CIT. Journal of Computing and Information Technology, Vol. 29, No. 2, June 2021, 89–111
doi: 10.20532/cit.2021.1005317

Providing Physical Layer Security for IoTs in the Last Mile

Hong Zhao[1] and Paul Ratazzi[2]

[1]Fairleigh Dickinson University, Teaneck, New Jersey, United States
[2]Air Force Research Laboratory, Rome, New York, United States

Communication security is one of the top security challenges for connected devices. Different from other links such as backhaul, the last mile technology also depends on the requirements of end users. Wireless technologies are generally selected for the mobility of users and ease of use. However, wireless medium has an open nature and thus wireless links are more prone to physical layer attacks compared to their wired counterparts. Moreover, simple end devices have constrained resources in both hardware and software, and it is not always feasible to apply conventional cryptographic approaches to provide security. We turn to chaos theory to provide security for simple devices at physical layer. The FM-DCSK and FM-CSK transmission system are built and implemented in the proposed secure communication system. The information message is embedded in wideband random-like signals, making the message remain covert. Transmission security is achieved by using the initial conditions and spreading factor as keys. To guard against active attacks, procedures for dynamic adjustment of initial conditions and other parameters are proposed. The scheme's cost effective features include the simplicity of communication setup and the low power consumption in generating and controlling the chaos signal. The sensitivity to initial condition and complex dynamic feature of chaotic function make it a promising approach for physical layer security.

ACM CCS (2012) Classification: Security and privacy → Network security → Mobile and wireless security

Keywords: physical layer security, chaos based communication, IoT security

Approved for Public Release; Distribution Unlimited: AFRL-2020-0025; Dated 05 AUG 2020. The views expressed are those of the authors and do not necessarily reflect the official policy or position of the Department of the Air Force, the Department of Defense, or the U. S. government.

1. Introduction

The upcoming 5G communication system is expected to support diverse services and applications with various characteristics and requirements, and Internet of Things (IoT) will play an important part in making this happen. With more devices connected, there will be more security problems introduced in a cyber system. Communication security is one of the top security challenges for connected devices, especially for physical devices connected through wireless technology for mobility. This part is often referred as the last mile—the last part where the user is served. Due to their open nature, wireless links are more vulnerable to security breaches (*e.g.* eavesdropping) compared to their wired counterparts. Most current wireless access networks apply conventional cryptographic approaches implemented on upper layer operations to provide confidentiality, authentication and data integrity. This generally requires high computational platform, which may not exist in all IoT devices. For example, the one of the most adopted last mile connection technologies-LoRaWAN, utilizes two layers of security: one for the network and one for the application. The network security ensures authenticity of the node in the network while the application layer of security ensures that the network operator does not have access to the end user's application data. Advanced Encryption Standard (AES) is used with the key exchange utilizing an IEEE EUI64 identifier [1]. This requires that each edge device should be able to store the keys and perform AES encryption/decryption, which are not suitable for

simple low end devices with limited hardware, and severe energy constraints. For these simple devices such as sensors and actuators, most of the available energy and computation must be devoted to executing core application functionality, and there may be little left over for supporting security. Thus, complexity and energy efficiency are critical aspects in design of security approaches for IoTs.

Physical Layer Security (PLS) takes advantage of intrinsic characteristics of wireless channels and realizes a keyless secure transmission via signal design and signal processing. Moreover, the unpredictable, but characteristic features of wireless channels may be exploited to generate keys for traditional encryption mechanisms. Typically, PLS techniques rely on relatively simple signal processing algorithms, incur less overhead, and thus they may have remarkably reduced computational complexity. As such, PLS approaches that apply the principles of information theoretic security and signal processing to physical layer systems [2], play an important role in securing these highly constrained devices.

In this paper, we propose a novel physical layer security system including secure transmitting of message at waveform level, and hardware assisted device authentication. The main contributions can be summarized as follows:

- implemented chaos-based FM-DCSK/FM-CSK communication systems;
- designed a filter to improve the performance of FM-DCSK under Rayleigh/Rician fading channels;
- conducted security analysis for both FM-DCSK and FM-CSK in terms of statistical property and key space;
- proposed a PUF based authentication scheme which does not require a large number of CRPs, thus reduced hardware overhead for low-cost IoT end devices;
- a security protocol in switching modulation schemes/setting up transmission parameters is proposed.

The rest of the paper is organized as follows: following a brief background in Section 2, the proposed physical layer security system is presented in Section 3. Performance analysis of the proposed approach and simulation results are discussed in Section 4. Section 5 analyzes security performance. Application of the proposed approach in IoT authentication is given in Section 6. Conclusions and future work are presented in Section 7.

2. Background

Security is a paramount challenge that needs to be addressed at every stage of communications as shown in Figure 1, from the high volume of endpoint devices including sensors that gather data and actuators that execute tasks, to cloud-based control systems through network infrastructure [6]. The security of wireless communications across the last mile marked as 1 is the focus of our work. The basic system that can be defined for communication at this stage consists of three nodes: one legitimate transmitter, one legitimate receiver and one eavesdropper/attacker. The challenges of providing security for this segment of the architecture include:

- wireless links use unguided medium as communication channels, and therefore intercepting, connecting and injecting wireless data transmissions is easier when compared to traditional cabled systems; wireless communication is thus prone to many security vulnerabilities from the very beginning, due to the lack of traditional physical barriers;
- IoT devices are resource-constrained and characterized by low capabilities in terms of both computation and energy capacity; for these simple devices such as sensors and actuators, most of the available energy and computation must be devoted to executing core application functionality, and there may be little left over for supporting security functions;
- conventional cryptographic approaches generally require high computation platform, which may not exist in all IoT devices.

