

*AuC*verifies MAC_3 and MAC_4 after the related key derivations. If the verifications are successful, *AuC*decrypts $\{Loc_2\}_{PTK2'}$and $\{Loc_1\}_{PTK1'}$by using the derived keys, PTK_2 and PTK_1, respectively. Only if theverifications are successful, *AuC* computes $L_1=h(Loc_1, R_2)$ and $L_2=h(Loc_2, R_1)$, updates both of the entry cells for PE_1 and PE_2 with L_1 and L_2, respectively.

Copyright ⓒ 2014 SERSC

After the successful mutual authentication, PE_1 and PE_2 generate the required keys as the same as in the master-slave networks and update their ownprivacy identities$PID_{PEi}=h(PID_{PEi}, R_i)$, respectively.*AuC*also updates the privacy identities for both of PE_1 and PE_2, respectively.

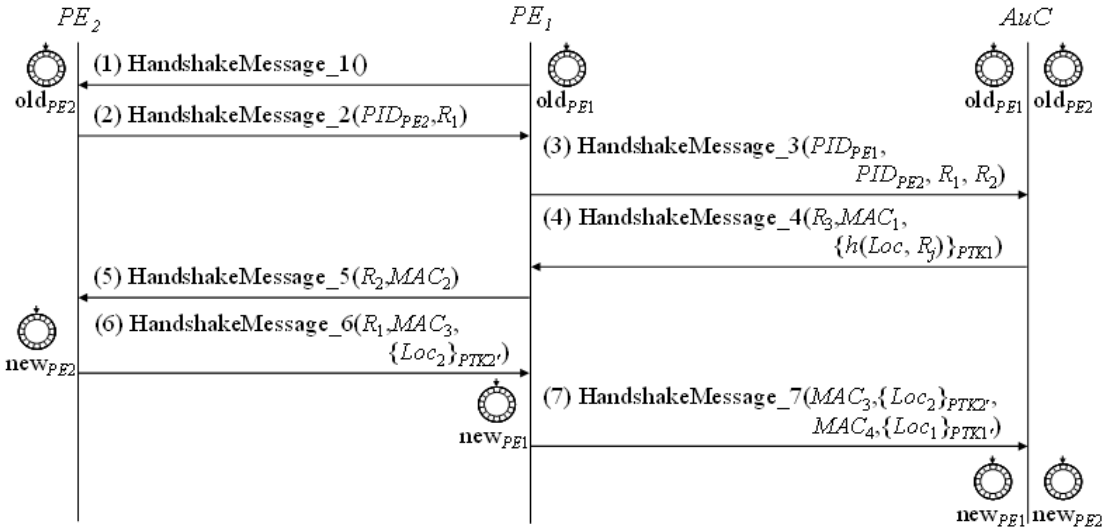


Figure 5. Authentication Protocol for Peer-to-Peer Network ($Auth_{PPN}$)

4. Analysis

This section discusses three analyses of security, performance, and functionality for the proposed authentication protocols, $Auth_{MSN}$and $Auth_{PPN}$. First of all, security analysis is discussed in detail based on [14, 20]. Furthermore, performance and functional analyses are given by comparing the proposed protocols with the related protocols in [14, 19, 20].

4.1. Security Analysis

Although it is important to provide a formal security proof on any cryptographic protocols, the formal security proof of authentication protocols remains one of the most challenging issues for cryptography research. Until now, a simple, efficient and convincing formal methodology for correctness analysis on security protocols is still an important subject of research and an open problem. Because of these reasons, most authentication protocols have been demonstrated with a simple proof. Therefore, we follow the approaches used in[20]for comparison purpose.

We will analyze the security of $Auth_{MSN}$and $Auth_{PPN}$ to verify the overall security requirements including passive and active attacks, resistant to carousel guessing attack, perfect forward secrecy, and two privacy issues as follows.

[Proposition 1]$Auth_{MSN}$and $Auth_{PPN}$ are secure against passive and active attacks.
Proof: We assume that an adversarysucceeds if the adversary finds the session dependent hash value L stored in the carousel or the key derived from L. Therefore, we show that probability to succeed in finding the two values is negligible due to the difficulty of the underlying symmetric cryptosystem and pseudo random function.

