Journal of
Sensor and Actuator Networks

MDPI

Article

Delegation Based User Authentication Framework over Cognitive Radio Networks

Hyunsung Kim [1,2] and Eun Kyung Ryu [3,*]

[1] Department of Cyber Security, Kyungil University, Gamasilgil 50, Kyungbuk 38428, Korea; kim@kiu.ac.kr
[2] Department of Mathematical Sciences, University of Malawi, P.O. Box 280, Zomba, Malawi
[3] School of Computer Science and Engineering, Kyungpook National University, Daehakro 80, Daegu 41566, Korea
* Correspondence: ekryu@knu.ac.kr; Tel.: +82-10-9720-5386

Received: 13 October 2017; Accepted: 28 November 2017; Published: 2 December 2017

Abstract: To address the ever increasing demand for wireless bandwidth, cognitive radio networks (CRNs) have been proposed to improve the efficiency of channel utilization. CRN permits unlicensed users to utilize the idle spectrum as long as it does not introduce interference to the primary users due to the Federal Communications Commission's recent regulatory policies. In this paper, we first identify some required distinctive security and privacy features for CRNs focused on ECMA-392, which is the first industrial standard for personal or portable devices in the television white spaces. After that, we propose a delegation based user authentication framework as a basic security and privacy module with full consideration of the required features over CRNs. The proposed framework provides privacy preserving yet accountable security within the CRN entities. Security and privacy analyses show that the proposed framework supports unlinkability, context privacy, anonymity, no registration and conditional traceability, which are the required security and privacy aspects in CRNs.

Keywords: cognitive radio network; cryptography; authentication framework; delegation

1. Introduction

The last decade has witnessed a growing demand for wireless radio spectrum. The inefficient usage of the limited spectrum resources has motivated the regulatory bodies such as the Federal Communications Commission (FCC) to review their policy and start to seek innovative communication technology that can exploit the wireless spectrum in a more intelligent and flexible way. The concept of cognitive radio (CR) was proposed by Mitola to address the issue of spectrum efficiency and has been receiving increasing attention in recent years [1–4]. The television (TV) broadcasting spectrum is seen as one of the first opportunities to adopt and implement innovative and more efficient dynamic spectrum assess models supported by CR technology. Encouraged by the acts of FCC, many international organizations have also started to define CR standards on TV white spaces (TVWS) including IEEE 802.22, IEEE 802.11af, IEEE 1990 and ECMA-392 and so on [5–9].

One of the primary requirements of CR networks (CRNs) is their ability to scan the entire spectral band for the presence or absence of primary users (PUs) [2]. This process is called spectrum sensing and is performed either locally by a secondary user (SU) that is the visitor of that network or collectively by a group of SUs. The available spectrum bands are then analyzed to determine their suitability for communication. Characteristics like signal-to-noise ratio, link error rate, delays, interference and holding time can be used to determine the most appropriate band. After the spectrum band is selected, SU transmission in that band takes place. If a SU or a network detects a PU transmission, it vacates the corresponding spectrum band and looks for another vacant band. CRNs face not only

traditional network security problems, but also unique security risks due to the intrinsic different characteristics. Any node can use vacant spectrum, so PUs will face the risk of being monitored and disturbed. Differences of the current security mechanisms lead to security problems that appear because of network merge [10–14]. Therefore, disadvantages of some wireless standards may result into the whole networks being unsecure when they are merged. Any node in CRNs adaptively adjusts transmission parameters according to the surrounding environment, which makes any node to be used as an attack node.

ECMA-392 standard is published for the first time as a standard operating on TV bands [8,9]. Its target applications are wireless home network and wireless Internet access at campus, park, hotspot, and so on, which are similar to IEEE 802.11af's [7]. The major differences between two standards are PU protection mechanisms and channel bandwidth to be supported. Basically both standards obtain an available channel list from TVWS database through Internet access, which has information of unused TV channels geometrically. ECMA-392 additionally supports the spectrum sensing functionality to periodically check the existence of PU signals on the current channel. It has specified the operation in only single TV channel which can be one of three channel bandwidths of 6 MHz, 7 MHz, or 8 MHz according to regulatory domain.

As with the other new developing network technologies, current research does not focus on the security issues over CRNs [12–18]. However, security becomes the key problems that need to be solved. CRNs face not only the traditional network security problems, but also the unique security risks due to the intrinsic different characteristics on CR technologies [19]. Any node can use vacant spectrum, so PUs will face the risk of being monitored and disturbed by attacker easily. Any node in CRNs adaptively adjusts transmission parameters according to surrounding environment, which makes any node to be used as an attack node. In the context of CRNs, the main security goals include confidentiality, integrity, authentication, non-repudiation, access control and availability as the general networks. We will only consider authentication, which is the basic and core security mechanism in any networks. Wang et al. proposed public key based entity authentication protocol with digital signature for CRNs [20]. However, their protocol does not consider the distinctive security features on CR technology. Kim proposed a location based authentication protocol for IEEE 802.22 structure, which uses carousel as the secret credential [21]. It tried to adopt the distinctive aspects on CR technology based on location information. However, it requires that each entity in a CRN needs to be synchronized with the carousel, which is weak against the desynchronization attack. Quite recently, Kim provided the required security features to devise authentication protocol over CRNs, which is based on delegation [15,16]. The analyses are withdrawn from the security problems of Tsai et al.'s secure delegation based authentication protocol in [22] that is weak against the smartcard breach attack and does no use user's identity, which is necessary for the conditional traceability. However, Kim did not provide any detailed solutions for the authentication.

There are two purposes of this paper, which are to withdraw some required distinctive security and privacy features for CRNs and to devise a delegation based user authentication framework based on the requirements. To solve the SU authentication problem in CRNs, we first withdraw some required features for authentication over CRNs focused on not only security but also privacy. They could give researchers guideline to design security and privacy schemes in CRNs. Based on the features, we propose a delegation based user authentication framework, which also has the purpose of solving the security and privacy problems in Tsai et al.'s protocol. We can argue that this is the first delegation based authentication for CRNs. For the privacy aspect, we consider unlinkability, context privacy and anonymity in the proposed framework. To secure CRNs, the proposed framework sets up goals to achieve PU protection, no registration and conditional traceability. We use Elliptic Curve Cryptosystem as the basic security building block to achieve the security and privacy goals of the proposed framework. It needs the similar computational cost with the other existing delegation based authentications but provides the required security and privacy features in CRNs that are not considered in the other authentications.

In the remainder of this paper, we first introduce the structure of the CRNs focused on ECMA-392, as well as CRN security threats it will have to face and the corresponding required security and privacy features. After that, we propose a delegation based user authentication framework over CRNs with the proper security and performance analyses.

