A New Fuzzy Key Generation Method Based on PHY-Layer Fingerprints in Mobile Cognitive Radio Networks

Ning Gao[12], Xiaojun Jing[12], Songlin Sun[12], Junsheng Mu[12] and Xiang Lu[3]
[1] School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[2] Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education, Beijing University of Posts and Telecommunications
[e-mail: gaoningfly@163.com]
[3] Institute of Information Engineering, Chinese Academy of Sciences, 100095 Beijing, China
*Corresponding author: Ning Gao

Received February 2, 2016; revised April 20, 2016; accepted June 5, 2016; published July 31, 2016

Abstract

Classical key generation is complicated to update and key distribution generally requires fixed infrastructures. In order to eliminate these restrictions researchers have focused much attention on physical-layer (PHY-layer) based key generation methods. In this paper, we present a PHY-layer fingerprints based fuzzy key generation scheme, which works to prevent primary user emulation (PUE) attacks and spectrum sensing data falsification (SSDF) attacks, with multi-node collaborative defense strategies. We also propose two algorithms, the EA algorithm and the TA algorithm, to defend against eavesdropping attacks and tampering attacks in mobile cognitive radio networks (CRNs). We give security analyses of these algorithms in both the spatial and temporal domains, and prove the upper bound of the entropy loss in theory. We present a simulation result based on a MIMO-OFDM communication system which shows that the channel response characteristics received by legitimates tend to be consistent and phase characteristics are much more robust for key generation in mobile CRNs. In addition, NIST statistical tests show that the generated key in our proposed approach is secure and reliable.

Keywords: Fuzzy key generation, PHY-layer security, PUE, SSDF, Mobile CRNs

1. Introduction

With the successive emergence in recent years of Bluetooth, ZigBee, UWB, RFID, Wibree, Z-Wave, and NFC, demand for more spectral resources has been growing significantly. However, according to recent studies, the utilization of the licensed radio spectrum is extremely low [1, 2]. To address this problem, researchers have proposed cognitive radio networks (CRNs) to increase the efficiency of spectrum utilization by enabling unlicensed, secondary users (SUs) equipped with CR functionality to co-exist with licensed, primary users (PUs). SUs have different features in terms of expenditure, communication distance, and networking capacity, but one problem with all the SUs is common: security of these users in CRNs. For example, due to the open nature of wireless communications—there is no physical boundary in CRNs—networks are susceptible to various attacks including eavesdropping, tampering, man-in-the-middle (MITM), and denial of service (DoS). One popular attack is called a primary user emulation (PUE) attack, in which the attacker may transmit with high power or emulation the specific features of a PU's signal and occupy the whole available spectrum by themselves, or waste the whole available spectrum when PUs are sleeping in CRNs. Another typical type of attack is the Spectrum Sensing Data Falsification (SSDF) attacks, in which the malicious attackers send a modified spectrum sensing result to the central combiner in a multi-node collaborative spectrum sensing strategy. Researchers have intensively studied both PUE attacks and SSDF attacks in the past few years [3-6].

Use of physical-layer security techniques can efficiently reduce the probability of a successful PUE attack to fill these gaps. R. Chen et al. [3] proposed a RSS-based method to detect the location of the attacker by deploying an additional sensor network. In order to enhance the positioning accuracy, L. Huang et al. [7] proposed a joint position verification method using the theories of both time difference of arrival (TDOA) and frequency difference of arrival (FDOA). Y. Liu et al. [8] introduced a helper node to defend against PUE attacks. The helper node acts as a "bridge" to enable SUs to verify cryptographic signatures carried by the helper node's signals using its private key, then learn the helper node's authentic link signatures, and finally verify the primary users' link signatures. However, the helper node's private key is not assumed to be secure across a long storage time. Furthermore, if the keys of cryptographic signatures are captured by PUE attackers, they will mimic the cryptographic signatures of the helper node to authenticate themselves such that an SU cannot distinguish them from a legitimate PU. Thus, updating the private key of cryptographic signatures is better. Z. Yuan et al. [9] proposed a defense strategy against the PUE attack in CRNs using belief propagation based on RSS. They assume that information can be exchanged without errors or falsified data. However, information exchanged between SUs is susceptible to modification or forgery, both in PUE attacks and SSDF attacks. This results in a lower detection rate.

The PHY-layer key generation algorithms solve these problems very effectively. Unlike traditional key generation algorithms such as Diffie-Hellman, which depend on mathematical problems, wireless physical-layer key generation algorithms use the principles of channel reciprocity and channel randomness to extract an identical secret key of two wireless users. This technique does not need to share the secret key beforehand, and its security is influenced by neither the attacker's computing power nor algorithm complexity, and is thus an important method for achieving perfect secrecy as defined by Shannon. [10].

The Received Signal Strength Indicator (RSSI) method is an attractive approach for key generation because it is more intuitive to measure than other physical layer information such

as channel phase [11, 12]. The RSSI value of real-time channels can be measured by SUs; with these values, we can generate a key for encryption. Wilson. R [13] presented numerical results and simulated the key lengths possible for indoor, ultra-wide-band channels. Madiseh. M G et al. [14] used the properties of Hamming (7,3) binary codes to ensure key agreement between the two UWB transceivers. However the UWB signal power is limited, and its envelope is hard to detect. Moreover, the Hamming error correcting code is invalid when the mismatch bit rate is too high. Chen C, Wallace. J. W et al. [15, 16] used a MIMO system to generate key. In this literature, the key generation rate can be greatly improved with the increase of the number of antennas. Aono. T et al. [17] proposed an improved scheme for the secret key generation. According to the controllability of the ESPAR antenna, they can artificially speed up the channel fluctuation and improve the rate at which key update. In order to improve the identity of the key, Azimi-Sadjadi. B et al. [18] applied an ad hoc communication node to generate key from the depth of the envelope and proposed a SFIR scheme. However, this scheme stays at the theoretical level and lacks practical application. Yasukawa. S et al. [19] proposed multi-level quantization, which used the extracted key as both a verify sequence and a candidate sequence. This scheme can improve the identity of the key, but it reduces the extract rate of the effective key. Huyen N T T, Jo M et al. [20] used the theory of the signal range and deployment error knowledge to analyze sensor nodes location information and proposed a polynomial-based key pre-distribution scheme. This scheme provides high connectivity and secure communication with better communication overhead.

Compared to the other key generation algorithms and applications in previous work, our proposed approach has the following advantages and usages:

- We propose a new secret fuzzy key generation scheme that we refer to as a fuzzy key generation scheme. It is based on wireless channel PHY-layer fingerprints information and a fuzzy extractor which is a method to generate strong key from biometric information. In our propose scheme, the running time is a polynomial time (poly($s \log n$)) [21], which is very efficient and only requires a few seconds on general computers.
- We demonstrate applications of our scheme for CRNs. We propose two algorithms to defend against eavesdropping attacks and tampering attacks in multi-node collaborative PUE attacks or SSDF attacks detection strategies. In addition, our scheme can be used to generate key for secure communication or identity authentication, which are applied by PUs or SUs.
- No additional cost is required in our approach for new hardware. In our work, we need to capture channel response characteristics, however, the channel estimate is necessary in most of the communication systems (i.e., OFDM based standards in IEEE 802.11a/g and 802.22). Specifically, 5G wireless communication networks show that the CR transmitters can rely on the channel reciprocity to estimate the channel coefficient themselves [23].