 Copyright ⓒ 2014 SERSC

1. A completeness of the protocols is already proven by describing the run of the protocols in Section 3.
2. The acceptance by all entities means that each MAC_iin the corresponding messageis successfully verified. That is, MAC_1 computed by using KCK_1 is verified by using the correct key KCK_1'from the synchronized carousel successfully, MAC_2 computed by using KCK_1' is verified with the key KCK_1, MAC_3 computed by using KCK_2 is verified with the key KCK_2', and MAC_4 computed by using KCK_2' is verified with the key KCK_2 in $Auth_{MSN}$. Similarly for $Auth_{PPN}$, MAC_1 computed by using KCK_1 is verified by using the correct key KCK_1'from the synchronized carousel successfully, MAC_2 computed by using KCK_2 is verified with the key KCK_2', MAC_3 computed by using KCK_2' is verified with the key KCK_2,and MAC_4 computed by using KCK_1' is verified with the key KCK_1. We show that if it is the case that entities accept the messages and continue the session, then the probability that the adversary have modified the messages being transmitted is negligible. And the only way for the adversary to find the secret credential is to solve the difficulty of the underlying symmetric cryptosystem and pseudo random function.
3. If the adversary is passive adversary, all the adversary can gather are as follows: PID_{PEi}, R_1,R_2,MAC_1,MAC_2, $\{Loc\}_{PTK1}$', MAC_3, andMAC_4 from $Auth_{MSN}$ and PID_{PE2}, R_1,PID_{PE1}, PID_{PE2}, R_2, R_3, MAC_1, $\{h(Loc, R_j)\}_{PTK1}$,MAC_2,MAC_3, $\{Loc_2\}_{PTK2'}$,MAC_3, MAC_4, and $\{Loc_1\}_{PTK1}$from $Auth_{PPN}$. However, it is negligible to find the related key information from them due to the difficulty of the underlying symmetric cryptosystem and pseudo random function.
4. Now, we consider the active adversary with following cases.
   (a) There is no way that an adversary could get the key related information L stored in the carousel due to the difficulty of the underlying hash function. Since $L$is computed by using the hash function which supports the uniform distribution, we can see that the hashed result$L$ remains under uniform distribution.
   (b) An adversary cannot impersonate $PE_i$to cheat AuC or PE_j. That is the attacker cannot generate a valid handshake message without knowing the key related value L, since the attacker cannot pass the verification of MAC_i in each step of our protocols. Even if the attacker has obtained the legal value from the previous sessions, the attacker still cannot generate the consequent valid messages, which could pass the verification at each step.
   (c) An adversary cannot impersonateAuC to cheat PE_i. As described above, only the legalAuCcan form the legal handshake message by including the proper secret from the carousel, which needs to be properly verified at the following steps. Even if the attacker uses the legal handshake message, the attacker still cannot get any useful information from the session information due to the difficulty of the underlying pseudo random function and symmetric cryptosystem, and cannot generate the consequent valid messages.

Finally, we could say our protocols are secure against passive and active attacks.

[Proposition 2]$Auth_{MSN}$and $Auth_{PPN}$ can resist carousel guessing attack.

Proof.The security of the proposed protocols is based on the difficulty that an adversary is faced with when attempting to reproduce an equivalent carousel for PE_i. As mentioned in the Section 3, every cell in the carousel is initialized with hashed values by using both location information and random value, which could not be known to the adversary. PE_i's location related information is updated in the carousel each time after

Copyright ⓒ 2014 SERSC

the successful authentication. Even if the adversary could monitor one of PE_i's locations, the adversary cannot know the correct hash value L which is dependent not only on the location information but also on a session dependent random number. Furthermore, the adversary could not know where the hashed value L is overwritten into the carousel.

[Proposition 3] $Auth_{MSN}$and $Auth_{PPN}$ can provide the perfect forward secrecy.
Proof.Perfect forward secrecy is provided in the situation that even though the credential is compromised, the adversarycannot derivethe previous session keys. To analyze this, suppose that an adversary knows asecurity related value L in the carousel. Then the attacker tries to find the previous session related keys from the information collected by passive attack from the past communication sessions, *i.e.*, PID_{PEi}, R_1,R_2,MAC_1,MAC_2, $\{Loc\}_{PTK1}$', MAC_3, andMAC_4 from $Auth_{MSN}$ and PID_{PE2}, R_1,PID_{PE1}, PID_{PE2}, R_2, R_3, MAC_1, $\{h(Loc, R_j)\}_{PTK1}$,MAC_2,MAC_3, $\{Loc_2\}_{PTK2}$',MAC_3, MAC_4, and $\{Loc_1\}_{PTK1}$'from $Auth_{PPN}$. However, the attacker cannot extract any information related to the session keys due to the difficulty of the underlying symmetric cryptosystem and pseudo random function. Furthermore, each session in each protocol requires two credentials to be authenticated each other and established necessary keys. Therefore, the proposed protocols provide the property of perfect forward secrecy.