In wireless communication networks, adversaries attack one or more of system security requirements including confidentiality, authentication, integrity and robustness. Confidentiality defines the secretness of the data between the

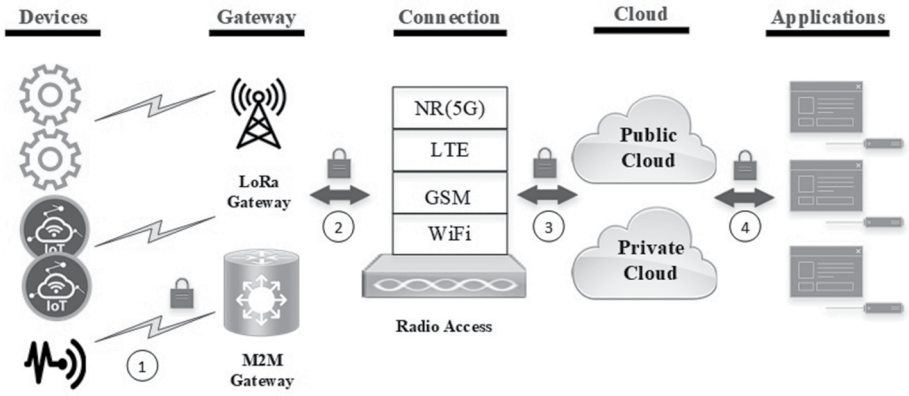


Figure 1. IoT security architecture.

origin and destination. Authentication is the act of confirming that the destination of data has access right. Integrity refers to the completeness and originality of the data during its life cycle. Robustness is defined for the communication system to remain operational under degrading effects. Keeping secret transmission of data and being able to authenticate each device at the physical layer are very important in securing wireless systems that are not well suited for conventional cryptographic approaches.

2.1. Last Mile Connection Technologies

The majority of IoT devices were not built or designed to interface with high-bandwidth networks. Connecting these devices requires technologies that provide long range communication with lower power, while at the same time providing robust security. Although there is still no unified connectivity solution for IoT at this point, there are a number of different technologies that are in operation, including cellular, satellite, Zigbee, Near Field Communication (NFC), Radio Frequency Identification (RFID), LoRaWAN, and so on. The various advantages and disadvantages of each all come down to a tradeoff between power consumption, range, and bandwidth. For IoT devices such as sensor nodes and tracking devices that are often placed remotely and battery-operated, distance and power consumption are the two main factors in selecting a particular last mile connection technology. To increase range while maintaining low power consumption, one must decrease the amount of data being sent. By optimizing this tradeoff, many sensors can be deployed to collect and send data over broad areas while easily lasting years on a single battery. As an example, LoRaWAN is one of the most adopted technologies to offer long distance communication while keeping power consumption low. LoRaWAN's primary application is for communication among sensors and actuators that are remotely located, such as those used to monitor the state of distant environmental or geologic parameters. The collected data is transmitted from each sensor to a LoRaWAN gateway node and then forwarded to edge of network. After processing at the edge by traditional computing platforms, control commands are returned to the actuators. While communications between the gateway node and the network edge could be secured using traditional means, such as a Virtual Private Network (VPN), the last mile communication between sensors/actuators and the gateway is subject to thermal noise, path loss and fading, making application of mechanisms designed for low latency, high bandwidth links problematic. In addition, even if the links were not disadvantaged, severe constrains in hardware/software of the simple sensor/actuator devices do not meet the computational requirements of conventional cryptography solutions.

2.2. Physical Layer Security

Existing physical layer security approaches can be classified as code based methods, sig-

naling based methods, and physical layer based encryption methods. The code based methods, including Error Correcting Coding and Spread Spectrum Coding, are typically used to improve resilience against jamming and eavesdropping. Physical layer based encryption methods exploit the wireless communication medium to develop secret keys over public channels. The signaling based methods provide data protection by using signaling design approaches. Common signal based schemes involve beam forming and artificial noise. Unfortunately, not all the existing physical layer security techniques are suitable for IoT applications due in part to the unique characteristics of low-end devices: limited signal processing capabilities, limited storage memory, and significant energy constraints. For example, most of the artificial noise (AN)-based PLS schemes rely on the deployment of multiple antennas at the transmitter, which is not possible given the low-cost and small-size requirements of IoT devices.

Physical Unclonable Functions (PUF) leverage uncontrollable and intrinsic physical characteristic patterns of silicon devices, which can be used in device authentication. Most current PUF based authentication schemes transmit Challenge-Response Pairs (CRPs) without any protection, requiring a large number of CRPs. Hence, in these applications, a strong PUF with more hardware overhead is needed, making it difficult to be used on simple IoT devices. Although the IoT authentication scheme described here is PUF based, our proposed authentication process does not require strong PUFs with exponential number of CRPs, as the CRPs are protected by the proposed chaos based communication system.

2.3. Chaos Modulations to Secure Data Transmission

In contrast to the aforementioned PLS methods, chaos based secure communication hides information at the waveform level by using chaotic signals as the carrier. The information message is embedded in wideband random-like signals, keeping the message covert. It has been proven that chaos based modulations have Low Probability of Interception (LPI) [4]. Thus, potential eavesdroppers are uncertain if transmissions are going on. Furthermore, the chaotic modulation schemes offer the simplicity of communication setup, low power-consuming devices to generate and control chaotic signals, and no need of using complicated and energy consuming devices to avoid nonlinearities [5]. Compared with conventional communication systems that require the intensive use of modulators, source encoders, channel encoders and filters, chaos based communications schemes can be implemented using only one subsystem to provide all the basic processing at each end of the communication link. These characteristics make the chaos based approach a promising approach for providing security to severely constrained IoT devices. Chaotic communication uses a chaotic signal to transmit information. Chaos mask modulations can utilize chaos signal as a communication carrier and chaos parameter modulation scheme is to embed information data into the chaos control parameters. Due to their complex behavior, noiselike and dynamic features, chaotic communication is aimed to provide security in transmission of information. Particularly, the spread spectrum feature of chaos dynamics makes chaotic communication a good candidate for security. The conventional spread spectrum communications for hiding message or resisting enemy efforts to jam the communication require to generate broadband signals to provide a secure communication channel. In chaos based schemes, such broadband signals are generated by the chaos generating device itself. In practice, this means that chaotic systems make use of the input energy to generate broadband signals. Among all the chaos modulation schemes, the non-coherent DCSK (Differential Chaotic Shift Keying) remains the best in terms of robustness against multi-path fading and channel imperfection. The coherent CSK (Chaotic Shift Keying) has the best performance in providing security of data transmission.

