Wireless Physical Layer Characteristics Based Random Number Generator: Hijack Attackers

Ning Gao*† Xiaojun Jing*† Shichao Lv‡§ Junsheng Mu*† Limin Sun‡§
*School of Information and Communication Engineering, Beijing University of Posts and Telecommunications.
†Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education,
Beijing University of Posts and Telecommunications, Beijing 100876, China.
‡School of Cyber Security, University of Chinese Academy of Sciences.
§Beijing Key Laboratory of IOT Information Security Technology, IIE CAS, Beijing 100093, China.
Emails: {ngao, jxiaojun}@bupt.edu.cn, {lvshichao, sunlimin}@iie.ac.cn

***Abstract*—Random numbers are widely used in 5G communication security. In this paper, we propose a wireless physical layer (PHY-layer) characteristics based random number generator in vehicular networks. Firstly, the closed form expression of random transmission success probability is derived under the presence of multiple jamming attackers in a Nakagami-m fading channel. Secondly, a novel Random Transmission Success Probability based Physical Random Number Generator (RTSP-PhRNG) is presented. Finally, numerical results are conducted and a Universal Software Radio Peripheral (USRP) based prototype is implemented to validate our proposed method. Furthermore, the standard randomness test suite from NIST shows that our proposed PhRNG reveals good randomness.**

***Index Terms*—Wireless security, PHY-layer, random transmission success probability, PhRNG.**

I. Introduction

Wireless communication is one of the most developed technologies that make substantial contribution to everyday life. However, owing to the broadcast nature of wireless communication, there is no physical boundary in wireless networks whose security becomes the decisive concern point. Wireless networks is susceptible to various attacks like jamming, man in the middle (MITM) and denial of service (DOS). However, traditional security solutions can not prevent some attacks (i.e. jamming attacks [1]) or consume a lot of resources to defend against them. It is necessary to find an alternative method that suit best practice in power limited networks. Consequently, 5G communication physical layer (PHY-layer) security has been sparked widespread interests [2], [3].

Many recent studies on PHY-layer security need to use random numbers [4]–[7]. In multiple-input and multiple-output orthogonal-frequency-division-multiplexing (MIMO-OFDM) system, the authors in [4] proposed two practical physical layer security schemes, one is the precoding matrix index based secret key generation with rotation matrix and another is the channel quantization based scheme. Both of them need to find a precoding matrix which is selected from the universal codebook by the receiver. Reference [5] proposed a physical layer key exchange method which transmits the key bits by encoding them within some phase randomization sequences that are selected according to a certain channel criterion. In this method, the transmitter generates pseudo modulated to carry the phase randomization book which is generated by a randomization vector generator. In cognitive radio networks, [6] introduced a helper node to defend against primary user emulation attacks (PUEAs). The helper node acts as a "bridge" to enable second user to verify cryptographic signature carried by the helper node's signal using its private key, then learn the helper node's authentic link signatures, and finally verify the primary user's link signature. However, the helper node's private key is not assumed to be secure across a long storage time. Thus, updating the private key of cryptographic signatures is better. The same security threat was considered in [7], the authors presented a reliable AES-assisted digital TV (DTV) scheme to accurately identify the authorized primary user, in which an AES-encrypted reference signal is generated at the TV transmitter and used as the sync bytes of each DTV data frame. The proposed authentication mechanism is based on the higher layer protocols and additional plug-in AES chips. Overall, the generation of unpredictable and reliable random numbers for cryptographic algorithms or authentication protocols is the most significant issue.

In general, random numbers should ideally be modeled as a mutually independent uniformly distributed random variable which is classified in two main types: pseudo random number and physical random number. Pseudo random number generators usually depend on complicated algorithms and generated seeds. However, their generated pseudo random numbers have obvious periodicity, and attackers are able to employ statistical theory and prior knowledge to crack them [8]. Physical Random Numbers Generator (PhRNG) utilized nondeterministic natural source as entropy to yield unpredictable and aperiodic true random numbers. Therefore, the generated physical random numbers are so outstanding that attackers have difficulty in predicting of the generator's output even if its design is known. In this paper, we present a novel Random Transmission Success Probability based PhRNG (RTSP-PhRNG). To the best of our knowledge, this method has not been disclosed in the previous works. The the key contributions include

- No additional cost and external integrated circuit are required. We not only avert design complicated algorithms or generated seeds using mathematic but also avoid using

978-1-5090-5935-5/17/$31.00 ©2017 IEEE

expensive hardware such as Field Programmable Gate Array (FPGA) and Application Specific Integrated Circuit (ASIC) technologies.