2. Overview of ECMA-392: Cognitive Radio Standard

This section briefs CR technology and reviews ECMA-392 as a CR standard, which could provide basic knowledge to understand the proposed authentication framework. Furthermore, we provide an assumed system model, which should be the basis of the proposed delegation based user authentication framework.

2.1. Cognitive Radio Technology

CR technology is the key technology that enables a CRN to use spectrum in a dynamic manner. The term CR can formally be defined as a radio that can change its transmitter parameters based on interaction with the environment in which it operates [23]. CRNs use a cognition cycle, which observes its environment and modifies its transmission characteristics accordingly, that includes radio scene analysis, channel state estimation and predictive modelling, and transmit power control and spectrum management commands by using following CR functions [1,24]:

- Spectrum sensing: Ability to scan the spectral band, identify vacant channels available for opportunistic transmission and determine a list of spectrum bands that are available. Since SUs do not get any direct feedback from PUs regarding their transmission, SUs have to depend on their own individual or cooperative sensing ability to detect PU transmissions.
- Spectrum analysis and decision: It decides on the most appropriate band from the list of available bands according to their quality of service requirements. It is important to characterize the spectrum band in terms of both radio environment and the statistical behaviors of the PUs.
- Spectrum sharing: It provides the capability to share the spectrum resource opportunistically with multiple SUs which allocates resources to avoid interference caused to the PUs. This function necessitates a CR medium access control (MAC) protocol, which facilitates the sensing control to distribute the sensing task among the coordinating SUs as well as spectrum access to determine the timing for transmission.
- Spectrum mobility: It refers to the agility of CRNs to dynamically switch between spectrum accesses. As SUs are not guaranteed continuous spectrum access in any of the licensed bands and the availability of vacant spectrum bands frequently changes over time, spectrum mobility becomes an important factor when designing cognitive protocols.

From this definition, two main characteristics of the CR can be defined as follows [25]

- Unlicensed usage of spectrum: In spectrum sharing, the FCC allocates spectrum for unlicensed or shared services.
- Higher priority of PUs: When an PU is detected in a given band, all SUs avoid accessing that band. However, when a SU is detected, other SUs may choose to share that same band. In other words, PUs have higher priority than SUs in accessing spectrum resources.

2.2. ECMA-392

ECMA-392 is launched as the first step towards realizing CR applications by creating and adopting industrial standard, called the first industrial standard for personal or portable devices in the TVWS [26]. ECMA-392 was mainly designed for communication between personal or portable devices as shown in Figure 1; specifically, in-home multimedia distribution. It supports both mesh and centralized networks. The standard defines an orthogonal frequency division multiplexing physical layer with modulation schemes of quadrature phase shift keying, 16-quadrature amplitude modulation (QAM), and 64-QAM. For forward error correction, concatenation of a Reed-Solomon outer code and a

convolutional inner code with puncturing provides five different coding rates. Channel widths of 6, 7, and 8 MHz are supported for TV channels in any regulatory domain. The maximum data rate of ECMA-392 is 31.64 MBPS. To protect PUs, dynamic frequency selection and transmit power control are included in the specifications.

Figure 1. Network configuration for ECMA-392.

The interoperability of various 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. 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.

2.3. Assumed System Model

This paper considers a CRN with a set of PUs and some unlicensed SUs, which is based on centralized structure as shown in Figure 2. Basically, the CRN consists of more than two networks, a primary network (*PN*) and some secondary networks. The centralized server in CRN, denoted as *SN*, performs CR functions by considering the presence of PUs by using common control channel [27,28]. Also, we can consider any CRN access model like overlay and underlay depending on the target application. However, we assume overlay as a mandatory access model. Furthermore, we assume that any SU should be supported by SU's registered *PN* and there should be any simple relationship between *SN* and *PN* as the same as in [29]. Only after SUs authenticated by the *SN* via *PN*, SUs can opportunistically use the free spectrum in the *SN*. However, SUs should follow the spectrum access policy and avoid interference to PU. That means that the concerned SU should quit the occupied band immediately and use new spectrum if it interferes to any PUs.

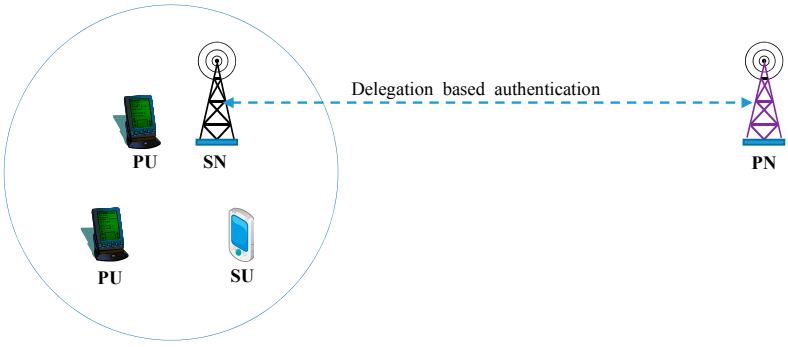

Figure 2. Assumed system model.

3. CRN Threats and Required Features

The purpose of this section is to extract out some required security and privacy features for the SU authentication over CRNs focused on ECMA-392 standard after briefly reviewing security and privacy threats on CRNs.

3.1. Threats on CRN

Attacks on CRNs could be defined as any activity that results in unacceptable interference to the licensed PUs or missed opportunities for SUs. When emulating a PU, a malicious entity can reduce the availability of spectrum for SUs. The misbehaving nodes can be categorized as [19,30–35]

- Selfish nodes: They seek to maximize their own gains at the expense of others.
- Malicious nodes: They act to degrade the system or individual node performance with no explicit intention to maximize their own gains and act as a PU and transmit false information to the SU.

An attack is considered strong if it involves a minimal number of adversaries performing minimal operations but causing maximum damage or loss to the PUs and or SUs in the network. A brief summary of these attacks is given in Table 1 [19,30–42].

Table 1. CRN attacks and properties.

Attacks	Properties
Intentional jamming attack [30–32] PU receiver jamming attack [30–32] Sensitivity amplifying attack [30–32] Overlapping SU attack [33]	SU jams PUs and the other SUs
Biased utility attack [33,34] Asynchronous sensing attack [35–38] Byzantine attack [39] False feedback attack [33] Selfish misbehaviour attack [39,40]	SU tweaks parameters of the utility function
Network Endo-parasite attack [33,34] Channel Ecto-parasite attack [33,34] Low cost ripple effect attack [33,34]	SU attempts to increase the interference
Key depletion attack [33,34]	High round trip times and frequent retransmissions increase key usage
Any attacks against confidentiality, integrity, authentication, non-repudiation, access control, and availability [19,33]	Any attacks on below layers from application layer impact adversely on the layer
Jellyfish attack [41] Routing information jamming attack [42]	Performed in a network layer but affected to the other layers

3.2. Required Security and Privacy Features

Security and privacy are essential in any networks. Security has been relatively well studied than privacy. In the context of CRNs, the main security goals include confidentiality, integrity, authentication, non-repudiation, access control and availability as the general networks. We will only consider the following authentication due to the main focus of this paper.