The rest of this paper is organized as follows. Section 2 is the preliminary work. Section 3 proposes two constructions of fuzzy extractor based on channel response characteristics in the Hamming metric. In Section 4, we present two algorithms to defend against eavesdropping attacks and tampering attacks in CRNs. We also present the complete scheme and demonstrate algorithm security in both spatial and temporal domains. Section 5 analyzes the results of the experimental performance. Finally, in Section 6, we summarize this paper.

2. Related Work

In this section, we introduce the preliminaries of key generation on PHY-+layer and fuzzy extraction. The security of our scheme is described as follows: Two legitimate secondary users in two different locations ($SU_l (l \in \{a,b\})$) have strongly correlated information due to the principle of channel reciprocity and the high unpredictability of the generated key for attackers. In fact, an eavesdropper (SU_e) at a third location more than a few wavelengths from SU_l will measure a different, uncorrelated radio channel [24, 25].

2.1 Background

Radio signals propagation from the transmitter to the receiver is generally affected by terrain or obstacles. This results in reflection, diffraction and other phenomena. Different paths have different signal amplitudes and phases. As a result, receivers usually receive multi-path copies of the transmitted signal. Due to multi-path fading, different paths of waves will be strengthened or weakened at the receiver's end. In addition, the Doppler effect makes wireless channel characteristics change distinctly. The received signal, which is the sum of signal copies, provides a wealth of information for key extraction. This behavior is captured by the the wireless channel response characteristics, following the equation

$$\begin{aligned} r(t) &= x(t) * h(t,\tau) \\ &= \Re\left\{\sum_{k=1}^{L} \beta_k(t) u(\tau - \tau_k(t))\right\}, \end{aligned} \tag{1}$$

where L is the number of paths; $\beta_k(t) = \alpha_k(t) e^{j(2\pi f_c \tau_k(t) + \Phi(t,\tau))}$; $\alpha_k(t)$ is a random process, which is a function of path loss and shadowing; the phase term $e^{j(2\pi f_c \tau_k(t) + \Phi_k(t,\tau))}$ is a random process, which represents the phase shift due to the k-th path component's Doppler effect plus any additional phase shifts which are encountered in the channel， f_c is the carrier frequency. Typically, it is assumed that these two random processes are independent.

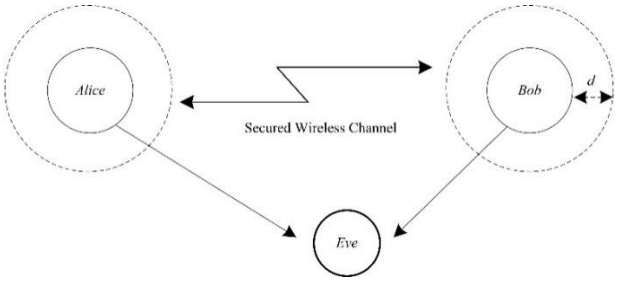


Fig. 1. The difference of channel response characteristics

Many works on key generation from noisy observations of a common random process have been proposed in the cryptography community. In our case, the random processes are mobile wireless channels, which provide a large number of stochastic information. **Fig. 1** illustrates an interesting physical scenario. Set H_{SU_a}, H_{SU_b}, as channel response characteristics of SU_a, SU_b, respectively. The illegitimate user SU_e wants to guess a portion of channel response characteristic values between SU_a and SU_b, which denote as H_{SU_e}. Thus, the

minimum entropy is defined as

$$\mathrm{H}_{\infty}(H_{SU_l}) \overset{def}{=} -\log\left[\max_{h_{SU_l}} \Pr(H_{SU_l})\right]. \tag{2}$$

The predictability of a legitimate random variable H_{SU_l} is $\max_{h_{SU_l}} \Pr(H_{SU_l} = h_{SU_l} \left| H_{SU_e} = h_{SU_e}\right.)$, correspondingly, the average case minimum entropy is defined as

$$\overline{\mathrm{H}}_{\infty}(H_{SU_l} \left| H_{SU_e}\right.) \overset{def}{=} -\log\left\{\Xi_{h_{SU_e} \leftarrow H_{SU_e}}[2^{-\mathrm{H}_{\infty}(H_{SU_l} \left| H_{SU_e}=h_{SU_e}\right.)}]\right\}. \tag{3}$$

Legitimate users SU_l communicate via a wireless channel and generate a shared key based on their respective channel response. However, illegitimate SU_e cannot capture the channel response that legitimate users receive. In this case, wireless channel response characteristics which called a PHY-layer fingerprints denotes as

$$\mathrm{H}_{\infty}(H_{SU_l}) - \overline{\mathrm{H}}_{\infty}(H_{SU_l} \left| H_{SU_e}\right.) \le \varepsilon, \tag{4}$$

where ε is a negligibly small number greater than zero. In other words, we expect that the maximum entropy loss of the extracted key between legitimate users is strictly small.

2.2 Attack Model

We assume two attack models in CRNs, which are an eavesdropping attack and a tampering attack. SU_e is a cognitive radio node equipped with attack functionality, which knows the algorithm of the key generation. Details are described as

1) Eavesdropping attack: In this model, SU_e can listen to the communication between legitimate users SU_l. In addition, during PUE attacks or SSDF attacks detection, SU_e can also measure the channel between herself and an SU_l, in which SU_l measures the channels between them for key generation.
2) Tampering attack: In this model, SU_e can not only listen to the communication between SU_l but also tamper the information which is sent between SU_l. In addition, during PUE attacks or SSDF attacks detection, SU_e can also measure the channels between herself and SU_l, in which each SU_l measures the channel for key generation.

3. Extractor with Channel Response

3.1 Strong Extractor

Let D_{SU_a} and D_{SU_b} be two key distributions on the same domain K. The statistical distance between these two probability distributions is

$$\left\|D_{SU_a} - D_{SU_b}\right\| = \frac{1}{2}\sum_{k\in\mathrm{K}}\left|D_{SU_a}(k) - D_{SU_b}(k)\right|. \tag{5}$$

Furthermore, we can also implement the statistical distance to evaluate the randomness of the generated key by

$$\left\| D_{SU_a} - D_U \right\| \le \mathrm{E}, \tag{6}$$

where D_{SU_l} is the key distribution of SU_l, D_U is uniform distribution on space K, respectively. The distribution of D_{SU_l} is called E-quasi-random on K [26]. The quantized channel response characteristic values of two legitimate users can be written as $Q_{SU_a} = \underset{i\in\{1,2,\cdots,\omega\}}{\|} q_{SU_{a_i}}$, and randomness as $r = \underset{i\in\{1,2,\cdots,\omega\}}{\|} r_i$, $s = \underset{i\in\{1,2,\cdots,\omega\}}{\|} s_i$.

Definition 1: Let *Ext*: $\{0,1\}^{\omega n} \to \{0,1\}^{\ell}$ be a polynomial-time probabilistic function which uses r bits of randomness. We call that *Ext* is an efficient average case $(\omega n, \omega m, \ell, \mathrm{E})$-strong extractor if for all pairs of random variables (Q_{SU_l}, Q_{SU_e}) such that Q_{SU_l} on $\{0,1\}^{\omega n}$ where $\overline{\mathrm{H}}_{\infty}(H_{SU_l} | H_{SU_e}) \ge \omega m$, we obtain $\left\| D_{(Ext(Q_{SU_l},r);Q_{SU_e};r)} - D_{(U_\ell;Q_{SU_e};r)} \right\| \le \mathrm{E}$, where r is uniform on $\{0,1\}^{\omega k}$.

Strong extractors are E-quasi-random, if they can extract at most $\ell = \omega m - 2\log(\frac{1}{\mathrm{E}}) + \mathrm{O}(1)$ bits [21].