[Proposition 4]$Auth_{MSN}$and $Auth_{PPN}$ can provide location privacy.
Proof. Each cell in the carousel stores a hashed value L, where $L=h(Loc, R_i)$. This hash operation is useful for protecting the location privacy. Adversary cannotget any useful information from the transmitted messages because the value L is derived by using both the location information Loc and the session dependent random value R_i. By applying the random value R_i to the value Loc, the protocols could effectively distinguish the distinct PE_iin the similar locations. Thereby, the proposed authentication protocols could support the location privacy because each cell of the carousel storesnot the real location value Locbut the digest value$L$. No one can leak the location related information from the carousel due to the onewayness of the hash function.

[Proposition 5]$Auth_{MSN}$and $Auth_{PPN}$ can provide identity privacy.
Proof.The identity privacy is provided by supporting anonymity of PE_i, whichis the state of being not identifiable to the adversary [25]. The proposed protocols use the privacy identity,PID_{CPEi} for PE_i instead of the real identity, ID_{PEi}. By using the session dependent privacy identity PID_{PEi} and the authentication keys PTK_i andKCK_i,the protocols could support session unlinkability. Unlinkabilityof messages in each session means that within the network from the adversary's perspective, these messages of interest are no more and no less related after the adversary's observation than they are related concerning the adversary's prior knowledge. This means that the probability of messages in each session of the proposed protocols from the adversary's perspective stays the same before and after the adversary's observation.

We compare the proposed protocols, $Auth_{MSN}$and $Auth_{PPN}$, with the existing representative authentication works in terms of security properties [19, 20, 14]. In Table 2, it can be seen that $Auth_{MSN}$and $Auth_{PPN}$ satisfy all above-mentioned requirements.

 Copyright ⓒ 2014 SERSC

Table 2. Security Comparison between Protocols

Property / Protocol	PR1	PR2	PR3	PR4	PR5	PR6
Vaidya et al.'s in [19]	Insecure	Provide	Provide	Provide	N/A	N/A
He et al.'s in [20]	Secure	Provide	Provide	N/A	Provide	N/A
Kuroda et al.'s in [14]	Secure	Provide	Provide	Provide	N/A	Provide
$Auth_{MSN}$	Secure	Provide	Provide	Provide	Provide	Provide
$Auth_{PPN}$	Secure	Provide	Provide	Provide	Provide	Provide

* PR1 : credential guessing attack, PR2 : mutual authentication, PR3 : session key agreement, PR4 : perfect forward secrecy, PR5 : identity privacy, PR6 : location privacy

It can be seen that Vaidya *et al.*, authentication protocol in [19] cannot provide off-line password guessing attack when the smart card is stolen and if the adversary could collect the user's previous session messages. With stolen smart card having $\{ID_C, ID_{SC}, h(), v_T, g_T, k_T, C_M\}$ and with the intercepted previous session information $\{ID_C, u_T, a_T, G\}$ at the step LA3, the adversary can compute $u_T \oplus v_T = h(PW)$, where $v_T = h(ID_C \oplus x) \oplus h(PW) \oplus K$ and $u_T = K \oplus h(ID_C \oplus x)$. Then, the adversary easily guesses a password PW' and verifies the guess in off-line manner by checking whether the equation $h(PW) = h(PW')$ holds or not. Therefore, Vaidya *et al.*, protocol is not secure gainst the password guessing attack.

In the case of He *et al.*, protocol in [20], it does not provide the perfect forward secrecy. If the long term secret N is revealed to an adversary, the adversary could easily get the important information from the previously intercepted messages $\{n, E, ID_{HA}, T_{MU}\}$ by computing $n \oplus ID_{HA} = (ID_{MU} || m)_N$. Then, the adversary computes $L = h(T_{MU} \oplus h(ID_{MU} || N))$after decrypting the encrypted data $(ID_{MU} || m)_N$with N, and decrypts the message E with L to find x_0 and x. By using these data, the adversary could compute the session key $k = h(h(h(N || ID_{MU}))x_0 || x)$. Thereby, He *et al.*, protocol does not provide the perfect forward secrecy.