3. The Proposed Physical Layer Security System

We turn to chaos based modulations to reduce hardware overhead in providing physical layer security for low-cost devices. In this paper, a discrete-time dynamical system Henon map is used as chaotic carrier, which is described in Equation (1):

$$x_{k+1} = 1 - ax_k^2 + y_k$$
$$y_{k+1} = bx_k \quad (1)$$

where a and b are control parameters of the Henon map. Depending on the values of a and b, the Henon map could be chaotic, intermittent or convert to a periodic point. In our experiment, $a = 1.4$, $b = 0.3$, which makes the Henon map chaotic. This chaotic signal is then used as a carrier to transmit data. In DCSK modulation, each symbol duration is split into two time slots. The first time slot serves as a reference while the second time slot carries information. If bit "1" is to be transmitted, a reference chaotic sequence is sent in the first time slot while in the second time slot, the time delayed reference copy is sent; if bit "0" is to be transmitted, the inverted copy of the chaotic reference sequence is sent in the second time slot. The l-th transmitted symbol is denoted by b_l, which is either +1 or −1, representing digital bit 1 and 0, respectively. During the l-th symbol duration T_b, the transmitted signal s_l is formed by the following Equation (2):

$$s_l = \begin{cases} \frac{1}{\sqrt{E_b}} x_k & k = (l-1)\beta + 1, \ldots, (2l-1)\frac{\beta}{2} \\ \frac{1}{\sqrt{E_b}} b_l x_{k-\frac{\beta}{2}} & k = (2l-1)\frac{\beta}{2} + 1, \ldots, l\beta \end{cases} \quad (2)$$

$$E_b = \sum_{k=1}^{\beta} x_k^2 \quad (3)$$

where β is a spreading factor, representing the number of chaotic data to transmit 1-bit information. During the first half of symbol duration T_b, $\beta/2$ chaotic data are transmitted as a reference signal and the $\beta/2$ chaotic data is either repeated or inverted during the second half of T_b, depending on the information to be transmitted. The chaotic sample function consists of β chaotic data, which keeps changing for each symbol. Thus, the transmitted signal has a different shape during every symbol duration T_b. As a result, the transmitted signal is never periodic and it is a wideband signal. Here, E_b is the energy per bit defined in Equation (3). One condition for chaotic modulations to reach their maximum noise performance is that chaotic sample functions should have constant energy per bit [8]. This can be achieved by applying chaos signal to a Frequency Modulator (FM). For AWGN channels, the FM-DCSK demodulation process could simply apply a Correlator to recover the message. The performance of FM-DCSK over AWGN is improved compared to DCSK. For multipath Rayleigh/ Rician fading channels, the signal strength will undergo large fluctuation and the message cannot be recovered at the receiver. The proposed receiver structure is shown in Figure 2. It shows the block diagram of the FM-DCSK communication system. At the receiver side in Figure 2, a noise filter is added. The demodulation process is carried out without any knowledge of channel state information. As both the reference signal and information bearing signal pass through the same channel, FM-DCSK is not sensitive to channel distortion. This is a great feature for long range wireless connections where multipath fading is a major issue. Both Rayleigh and Rician fading channels are considered in this paper to evaluate the performance of the communication system in Figure 2. The performance analysis is discussed in Section 4. The security of FM-DCSK is implemented at waveform level. The chaotic signal has the advantages of being non-periodic and being difficult to predict. The chaotic sequences used as carrier are different for every bit of the message to be transmitted, even if the same bit is transmitted repeatedly. For passive attacks such as eavesdropping, it is difficult to even estimate the spreading factor. Considering some IoT devices which are not physically protected, we propose to use the spreading factor β as a key and dynamically update it to protect against attacks. Spreading factor β has different impacts on FM-DCSK performance under AWGN and Rayleigh/Recian channels. For multi-path fading channels, our experiments show that the range of β is limited in order to receive better performance. From the cryptographic point of view, the key space is relatively small. Furthermore, the reference signal included in the transmission also brings security concerns. Coherent demodulation needs the receiver to reconstruct the chaos carrier signal, which means that the security

is better provided than with noncoherent demodulation, but it needs complex hardware to realize synchronization.

Figure 3 shows coherent Frequency Modulated Chaos Shift Keying (FM-CSK). (Note that a local chaos generator is needed at the receiver to reconstruct the chaos carrier signal.) Chaos signal is very sensitive to its initial conditions and parameters. Thus, stronger security could be provided in FM-CSK than in FM-DCSK. In the antipodal CSK modulation, the transmitted signal s_l during l-th symbol duration T_b is either x_k or its inversion, and is determined by whether the binary symbol " + 1", or " − 1", which is given in Eq.(4).

$$s_l = \begin{cases} x_k, & k = (l-1)\beta + 1, ..., l\beta, \ b_l = 1 \\ -x_k, & k = (l-1)\beta + 1, ..., l\beta, \ b_l = -1 \end{cases} \quad (4)$$

Here, β is the spreading factor and E_b is the energy per bit defined in Equation (3), which will be kept constant via FM. The block diagram is shown in Figure 3. The demodulation process requires the local chaos generator having the same control parameters as the ones used at the transmitter. Both chaos generators should start

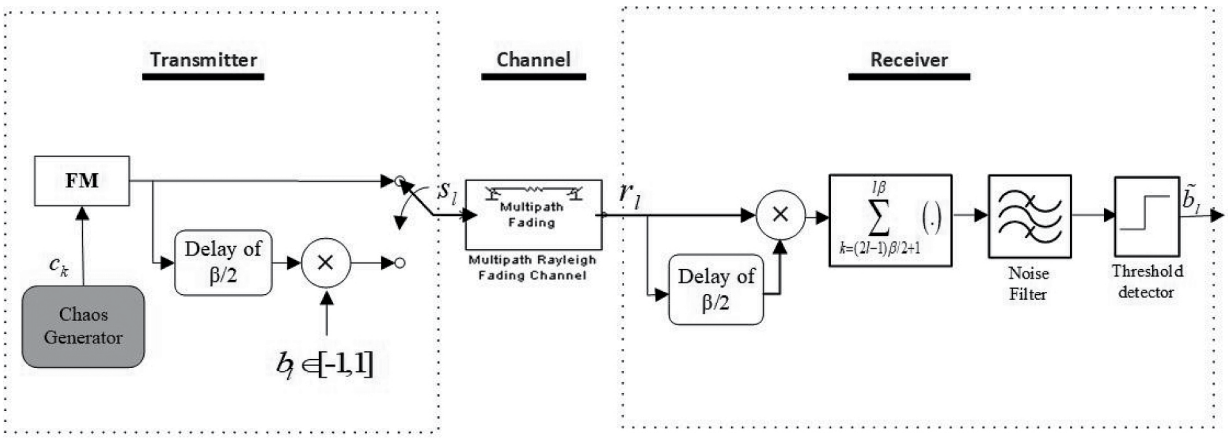


Figure 2. FM-DCSK communication systems.