- Authentication: It assures that the communicating entity is the one that it claims to be. There is an inherent requirement to distinguish between PUs and SUs. Therefore, authentication can be considered as one of the basic requirements for the security and privacy of CRNs. The primary objective of an authentication is to prevent unauthorized users from gaining access to the protected systems. It is a necessary procedure for verifying both an entity's identity and authority. Several aspects of authentication issues should be considered when securing collaborative works in CRNs.

Compared with the security, privacy issues have received little attention in CRNs so far. Privacy is primarily regarded as preserving the anonymity of network entities. The definition of privacy also varies with the application scenarios [12–16]. In the context of CRNs, we consider the following privacy services indispensable

- Unlinkability: Different communication sessions associated with the same user should not be linkable. An adversary cannot link the communication activities of a particular user together and thus establish the user's profile, which contains much private information.
- Context privacy: An adversary should not be able to learn the exact access context information (duration, type of service request, etc.) of a SU without the SU's prior approval or knowledge.
- Anonymity: The identity of the origin and the destination of a conversation is hidden from adversaries unless it is intentionally disclosed by the user. Anonymity mechanisms should allow SUs to use the network services while protecting the identity or other identification information from possible abuse. For keeping SU anonymous, there should not be possibility to link any parameters of the SU identity with any context-based information.

By considering with the above privacy services, authentication service needs to provide the following features over CRNs. In CRNs, users are divided into two categories: (i) PUs or incumbent users that hold a license for a specific portion of the spectrum, and (ii) SUs that use parts of the spectrum in an opportunistic way, so as not to cause harmful interference to the PUs [15,16,19].

- PU protection: SUs can borrow idle spectrum from those who hold licensees, PUs, without causing harmful interference. Unlike traditional radios, CRs constantly monitor the spectrum and intelligently share the spectrum in an opportunistic manner, both in licensed and unlicensed bands. The most important regulatory aspect of these networks is that SUs must relinquish their operating channels and move to another available channel as soon as they learn or sense the presence of a PU on that channel.
- No registration: A fundamental characteristic of a CR is its ability for spectrum sensing, as it shall use the spectrum in an opportunistic manner. This means that the SU has to vacate a currently used spectrum band if a PU signal is detected. Thereby, it is necessary for SUs not to be registered to ***SN***.
- Conditional traceability: Under SU misbehavior, the SU acts maliciously by providing false information about sensing and resource requirements. By doing so, they can either access more resources or prevent other SUs from gaining fair access. Thereby, both of ***SN*** and ***PN*** need to take rights to trace the misbehaving users.

Thereby, it is necessary to provide the required security features on the proposed SU authentication over CRNs. Table 2 summarizes the required security features for the SU authentication in CRNs by providing comparisons with the generalized networks.

Table 2. Comparison of required security features in authentication.

Feature \ Network	General Network	CRN
Consideration of PU protection	Not required	Required
Relationship between *SN* and *PN*	Required	Need not or need partially for traceability
Authentication when SU visits the other networks	Delegation	Delegation

4. Delegation Based User Authentication Framework

Unlike the traditional radios, CRNs constantly monitor the spectrum and intelligently share the spectrum in an opportunistic manner, both in the licensed bands, *PN*s and the unlicensed bands, *SN*s.

It means that SUs over CRNs could borrow idle spectrum from PUs who hold licenses without causing harmful interference. Thereby, in our delegation based user authentication framework, SUs should be serviced by *SN* over the CRN by delegating authentication from *PN*, which achieves the security and privacy from selfish nodes and malicious nodes by providing authentication, unlinkability, context privacy, anonymity, PU protection, no registration and conditional traceability. Thereby, this section proposes a delegation based user authentication framework as a basic security and privacy module for CRNs over the assumed system model.

The concept of delegation is used in various business corporations. In a business corporation, manager uses his (or her) private key to sign a document and his (or her) staff can verify the document based on manager's public key. If the manager cannot sign a document because he (or she) is away on business, he (or she) can delegate the signature authority to his (or her) trustworthy assistant to sign the document without giving the assistant his (or her) private key. His (or her) staff member verifies that the document is still based on the manager's public key. The proposed authentication framework also uses this delegation concept for SU authentication, which uses *PN* for the manager and *SN* for the staff.

There are three phases in the proposed authentication framework, setup, online authentication and offline authentication based on Table 3 notations. Authentication is divided into two parts, online and offline. In the online authentication, the process requires that *SN* must connect to *PN* when a new SU demands authentication. However, without connecting to *PN*, offline authentication is performed by *SN* locally according to the parameters obtained from *PN* in advance. Note that the first authentication must be performed on-line and the subsequent authentications can be continually performed offline.

Table 3. Notations.

Notation	Definition
p, q	The prime numbers satisfying $q \mid (p\text{-}1)$
g	A generator in Z_p
ID_{SU}, ID_{SN}, ID_{PN}	The identities of SU, *SN* and *PN*
AID_{SU}	The amplified identity of SU
PW_{SU}	The password of SU
$[M]_K$	A symmetric encryption for message M with the key K
K_{PS}	A symmetric key between *SN* and *PN*
G	A cyclic additive group
P	The generator of the cyclic additive group G
$h()$	One way hash function such that $h():Z_p \rightarrow Z_p$
$f()$	One way hash function such that $f():G \rightarrow Z_p$
(K,σ)	A proxy key pair of SU
SK	A session key established between any two parties
$\oplus$	The exclusive-or operation
$\mid\mid$	The string concatenation operation

4.1. Setup and Registration

First of all, *PN* selects two distinct large primes p and q satisfying $q \mid p\text{-}1$ and a generator P in the cyclic additive group G. *PN* chooses two private keys x and x_v, and computes their corresponding public keys $V = x \cdot P$ and $Y_v = x_v \cdot P$, respectively. Then, *PN* shares K_{PS}, x_v and V with *SN* after selecting a random key K_{PS}. *PN* also generates a random k and computes a proxy key pair $K = k \cdot h\ (AID_{SU}) \bmod p$ and $\sigma = x \cdot f(K) \bmod q$ and $W = h\ (AID_{SU} \mid\mid APW_{SU}) \oplus (K,\sigma)$ for each SU, where $h\ ()$ and $f\ ()$ are the secure one-way hash functions and $AID_{SU} = h\ (ID_{SU} \mid\mid d)$ and $APW_{SU} = h\ (PW_{SU} \mid\mid d)$ are the amplified identity and password selected and computed by SU with a random number d. Note that a key pair (K,σ) is used as SU's proxy key. The computed value W, the hash function $h\ ()$ and the public key Y_v are stored in each corresponding SU's smart card, respectively. SU needs to compute $D = h\ (ID_{SU} \mid\mid PW_{SU}) \oplus d$ and store it in the issued smart card after the registration to *PN*.