- Make full use of jamming attacks, we turn the harm into a benefit. We detect the jamming attacks and then generate random numbers in this phase. The randomness of the generated numbers only depend on random transmission success probability, which is a physical random process that attackers are difficult to predict or copy it with their prior knowledge.
- Our proposed algorithm is suitable for wireless networks which has numerous direct application including cryptographic key generation, cryptographic protocol, frequency-hopping or "one-time pad" communications.

The remainder of this paper is organized as follows. Section II gives the system model. Section III discusses our proposed RTSP-PhRNG and gives the complete algorithm. In section IV, we execute performance analysis and security evaluation. Concluding remarks are given in section V.

II. Preliminary

In this section, we give the detailed description of the considered system model and the jamming attack models.

A. System Model

This paper considers vehicular networks that consist of two legitimate vehicles, Alice & Bob, and K jamming attackers. Both Alice and Bob have two modes, which are communication mode and PhRNG mode. Alice and Bob can communicate with each other, and we assume Alice is the initiator of the communication. Meanwhile, they are subjected to K jamming attackers' independent and identically distributed (i.i.d) co-channel interferences in Nakagami-m fading channels, and interferences plus noise are regarded as uncorrelated with the desired signal. The received signal can be written as

$$\mathcal{R}_{A,B}(t) = \underbrace{\sqrt{\mathcal{P}_s} h_s(t) d_s}_{\mathcal{D}_s} + \underbrace{\sqrt{\mathcal{P}_j} \sum_{k=1}^{K} h_k(t) d_k}_{\mathcal{I}_{tot}} + n_{A,B}(t) \quad (1)$$

where $h_s(t)$ is the channel fading coefficient between Alice and Bob, which follows Nakagami-m distribution, $h_k(t)$ is the Nakagami-m channel fading coefficient of the k-th jamming, d_s is the unit-energy desired signal, d_k is the k-th unit-energy jamming signal, $\mathcal{P}_s$ is the desired signal energy, $\mathcal{P}_j$ is the energy of the jamming signal, and $n_{A,B}(t)$ is the Additional White Gaussian Noise (AWGN) with zero mean and variance N_0. It is straightforward to show that $\mathcal{D}_s$ is the desired signal and $\mathcal{I}_{tot}$ is the total of K jamming attackers' signals.

B. Jamming Attack Models

We consider random jamming attacks [9] which can alternate theirs mode between sleeping and jamming depend on time t. Generally, after jamming launch for t_j time slot with a constant power, the attackers turn off theirs radio, and turn into sleeping modes. They will re-launch attacks after sleeping for t_s time. Time $t = \{t_j, t_s\}$ can be either random which follows a certain distribution or fixed which is a constant. The goal of these attacks is to take energy conservation into consideration, and maximize jamming to the legitimate users (Alice & Bob).

III. Physical Random Number Generator

In this section, we first give the Probability Density Function (PDF) of SINR and the closed form expression of random transmission success probability. Then, we present the complete RTSP-PhRNG algorithm.

A. PDF of SINR

Signal-to-Interference and Noise Ratio (SINR) at Bob can be given as [10]

$$\begin{aligned} \gamma &= \frac{\mathcal{P}_s |h_s(t)|^2 |d_s|^2}{\mathcal{P}_j \sum_{k=1}^{K} |h_k(t)|^2 |d_k|^2 + N_0} \\ &= \frac{|\mathcal{D}_s|^2 / N_0}{|\mathcal{I}_{tot}|^2 / N_0 + 1} \\ &= \frac{\gamma_{SN}}{\gamma_{IN} + 1}, \end{aligned} \quad (2)$$

where $\gamma_{SN} = |\mathcal{D}_s|^2 / N_0$ is the SNR power and $\gamma_{IN} = |\mathcal{I}_{tot}|^2 / N_0$ represents the sum of K attackers' Interference to Noise Ratio (INR) power.

The SNR power in Nakagami-m fading is a gamma distributed random variable whose PDF is given by

$$f_{SN}(\gamma_{SN}) = (\frac{m_s}{\Omega_s})^{m_s} \frac{\gamma_{SN}^{m_s - 1}}{\Gamma(m_s)} exp(-\frac{m_s}{\Omega_s} \gamma_{SN}), \ \gamma_{SN} \geq 0, \quad (3)$$

where Ω_s is the average SNR power and m_s is the Nakagami-m fading parameter.