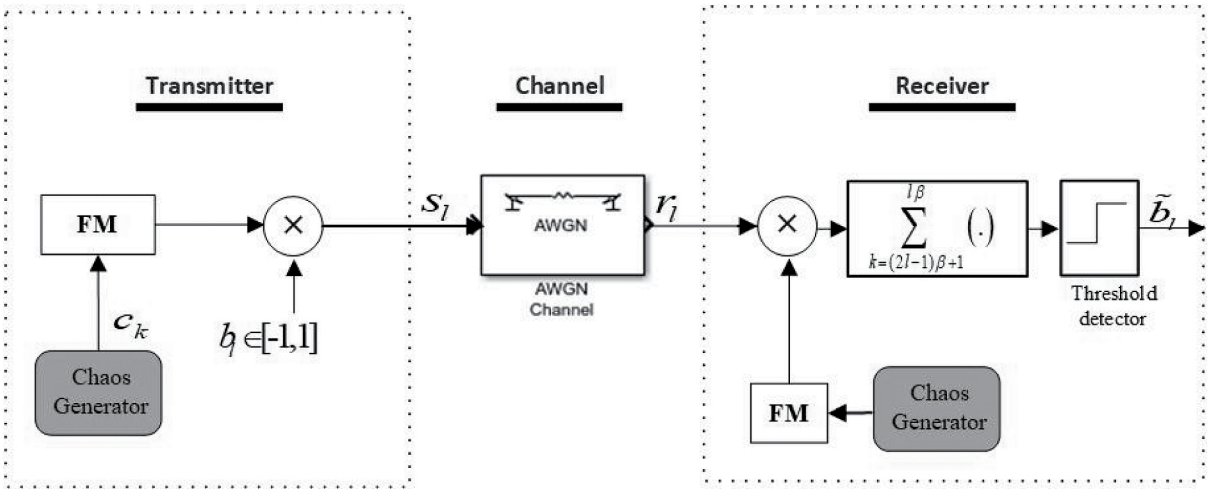


Figure 3. FM-CSK communication systems.

from the same initial condition μ_0 in order to recover the data sent from the transmitter.

Sensitivity to initial conditions is a main feature of chaos dynamical system. Two neighboring initial values of μ_0 and $\tilde{\mu}_0$ can evolve to different trajectories under the same value of control parameters. After a certain time, a tiny difference grows to an enormous one. The chaotic sample function in FM-CSK contains $\beta = 100$ chaotic data, which will be changing for every bit data to be transmitted. If there is a minor difference in guessing the initial value used at the transmitter side, the resulted sample function will be completely different, resulting in bit errors at the receiver site. The initial condition is used as a key in our proposed PLS approach. The security in noncoherent demodulation is not as strong as coherent demodulation, but it is easier to implement and the hardware cost is much lower. A protocol of switching modulation schemes and the security performance are discussed in Section 5.

4. Performance Analysis and Results

In wireless communications, especially for long range ones, multipath fading is often a major factor that influences the performance. The transmitted signal follows many different paths before arriving at the receiving antenna, and it is the aggregate of these paths that constitute the multipath radio propagation channel. This causes the received signal to vary greatly in amplitude and phase, which is referred as multipath fading. Rayleigh and Rician fading channels are useful models of real-world phenomena in wireless communications. These phenomena include multipath scattering effects, time dispersion, and Doppler shifts that arise from relative motion between the transmitter and receiver. A discrete multipath Rayleigh fading channel model in [10] is considered. Let s_i denote the set of samples at the input to the channel. Then the samples y_i at the output of the channel are related to s_i through:

$$y_i = \sum_{n=-N_1}^{N_2} s_{i-n} g_n \tag{5}$$

where g_n is a set of tap weights given by

$$g_n = \sum_{k=1}^{K} a_k sinc\left[\frac{\tau_k}{T_s} - n\right],\ N_1 \le n \le N_2 \tag{6}$$

T_s is the input sample period to the channel. N_1, N_2 are chosen so that $|g_n|$ is small when n is less than $-N_1$ or greater than N_2. τ_k is the set of path delays, $1 \le k \le K$, and K is the total number of paths. The fading process, a_k, $1 \le k \le K$, a set of complex path gains, is generated by either filtered Gaussian noise or sum of sinusoids techniques according to [10]. These path gains are uncorrelated with each other. The complex process resulting from either technique, z_k is then scaled to obtain the fading process a_k. In the case of the Rayleigh fading channel, a_k is obtained as:

$$a_k = \sqrt{\Omega_k} z_k \tag{7}$$

where $\Omega_k = E\left[|a_k|^2\right]$. In the case of the Rician channel, the fading process is obtained as:

$$a_k = \sqrt{\Omega_k}\left[\frac{z_k}{\sqrt{K_{r,k}+1}} + \sqrt{\frac{K_{r,k}}{K_{r,k}+1}} e^{j(2\pi f_{d,\,LOS,\,k} + \theta_{LOS,\,k})}\right] \tag{8}$$

$K_{r,\,k}$ is the Rician K factor of the k-th path, $f_{d,\,LOS,\,k}$ is the Doppler shift of the line-of-sight component of the k-th path, and $\theta_{LOS,\,k}$ is the initial phase of the k-th path. As *sinc* function in Equation (6) decreases rapidly, a two-way ($K = 2$) Rayleigh/Rician fading channel with Doppler power spectrum discrete model in Figure 4 is considered in our experiments. Relative motion between transmitter and receiver causes Doppler shifts in signal frequency. Sensors/acutors are moving relatively slowly, the maximum doppler shift 20 Hz with Jake Doppler spectrum considered in our experiments.

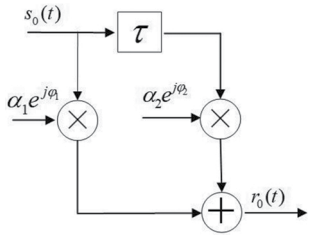


Figure 4. Two-way fading channel model.