Lemma 1: Assume a family of functions $\{H_x : \{0,1\}^{\omega n} \to \{0,1\}^{\ell}\}_{x\in X}$ is universal: we call H_x the generalized leftover hash functions if for all $a \ne b \in \{0,1\}^{\omega n}$, $\Pr_{x\in X}[H_x(a) = H_x(b)] = 2^{-\ell}$. Then, for any random variables Q_{SU_l} and Q_{SU_e},

$$\left\| D_{(H_x(Q_{SU_l});X;Q_{SU_e})} - D_{(U_\ell;X;Q_{SU_e})} \right\| \ge \frac{1}{2}\sqrt{2^{-\overline{\mathrm{H}}_{\infty}(H_{SU_l}|H_{SU_e})+\ell}}. \tag{7}$$

Universal hash functions are $(\omega n, \omega m, \ell, \mathrm{E})$-strong extractors whenever $\ell \le \omega m - 2\log(\frac{1}{\mathrm{E}}) + 2$.

3.2 Secure Sketch

We assume that Ω is a finite set, and will concentrate on the space $\Omega = F^n$ under the Hamming metric. A metric space can be defined as an ordered pair (Ω, d), where Ω is a set and d is a distance function on $\Omega \times \Omega \to R^+$.

Definition 2: An average case $(\Omega, m, \overline{m}, t)$-secure sketch is a pair of randomized procedures, "sketch" (*SS*) and "recover" (*Rec*), with the following properties:

1) The sketching procedure *SS* on input $q_{SU_{a_i}} \subseteq \Omega$ returns a bit string s_i.
2) The recovery procedure *Rec* takes an element $q_{SU_{b_i}} \subseteq \Omega$ and a bit string s_i. The correctness property of secure sketches guarantees that if $d(q_{SU_{a_i}}, q_{SU_{b_i}}) \le t$, then $\mathrm{Re}\, c(q_{SU_{b_i}}; SS(q_{SU_{a_i}})) = q_{SU_{a_i}}$. If $d(q_{SU_{a_i}}, q_{SU_{b_i}}) > t$, then no guarantee is provided about the output of Rec.
3) The security property guarantees that for any distribution $q_{SU_{l_i}}$ over Ω and

$q_{SU_{e_i}}$ over $\{0,1\}^*$ such that $\overline{\mathrm{H}}_\infty(q_{SU_{l_i}} \mid q_{SU_{e_i}}) \geq m$, the value of $q_{SU_{l_i}}$ can be recovered by SU_e who observes s_i with probability no greater than $2^{-\overline{m}}$. That is $\overline{\mathrm{H}}_\infty(q_{SU_{l_i}} \mid (SS(q_{SU_{l_i}}); q_{SU_{e_i}})) \geq \overline{m}$.

The upper bound of entropy loss in the secure sketch can be defined as

$$\begin{aligned} &\overline{\mathrm{H}}_\infty(q_{SU_{l_i}} \mid q_{SU_{e_i}}) - \overline{\mathrm{H}}_\infty(q_{SU_{l_i}} \mid (SS(q_{SU_{l_i}}); q_{SU_{e_i}})) \\ &= m - \overline{m} \\ &= \lambda \end{aligned}$$

Lemma 2: For a known algorithms of *SS*, *Rec* of a secure model with a known value t, and the output of SS has size at most 2^λ, then for any min-entropy threshold m, the value of entropy loss $m - \overline{m} \leq \lambda$.

Proof: If SS has size at most 2^λ values, for any $(q_{SU_{l_i}}, q_{SU_{e_i}})$,

$$\begin{aligned} &\overline{\mathrm{H}}_\infty(q_{SU_{l_i}} \mid (SS(q_{SU_{l_i}}); q_{SU_{e_i}})) \\ &\geq \overline{\mathrm{H}}_\infty((q_{SU_{l_i}}; SS(q_{SU_{l_i}})) \mid q_{SU_{e_i}}) - \lambda \\ &\geq \overline{\mathrm{H}}_\infty(q_{SU_{l_i}} \mid q_{SU_{e_i}}) - \lambda \\ &= m - \lambda \end{aligned}$$

We obtain $m - \overline{m} \leq \lambda$.

3.3 Fuzzy Extractor with Channel Response Characteristics

Well-known techniques from fuzzy commitment scheme [22] and channel response characteristics are combined to achieve a new type of PHY-layer key generation primitive that we refer to as a fuzzy key generation scheme. It is hard for an attacker to learn the encoded value, and also for the decoder to decode a value in more than one way. In order to reduce the error rate, if you want to extract B length bits, $\omega = \frac{B}{n}$ rounds of negotiation are required. We assume the randomized procedures *SS*, *Gen* for SU_a's end and randomized procedures *Rec*, *Rep* for SU_b's end. The i th-round quantization value of the channel response characteristics are $q_{SU_{l_i}} \subseteq Q_{SU_l}$, and neighbors of SU_l share a random number r_0 in advance. In the eavesdropping attack model, the construction of secure sketch under the Hamming metric satisfied

SS:

select random number $r_i \in \{0,1\}^k$;

input $q_{SU_{a_i}}, c \in \{0,1\}^n$;

let $q_{SU_{a_i}} \oplus c(r_i) = s_i$;

store $q_{SU_{a_i}}, r_i$;

send $F_i(s_i \| Hash(q_{SU_{a_i}}))$.

Rec:

input $q_{SU_{b_i}} \in \{0,1\}^n$;

receive $F_i(s_i \| Hash(q_{SU_{a_i}}))$;

for any sequence $q_{SU_{a_i}}, q_{SU_{b_i}}$;

if $dis(q_{SU_{b_i}} \oplus s_i; c(r_i)) \le t$;

then $\mathrm{Re}\, c(q_{SU_{b_i}}, s_i) = f(q_{SU_{b_i}} \oplus s_i) \oplus s_i$;

if $Hash(q'_{SU_{a_i}}) = Hash(q_{SU_{a_i}})$;

then store $q_{SU_{a_i}}, r_i$.

where $f(\cdot)$ is the error correction function of codeword c, $q_{SU_{a_i}}$ and $q_{SU_{b_i}}$ are approximate channel response characteristics , both of them are n-bit strings.

In the tampering attack model, we employ a one-way hash chain $r_0 \to r_1 \cdots \to r_\omega$, where $r_i = Hash(r_{i-1})$. Considering SU_l's costs, for each hash chain, they will only verify $r_i = Hash(r_{i-1})$ to confirm whether F_i has been tampered with or not. The construction of secure sketch under the Hamming metric satisfied

SS:

select random number $r_i = Hash(r_{i-1}) \in \{0,1\}^k$;

input $q_{SU_{a_i}}, c \in \{0,1\}^n$;

let $q_{SU_{a_i}} \oplus c(r_i) = s_i$;

store $q_{SU_{a_i}}, r_i$;

send $F_i(s_i \| r_i \| Hash(q_{SU_{a_i}}))$.

Rec:

input $q_{SU_{b_i}} \in \{0,1\}^n$;

receive $F_i(s_i \| r_i \| Hash(q_{SU_{a_i}}))$;

for any sequence $q_{SU_{a_i}}, q_{SU_{b_i}}$;

if $dis(q_{SU_{b_i}} \oplus s_i; c(r_i)) \le t$ and $r_i = Hash(r_{i-1})$;

then $\mathrm{Re}\, c(q_{SU_{b_i}}, s_i) = f(q_{SU_{b_i}} \oplus s_i) \oplus s_i$;

if $Hash(q'_{SU_{a_i}}) = Hash(q_{SU_{a_i}})$;

then store $q_{SU_{a_i}}, r_i$.