The PDF of the k-th INR power $\gamma_{IN,k} = \mathcal{P}_j |h_k(t)|^2 |d_k|^2 / N_0$ can be represented by

$$f_{IN}(\gamma_{IN,k}) = (\frac{m_k}{\Omega_k})^{m_k} \frac{\gamma_{IN,k}^{m_k - 1}}{\Gamma(m_k)} exp(-\frac{m_k}{\Omega_k} \gamma_{IN,k}), \gamma_{IN,k} \geq 0. \quad (4)$$

Owing to the sum of k different gamma distributions $\gamma_{IN} = \gamma_{IN,1} + \gamma_{IN,2} + \cdots + \gamma_{IN,k}$ is approximated by an equivalent gamma distribution, the PDF of the total INR power is

$$f_{IN}(\gamma_{IN}) = (\frac{m_i}{\Omega_i})^{m_i} \frac{\gamma_{IN}^{m_i - 1}}{\Gamma(m_i)} exp(-\frac{m_i}{\Omega_i} \gamma_{IN}), \ \gamma_{IN} \geq 0 \quad (5)$$

with the average INR power Ω_i and the Nakagami-m fading parameter m_i. Parameters Ω_i and m_i are calculated by

$$\Omega_i \simeq \sum_{k=1}^{K} \Omega_k \qquad m_i \simeq \frac{\left(\sum_{k=1}^{K} \Omega_k \right)^2}{\sum_{k=1}^{K} \Omega_k^2 / m_k}. \quad (6)$$

Using the quotient distribution of two random variables, $f_Z(z) = \int_{-\infty}^{+\infty} f_X(x) f_Y(xz) |x| dx$, the PDF of SINR at Bob is given by

$$f_{SIN}(\gamma) = \int_1^{+\infty} f_{IN}(x-1) f_{SN}(x\gamma) x dx, \quad \gamma \geq 0. \quad (7)$$

Substituting (3) and (5) into (7) we obtain

$$f_{SIN}(\gamma) = \frac{(\frac{m_s}{\Omega_s})^{m_s}(\frac{m_i}{\Omega_i})^{m_i}\gamma^{m_s-1}exp(-\frac{m_s}{\Omega_s}\gamma)}{\Gamma(m_s)\Gamma(m_i)} \times \int_1^{+\infty}(x-1)^{m_i-1}x^{m_s}exp(-x(\frac{m_s}{\Omega_s}\gamma+\frac{m_i}{\Omega_i}))dx, \quad \gamma \geq 0. \quad (8)$$

Let $t = x-1, t > 0$

$$f_{SIN}(\gamma) = \frac{(\frac{m_s}{\Omega_s})^{m_s}(\frac{m_i}{\Omega_i})^{m_i}\gamma^{m_s-1}exp(-\frac{m_s}{\Omega_s}\gamma)}{\Gamma(m_s)\Gamma(m_i)} \times \int_0^{+\infty}t^{m_i-1}(1+t)^{m_s}exp(-t(\frac{m_s}{\Omega_s}\gamma+\frac{m_i}{\Omega_i}))dt, \quad \gamma \geq 0. \quad (9)$$

We obtain

$$f_{SIN}(\gamma) = \frac{(\frac{m_s}{\Omega_s})^{m_s}(\frac{m_i}{\Omega_i})^{m_i}\gamma^{m_s-1}exp(-\frac{m_s}{\Omega_s}\gamma)}{\Gamma(m_s)} \times\Psi(m_i, m_s+m_i+1, \frac{m_s}{\Omega_s}\gamma+\frac{m_i}{\Omega_i}), \quad \gamma \geq 0, \quad (10)$$

where $\Psi(a,b,z)$ is the confluent hypergeometric function of the second kind. For all value of a, b and z, it has one and only one differentiable value [11]. Furthermore, when $b-a$ is a positive integer, the function $\Psi(a,b,z)$ can be denoted as

$$\Psi(a,b,z) = z^{-a}\sum_{m=0}^{b-a-1}\binom{b-a-1}{m}\frac{a^{(m)}}{z^m}, a > 0, \quad (11)$$