Figure 5 shows the two-way Rayleigh fading channel path gains. The FM-DCSK signals are first converted to complex signals and then applied to the Rayleigh multipath fading channel. At the receiver side, the real part of the received complex signals is used to recover the information data. Due to big signal fluctuation in multipath fading channel shown in Figure 5, the regular receiver structure is not able to recover FM-DCSK signal after multi-path fading channel models described above. Thus, the receiver is modified by adding a noise filter shown in Figure 2. Figure 6 shows the performance of FM-DCSK over a two-way Rayleigh fading channel. The transmitted message data in Figure 6 (a) is fully recovered and is shown in Figure 6 (e). In testing FM-DCSK under a two-way Rician fading channel, the following parameters are chosen: discrete path delay vector as $[0, 2e-6](s)$, K factor vector $K_{r,k} = [1, 1]$, Doppler shifts of line-of-sight components as $f_{d,LOS,k} = [5, 5]$(Hz), the initial phases $\theta_{LOS,k}$ for both pathes are selected as 0, and the maximum diffuse Doppler shift as 5 Hz with Jake spectrum. Figure 7 shows the performance of FM-DCSK under 2-way Rician channel. The simulation results show that FM-DCSK has high resistance to interference and strong immunity against multipath effects, which is a big concern in long distance wireless connection.

The cross-correlation, which will be discussed in Section 5, is lower between segments of chaotic waveforms than between pieces of periodic waveforms. This also contributes a better performance under multi-path fading channels. Concerning the overall implementation, conventional communication systems require the intensive use of modulators, source encoders, channel encoders and filters. The proposed approach can be implemented using only one subsystem which provides all the basic processing. All the above features make it a promising approach for physical layer security.

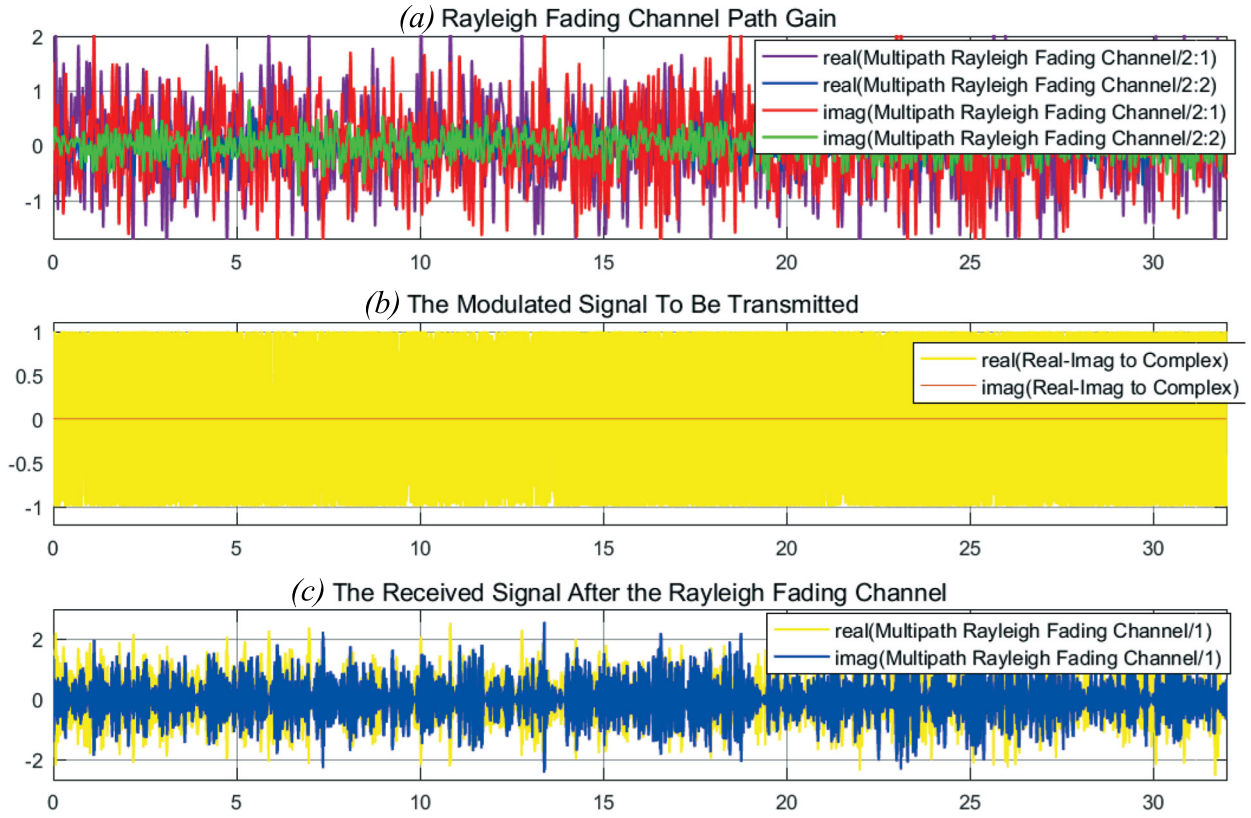


Figure 5. The signal fluctuation after the two-way Rayleigh fading channel.