4.2. Online Authentication

When SU roams to an unlicensed network *SN*, it must use a connection to *SN* via *PN* after the proper authentication. The detailed online authentication phase is as follows

Step1 SU sends a login request to *SN*.

Step2 *SN* generates a new random number n_1, selects the permitted number of sessions, n and makes a response $\{ID_{SN}, n_1, n\}$ to SU, where ID_{SN} is the identity of *SN*.

Step3 SU inserts his (or her) smart card into the card reader and inputs ID_{SU} and PW_{SU}. Smart card generates two random numbers t and n_2, computes a hash chain $N_1 = h(N_2)$, $N_2 = h(N_3)$, . . . , $N_{n\text{-}1} = h(N_n)$ and $N_n = h(n_1||n_2)$, stores the hash chain in its memory and sets N_1 as its current secret of the session. Note that N_1 could be computed after applying n times of hash operations from both of n_1 and n_2. After that, smart card computes $d = D \oplus h(ID_{SU}||PW_{SU})$, $AID_{SU} = h(ID_{SU}||d)$, $APW_{SU} = h(PW_{SU}||d)$, $(K,\sigma) = W \oplus h(AID_{SU}||APW_{SU})$, $r_1 = t \cdot P$, $r_2 = h(t \cdot Y_v) \oplus (K, N_1)$ and $v_1 = \sigma \cdot h(ID_{SN}||ID_{PN}||N_1||n_1||r_1||r_2) + t \bmod p$, and makes a response $\{ID_{SN}, ID_{PN}, r_1, r_2, v_1\}$ to ***SN***.

Step4 ***SN*** first uses x_v to retrieve K and N_1 by computing $r_2 \oplus h(x_v \cdot r_1)$. After that, ***SN*** computes $v_1 \cdot P$ and $h(ID_{SN}||ID_{PN}||N_1||n_1||r_1||r_2)(V \cdot f(K)) + r_1 \bmod p$, and verifies whether the two computed values are the same. If the verification is successful, ***SN*** computes $CT_1 = [N_1||n_1||K]_{K_{PS}}$ and $v_2 = h(ID_{SN}||ID_{PN}||N_1||CT_1)$, which $[]_{K_{PS}}$ is an encryption based on the symmetric key cryptosystem like AES by using the encryption key K_{PS}, and sends $\{ID_{SN}, ID_{PN}, CT_1, v_2\}$ to ***PN***. Otherwise, ***SN*** denies the login request.

Step5 ***PN*** obtains N_1, n_1 and K by decrypting CT_1 with the secret key K_{PS}. After that, ***PN*** computes its corresponding $\sigma = x \cdot f(K) \bmod q$ and $v_2' = h(ID_{SN}||ID_{PN}||N_1||CT_1)$, and validates v_2 by checking whether it is the same with v_2'. Only if the verification is successful, ***PN*** generates a random number n_3, computes $SK_{PU} = h(N_1||n_1||\sigma)$, $CT_2 = [N_1||n_3||ID_{SN}]_{SK_{PU}}$ and $CT_3 = [CT_2||n_3||n_1]_{K_{PS}}$ and makes a response $\{ID_{SN}, ID_{PN}, CT_3\}$ to ***SN***.

Step6 ***SN*** obtains CT_2, n_3 and n_1 by decrypting CT_3 with the secret key K_{PS} and then verifies n_3 and n_1. If the verifications hold, ***SN*** computes $SK_{SS} = h(N_1||n_1||n_3||K)$ and $v_3 = h(ID_{SN}||ID_{PN}||SK_{SS}||CT_2)$, and makes a response $\{ID_{SN}, CT_2, v_3\}$ to SU.

Step7 After computing $SK_{PU}' = h(N_1||n_2||\sigma)$, SU obtains N_1, n_3 and ID_{SN} by decrypting CT_2 with SK_{PU}' and checks the existence of N_1 and ID_{SN} in CT_2. After that SU computes $SK_{SS}' = h(N_1||n_1||n_3||K)$ and $v_3' = h(ID_{SN}||ID_{PN}||SK_{SS}||CT_2)$, and verifies v_3 by comparing it with v_3'. Only if the condition holds, SU authenticates ***SN*** and uses the session key with N_1 for the further communications.

4.3. i-th Offline Authentication

SU retrieves $N_i = h^{(n\text{-}i+1)}(n_1||n_2)$ from the hash chain in his (or her) smart card and sends $[N_i]_{SK_{SS}}$ to ***SN***. Upon receiving $[N_i]_{SK_{SS}}$, ***SN*** decrypts it by using the session key SK_{SS} and computes $h(N_i)$. After that, ***SN*** verifies whether the computed value is the same as the previous key, $N_{i\text{-}1}$. If the condition holds, ***SN*** replaces $N_{i\text{-}1}$ into N_i, and updates $SK_{SS} = h(h(N_i)||SK_{SS})$ and increases i by one.

A hash key chain from two parameters of n_1 and n_2 are very important for the offline authentication as we derived from Step 3 in online authentication. For security considerations, it is not recommendable to perform offline authentication all the time while the first online authentication is successfully finished. Thereby, a predefined n should be set to a reasonable period constraint to perform offline authentication.

5. Security and Privacy Analysis

This section provides analysis on the security along with the privacy and the performance analysis of the proposed delegation based user authentication framework over CRNs. It is reasonable to assume that *PN* is trustworthy because we must register it with SU's private information to obtain the service.

We discuss security and privacy issues on the proposed framework with the hypothesis under the following assumptions:

1. An adversary A can be either a SU or a SN. That means that SU as well as SN can act as an adversary.
2. A can eavesdrop on every communication across public channels. He (or she) can capture any message that is exchanged among SU, SN and PN.
3. A has the ability to alter, delete or reroute the captured message.
4. Information can be extracted from the smart card by examining the power consumption of the card.

5.1. Proof Using BAN Logic

Formal security analysis of the proposed framework is verified with the help of Burrows, Abadi and Needham (BAN) logic [43]. The formal analysis of a network security protocol using BAN logic involves following steps: (1) Converting original scheme statements to their idealized form; (2) Determining the assumptions about the initial state of the system; (3) Representation of the state of the system after executing each statement as logical assertions by attaching logical formulas to each statement; (4) Application of logical postulates to assumptions and assertions.