where $a^{(m)} = \Gamma(a+m)/\Gamma(a)$. When b is a negative integer, we can use Kummer's transformations $\Psi(a,b,z) = z^{1-b}\Psi(1+a-b, 2-b, z)$ [12]. Thus, when m_s+m_i is integer[1], the PDF of SINR can be express as

$$f_{SIN}(\gamma) = \frac{(\frac{m_s}{\Omega_s})^{m_s}(\frac{m_i}{\Omega_i})^{m_i}\gamma^{m_s-1}exp(-\frac{m_s}{\Omega_s}\gamma)}{\Gamma(m_s)} \times(\frac{m_s}{\Omega_s}\gamma+\frac{m_i}{\Omega_i})^{-m_i}\sum_{m=0}^{m_s}\binom{m_s}{m}\frac{m_i^{(m)}}{(\frac{m_s}{\Omega_s}\gamma+\frac{m_i}{\Omega_i})^m}, \quad \gamma \geq 0. \quad (12)$$

B. Random Transmission Success Probability

We define random transmission success probability as a random variable that describes the probability of achieving to satisfy signal reception for a desired receiver. Identically, it can be evaluated by a random threshold, γ_{rv}, follows a certain distribution (i.e. Gaussian distribution). Thus, the random transmission success probability is given by

$$P_s = \mathbb{P}(SINR > \gamma_{rv}). \quad (13)$$

[1]In order to simplify the discussion, we only consider the case that b is integer which has no effect on our proposed PhRNG algorithm.

Substituting (9) into (13), we get

$$P_s = \int_{\gamma_{rv}}^{\infty}\frac{(\frac{m_s}{\Omega_s})^{m_s}(\frac{m_i}{\Omega_i})^{m_i}\gamma^{m_s-1}exp(-\frac{m_s}{\Omega_s}\gamma)}{\Gamma(m_s)\Gamma(m_i)} \times\int_0^{+\infty}t^{m_i-1}(1+t)^{m_s}exp(-t(\frac{m_s}{\Omega_s}\gamma+\frac{m_i}{\Omega_i}))dtd\gamma.$$

Change integration order, we can obtain

$$P_s = \frac{(\frac{m_s}{\Omega_s})^{m_s}(\frac{m_i}{\Omega_i})^{m_i}}{\Gamma(m_s)\Gamma(m_i)} \times \int_0^{+\infty}t^{m_i-1}(1+t)^{m_s}exp(-\frac{m_i}{\Omega_i}t)) \times \left\{\int_{\gamma_{rv}}^{+\infty}\gamma^{m_s-1}exp(-\frac{m_s}{\Omega_s}(t+1)\gamma)d\gamma\right\}dt.$$

Due to $\Gamma(v,s) = \int_s^{\infty}q^{v-1}exp(-q)dq, v > 0$, where $\Gamma(v,s)$ is the upper incomplete gamma function. Thus,

$$P_s = \frac{(\frac{m_i}{\Omega_i})^{m_i}}{\Gamma(m_s)\Gamma(m_i)}\int_0^{+\infty}t^{m_i-1}exp(-\frac{m_i}{\Omega_i}t) \times \Gamma(m_s, \frac{m_s}{\Omega_s}(t+1)\gamma_{rv})dt. \quad (14)$$

When v is an integer value, $\Gamma(v,s)$ can be written as

$$\Gamma(v,s) = \Gamma(v)e^{-s}e_{v-1}(s), \quad (15)$$

where $e_{v-1}(s) = \sum_{n=0}^{v-1}s^n/n!$. Substituting (15) into (14) and simplifying, the expression for random transmission success probability is given by

$$P_s = (\frac{m_i/\Omega_i}{\frac{m_s}{\Omega_s}\gamma_{rv}+\frac{m_i}{\Omega_i}})^{m_i}exp(-\frac{m_s}{\Omega_s}\gamma_{rv})\sum_{n=0}^{m_s-1} \times \frac{(m_s\gamma_{rv}/\Omega_s)^n}{n!}\sum_{m=0}^{n}\binom{n}{m}\frac{(m_i)^{(m)}}{(\frac{m_s}{\Omega_s}\gamma_{rv}+\frac{m_i}{\Omega_i})^m}. \quad (16)$$

Obviously, the obtained P_s provides insightful guideline to illustrate that it is a function of random variable $m_s\gamma_{rv}/\Omega_s$, which contains the PHY-layer characteristics such as average SNR power Ω_s and Nakagami-m fading parameter m_s. According to Theorem 1, P_s is a random variable distributed uniformly on $\mathcal{U}(0,1)$.