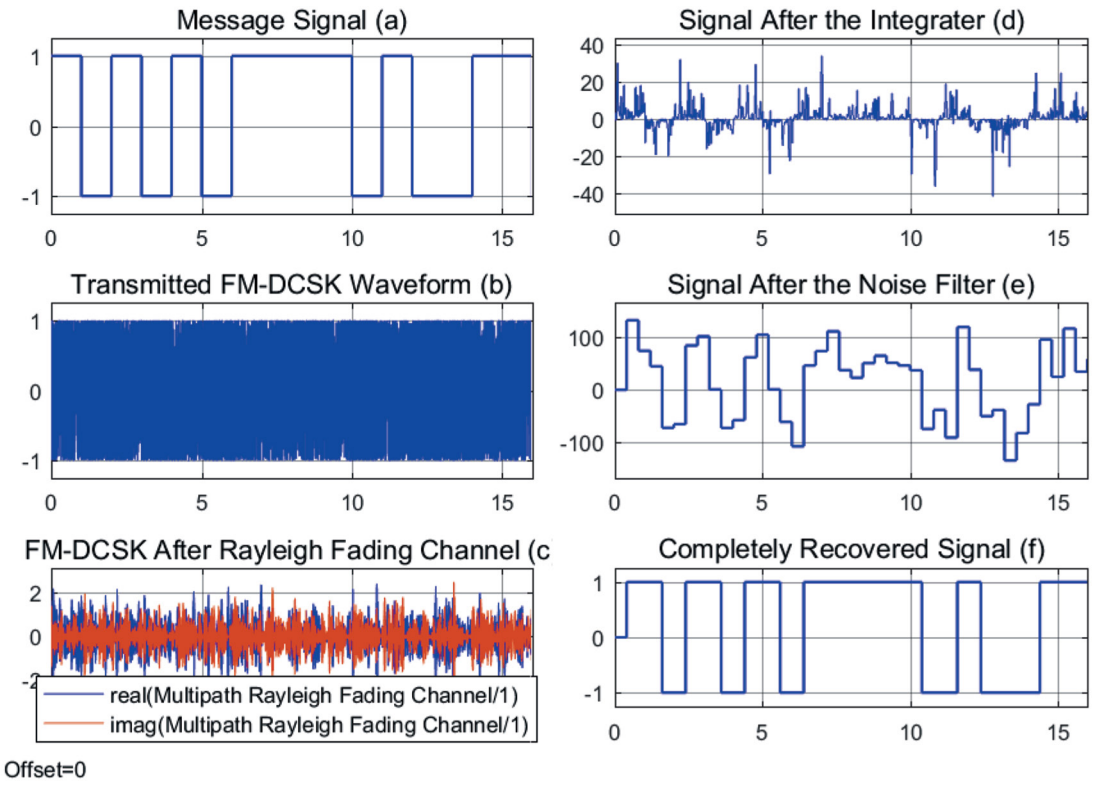


Figure 6. Performance of FM-DCSK under Rayleigh channel.

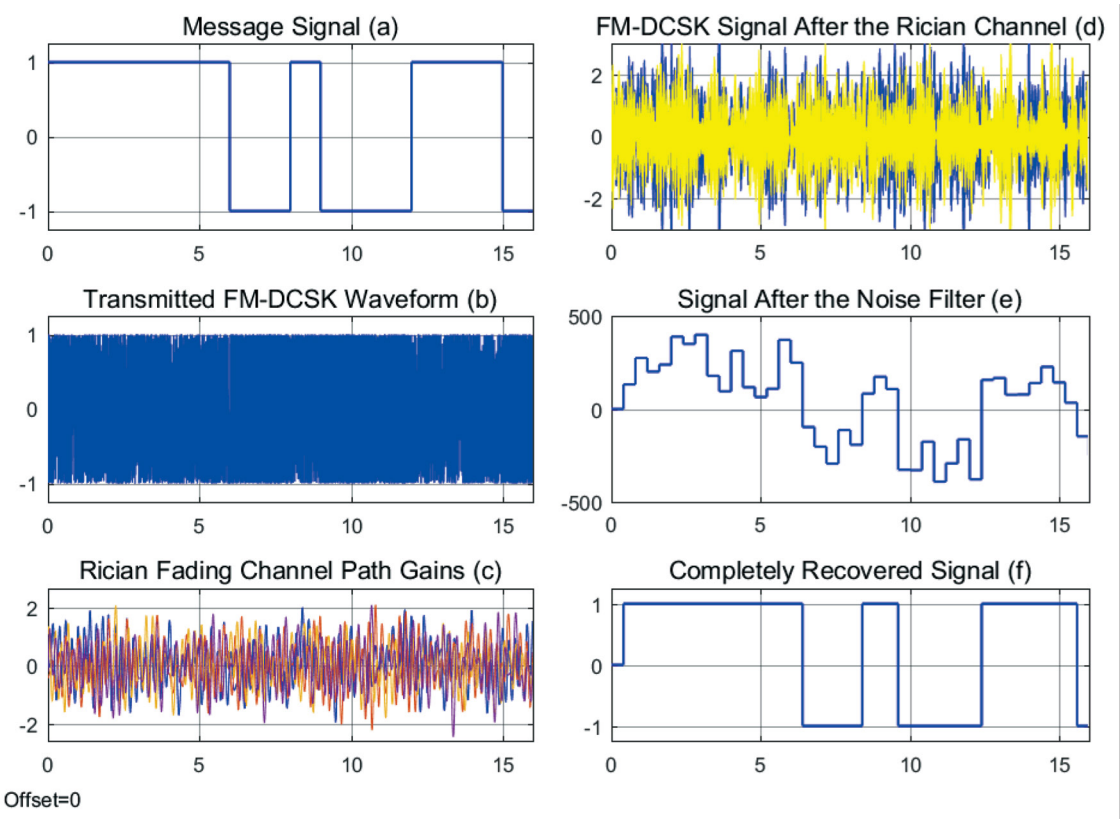


Figure 7. Performance of FM-DCSK under Rician channel.

The performance behavior of the FM-DCSK system under the above described 2-way Rayleigh and Rician fading channels for different spreading factors (β) is also studied through simulations. The simulation results show that spreading factor values under $\beta = 40$ minimize bit error rates at fixed E_b/N_0. Spreading factor values $\beta = 30$, $\beta = 20$ are selected for both Rayleigh and Rician channels to obtain good performance shown in Figs. 6 and 7. Another benefit is that low spreading factor values make this system implementation feasible even for a moderate bandwidth.

5. Security Performance

Measurement of the security aspects of any communication system is not an easy, but an important task. We will address security performance of the proposed PLS approach from the following three aspects:

- covertness of the chaotic communication,
- autocorrelation and cross-correlation property of the chaotic carrier,
- key space of the proposed approach.

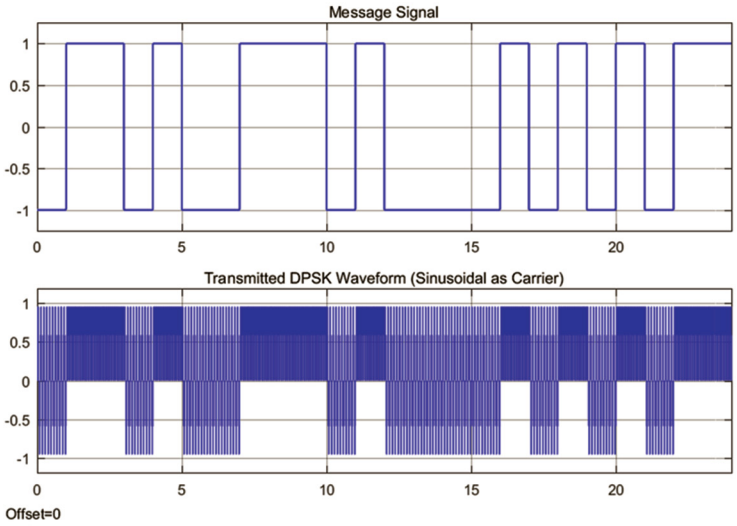
5.1. Information is Hidden in Chaotic Carrier