The following notations are used in formal security analysis using the BAN logic:

- $Q \mid\equiv X$: Principal Q believes the statement X.
- $\#(X)$: Formula X is fresh.
- $Q \mid\Rightarrow X$: Principal Q has jurisdiction over the statement X.
- $\mid \xrightarrow{K} Q$: Principal Q has a public key K.
- $Q \lhd X$: Principal Q sees the statement X.
- $Q \mid\sim X$: Principal Q once said the statement X.
- (X, Y): Formula X or Y is one part of the formula (X, Y).
- $\langle P \rangle_Q$: Formula P combined with the formula Q.
- $Q \overset{SK}{\leftrightarrow} R$: Principal Q and R may use the shared session key, SK to communicate among each other. The session key SK is good, in that it will never be discovered by any principal except Q and R.

In addition, the following four BAN logic rules are used to prove that the proposed framework provides a secure mutual authentication among SU, SN and PN:

Rule 1. Message-meaning rule: $\frac{R \mid\equiv R \overset{Y}{\leftrightarrow} S,\ \ R \lhd \langle X \rangle_Y}{R \mid\equiv S \mid\sim X}$ concerns the interpretation of messages.

Rule 2. Nonce-verification rule: $\frac{R \mid\equiv \#(X),\ \ R \mid\equiv S \mid\sim X}{R \mid\equiv S \mid\equiv X}$ shows how to check that a message is fresh and that the sender believes so as well.

Rule 3. Jurisdiction rule: $\frac{R \mid\equiv S \mid\Rightarrow X,\ \ R \mid\equiv S \mid\equiv X}{R \mid\equiv\ X}$ states that a principal R sill trust the beliefs that S has jurisdiction over.

Rule 4. Freshness-concatenation rule: $\frac{R \mid\equiv \#(X)}{R \mid\equiv \#(X,Y)}$ shows freshness of the entire formula if any given part of a formula is fresh and the formula cannot be altered.

In order to show that the proposed framework provides secure mutual authentication between among SU, SN and PN, we need to achieve the following goals:

Goal 1: $SU \mid\equiv (SU \overset{SK_{SS}}{\leftrightarrow} SN)$

Goal 2: $SU \mid\equiv (SU \overset{SK_{PU}}{\leftrightarrow} PN)$

Goal 3: $SN \mid\equiv (SN \overset{SK_{SS}}{\leftrightarrow} SU)$

Goal 4: $PN \mid\equiv (PN \overset{SK_{PU}}{\leftrightarrow} SU)$

Goal 5: $SN \mid\equiv \mid\equiv (SN \overset{SK_{SS}}{\leftrightarrow} SU)$

Goal 6: $PN \mid\equiv \mid\equiv (PN \overset{SK_{PU}}{\leftrightarrow} SU)$

These goals can be divided in two groups. First of all, for Goals 1 and 3, both parties believe themselves that the key SK_{SS} is a good key for communication between SU and SN and for Goals 2 and 4, SU and PN believe that the key SK_{PU} is a good session key between them. Secondly, for Goals 5 and 6, both entities also believe that the other entity believes in the key.

Idealized form: The arrangement of the transmitted messages among SU, SN and PN in the proposed framework to the idealized forms is as follows:

Message 1. $SU \rightarrow SN$: *Login Request*
Message 2. $SN \rightarrow SU$: ID_{SN}, n_1, n
Message 3. $SU \rightarrow SN$: ID_{SN}, ID_{PN}, $<r_1>_t$, $<r_2>_{Yv}$, $<v_1>_{Yv}$
Message 4. $SN \rightarrow PN$: ID_{SN}, ID_{PN}, $<CT_1>_{K_{PS}}$, $<v_2>_K$
Message 5. $PN \rightarrow SN$: ID_{SN}, ID_{PN}, $<CT_3>_{K_{PS}}$
Message 6. $SN \rightarrow SU$: ID_{SN}, $<CT_2>_{SK_{PU}}$, $<v_3>_{SK_{SS}}$

Assumptions: The following are the initial assumptions of the proposed framework:

A1: $SU \mid\equiv \#(t, n_2)$
A2: $SN \mid\equiv \#(n_1)$
A3: $PN \mid\equiv \#(n_3)$
A4: $SU \mid\equiv (SU \overset{(K, \sigma)}{\leftrightarrow} PN)$
A5: $PN \mid\equiv (PN \overset{(K, \sigma)}{\leftrightarrow} SU)$
A6: $SU \mid\equiv \mid \overset{Y_v}{\rightarrow} SN$
A7: $SN \mid\equiv (SN \overset{K_{PS}}{\leftrightarrow} PN)$
A8: $PN \mid\equiv (PN \overset{K_{PS}}{\leftrightarrow} SN)$
A9: $SU \mid\equiv SN \mid\Rightarrow SU \overset{SK_{SS}}{\leftrightarrow} SN$
A10: $SN \mid\equiv SU \mid\Rightarrow SU \overset{SK_{SS}}{\leftrightarrow} SU$
A11: $SU \mid\equiv PN \mid\Rightarrow SU \overset{SK_{PU}}{\leftrightarrow} PN$
A12: $PN \mid\equiv PN \mid\Rightarrow SU \overset{SK_{PU}}{\leftrightarrow} SU$

Proof.

In the following, we prove the test goals in order to show the secure authentication using the BAN logic rules and the assumptions.

Based on Message 2, we could derive:
Step 1. $SU \lhd ID_{SN}, n_1, n$
According to assumption A2 and the message meaning rule, we could get:
Step 2. $SU \mid\equiv SN \mid\sim (ID_{SN}, n_1, n)$
According to assumption A1 and the freshness concatenation rule, we could get:
Step 3: $SU \mid\equiv \#(ID_{SN}, n_1, n)$
According to Step 2, Step 3 and the nonce verification rule, we could get:
Step 4. $SU \mid\equiv SN \mid\equiv (ID_{SN}, n_1, n)$
Based on Message 3, we could derive
Step 5. $SN \lhd ID_{SN}, ID_{PN}, <r_1>_t, <r_2>_{Yv}, <v_1>_{Yv}$
According to the message meaning rule, we could get:
Step 6. $SN \mid\equiv SU \mid\sim (ID_{SN}, ID_{PN}, <r_1>_t, <r_2>_{Yv}, <v_1>_{Yv})$