The F_i representing the generated witness, if $r_i = Hash(r_{i-1})$, then the received message has been successfully decoded. Otherwise, F_i is a tampering witness.

A fuzzy extractor of *Gen* and *Rep* can be obtained based on the secure sketch introduced above. We write the expressions as

$$Gen\left\langle \mathop{\|}_{i\in\{1,2,\cdots,\omega\}} r_i; \mathop{\|}_{i\in\{1,2,\cdots,\omega\}} q_{SU_{a_i}} \right\rangle \Rightarrow K, \tag{8}$$

$$\mathrm{Re}\, p\left\langle \mathop{\|}_{i\in\{1,2,\cdots,\omega\}} r_i; \mathop{\|}_{i\in\{1,2,\cdots,\omega\}} q_{SU_{a_i}}; s_i \right\rangle \Rightarrow K. \tag{9}$$

4. Defending Against PUE Attacks and SSDF Attacks in CRNs

In this section, we present the complete fuzzy key generation scheme based on channel response characteristics. Firstly, we describe the fuzzy key generation algorithm combined with the circumstances of CRN channels. Secondly, we design a fuzzy key generation scheme for defending against eavesdropping attacks and tampering attacks. Finally, we summarize the complete scheme and demonstrate security both in spatial and temporal domains.

4.1 Fuzzy Key Generation Algorithm to Defend Against Eavesdropping Attacks

In CRNs, the SU_l will, most likely, group together as a defense to detect the location of the PUEs. No matter how much data is exchanged between the neighboring users, the data which is used as a "belief" to detect the PUE attacks is assumed to also be eavesdropped by SU_e, which is equipped with eavesdropping functionality. Consequently, the accuracy of the PUE attack's detection will be somewhat reduced. Therefore, it is necessary to use an independent key generate-update strategy to encrypt this "belief" data against eavesdropping attacks. We now provide the details of our scheme.

We assume that when the scheme is executed, SU_l alternately measure the channel response between them. After a period of time, SU_a stores a sufficiently large number of channel response characteristic values $q_{SU_{a_i}}$, and SU_b employs the secure sketch to recover $q_{SU_{a_i}}$ from $q_{SU_{b_i}}$. Once the bits extracted are adequate to generate the key, an $(\omega n, \omega m, \ell, \mathrm{E})$-strong extractor is applied to generate the final key. The fuzzy key generation algorithm for defending against eavesdropping attacks we abbreveate as EA algorithm and summarize in Algorithm 1.

Algorithm 1	EA algorithm
Input:	
Channel response characteristic values: [$q_{SU_{a1}}, q_{SU_{a2}}, \cdots, q_{SU_{a\omega}}$].	
Channel response characteristic values: [$q_{SU_{b1}}, q_{SU_{b2}}, \cdots, q_{SU_{b\omega}}$].	
Random number r_0.	
Output:	
A 256-bit secret key K.	

***SUa*'s end:**

1: **for** $i \leftarrow 1$ **to** ω **do**

2: $SS\left\langle r_i; q_{SU_{a_i}} \right\rangle \Rightarrow F_i(s_i \parallel Hash(q_{SU_{a_i}}))$

3: *SUa* sends F_i to *SUb*

4: **if** *SUa* receives command 'reject' (again) from *SUb* **then**

5: *SUa* deletes $q_{SU_{ai}}$ and re-extracts

6: **else**

7: *SUa* stores $q_{SU_{a_i}}, r_i$

8: **end if**

9: **end for**

10: $Gen\left\langle \underset{i\in\{1,2,\cdots,\omega\}}{\parallel} r_i; \underset{i\in\{1,2,\cdots,\omega\}}{\parallel} q_{SU_{a_i}} \right\rangle \Rightarrow K$

***SUb*'s end:**

11: **for** $i \leftarrow 1$ **to** ω **do**

12: $\mathrm{Re}c\left\langle q_{SU_{b_i}}, s_i \right\rangle \Rightarrow q'_{SU_{a_i}}$

13: **if** $Hash(q'_{SU_{a_i}}) = Hash(q_{SU_{a_i}})$ **then**

14: *SUb* stores $q_{SU_{a_i}}, r_i$

15: **else**

16: *SUb* sends command 'reject' (again) to *SUa*

17: *SUb* deletes $q'_{SU_{ai}}$ and re-extracts

18: **end if**

19: **end for**

20: $\mathrm{Re}\, p\left\langle \underset{i\in\{1,2,\cdots,\omega\}}{\parallel} r_i; \underset{i\in\{1,2,\cdots,\omega\}}{\parallel} q_{SU_{a_i}}, s_i \right\rangle \Rightarrow K$

4.2 Fuzzy Key Generation Algorithm to Defend Against Tampering Attacks

The details of the algorithm for defending against tampering attacks are the same as the EA algorithm in the first few steps. The difference is that in multi-node collaborative detection against PUE attacks or SSDF attacks, malicious SU_e have ability to tamper with information exchanging between legitimate users. If SU_e listens to the communication between their legitimate neighbors and tampers with the information which is negotiation between them, Then SU_e will send the "fake" information, spoofing a legitimate user and disrupting the protocol without revealing his presence, which makes it difficult to precisely detect attacks. In this case, SU_a will employ the key generation algorithm proposed here to generate a key through a one-way hash chain from r_i to form a data origin authentication and use the key to encrypt "belief" data for attack detection. Furthermore, without use of the same key as the legitimate sides, the "fake" information send by the malicious SU_e will be rejected. Fuzzy

key generation algorithm to defend against tampering attacks we abbreviate as TA algorithm and summarize in Algorithm 2.

Algorithm 2 TA algorithm

Input

Channel response characteristic values: [$q_{SU_{a1}}, q_{SU_{a2}}, \cdots, q_{SU_{a\omega}}$].

Channel response characteristic values: [$q_{SU_{b1}}, q_{SU_{b2}}, \cdots, q_{SU_{b\omega}}$].

Random number r_0.

Output

A 256-bit secret key K.

***SUa*'s end:**

1: **for** $i \leftarrow 1$ **to** ω **do**

2: $SS\left\langle r_i; q_{SU_{a_i}} \right\rangle \Rightarrow F_i(s_i \parallel r_i \parallel Hash(q_{SU_{a_i}}))$

3: *SUa* sends F_i to *SUb*

4: **if** *SUa* receives command 'reject' (again) from *SUb* **then**

5: *SUa* deletes $q_{SU_{ai}}$ and re-extracts

6: **else**

7: *SUa* stores $q_{SU_{a_i}}, r_i$

8: **end if**

9: **end for**

10: $Gen\left\langle \underset{i\in\{1,2,\cdots,\omega\}}{\parallel} r_i; \underset{i\in\{1,2,\cdots,\omega\}}{\parallel} q_{SU_{a_i}} \right\rangle \Rightarrow K$

***SUb*'s end:**

11: **for** $i \leftarrow 1$ **to** ω **do**

12: $\mathrm{Re}c\left\langle q_{SU_{b_i}}, s_i \right\rangle \Rightarrow q'_{SU_{a_i}}$

13: **if** $r'_i = Hash(r_{i-1}) \,\&\, Hash(q_{SU_{a_i}}) = Hash(q'_{SU_{a_i}})$ **then**

14: *SUb* stores $q_{SU_{a_i}}, r_i$

15: **else**

16: *SUb* sends command 'reject' (again) to *SUa*

17: *SUb* deletes $q'_{SU_{ai}}$ and re-extracts

18: **end if**

19: **end for**

20: $\mathrm{Re}\, p\left\langle \underset{i\in\{1,2,\cdots,\omega\}}{\parallel} r_i; \underset{i\in\{1,2,\cdots,\omega\}}{\parallel} q_{SU_{a_i}}, s_i \right\rangle \Rightarrow K$

4.3 Complete Scheme

Our fuzzy key generation scheme consists of two components, namely quantization and fuzzy generation. In our scheme, SU_a is the initiator of the channel measurements. The fuzzy key generation scheme for SU_a and SU_b is shown in **Fig. 2**.