Kuroda, *et al.*, authentication protocol in [14] cannot provide identity privacyand thereby, could not support the session unlinkability. Furthermore, the protocol could not support the network for the ECMA-392.

4.2. Performance and Functional Analyses

This sub-section evaluates the performance and functionality of $Auth_{MSN}$and $Auth_{PPN}$and makes comparisons with the related works in [19, 20, 14] as shown in Table 3.

Copyright ⓒ 2014 SERSC

Table 3. Performance and Functionality Comparison between Protocols

Property / Protocol	PE1	PE2	FU1	FU2	FU3
Vaidya et al.'s in [19]	Extremely low	Low	Not required	Not provided	Not provided
He et al.'s in [20]	Low	Extremely low	Required	Not provided	Not provided
Kuroda et al.'s in [14]	Low	Low	Required	Provided	Not provided
$Auth_{MSN}$	Extremely low	Extremely low	Not required	Provided	Provided
$Auth_{PPN}$	Low	Low	Not required	Provided	Provided

* PE1: computational cost, PE2 : communicational cost, FU1 : public key infrastructure,FU2 : EAP compatibility, FU3 : ECMA-392 compatibility

The performance of authentication protocols can be approximated in terms of communication and computation loads. The number of steps is considered as a factor for the communication load, while the required operations, which are hash function, symmetric-key cryptosystem operation, and public-key cryptosystem operation, are basic factors to the computation load. The functionalities are focused on the requirements from the ECMA-392, which are including public key infrastructure and EAP compatibility.

It can be seen that Vaidya, *et al.*, protocol has good properties in terms of the computational cost which requires hash functions and symmetric-key cryptosystem operations. The required operations have relatively low overhead than the public-key cryptosystem operations. In the perspective of the communicational cost, Vaidya *et al.*, protocol and He *et al.*, protocol require 6 and 4 messages, respectively. However, they cannot be used in the CRN due to the network environmental difference in them and the incompatibility with EAP.

Kuroda, *et al.*, protocol has similar performance and functionalities to that of the proposed authentication protocol, which requires low computational and communicational costs, and supports location-based authentication and EAP compatibility. However, Kuroda, *et al.*, protocol requires public key infrastructure, which has a big overhead in terms of computation for the system.

In $Auth_{MSN}$and $Auth_{PPN}$, the computational cost and communicational cost are comparable with the other protocols. However, our protocols can achieve the better security and more functionalities than the others over the CRN for the ECMA-392 as shown in Table 3.

5. Conclusion

The first CR networking standard for personal/portable devices utilizing TV white spaces is developed by ECMA-International. The ECMA-392addresses fixed and portable devices and targets in-home, in-building and neighborhood-area applications. While the authentication protocol supported by the ECMA-392 provides a base line of the link layer security, it does not specifically designed for protecting end-to-end traffic and data at upper layers in the CRN. Hence, in order to overcome the shortfalls, this paper proposed two new authentication protocols,named as $Auth_{MSN}$and $Auth_{PPN}$, to support end-to-end security for the ECMA-392. They use location information as thesecurecredentialfor the authentication. $Auth_{MSN}$and $Auth_{PPN}$ could be supported privacy issues of consumer

 Copyright ⓒ 2014 SERSC

premise equipments and are designed to support a set of requirements for EAP including generation of symmetric keying material, key strength, mutual authentication support, shared state equivalence, resistance to dictionary attacks, protection against man-in-the-middle attacks, and protected ciphersuits negotiation. Our protocols could be used in conjunction with the link layer protocol from the ECMA-392 to meet the needs of the most security conscious organizations over the CRN.

Acknowledgements

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2010-0021575).