According to assumption A1 and the freshness concatenation rule, we could get:
Step 7: $SN \mid\equiv \#(ID_{SN}, ID_{PN}, <r_1>_t, <r_2>_{Yv}, <v_1>_{Yv})$
According to Step 6, Step 7 and the nonce verification rule, we could get:
Step 8. $SN \mid\equiv SU \mid\equiv (ID_{SN}, ID_{PN}, <r_1>_t, <r_2>_{Yv}, <v_1>_{Yv})$
According to Step 8, assumption A6 and the believe rule, we could get:
Step 9. $SN \mid\equiv SU \mid\equiv \mid\overset{Y_v}{\rightarrow} SN$
Based on Message 4, we could derive
Step 10. $PN \lhd ID_{SN}, ID_{PN}, <CT_1>_{K_{PS}}, <v_2>_K$
According to assumptions A5 and A8 and the message meaning rule, we could get:
Step 11. $PN \mid\equiv SN \mid\sim (ID_{SN}, ID_{PN}, <CT_1>_{K_{PS}}, <v_2>_K)$
According to assumption A1 and the freshness concatenation rule, we could get:
Step 12: $PN \mid\equiv \#(ID_{SN}, ID_{PN}, <CT_1>_{K_{PS}}, <v_2>_K)$
According to Step 11, Step 12 and the nonce verification rule, we could get:
Step 13. $PN \mid\equiv SN \mid\equiv (ID_{SN}, ID_{PN}, <CT_1>_{K_{PS}}, <v_2>_K)$
According to Step 13, assumption A7 and the believe rule, we could get:
Step 14. $PN \mid\equiv (PN \overset{K_{PS}}{\leftrightarrow} SN)$
According to Step 13, assumption A12 and the jurisdiction rule, we could get:
Step 15. $PN \mid\equiv (PN \overset{SK_{PU}}{\leftrightarrow} SU)$ (Goal 4)
Based on Message 5, we could derive
Step 16. $SN \lhd ID_{SN}, ID_{PN}, <CT_3>_{K_{PS}}$
According to assumptions A7 and the message meaning rule, we could get:
Step 17. $SN \mid\equiv PN \mid\sim (ID_{SN}, ID_{PN}, <CT_3>_{K_{PS}})$
According to assumption A3 and the freshness concatenation rule, we could get:
Step 18: $SN \mid\equiv \#(ID_{SN}, ID_{PN}, <CT_3>_{K_{PS}})$
According to Step 17, Step 18 and the nonce verification rule, we could get:
Step 19. $SN \mid\equiv PN \mid\equiv (ID_{SN}, ID_{PN}, <CT_3>_{K_{PS}})$
According to Step 19, assumption A8 and the believe rule, we could get:
Step 20. $SN \mid\equiv PN \mid\equiv (PN \overset{K_{PS}}{\leftrightarrow} SN)$
According to Step 19, assumption A10 and the jurisdiction rule, we could get:
Step 21. $SN \mid\equiv (SN \overset{SK_{SS}}{\leftrightarrow} SU)$ (Goal 3)
Based on Message 6, we could derive
Step 22. $SU \lhd ID_{SN}, <CT_2>_{SK_{PU}}, <v_3>_{SK_{SS}}$
According to assumption A4 and the message meaning rule, we could get:
Step 23. SU $\mid\equiv$ SN $\mid(ID_{SN}, <CT_2>_{SK_{PU}}, <v_3>_{SK_{SS}})$
According to assumption A1 and the freshness concatenation rule, we could get:
Step 24: $SU \mid\equiv \#(ID_{SN}, <CT_2>_{SK_{PU}}, <v_3>_{SK_{SS}})$
According to Step 23, Step 24 and the nonce verification rule, we could get:
Step 25. $SU \mid\equiv \mid\equiv (ID_{SN}, <CT_2>_{SK_{PU}}, <v_3>_{SK_{SS}})$
According to Step 25, assumption A4 and the believe rule, we could get:
Step 26. $SU \mid\equiv SN \mid\equiv (SN \overset{SK_{SS}}{\leftrightarrow} SU)$ (Goal 5)
According to assumption A9 and the jurisdiction rule, we could get:
Step 27. $SU \mid\equiv (SU \overset{SK_{SS}}{\leftrightarrow} SN)$ (Goal 1)
According to Step 25, assumption A4 and the believe rule, we could get:
Step 28. $SU \mid\equiv PN \mid\equiv (PN \overset{SK_{PU}}{\leftrightarrow} SU)$ (Goal 6)
According to assumption A11 and the jurisdiction rule, we could get:
Step 29. $SU \mid\equiv (SU \overset{SK_{PU}}{\leftrightarrow} PN)$ (Goal 2)

5.2. Casual Analysis

In this section, we provide casual security and privacy analysis of the proposed framework and provide a comparison among the related protocols in [21,22] with the proposed framework as summarized in Table 4.

Table 4. Security and privacy feature comparison among the related protocols.

Feature	Protocol	Kim's in [21]	Tsai et al.'s in [22]	Proposed Framework
Security Issue	PU protection	Provide	N/A	Provide
	No registration	N/A	Provide	Provide
	Weakness	Weak against carousel Desynchronization attack	Weak against smartcard breach attack	No security weakness
Privacy Issue	UL and CP	N/A	N/A	Provide
	UA	Provide	N/A	Provide
	NR and CT	Provide	N/A	Provide

UL: Unlinkability, CP: Context privacy, UA: User anonymity, NR: Nonrepudiation, CT: Conditional traceability.

5.2.1. Unlinkability and Context Privacy

The proposed framework securely sends the authentic value (K, N_1) such that unlinkability (UL) is achieved. Even if adversaries attempt to trace whether a legal SU has previously requested to login SN via PN, they will not be able to plot this attack successfully. In each online authentication session, the authentic messages $\{ID_{SN}, ID_{PN}, r_1, r_2, v_1\}$ in Step3 of online authentication are always different in each trial, since the contents of the message are randomized by the random number t and the session dependent key N_1. It is impossible to link two different values $\{r_1, r_2, v_1\}$ into the same SU even all the authentic messages are learned by the adversary. In addition, without knowing the private key of SN, adversaries cannot retrieve the value (K, N_1) from the variable $r_2 = h(t \cdot Y_v) \oplus (K, N_1)$ that is sent from SU in Step3 of online authentication phase. Adversaries even cannot know any contexts of the messages from a session or some sessions due to UL and confidentiality on the messages.

5.2.2. Anonymity of SU

Various network protocols provide weak user anonymity (UA) since user must deliver his (or her) real identity to the network for authentication. However, in the proposed framework, the real identity of SU is never transmitted over the entire network for authentication purposes. Because we use pseudonym AID_{SU} generated by SU in the registration phase to represent the identity of SU in the network, no one except PN can obtain any information about the identity of SU. Even SN can only verify the legality of SU based on the public key of PN in Step 4 of online authentication, which discloses nothing about the identity of SU. Hence, the proposed framework provides UA.

5.2.3. Nonrepudiation and Conditional Traceability

No doubt, public key based systems can provide conditional traceability (CT) by benefitting of nonrepudiation (NR) feature from the public key cryptosystem. In the proposed framework, each SU gets a different pair key from PN in the registration phase, which has a connection between the identity of SU and the secret key of PN. This authorization makes SN transfer its trust in PN to the requested legal pseudonym of SU. Because only PN has the ability to authorize SU to sign on his (or her) behalf, PN cannot deny this in the event a disputation occurs. Of course, PN has the ability to identify the misused SU. Thus, the proposed framework can also provide the feature of CT.