SU_a transmits probing sequences to SU_b. After receiving the probing sequences, SU_b can collect the channel response's characteristic values on his antennas, then vice versa. Each pair of neighbor nodes SU_l use the secure sketch under the Hamming metric to reconcile information. When both sides have collected enough data, SU_a and SU_b will utilize an $(\omega n, \omega m, \ell, \mathrm{E})$ - strong extractor to complete the key generation.

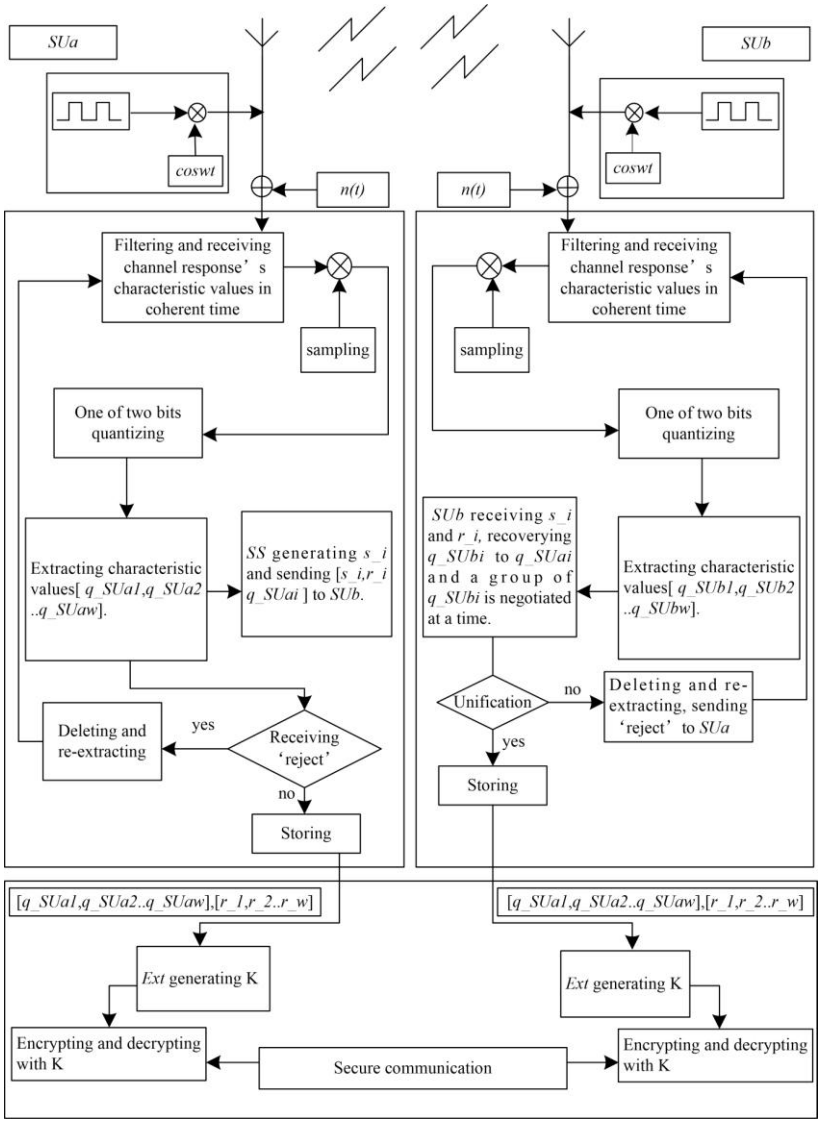


Fig. 2. The complete scheme flow used in fuzzy key generation

4.4 Security Analysis

The spatial security of the scheme is guaranteed based on the previous assumption that the SU_e at a third location whose distance is more than a few wavelengths from either legitimate endpoint will measure a different, uncorrelated radio channel. This spatial security assumption is applied in most PHY-layer security scheme and has been proven correct by practical experience, such as [24, 25]. For example, in view of a mobile CRN system with a moving speed $v = 72$ km/h, average SU_l distance $d = 150$ m, and carrier frequency $f_c = 900$ MHz, if SU_e is located more than 16 cm away from SU_a and SU_b, his observations $q_{SU_{e_i}}$ do not reveal enough correlating information with $q_{SU_{a_i}}$ or $q_{SU_{b_i}}$.

The temporal security is guaranteed based on the fuzzy commitment scheme. A fuzzy commitment scheme allows one to extract some randomness K from Q_{SU_a} and then successfully reproduce K from any string Q_{SU_b} that is close to Q_{SU_a}. The reproduction utilizes the helper string $F = \underset{i\in\{1,2,\cdots,\omega\}}{\|} F_i$, which is produced during the initial extraction, yet F does not need confidentiality, because K looks truly random even given F so long as any two values F_j, F_k are independent.

Lemma 3: Assume (*SS*, *Rec*) is an $(\Omega, m, \overline{m}, t)$-secure sketch, and let *Ext* be an average case $(\omega n, \omega m, \ell, \mathrm{E})$-strong extractor. An $(\Omega, \omega\overline{m}, \ell, t, \mathrm{E})$-fuzzy extractor has two following parts (*Gen*, *Rep*):

$Gen(Q_{SU_a}, r)$
set $F = \underset{i\in\{1,2,\cdots,\omega\}}{\|} F_i, K = Ext(Q_{SU_a}, r)$;
output $K = Ext(Q_{SU_a}, r)$

$\mathrm{Re}\, p(Q_{SU_b}, s, r)$
recover $Q_{SU_b} = \underset{i\in\{1,2,\cdots,\omega\}}{\|} \mathrm{Re}c(q_{SU_{b_i}}, s_i)$;
output $K = Ext(Q_{SU_a}, r)$.

Proof: From the definition 1, we can get *Ext* is an average case $(\omega n, \omega m, \ell, \mathrm{E})$-strong extractor,

$$\left\| D_{[Ext(Q_{SU_l}, r); Q_{SUe}; r]} - D_{[U_\ell; Q_{SU_e}; r]} \right\| \le \mathrm{E}.$$

If (*SS*, *Rec*) is an $(\Omega, m, \overline{m}, t)$-secure sketch and *Ext* is an $(\omega n, \omega m, \ell, \mathrm{E})$-strong extractor given by universal hashing, then we can get lemma 4. Without loss of generality, we assume that min-entropy threshold is m in each round, the upper bound of the entropy loss is given as

Lemma 4: For a known algorithms of *SS*, *Rec* of a secure sketch with a known value t, the output of *SS* has size at most 2^λ. For any min-entropy threshold m, there exists an average case $(\Omega, \omega m - \omega\lambda - 2\log(\frac{1}{\mathrm{E}}) + 2, t, \mathrm{E})$-fuzzy extractor for Q_{SU_l}. The upper bound of the

entropy loss is $\omega\lambda + 2\log(\frac{1}{\mathrm{E}}) - 2$.