References

[1] B. Fette, "Cognitive Radio Technology-second edition", Academic Press, **(2009)**.
[2] J. Mitola, "Cognitive Radio for Flexible Mobile Multimedia Communications", Mobile Networks and Applications, vol. 6, no. 5, **(2001)**, pp. 435-441.
[3] I. F. Akyildiz, W. Y. Lee, M. C. Vuran and S. Mohanty, "A Survey on Spectrum Management in Cognitive Radio Networks", IEEE Communications Magazine, vol. 46, **(2008)**, pp. 40-48.
[4] I. F. Akyildiz, W. Lee and K. R. Chowdhury, "CRAHNs: Cognitive radio ad hoc networks", Ad hoc networks, vol. 7, **(2009)**, pp. 810-836.
[5] Y. Tachwali, F. Basma and H. H. Refai, "Cognitive radio architecture for rapidly deployable heterogeneous wireless networks", IEEE Transactions on Consumer Electronics, vol. 56, no. 3, **(2010)**, pp. 1426-1432.
[6] IEEE 802.22, IEEE P802.22/D1.0 draft standard for wireless regional area networks part 22: Cognitive wireless RAN medium access control (MAC) and physical layer (PHY) specifications: Policies and procedures for operation in the TV bands, **(2008)**.
[7] J. Wang, M. S. Song, S. Santhiveeran, K. Lim, S. H. Hwang, M. Ghosh, V. Gaddam and K. Challapali, "First Cognitive Radio Networking Standard for Personal/Portable Devices in TV White Spaces", ECMA/TC48-TG1/2009/132, white paper, **(2009)**.
[8] "ECMA-International, MAC and PHY for operation in TV white space", Standard ECMA, vol. 392, **(2009)**.
[9] T. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment", Mobile Networks and Applications, vol. 13, no. 5, **(2008),** pp. 516-532.
[10] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation", Crown Com., **(2008),** pp. 1-8.
[11] R. Chen and J. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks", IEEE Workshop on Networking Technologies for SDR, **(2006)**, pp. 110-119.
[12] R. Chen, J. Park and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks", IEEE Journal on Selected Areas in Communications, vol. 26, no. 1, **(2008)**, pp. 25-37.
[13] "Interlink Networks", Link layer and network layer security for wireless networks, white paper, **(2006)**.
[14] M. Kuroda, R. Nomura and W. Trappe, "A radio-independent authentication protocol (EAP-CRP) for networks of cognitive radios, SECON, **(2007)**, pp. 70-79.
[15] C. S. Tsai, C. C. Lee and M. S. Hwang, "Password authentication schemes: Current status and key issues", International Journal of Network Security, vol. 3, no. 2, **(2006)**, pp. 101-115.
[16] S. W. Lee, H. S. Kim and K. Y. Yoo, "Improved efficient remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, **(2004)**, pp. 565-567.
[17] E. J. Yoon, E. K. Ryu and K. Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 50, no. 2, **(2004)**, pp. 612-614.
[18] D. Daiz-Sanchez, A. Marin, F. Almenarez and A. Cortes, "Sharing conditional access modules through the home network for pay TV access", IEEE Transactions on Consumer Electronics, vol. 55, no. 1, **(2009)**, pp. 88-96.
[19] B. Vaidya, J. H. Park, S. Yeo and J. J. P. C. Rodrigues, "Robust one-time password authentication scheme using smart card for home network environment", Computer Communications, vol. 34, no. 3, **(2010)**, pp. 326-336.
[20] D. He, M. Ma, Y. Zhang, C. Chen and J. Bu, "A strong user authentication scheme with smart cards for wireless communications", Computer Communications, vol. 34, no. 3, **(2010)**, pp. 367-374.

Copyright ⓒ 2014 SERSC

[21] P. Kocher, J. Jaffe and B. B. Jun, "Differential power analysis", Proceedings of Advances in Cryptology, **(1999),** pp. 388-397.
[22] T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks", IEEE Transactions on Computers, vol. 51, no. 5, **(2002),** pp. 541-552.
[23] Y. Cho, L. Bao and M. Goodrich, "Secure access control for location-based applications in WLAN systems", MASS'06, **(2006),** pp. 852-857.
[24] J. Hightower and G. Borrriello, "Location systems for ubiquitous computing", IEEE Computer Magazine, vol. 34, no. 8, **(2001)**, pp. 57-66.
[25] A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, unobservability, pseudonymity, and identity management – A consolidated proposal for terminology, http://dud.inf.tu-dresden.de/Anon_Terminology.shtml, **(2008).**

Authors

Hyunsung Kim, he is a professor at the Department of Cyber Security, Kyungil University, Korea from 2012. Hereceived the M.S. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Republic of Korea, in 1998 and 2002, respectively. From 2000 to 2002, he worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2012 with the Department of Computer Engineering, Kyungil University. His research interests include cryptography, VLSI, authentication technologies, network security and ubiquitous computing security.

 Copyright ⓒ 2014 SERSC