C. Transform Theorem

For converting random variable with any given continuous distribution to another random variable with uniform distribution, [13] gave a very interesting and useful theorem which is called probability integral transform theorem.

Lemma 1: If a random variable X has Cumulative Distribution Function (CDF) $\mathbb{P}(\cdot)$. Then for all real x, $P\{\mathbb{P}(X) \leq \mathbb{P}(x)\} = \mathbb{P}(x)$.

Proof : $\{\mathbb{P}(X) \leq \mathbb{P}(x)\} = [\{\mathbb{P}(X) \leq \mathbb{P}(x)\}\bigcap\{X \leq x\}]\bigcup[\{\mathbb{P}(X) \leq \mathbb{P}(x)\}\bigcap\{X > x\}]$. Since $\mathbb{P}(\cdot)$ is a nondecreasing function, $\{X \leq x\} \subset \{\mathbb{P}(X) \leq \mathbb{P}(x)\}$. In addition, $\{\mathbb{P}(X) < \mathbb{P}(x)\}\bigcap\{X > x\}$ is empty. Thus, we can get that, $\{\mathbb{P}(X) \leq \mathbb{P}(x)\} = \{X \leq x\}\bigcup[\{\mathbb{P}(X) = \mathbb{P}(x)\}\bigcap\{X > x\}]$. However, the probability of $[\{\mathbb{P}(X) = \mathbb{P}(x)\}\bigcap\{X > x\}]$ is

0, as a consequence, $\{\mathbb{P}(X) \leq \mathbb{P}(x)\} = \{X \leq x\}$. Then, $P\{\mathbb{P}(X) \leq \mathbb{P}(x)\} = P\{X \leq x\} = \mathbb{P}(x)$.

Theorem 1: (Probability Integral Transform Theorem): If the CDF $\mathbb{P}(\cdot)$ for a random variable X is continuous, then a new random variable $Y = \mathbb{P}(X)$ will be distributed uniformly on $\mathcal{U}(0,1)$.

Proof : Let $y \in (0,1)$, since $Y = \mathbb{P}(X)$ and $\mathbb{P}(\cdot)$ is continuous, there must exist a real x such that $\mathbb{P}(x) = y$. Then, $P\{Y \leq y\} = P\{\mathbb{P}(X) \leq y\} = P\{\mathbb{P}(X) \leq \mathbb{P}(x)\} = P\{X \leq x\} = \mathbb{P}(x) = y$, indicating that random variable Y is distributed uniformly on $\mathcal{U}(0,1)$.

D. Complete Algorithm

Using random transmission success probability and theorem 2, we present the complete algorithm which is called RTSP-PhRNG algorithm. The RTSP-PhRNG algorithm includes detection algorithm and generation algorithm. In detection algorithm, we use the signal energy detection to decide whether random jamming attacks are present or not, which we called hijack attackers. The rationale behind using this measurement is that the signal energy distribution may be affected by the presence of attackers. The signal energy distribution which is evaluated by N samples of the received signal $\mathcal{R}(t)$ in time slot s is represented as

$$Y = \frac{1}{N}\left(\sum_{s}^{s-N+1} \mathcal{R}(s)^2\right). \tag{17}$$

The binary hypothesis test of the random jamming detection using a posterior probability criterion with a energy threshold, Θ that is suitably chosen by considering tradeoffs between probability of detection and false alarm, can be written as

$$\begin{aligned} \mathcal{H}_0 &: P(D_1|Y) < \Theta, \\ \mathcal{H}_1 &: P(D_1|Y) \geq \Theta. \end{aligned} \tag{18}$$

Where D_1 represents attackers are present, and Y represents the received signal energy of Alice. When attackers are detected, Alice extracts random numbers in generation algorithm. The complete algorithm is shown in algorithm 1.

Theorem 2: If a continuous random variable X is distributed uniformly on $\mathcal{U}(0,1)$, the discrete random variable Y which is discrete of X by a quantization threshold $\lambda = 1/2$, follows a binary uniform distribution $\mathcal{U}_b(0,1)$.