Proof: If *SS* has size at most 2^{λ} values, for any $Ext(Q_{SU_l}, r)$,

$$\begin{aligned}
&\overline{\mathrm{H}}_{\infty}(Ext(Q_{SU_l}, r) \mid (SS(Q_{SU_l}); Q_{SU_e})) \\
&\geq \overline{\mathrm{H}}_{\infty}((Ext(Q_{SU_l}, r); SS(Q_{SU_l})) \mid Q_{SU_e}) - \omega\lambda \\
&\geq \overline{\mathrm{H}}_{\infty}(Ext(Q_{SU_l}, r) \mid Q_{SU_e}) - \omega\lambda \\
&= \omega m - 2\log(\frac{1}{\mathrm{E}}) + 2 - \omega\lambda .
\end{aligned}$$

We obtain $\omega m - \omega\overline{m} \leq \omega\lambda + 2\log(\frac{1}{\mathrm{E}}) - 2$.

5. Experimental Results and Analysis

The computer simulation is based on a 802.11n MIMO-OFDM communication system in Rayleigh fading environment, and gray code is utilized to reduce the bit error probability. In our simulation, the complex data are modulated onto subcarriers. The cyclic prefix (CP) is inserted at the beginning of each OFDM symbol to prevent inter-symbol interference (ISI) and to preserve the mutual orthogonality of subcarriers. Following a parallel to serial conversion, each OFDM symbol is finally transmitted from transmitter antennas through a multipath channel with uncorrelated taps.

In order to reconstructed the receive signal from receiver antennas, the sampling rate should be greater than or equal to the Nyquist rate $f_s = \frac{1}{T_s} = 2 f_c$. Despite Doppler and time variation of the channel, SU_a and SU_b are observing highly correlated observations of the same phenomena, in other word, SU_a and SU_b each can generate N_s samples by fully exploiting the coherence time interval. Assuming that transmission delay is ϑ, delay spread is τ, and coherence time is T_{ct}, respectively if we neglect the processing delay, then the observation time is $T_o < \frac{T_{ct}}{2} - \vartheta - \tau$. Furthermore, assuming transmission delay ϑ, and delay spread τ are very small, then maximum observation time and samples can be approximated to $T_o \approx \frac{T_{ct}}{2}$, $N_s \approx \frac{T_{ct} f_s}{2}$, respectively. Choosing a mobile CRN node with a movement velocity $v = 72$ km/h, we deduce $f_d = 60$ Hz and $T_{ct} = \frac{0.432}{f_d} = 7.2$ ms. Setting the observation time $T_o = 150\mu s$, one of two bits [19, 27] quantization method is used to extract $B = 128$ length bits with $[32, 15, 8]_2$-BCH codes. Thus, the number of required negotiation rounds is $\omega = \frac{B}{n} = \frac{128}{32} = 4$. Thus, the bit-extraction rate should reach 10^6 bit/s theoretically. The strong extractor uses an SHA-256 algorithm to generate the final key based on channel

response characteristics from the quantized amplitude values and quantized phase values, respectively. Some experimental parameters and details are shown in **Table 1**.

Table 1. Experimental parameters based on 802.11n MIMO-OFDM communication system in Rayleigh fading environment

Subcarriers Number	128
FFT	256
CP Length	64
Carrier Frequency	2.4GHz
OFDM Symbol Number	10
Constellation Number	16
Uncorrelated Taps Number	8
Transmitter Antennas Number	4
Receiver Antennas Number	4
Observation Time	150 μs
Movement Velocity	72km/h
Hash Algorithm	SHA-256

Fig. 3 plots the initial location of SU_a, SU_b and SU_e in our simulation. We assume that there is only one SU_e with the same transmission power as SU_l and SU_a moving at a speed of 72km/h. The initial location of SU_e is at (-3.2m, 7.3m), and SU_a, SU_b are respectively at (0.91m, 3.66m), (3.2m, 5.5m).

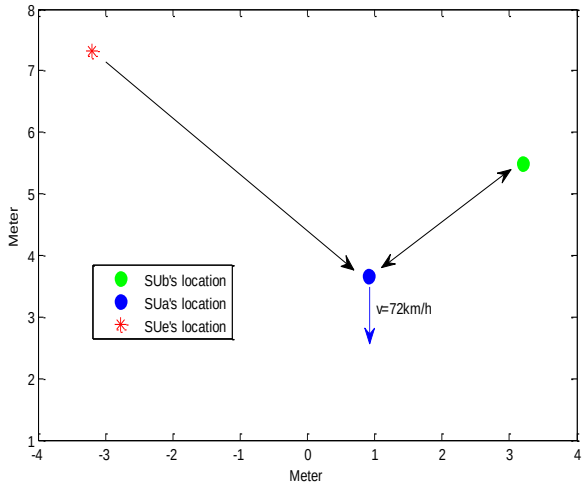


Fig. 3. Simulation scenario of SU_a, SU_b and SU_e in mobile CRNs.

Response Characteristics Correlation

Simulation results of amplitude values in signal-to-noise (SNR) of 25 dB between SU_a and SU_b, SU_e and SU_l are shown in **Fig. 4**. Correspondingly, simulation results of phase values in SNR of 25 dB between SU_a and SU_b, SU_e and SU_l have been shown in **Fig. 5**.

The results show that the values of channel response characteristic observed by SU_l are consistent. However, the values observed between SU_l and SU_e are significantly different.

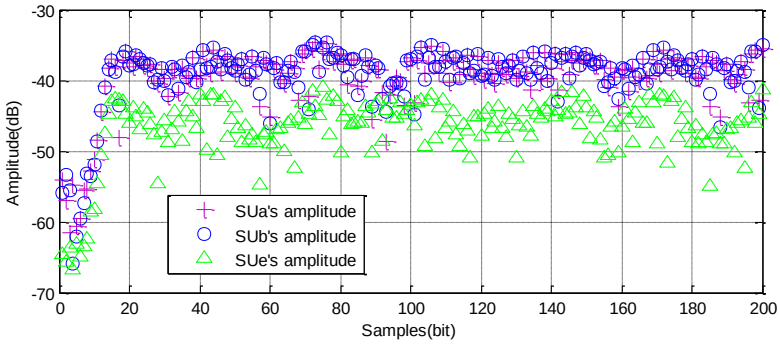


Fig. 4. Amplitude values of channel response characteristics received by SU_a, SU_b, SU_e in SNR of 25 dB.

Setting expectations of the quantized channel response characteristics of SU_a and SU_b, to have means of μ_{SU_a} and μ_{SU_b} and standard deviations σ_{SU_a} and σ_{SU_b}, respectively, the correlation coefficient can be expressed as

$$\rho_{SU_{ab}} = \frac{E[(Q_{SU_a} - \mu_{SU_a})(Q_{SU_b} - \mu_{SU_b})]}{\sigma_{SU_a}\sigma_{SU_b}} \tag{10}$$

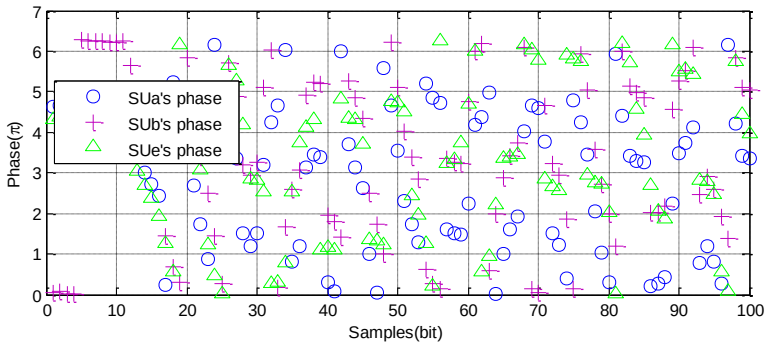


Fig. 5. Phase values of channel response characteristics received by SU_a, SU_b, SU_e in SNR of 25 dB.