Instead of using sinusoidal/chirp signal, chaotic signal is used as a carrier in data transmission. Chaotic signals are irregular, aperiodic, uncorrelated, broadband, and impossible to predict over long time. The security of chaos modulation is directly implemented at waveform level. Let us take a look at DPSK (Differential Phase Shift Keying) using sinusoidal signal and chirp signal as carrier. Figure 8 shows the transmitted signal waveforms using sinusoidal in Figure 8 (a) and chirp signal in Figure 8 (b) as carrier, respectively. Once the transmitted signal is captured, an attacker can easily figure out the message in an open environment. Figure 8 (c) shows the transmitted waveform using chaotic signal as carrier. The information is hidden in the chaotic carrier signal. (Note that the chaotic sequences used as carrier are different for every bit of the message, even if the same bit is transmitted repeatedly.) The continuously varying waveforms make it very hard to find a mathematical model for the detection problem. In the proposed scheme, β is defined as the spreading factor, representing the number of chaotic data to transmit 1-bit information. It is difficult to predict or even estimate the chaotic spreading sequence, making attackers difficult to decode the message. As the transmitted waveforms are wideband signals, attackers may not even know the communication is going on. The performance of detection probability of chaotic signals has been analyzed in [4]. The authors compared the binary PN (Pseudo Noise) sequence with the chaotic spreading sequence in the DS-SS (Direct Sequence Spread Spectrum) system. By considering different types of intercept receivers and energy detectors, LPI performance advantages of chaotic signals are observed. Noise-like chaotic signals as carrier in both FM-CSK and FM-DCSK can be used to conceal signals and improve the covertness of communications.

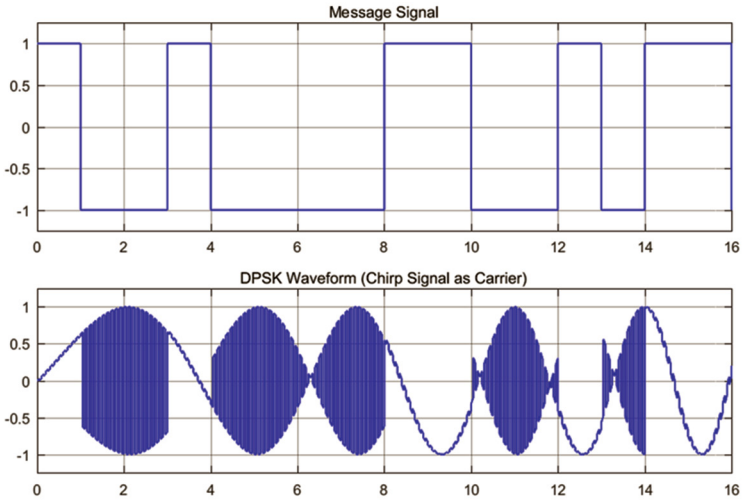
5.2. Statistical Property of Chaotic Signal

Due to the open nature of wireless links, attackers are able to receive all the signals sent to a legitimate user. This is similar to cipher-text only attack in cryptography: Eve has the cyphertext that she can analyze. Two approaches are used: brute force and statistical analysis. By searching through all keys, brute force tries to find the correct key (Key sensitivity and its space are two important factors which will be discussed in Section 5.3). It is well known that many ciphers have been successfully analyzed with the help of statistical analysis and several statistical attacks have been devised on them. In this section, we evaluate the robustness of the proposed security approach by investigating the autocorrelation and cross-correlation of the chaotic carrier sequences. Cross-correlation measures the similarity of two discrete time series X and Y. Given the two chaotic carrier sequences: X_1, X_2, ..., X_N, and Y_1, Y_2, ..., Y_N measured at t_1, t_2, ..., t_N, the cross-correlation is calculated as:

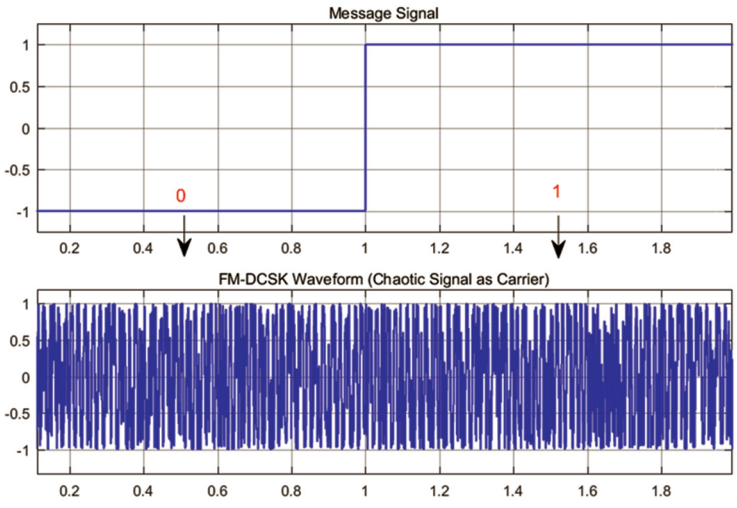
$$\hat{R}_{XY}(m) = \begin{cases} \sum_{n=0}^{N-m-1} X_{n+m} Y_n^* & m \geq 0 \\ \hat{R}_{XY}(-m) & m < 0 \end{cases}. \quad (9)$$



(a) Sinusoidal carrier.



(b) Chirp carrier.



(c) Chaos carrier.

Figure 8. Waveform comparison of chirp, sinusoidal and chaotic signals used as carrier.

The cross-correlation output is

$$C(m) = \hat{R}_{XY}(m-N),$$

$$m = 1, 2, ..., 2N-1.$$

In general, the crosscorrelation function requires normalization to produce an accurate estimate. The normalized cross-correlation coefficient is defined as:

$$\rho_{XY}(m) = \frac{\hat{R}_{XY}(m)}{\sqrt{\hat{R}_{XX}(0)\hat{R}_{YY}(0)}}, \quad m = 1, 2, ..., 2N-1 \tag{10}$$

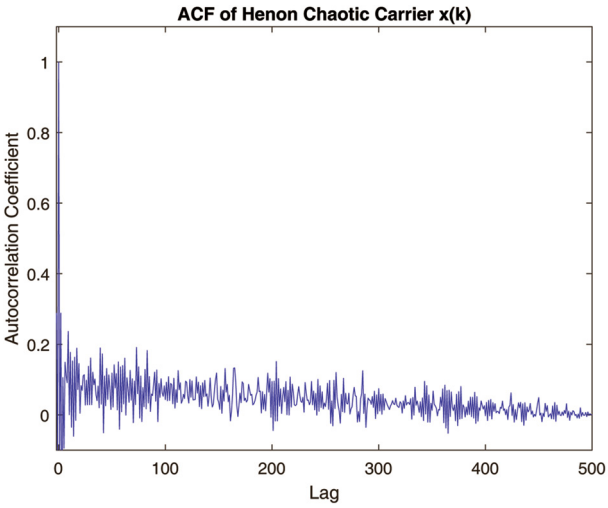


Figure 9. The autocorrelation of Henon chaotic carrier for the first 500 data.