Proof :

$$\text{Let } y = \begin{cases} 1, & \text{for } x > \lambda, \\ 0, & \text{for } x \leq \lambda. \end{cases}$$

Since $P(Y = 0) = \mathbb{P}(X \leq \lambda) = \mathbb{P}(X \leq 1/2) = 1/2$ and $P(Y = 1) = \mathbb{P}(X > \lambda) = 1 - \mathbb{P}(X \leq 1/2) = 1/2$, the discrete random variable Y follows a binary uniform distribution

$$P(Y = y) = \begin{cases} 1/2, & \text{for } y = 1, \\ 1/2, & \text{for } y = 0. \end{cases}$$

Algorithm 1 RTSP-PhRNG

Input:
Alice's random transmission success probability P_s.
Output:
Binary random numbers $R \sim \mathcal{U}_b(0,1)$.

```
Random jamming attackers detection using Eq. (18);
if state H_0 then
    Alice communicates with Bob in communication mode;
else
    Alice switches to PhRNG mode and generates random
    transmission success probability P_s;
    Set quantization threshold λ = 1/2;
    for j ← 1 to length |P_s| do
        if P_s(j) ≥ λ then
            P_s(j) = 1;
        else
            P_s(j) = 0;
        end if
        R(j) = P_s(j);
    end for
    Return binary random numbers R.
end if
```

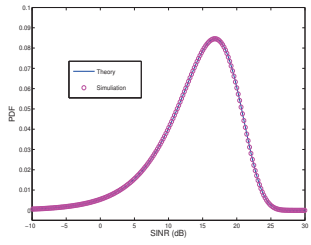
IV. Results and Evaluation

In Fig.1(a)., numerical simulation is conducted to compare the theory PDF (expression 16) and the simulation PDF with fading parameter $m_s = 2$, $m_i = 1$, SNR $\Omega_s = 25$dB, and INR $\Omega_i = 11$dB, respectively. It characterizes the numerical characteristic of SINR. The CDF of random transmission success probability for some selected cases are shown in Fig.1(b). In case 1 vs. case 2, we analyze the average SNR power, Ω_s, impacts on generation performance. The result suggests that the higher SNR the larger random transmission success probability is obtained under the same threshold. In case 2 vs. case 3, the average INR power, Ω_i, has a remarkable influence on random transmission success probability, which implies that a higher interferences power may lead to a lower random transmission success probability. In case 1 vs. case 4, the influence of m_i is analyzed, and in case 1 vs. case 5, the fading parameter m_s is compared. Both of them show that different degrees of fading have different degrees effect on the algorithm performance, especially for parameter m_i.

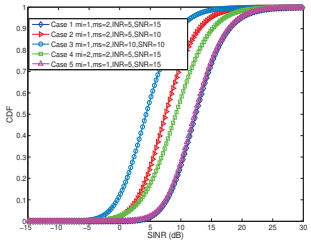
We also implement a USRP-based prototype to generate random numbers using RTSP-PhRNG. The USRP N210 is the second generation of the Universal Software Radio Peripheral (USRP), which is a flexible low-cost platform for software defined radios. In our experiment, we define that if Alice intends to send out n packets one time, but only m of them go through, the transmission success probability is m/n. Random threshold γ_{rv} is controlled by changing the transmission power randomly (Gaussian random variable). We set quantization threshold $\lambda = 1/2$, set the packet rate 25×10^3 packets/s, and use QPSK modulation. Two laptops with two USRPs act as Alice and Bob while one laptop with a USRP acts

TABLE I
PERFORMANCE COMPARISONS OF THE PROPOSED RTSP WITH THE STATE OF THE ART QRNG AND MPDG.

STATISTICAL TEST	Runs	FFT	Rank	Serial	NonOverlapT	OverlappingT	CumulativeSums	BlockFrequency	ApproximateEntr
P-values (RTSP)	**0.572**	0.042	0.463	**0.874**	0.258	**0.381**	0.615	**0.849**	0.269
P-values (QRNG)	0.367	0.081	0.596	0.596	0.494	0.172	0.898	0.637	0.437
P-values (MPDG)	0.475	0.030	0.456	0.851	0.936	0.225	0.740	0.059	0.163

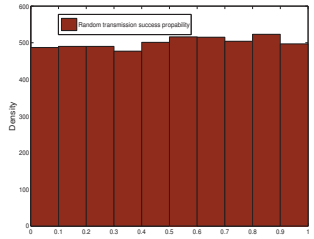


(a) Simulation PDF vs. theory PDF

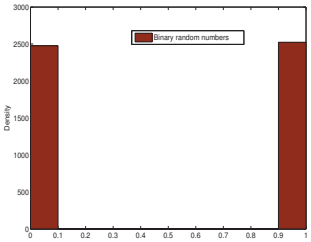


(b) The CDF of random transmission success probability in a Nakagami-m fading environment for some selected cases.