5.3. Performance Analysis

In this section, we provide performance analysis of the proposed framework in terms of the computational complexity by comparing it with the other related protocols in [21,22]. The computational overhead analysis of any cryptographic protocol is generally conducted by focusing on operations performed by each party within the protocol. Therefore, to analyze the computational costs, we concentrated on the operations of the online authentication only that are required by the parties in the network: namely a user and two networks. In order to facilitate the analysis of the computational costs, we define the following notations.

- T_h: the time to execute a one-way hash operation
- T_s: the time to compute a symmetric key encryption or decryption
- T_e: the time to compute an encryption or decryption operation in ECC-160 algorithm

In order to achieve accurate measurement, we performed an experiment. This experiment was performed using the Crypto++ Library [44] on a system using the 64-bits Windows 7 operating system, 3.2 GHz processor, 4 GB memory, Visual C++ 2013 Software, the SHA-1 hash function, the AES symmetric encryption/decryption function, and the ECC-160 function. According to our experiment, T_h is nearly 0.0002 seconds, T_s is nearly 0.0087 seconds and T_e is nearly 0.6 seconds.

Table 5 shows a comparative analysis of the computational cost among the related protocols. Even though the proposed framework has similar computational overhead with the other protocols, as shown in Table 4, the proposed framework could assure higher security and privacy than the others, and afford resistance to the most well known attacks while providing the functionality required for CRNs.

Table 5. Performance comparison among the related protocols.

Overhead \ Protocol	Kim's in [21]	Tsai et al.'s in [22]	Proposed Framework
SU (MS)	$6T_h+5T_s$	$3T_h+2T_e$	$9T_h+1T_s+2T_e$
SN (VLR)	$6T_h+5T_s+1T_e$	$3T_h+2T_s+2T_e$	$6T_h+2T_s+2T_e$
PN (HLR)	$1T_h+2T_s+1T_e$	$1T_h+3T_s$	$3T_h+2T_s+1T_e$
Total	$13T_h+12T_s+2T_e$	$7T_h+5T_s+4T_e$	$18T_h+5T_s+5T_e$

6. Conclusions

CRNs can access the under-utilized spectrum in an opportunistic manner. However, as CRNs are wireless in nature, they face all common security threats present in traditional wireless networks and should even consider additional security and privacy aspects focused on CR technology. This paper has withdrawn some required security and privacy features focused on ECMA-392, which are unlinkability, context privacy, anonymity, PU protection, no registration and conditional traceability. We have proposed a delegation based user authentication framework as a basic security and privacy solution over CRNs, which is based on the withdrawn security and privacy features. The proposed framework has two purposes of solving the security and privacy problems in Tsai et al.'s protocol and proposing the first delegation based authentication for CRNs. Security and privacy analyses show that the proposed framework supports unlinkability, context privacy, anonymity, PU protection, no registration and conditional traceability, which are the required aspects in CRNs.

Acknowledgments: This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

Author Contributions: Hyunsung Kim leaded the research and devised the proposed framework, while Eun Kyung Ryu performed security and privacy analysis of the proposed framework together with additional improvements advices of the framework.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mitola, J. Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio. Ph.D. Thesis, KTH Royal Institute of Technology, Stockholm, Sweden, 2000.
2. Liu, K.J.R.; Wang, B. *Cognitive Radio Networking and Security*; Cambridge University Press: Cambridge, UK, 2011; ISBN 0521762316 9780521762311.
3. Facilitating the Provision of Spectrum-Based Services to Rural Areas and Promoting Opportunities for Rural Telephone Companies to Provide Spectrum-Based Services. Available online: https://www.fcc.gov/document/facilitating-provision-spectrum-based-services-rural-areas-and-promoting-opportunities-2 (accessed on 30 November 2017).
4. Guimaraes, D.A.; Silva, C.R.N.; Souza, R.A.A. Cooperative spectrum sensing using eigenvalue fusion for OFDMA and other wideband signals. *J. Sens. Actuator Netw.* **2013**, *2*, 1–24. [CrossRef]
5. Stevenson, C.R.; Chouinard, G.; Lei, Z.; Hu, W.; Shellhammer, S.J.; Caldwell, W. IEEE 802.22: The first cognitive radio wireless regional area network standard. *IEEE Commun. Mag.* **2009**, *47*, 130–138. [CrossRef]
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. Available online: https://mentor.ieee.org/802.22/dcn/13/22-13-0151-00-000b-802-22b-draft-1-0.pdf (accessed on 29 November 2017).
7. IEEE 802.11, IEEE 802.11af/D1.01 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: TV White Spaces Operation. Available online: https://pdos.csail.mit.edu/archive/decouto/papers/802.11a.pdf (accessed on 29 November 2017).
8. Khattab, A.; Bayoumi, M.A. An overview of IEEE standardization efforts for cognitive radio networks. In Proceedings of the 2015 IEEE International Symposium on Circuits and Systems, Lisbon, Portugal, 24–27 May 2015; pp. 982–985.
9. Um, J.; Hwang, S.; Jeong, B.J. A Comparison of PHY Layer on the Ecma-392 and IEEE 802.11af Standards. In Proceedings of the Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), Stockholm, Sweden, 18–20 June 2012; pp. 315–319.
10. Mao, H.; Zhu, L. An investigation on security of cognitive radio networks. In Proceedings of the International Conference on Management and Service Science, Wuhan, China, 2–14 August 2011; pp. 1–4.
11. Mansour, I.; Chalhoub, G.; Lafourcade, P. Key Management in Wireless Sensor Networks. *J. Sens. Actuator Netw.* **2015**, *4*, 251–273. [CrossRef]
12. Akyildiz, I.F.; Lee, W.Y.; Chowdhury, K.R. CRAHNs: Cognitive radio ad hoc networks. *Ad Hoc Netw.* **2009**, *7*, 810–836. [CrossRef]
13. Kim, H. Security on Cognitive Radio—Effort on IEEE 802.22. In Proceedings of the Conference on Convergence, Smart and Cloud, Daegu, Korea, 14–16 October 2012; pp. 73–80.
14. Jang, D.; Kim, H. Security standardization status of ECMA-International for personal/portable devices supporting cognitive radio networking. *J. Secur. Eng.* **2011**, *8*, 553–565.
15. Kim, H. Security aspects analysis for secondary user authentication over cognitive radio network. In Proceedings of the Conference on Convergence, Smart and Cloud, Daegu, Korea, 14–16 October 2013; pp. 56–59.
16. Kim, H. Analysis on delegation-based authentication protocol for wireless roaming service. *IEEE Commun. Lett.* **2014**, *16*, 1100–1102.
17. Zhang, T. Security Issues in Cognitive Radio Networks. Ph.D. Thesis, University of Calgary, Calgary, AB, Canada, 2014.
18. Katiyar, H.; Rastogi, A.; Agarwal, R. Cooperative communication: A review. *IETE Tech. Rev.* **2011**, *28*, 409–417. [CrossRef]
19. Kim, H. Privacy preserving security framework for cognitive radio networks. *IETE Tech. Rev.* **2013**, *30*, 142–148. [CrossRef]
20. Wang, C.; Guo, J. Public-keys-based entity authentication protocol with digital signature for cognitive radio networks. *Lect. Notes Electr. Eng.* **2012**, *140*, 341–346. [CrossRef]
21. Kim, H. Location-based authentication protocol for first cognitive radio networking standard. *J. Netw. Comput. Appl.* **2011**, *34*, 1160–1167. [CrossRef]