We calculated the simulation result of the channel response values received by SU_a and SU_b in SNR from -5 dB to 35 dB. The Doppler shift is $f_d = 60$ Hz. **Fig. 6** plots the correlation coefficients of neighbor SU_l in different SNR.

The experiment results show that the principle of channel reciprocity is obvious between a pair of neighbor nodes SU_a and SU_b in the coherence time. We can observe in Fig. 5 that when the SNR increases, correlation coefficient increases, and the correlation coefficient of amplitude values converge quickly to 1. We can also observe that the correlation of amplitude values is much better than the phase values. **Fig. 7** shows that the correlation coefficient between SU_l and SU_e is low, furthermore, quantized amplitude values are positive

correlation while quantized phase values are negative correlation.

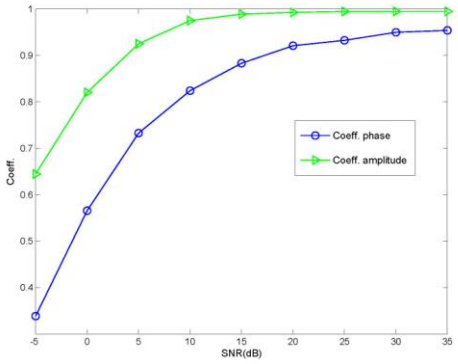


Fig. 6. Correlation coefficients of quantized amplitude values vs quantized phase values between SU_l in different SNR.

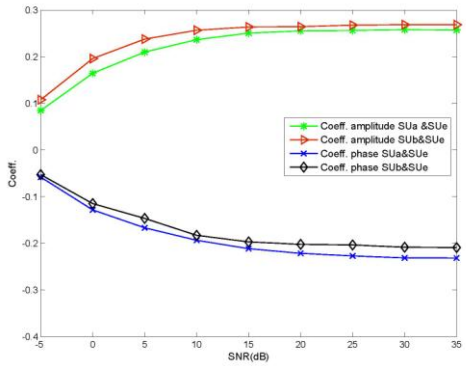


Fig. 7. Correlation coefficient of quantized amplitude values vs quantized phase values between SU_l and SU_e in different SNR.

5.2 Bit Mismatch Rate

For the key generation scheme, the bit mismatch rate P_m can be used to estimate the success probability of bit extraction before information reconciliation. With a pair of SU_l, the bit mismatch rate is defined as the proportion of the number of bits that do not match to the total number of bits extracted.

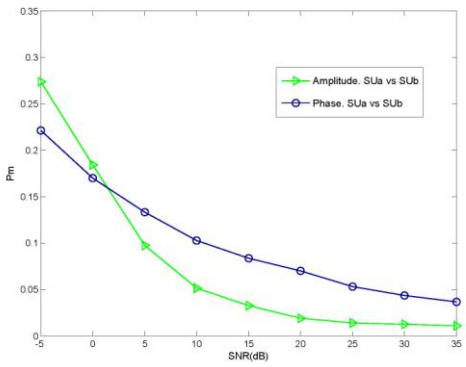


Fig. 8. Bit mismatch rate P_m of quantized amplitude values vs quantized phase values between SU_l in different SNR, one of two bits quantization method.

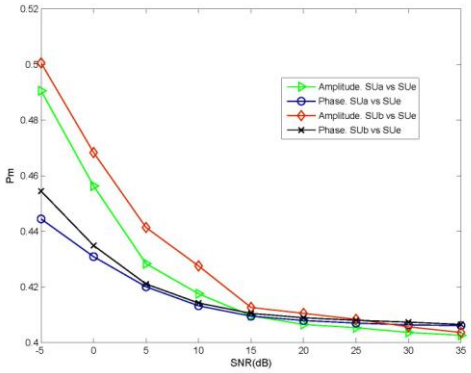


Fig. 9. Bit mismatch rate P_m of quantized amplitude values vs quantized phase values between SU_l and SU_e in different SNR, one of two bits quantization method.

Fig. 8 provides the bit mismatch rate of quantized amplitude values and quantized phase values between SU_l. The simulation results suggest that $[32, 15, 8]_2$-BCH codes are enough to recover bits in our fuzzy key generation scheme. It shows a phenomenon that the bit mismatch rate of quantized amplitude values are higher than quantized phase values in low SNR. With the SNR increasing, the phenomenon is slightly obvious, when SNR changes from 5 dB to higher, the bit mismatch rate of quantized phase values are higher than quantized amplitude values. This proves that phase characteristics are better than amplitude

characteristics to generate bits in a low SNR environment. It also proves that variation trend of P_m in phases is slower than amplitudes, which means that phase characteristics are much more robust for key generation in mobile environments. **Fig. 9** shows that the range of the mismatch rate between SU_l and SU_e is about 40%-50% at different SNR.

5.3 Key Randomness

To evaluate that the key is adequately random in our scheme, the standard randomness test suite from NIST [28] is employed to demonstrate the effectiveness. Tests employed are the Block Frequency test, Frequency test, Runs test, FFT test, Approximate entropy test, Cumulative Sums test, and Serial test. **Table 2** presents the randomness test results for the key generated from quantized amplitude characteristics, as well as the randomness test results for the key generated from quantized phase characteristics are shown in **Table 3**.

Table 2. NIST statistical test results of key generated from quantized amplitude characteristics. The P-VALUE for this test is much greater than 0.01

STATISTICAL TEST	P-VALUE
Block Frequency	0.7839
Frequency	0.6341
Runs	0.8671
FFT	0.6902
Approximate Entropy	0.9715
Cumulative Sums(Fwd)	0.8960
Cumulative Sums(Rev)	0.8293
Serial	0.8035,0.9982

Table 3. NIST statistical test results of key generated from quantized phase characteristics. The P-VALUE for this test is much greater than 0.01

STATISTICAL TEST	P-VALUE
Block Frequency	0.8331
Frequency	0.7597
Runs	0.8150
FFT	0.9026
Approximate Entropy	0.9168
Cumulative Sums(Fwd)	0.9660
Cumulative Sums(Rev)	0.7914
Serial	0.8812,0.9895

The NIST statistical test results show that all of the P-VALUE for the key generated are much greater than 0.01, which suggest that the key has great randomness. It is clarify that the fuzzy key generation scheme proposed in this paper can be used to generate secure key in mobile CRNs.

6. Conclusion

In this paper, we propose a novel fuzzy key generation scheme based on PHY-layer fingerprints in mobile CRNs. Our proposed approach is derived from biological fingerprints

extraction methods; we use the unique wireless channel response characteristics as PHY-layer fingerprints to fuzzy-extract a key. Firstly, in the existing literatures, key agreement of PHY-layer based key generation is a pervasive problem. To address this problem, we constructed a new secure sketch in the Hamming metric space. Secondly, we provide the EA algorithm and the TA algorithm to defend against eavesdropping attacks and tampering attacks which are likely to occur in existing multi-node collaborative defense strategies against PUE attacks or SSDF attacks. Security analyses of these algorithms are given in both spatial and temporal domains, we also prove the upper bound of the entropy loss in theory. Finally, the simulation result indicates that our proposed scheme can effectively extract secret key in a coherence period. The bit mismatch rate is strikingly lower than existing work, which is very efficient and only requires a few seconds on general computers. In addition, simulation results prove that phase characteristics are better than amplitude characteristics to extract bits in low SNR, and phase characteristics are much more robust for key generation in mobile environments. NIST tests of the generated key demonstrate the randomness is excellent. Based on the fuzzy key generation scheme, we can update and distribute key to realize one-time pad communication and message authentication in mobile CRNs.

