Wireless Physical Layer Characteristics Based Random Number Generator: Hijack Attackers

V.Samyuktha

IITH

July 4, 2021

About the paper

Authors

- Nin Gao
- Xiaojun Jing
- Shichao Lv
- Junsheng Mu
- Limin Sun

Abstract

- Random numbers are widely used in 5G communication security. The most significant issue here is the generation of random numbers that are **unpredictable** and **reliable**.
- Proposed here is a wireless physical layer (PHY-layer) characteristics based random number generator in vehicular networks.

Why use PHY-layer?

Failure of traditional methods

- Cannot prevent some attacks (eg: Jamming attacks)
- Heavy resource consumption, not suited for power limited networks.

Advantage of Physical Random Numbers Generator(PhRNG)

- Utilize nondeterministic natural source as entropy to yield aperiodic and **true random numbers**. Hard to predict generator's output even if its design is known.
- No additional cost or complicated seed-generating algorithms.

Scenario

System model

- Vehicular network with two legitimate vehicles, where A is the initiator and B is the recipient.
- K independent and identically distributed jamming attackers.
- Additional White Gaussian Noise(AWGN) with zero mean and variance N_0.

Jamming attacks model

- Each attacks alternates between **sleeping** and **jamming** depending on time t.
- Jamming launch for time t_j with constant power and then sleep for time t_s. Time $t = \{t_j, t_s\}$ can either be random and follow a distribution or be constant.

Formula for Recieved Signal

$$R_{A,B}(t) = \underbrace{\sqrt{P_s} h_s(t)\, d_s}_{D_s} + \underbrace{\sqrt{P_j} \sum_{k=1}^{K} h_k(t)\, d_k}_{I_{tot}} + n_{A,B}(t) \quad (1)$$

Where,

- $h_s(t)$ is the channel fading coeff. between A and B
- $h_k(t)$ is the channel fading coeff. of the k-th jamming
- d_s is the unit energy desired signal
- d_k is the k-th unit energy jamming signal
- P_s is the desired signal energy
- P_j is the energy of the jamming signal
- $n_{A,B}(t)$ is the AWGN

Hence,

- D_s is the desired signal
- I_{tot} is the total of K jamming attackers' signals

Physical Random Number Generator

To arrive at the working of the proposed Random Transmission Success Probability based Physical Random Number Generator (RTSP-PhRNG) and describe the algorithm, we will first go through the following:

- PDF of Signal-to-Interference and Noise Ratio(SINR)
- Random Transmission Success Probability(RTSP)
- Transform Theorem
- The complete algorithm

PDF of SINR

SINR at B is given by:

$$\gamma = \frac{P_s \left|h_s(t)\right|^2 \left|d_s\right|^2}{P_j \sum_{k=1}^{K} \left|h_k(t)\right|^2 \left|d_k\right|^2 + N_0}$$
$$= \frac{\left|D_s\right|^2 / N_0}{\left|I_{tot}\right|^2 / N_0 + 1}$$
$$= \frac{\gamma_{SN}}{\gamma_{IN} + 1} \tag{2}$$

Where γ_{SN} is the SNR power and γ_{IN} is the sum of K attackers' Intereference to Noise Ratio (INR) power. These variables follow gamma distribution.

PDF of SINR

PDF of SNR power:

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

where Ω_s is the average SNR power and m_s is the Nakagami-m fading parameter.
If k-th INR power is given by:

$$\gamma_{IN,k} = P_j \left|h_k\left(t\right)\right|^2 \left|d_k\right|^2 / N_0$$

Then PDF of the k-th INR power is:

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

PDF of SINR

Adding up the k different gamma distributions,

$$\gamma_{IN} = \gamma_{IN,1} + \gamma_{IN,2} + \dots + \gamma_{IN,k}$$

Hence, the PDF of total INR power is given by:

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

where Ω_i is the average INR power and m_i is the Nakagami-m fading parameter.

Parameters Ω_i and m_i are given by:

$$\Omega_i \approx \sum_{k=1}^{K} \Omega_k \ , \ m_i \approx \frac{\left(\sum_{k=1}^{K} \Omega_k\right)^2}{\sum_k^2 / m_k} \quad (6)$$

PDF of SINR

Quotient distribution of two random variables is given by:

$$f_Z(z) = \int_{-\infty}^{\infty} f_X(x) f_Y(xz) |x| \, dx$$

Using this with (2), PDF of SINR at B is given by:

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

Substituting (3) and (5) into (7), and after solving the integral, we get:

Final equation for PDF of SINR

$$\begin{aligned} f_{SIN}(\gamma) &= \frac{\left(\frac{m_s}{\Omega_s}\right)^{m_s} \left(\frac{m_i}{\Omega_i}\right)^{m_i} \gamma^{m_s-1} \exp\left(-\frac{m_s}{\Omega_s}\gamma\right)}{\Gamma(m_s)} \\ &\times \left(\frac{m_s}{\Omega_s}\gamma + \frac{m_i}{\Omega_i}\right)^{-m_i} \sum_{m=0}^{m_s} \binom{m_s}{m} \frac{m_i^{(m)}}{\left(\frac{m_s}{\Omega_s}\gamma + \frac{m_i}{\Omega_i}\right)^m}, \gamma \geq 0 \end{aligned} \tag{8}$$

Random Transmission Success Probability

Defined as a random variable that describes the **probability of achieving signal reception** by a desired receiver.

It can be evaluated by a random threshold, γ_{rv}, and follows a Gaussian distribution.