Fig. 1. Simulation results



(a) The actual distribution of transmission success probability using USRP N210.



(b) The actual distribution of generated binary random numbers using RTSP-PhRNG.

Fig. 2. Experiment results

as a jamming attacker. Each laptop with a USRP can change location with a random velocity either due to slow-walk or rotation, roughly in a 15m $\times$ 20m indoor area. Fig.2(a) 2(b). plots the actual distribution of transmission success probability and our generated random numbers at one second. The result suggest that the random numbers nearly contain same number of 0's and 1's. We deduce that the generate rate is depend on packet rate and packet number n, and the maximum generate rate of our RTSP-PhRNG is 250bits/0.01s =25Kbps.

To evaluate the randomness, the standard randomness test suite from NIST [14] is employed. In this test, the P-values greater than 0.01 are regarded as random and pass. We generate 100 sequences, each composed by 10^6 bits, to compare the performance of our proposed RTSP-PhRNG with Quantum Random Number Generator (QRNG) [15], and Multi-source Physical Data Generator (MPDG) [16]. The test results of our proposed method are shown in table I. The result shows that all of the P-values of our proposed method are much greater than 0.01, and four add black test results are outperform other state-of-the-art methods. The evaluation suggest that our proposed RTSP-PhRNG algorithm has a good performance.

V. CONCLUSION

In this paper, a wireless PHY-layer characteristics based random numbers generator in vehicular networks has been proposed. The closed form expression is derived in terms of the random transmission success probability using a random threshold. Interestingly, we hijack jamming attackers and play on them. Combining with probability integral transform theorem, we present the RTSP-PhRNG algorithm to generate random numbers. Meanwhile, both the simulation and the USRP based experiment results show that our proposed algorithm is secure and effective.

REFERENCES

[1] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1746–1759, Aug. 2014.

[2] N. Yang, L. Wang, G. Geraci, and M. Elkashlan, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[3] H. M. Wang, T. X. Zheng, J. Yuan, and D. Towsley, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

[4] C. Y. Wu, P. C. Yeh, and C. H. Lee, "Practical physical layer security schemes for mimo-ofdm systems using precoding matrix indices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1687–1700, Sep. 2013.

[5] H. Taha and E. Alsusa, "Physical layer secret key exchange using phase randomization in mimo-ofdm," in *Proc. IEEE Globecom*, 2015.

[6] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Proc. IEEE Symposium on Security and privacy*, 2010.

[7] A. Alahmadi, M. Abdelhakim, J. Ren, and T. Li, "Mitigating primary user emulation attacks in cognitive radio networks using advanced encryption standard," in *Proc. IEEE Globecom*, 2013.

[8] R. Vaidyanathaswami and A. Thangaraj, "Robustness of physical layer security primitives against attacks on pseudo random generators," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 1070–1079, Mar. 2014.

[9] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2005.

[10] M. Haenggi and R. K. Ganti, "Interference in large wireless networks," *Foundations & Trends in Networking*, vol. 3, no. 2, pp. 127–248, Feb. 2009.

[11] L. J. Slater, *Confluent hypergeometric functions*. Cambridge, U.K.: Cambridge Univ. Press, 1960.

[12] I. S. Gradshteyn and I. M. Ryzhik, "Table of integrals, series, and products (seventh edition)," *Table of Integrals*, vol. 103, no. 1, pp. 1141–1144, Jan. 2007.

[13] J. E. Angus, "The probability integral transform and related results," *Siam Review*, vol. 36, no. 4, pp. 652–654, Apr. 1994.

[14] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudo random number generators for cryptographic applications," DTIC Document, Tech. Rep., 2001.

[15] M. Stipcevic and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," *Review of Scientific Instruments*, vol. 78, no. 4, pp. 275–315, Apr. 2007.

[16] V. Gaglio, A. De Paola, M. Ortolani, and G. Lo Re, "A TRNG exploiting multi-source physical data," in *Proc. ACM Workshop on Qos and Security for Wireless and Mobile Networks*, 2010.