References

[1] Haykin S, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201-220, 2005. Article (CrossRef Link)

[2] Cordeiro C, Challapali K, Birru D, et al., "IEEE 802.22: An Introduction to the First Wireless Standard based on Cognitive Radios," *Journal of Communications*, vol. 1, no. 1, 2006. Article (CrossRef Link)

[3] Chen R, Park J M, Reed J H, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25-37, 2008. Article (CrossRef Link)

[4] Alahmadi A, Abdelhakim M, Ren J, et al. , "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 9, pp. 772-781, 2014. Article (CrossRef Link)

[5] Le T N, Chin W L, Kao W C, "Cross-Layer Design for Primary User Emulation Attacks Detection in Mobile Cognitive Radio Networks," *IEEE Communications Letters*, vol. 19, no. 5, pp. 1-1, 2015. Article (CrossRef Link)

[6] Hyder C S, Grebur B, Li X, et al. , "ARC: Adaptive Reputation based Clustering Against Spectrum Sensing Data Falsification Attacks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1707-1719, 2014. Article (CrossRef Link)

[7] Huang L, Xie L, Yu H, et al., "Anti-PUE Attack Based on Joint Position Verification in Cognitive Radio Networks," in *Proc. of 2010 International Conference on Communications and Mobile Computing (CMC). IEEE*, pp. 169-173, 2010. Article (CrossRef Link)

[8] Liu Y, Ning P, Dai H, "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures," in *Proc. of IEEE Symposium on Security and Privacy. IEEE Computer Society*, pp. 286-301, 2010. Article (CrossRef Link)

[9] Ying Z, Hui Z, Wei T, et al. , "Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 30, pp. 1850-1860, 2012. Article (CrossRef Link)

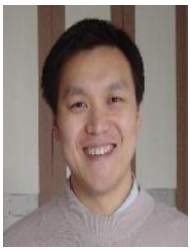
[10] Shannon C E, "Communication Theory of Secrecy Systems," *Md Comput*, vol. 28, no. 4, pp. 656-715, 1948. Article (CrossRef Link)

[11] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. of IEEE International Conference on Acoustics*, pp. 3013-3016, 2008. Article (CrossRef Link)

[12] Wang Q, Su H, Ren K, et al., "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. of IEEE INFOCOM*, , vol. 8, no. 1, pp. 1422-1430, 2011. Article (CrossRef Link)
[13] Wilson R, Tse D, Scholtz R A, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 364-375, 2007. Article (CrossRef Link)
[14] Madiseh M G, McGuire M L, Neville S S, et al., "Secret key generation and agreement in UWB communication channels," in *Proc. of IEEE GLOBECOM*, pp. 1-5, 2008. Article (CrossRef Link)
[15] Chen C, Jensen M A, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Transactions on Mobile Computing*, vol. 10, no. 2, pp. 205-215, 2011. Article (CrossRef Link)
[16] Wallace J W, Chen C, Jensen M A, "Key generation exploiting MIMO channel evolution: algorithms and theoretical limits," in *Proc. o European Conference on Antennas and Propagation. IEEE*, pp. 1499-1503, 2009. Article (CrossRef Link)
[17] Aono T, Higuchi K, Taromaru M, et al., "Wireless secret key generation exploiting the reactance-domain scalar response of multipath fading channels: RSSI interleaving scheme," *European Conference on Wireless Technology. IEEE*, pp. 173-176, 2005. Article (CrossRef Link)
[18] Azimi-Sadjadi B, Kiayias A, Mercado A, et al., "Robust key generation from signal envelopes in wireless networks," in *Proc. of the 14th ACM conference on Computer and Communications Security. ACM*, pp. 401-410, 2007. Article (CrossRef Link)
[19] Yasukawa S, Iwai H, Sasaoka H, "A secret key agreement scheme with multi-level quantization and parity check using fluctuation of radio channel property," in *Proc. of Information Theory, 2008. ISIT 2008. IEEE International Symposium on. IEEE*, pp. 732-736, 2008. Article (CrossRef Link)
[20] Huyen N T T, Jo M, Nguyen T D, et al., "A beneficial analysis of deployment knowledge for key distribution in wireless sensor networks," *Security and Communication Networks*, vol. 5, no. 5 pp. 485-495, May 2012. Article (CrossRef Link)
[21] Dodis Y, Reyzin L, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," in *Proc. of the international Conference on Advances in Cryptology Lecture*, vol. 38, no.1, pp. 523-540, 2004. Article (CrossRef Link)
[22] Juels A, Wattenberg M, "A fuzzy commitment scheme," in *Proc. of ACM Conference on Computer and Communications Security. EP*, pp. 28-36, 1999. Article (CrossRef Link)
[23] Wang C X, Haider F, Gao X, et al., "Cellular architecture and key technologies for 5G wireless communication networks," *Communications Magazine IEEE*, vol. 52, no. 2, pp. 122-130, 2014. Article (CrossRef Link)
[24] Truman T E, Brodersen R W, "A measurement based characterization of the time variation of an indoor wireless channel," in *Proc. of IEEE, International Conference on Universal Personal Communications Record, 1997. Conference Record*, vol. 2, pp. 561-2, 1974. Article (CrossRef Link)
[25] Goldsmith A, "Wireless Communications, First Edition," 2005. Article (CrossRef Link)
[26] Nisan N, Zuckerman D, "Randomness is Linear in Space," *Journal of Computer and System Sciences*, vol. 52, no. 1, pp. 43-52, 1993. Article (CrossRef Link)
[27] Patwari N, Croft J, Jana S, et al., "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17-30, 2010. Article (CrossRef Link)
[28] Rukhin A, Soto J, Nechvatal J, et al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *ITLB*, vol. 22, no. 7, pp. 1645-179, 2001. Article (CrossRef Link)

Ning Gao received B.S. degree in electronic information science and technology from Liaocheng University in 2012. M.S. degree in Operational Research and Cybernetic from Shandong University of Science and Technology, in 2015. Now he is currently working towards the Ph.D. degree in Information and Communication Engineering at Beijing University of Posts and Telecommunications. His research interests in spectrum sensing, dynamic spectrum management and security in cognitive radio networks.

Xiaojun Jing received the M.S. and Ph.D. degree from National University of Defense Technology in 1995 and 1999, respectively. He is currently a professor at Beijing University of Posts and Telecommunications. His research interests include information security, image processing.



Songlin Sun received B.S. and M.S. degree from Shandong University of Technology in 1997 and 2000, respectively, and his Ph.D. degree from Beijing University of Posts and Telecommunications in 2003. He is currently a professor at Beijing University of Posts and Telecommunications. His research interests include signal processing in wireless communications and multimedia technology.

Junsheng Mu received B.S. and M.S. degrees in 2012 and 2015, respectively, and currently working towards the Ph.D. degree in Information and Communication Engineering at Beijing University of Posts and Telecommunications. His research interests in spectrum sensing and security in cognitive radio networks.

Xiang Lu received his Ph.D. degree in computer science from Xidian University, China, in 2013, and his B.S. degree in electrical engineering also from Xidian University in 2005. From 2009 to 2012, he was a visiting Ph.D. student in the Department of Electrical and Computer Engineering, North Carolina State University. He is currently an Associate Professor at the Institute of Information Engineering, Chinese Academy of Sciences. His current research is related to computer and network security, with an emphasis on performance and vulnerability analysis of security schemes in practical applications and systems. He is the reviewer of a number of conference and journals, including IEEE INFOCOM and IEEE Transactions on Mobile Computing. He is also served on the technical program committee for IEEE ICC 2015.