RTSP is given by:

$$P_s = \mathbb{P}\left(SINR > \gamma_{rv}\right) \tag{9}$$

Substituting for $f_{SIN}(\gamma)$, and solving the integral, we get:

Final Expression for RTSP

$$\begin{aligned} P_s = {} & \left(\frac{m_i/\Omega_i}{\frac{m_s}{\Omega_s}\gamma_{rv} + \frac{m_i}{\Omega_i}}\right)^{m_i} \exp\left(-\frac{m_s}{\Omega_s}\gamma_{rv}\right) \sum_{n=0}^{m_s-1} \\ & \times \frac{\left(m_s\gamma_{rv}/\Omega_s\right)^n}{n!} \sum_{m=0}^{n} \binom{n}{m} \frac{\left(m_i\right)^{(m)}}{\left(\frac{m_s}{\Omega_s}\gamma_{rv} + \frac{m_i}{\Omega_i}\right)^m} \end{aligned} \tag{10}$$

Random Transmission Success Probability

- We can see that RTSP is a function of the random variable $m_s \gamma_{rv} / \Omega_s$.
- It contains the PHY-layer characteristics such as average SNR power Ω_s and Nakagami-m fading parameter m_s.
- According to the Transfer Theorem (explained next), P_s **is a random variable distributed uniformly on** $U(0, 1)$.

Probability Integral Transform Theorem

Supporting Lemma

If a random variable X has CDF $\mathbb{P}(.)$. Then for all real x,
$P\{\mathbb{P}(X) \leq \mathbb{P}(x)\} = \mathbb{P}(x)$

Statement

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

Proof

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

Complete Algorithm

RTSP-PhRNG algorithm consists of **detection algorithm** and **generation algorithm**.

Detection algorithm

Keep track of signal energy to detect random jamming attacks. The signal energy distribution evaluated by N samples of the received signal $R(t)$ in time slot s is represented as

$$Y = \frac{1}{N}\left(\sum_{s}^{s-N+1} R(s)^2\right) \tag{11}$$

The binary hypothesis test uses an energy threshold Θ that is chosen after considering tradeoffs between probability of detection and false alarm.

$$\begin{aligned} H_0 &: P(D_1|Y) < \Theta, \\ H_1 &: P(D_1|Y) \geq \Theta. \end{aligned} \tag{12}$$

D_1 represents attacker present and Y represents the received signal energy.

Complete Algorithm

Supporting Theorem

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

Proof

Let

$$y = \begin{cases} 1, & \text{for } x > \lambda \\ 0, & \text{for } x \leq \lambda \end{cases} \tag{13}$$

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

$$P(Y=y) = \begin{cases} 1/2, & \text{for } y = 1, \\ 1/2, & \text{for } y = 0. \end{cases} \tag{14}$$

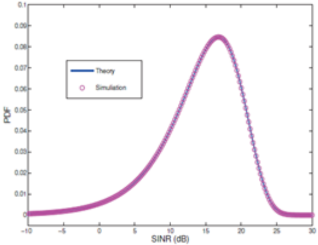
Complete Algorithm

Algorithm 1 RTSP-PhRNG

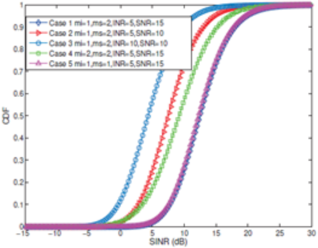
Input:
A's Random Transmission Success Probability P_s
Output:
Binary random numbers $R \sim U(0,1)$

Random jamming attackers detection using Eq.(12)
if state H_0 **then**
    A communicates with B in communication mode.
else
    A switches to PhRNG mode and generates random transmission success probability P_s
    Set quantization threshold $\lambda = 1/2$
    for $j \longleftarrow 1$ to length $|P_s|$ **do**
        if $P_s(j) \geq \lambda$ **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

Results and Simulation



(a) Simulation PDF vs. theory PDF



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

Figure: Simulation Results

In graph (a), simulation PDF is compared with theory PDF for fading parameter $m_s = 2$, $m_i = 1$, SNR $\Omega_s = 25dB$, and INR $\Omega_i = 11dB$, respectively.

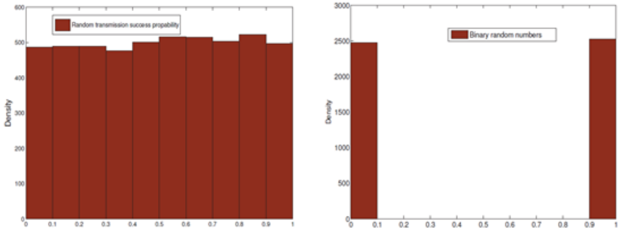
In (b), we analyze the impact of Ω_s on generation performance.

Results and Simulation

Inference

- Higher SNR leads to larger RTSP for the same threshold.
- Average INR power has a remarkable influence. Higher interference leads to lower RTSP.
- Different degrees of fading also have effect on the performance.

Experimental Results



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

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

Figure: Experiment Results

If A sends out n packets one time, but if only m of them go, then RTSP is m/n. Random threshold γ_{rv} is controlled by changing transmission power randomly (Gaussian random variable).
$\lambda = 1/2$ and packet rate $= 25 \times 10^3$ per second.
The communicators and a jammer move in an indoor area randomly.

Experimental Results

Inference

- The generated random numbers contain nearly the same number of 0s and 1s.
- Generation rate depends on packet rate and packet number n. (For this paper, max rate is 25 Kbps).
- Compared with Quantum random number generator and verified good effectiveness of result.

Conclusion

Final Points

- A wireless PHY-layer characteristics based random numbers generator for vehicular networks has been proposed.
- Expression derived in terms of RTSP using a random threshold.
- Hijack the jamming attackers themselves.
- Effectiveness proved by simulation and results.