22. Tsai, J.; Lo, N.; Wu, T. Secure Delegation-Based Authentication Protocol for Wireless Roaming Service. *IEEE Commun. Lett.* **2012**, *16*, 1100–1102. [CrossRef]
23. Notice of Proposed Rule Making and Order. Available online: http://web.cs.ucdavis.edu/~liu/289I/Material/FCC-03-322A1.pdf (accessed on 30 November 2017).
24. Ding, G.; Wang, J.; Wu, Q.; Zhang, L.; Zou, Y.; Yao, Y.D.; Chen, Y. Robust spectrum sensing with crowd sensors. *IEEE. Trans. Commun.* **2014**, *62*, 3129–3143. [CrossRef]
25. Raychaudhuri, D.; Jing, X.; Seskar, I.; Le, K.; Evans, J.B. Cognitive radio technology: From distributed spectrum coordination to adaptive network collaboration. *Pervasive Mob. Comput.* **2008**, *4*, 278–302. [CrossRef]
26. Baykas, T.; Kasslin, M.; Cummings, M.; Kang, H.; Kwak, J.; Paine, R.; Reznik, A.; Saeed, R.; Shellhammer, S.J. Developing a Standard for TV White Space Coexistence: Technical Challenges and Solution Approaches. *IEEE Wirel. Commun.* **2012**, *19*, 10–22. [CrossRef]
27. Liang, Y.C.; Chen, K.C.; Li, G.Y.; Mähönen, P. Cognitive radio networking and communications: An overview. *IEEE Tran. Veh. Tech.* **2011**, *60*, 3386–3407. [CrossRef]
28. Chakravarthy, V.; Li, X.; Wu, Z.; Temple, M.A.; Garber, F.; Kannan, R.; Vasilakos, A. Novel overlay/underlay cognitive radio waveforms using SD-SMSE framework to enhance spectrum efficiency-Part I: Theoretical framework and snalysis in AWGN channel. *IEEE Trans. Commun.* **2009**, *57*, 3794–3804. [CrossRef]
29. Parvin, S.; Han, S.; Tian, B.; Hussain, F.K. Trust-Based Authentication for Secure Communication in Cognitive Radio Networks. In Proceedings of the 2010 IEEE/IEIP International Conference on Embedded and Ubiquitous Computing, Hong Kong, China, 11–13 December 2010; pp. 589–596.
30. Slimeni, F.; Scheers, B.; Chtourou, Z.; Nir, V.L. Jamming mitigation in cognitive radio networks using a modified Q-learning algorithm. In Proceedings of the 2015 International Conference on Military Communications and Information Systems, Cracow, Poland, 18–19 May 2015.
31. Slimeni, F.; Scheers, B.; Chtourou, Z. Security threats in military cognitive radio networks. In Proceedings of the 2015 International Conference on Military Communications and Information Systems, Cracow, Poland, 18–19 May 2015.
32. Al-Hraishawi, H.; Baduge, G.A.A.; Schaefer, R.F. Artificial noise-aided physical layer security in underlay cognitive massive MIMO systems with pilot contamination. *Entropy* **2017**, *19*, 349. [CrossRef]
33. Li, J.; Feng, A.; Feng, Z.; Zhang, P. A survey of security issues in cognitive radio networks. *China Commun.* **2015**, *13*, 132–150. [CrossRef]
34. Naveed, A.; Kanhere, S.S. NIS07-5: Security vulnerabilities in channel assignment of multi-radio multi-channel wireless mesh networks. In Proceedings of the IEEE Globecom, San Francisco, CA, USA, 11 November–1 December 2006; pp. 1–5.
35. Zhang, J.; Cai, L.; Zhang, S. Malicious cognitive user identification algorithm in centralized spectrum sensing system. *Futur. Int.* **2017**, *9*, 79. [CrossRef]
36. Ye, F.; Zhang, X.; Li, Y. Comprehensive reputation-based security mechanism against dynamic SSDF attack in cognitive radio networks. *Symmetry* **2016**, *8*, 147. [CrossRef]
37. Ye, F.; Zhang, X.; Li, Y.; Tang, C. Faithworthy collaborative spectrum sensing based on credibility and evidence theory for cognitive radio networks. *Symmetry* **2017**, *9*, 36. [CrossRef]
38. Guimarães, D.A.; Souza, R.A.A.; Barreto, A.N. Performance of cooperative eigenvalue spectrum sensing with a realistic receiver model under impulsive noise. *J. Sens. Actuator Netw.* **2013**, *2*, 46–69. [CrossRef]
39. Zhang, L.; Ding, G.; Wu, Q.; Zou, Y.; Han, Z.; Wang, J. Byzantine Attack and Defense in Cognitive Radio Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1341–1363. [CrossRef]
40. Wu, H.; Hui, N.; Zhou, X.; Bai, B. Puzzle-based selfish behavior punishment mechanism of MAC layer in cognitive radio networks. In Proceedings of the IET 3rd International Conference on Wireless, Mobile and Multimedia Networks, Beijing, China, 26–29 September 2010; pp. 213–216.
41. Das, D.; Das, S. Intelligent resource allocation scheme for the cognitive radio network in the presence of primary user emulation attack. *IET Commun.* **2017**, *15*, 2370–2379. [CrossRef]
42. El-Malek, A.H.A.; Salhab, A.M.; Zummo, S.A. New bandwidth efficient relaying schemes in cooperative cognitive two-way relay networks with physical layer security. *IEEE Trans. Veh. Technol.* **2017**, *66*, 5372–5386. [CrossRef]
43. Burrow, M.; Abadi, M.; Needham, R. A Logic of Authentication. *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36. [CrossRef]

44. Dai, W. Crypto++ Library 5.6.1. Available online: http://www.cryptopp.com (accessed on 5 December 2016).