The autocorrelation (ACF) is the correlation between two values of the same variable at times t_i and t_{i+m}, which means that the signal is being compared (for similarity) with a time shift. This can be calculated as in Equation (9) with same variable inputs. The autocorrelation is also normalized so that the autocorrelations at zero lag equal to 1.

Figure 9 shows the normalized autocorrelation coefficients of the Henon chaotic carrier with parameters $a = 1.4$, $b = 0.3$ and initial condition $\mu_0 = 0.2$. The lag (1) indicates the correlation between values that is one time period apart, and a lag (k) autocorrelation is the correlation between values that is k time periods apart. We could see that the autocorrelation coefficient has a strong peak as $\rho_{XX}(0) = 1$ at lag $k = 0$ and has small values approaching to 0 with large k. It verifies that the chaotic signal is a white noise-like signal, with high unpredictability. In both FM-DCSK and FM-CSK, the chaotic sequence used to transmit 1-bit information is different, even though the same message is repeated. For this reason, we compared the ACF of the first set of 500 chaotic data with the second set of 500 chaotic data as shown in Figure 10. Please note that $\rho_{XX}(k)$ in red line (representing the second 500 data) is smaller than the $\rho_{XX}(k)$ in blue line (representing the first 500 data) with lag increasing. This indicates that transmitted waveforms are becoming more noise-like and harder to be detected as time is going on.

Let us consider a scenario where both parameters and modulation scheme are known to an unauthorized user. The initial condition $\mu_0 = 0.2$ will be agreed on at the beginning of communication between the sender and the legitimate receiver. The attacker would guess/estimate the initial condition, say $\tilde{\mu}_0 = 0.20000001$. The two generated sequences $x(k)$ with $\mu_0 = 0.2$ and $y(k)$ with $\tilde{\mu}_0 = 0.20000001$ should be similar in order to recover the message signal sent from the sender. Cross-correlation is calculated to measure the similarity between $x(k)$ and $y(k)$. Figure 11 shows the normalized cross-correlation of chaotic sequences $x(k)$ and $y(k)$ for the first 500 data set in blue line and the second 500 data set in red line. For all lags, the cross-correlation coefficients are smaller than 0.3, which suggests that there is little correlation. Note that the difference between the two initial conditions, 0.00000001, is small, but the resulting sequence is very different than the one used at the transmitter. Let us check if the attacker with a very close initial value ($\tilde{\mu}_0 = 0.2000000000000001$) is able to recover a message. The message at the sender side is modulated by Henon chaotic sequence with $\mu_0 = 0.2$, the original message is shown in Figure 13 (a); Figure 13 (b) shows that the message is hidden in chaotic sequence; after transmission under AWGN channel, noise is added shown in Figure 13 (c); Figure 13 (f) shows the recovered message by the attacker, which does not even make sense to the attacker. We sim-

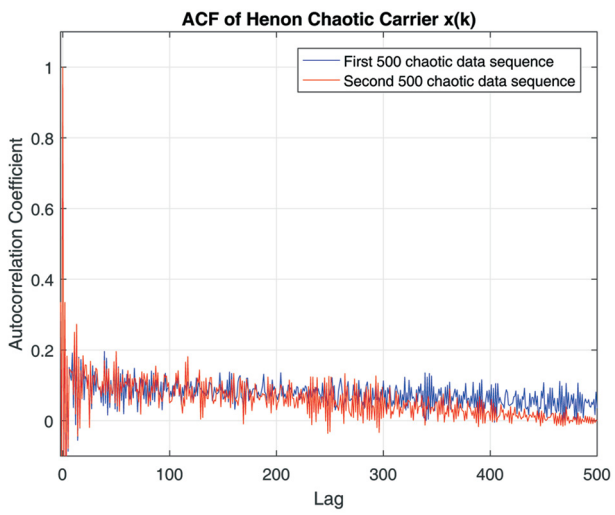


Figure 10. The comparison of ACF.

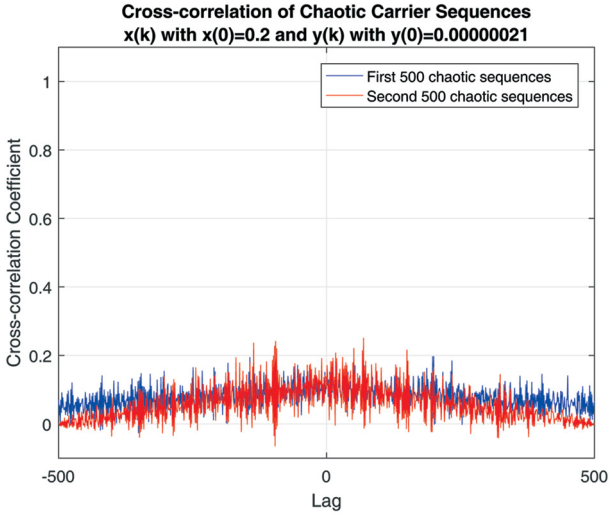


Figure 11. The comparison of cross correlation.

ulated 8-bit transmission, the attacker is not even able to interpret the recovered data. In the proposed scheme, the initial condition is considered as a key and the key space will be discussed in the following subsection to evaluate the security performance.

5.3. Key Space Analysis

In cryptography, an algorithm's key space refers to the set of all possible permutations of a key. To prevent an adversary from using a brute-force attack to find the key used to encrypt a message, the key space is usually designed to be large enough to make such a search infeasible. Now let us investigate the space of initial condition used as a key in FM-CSK. In Figure 12, both transmitter and receiver have the same initial value $\mu_0 = \tilde{\mu}_0 = 0.2$, μ_0 and $\tilde{\mu}_0$ representing initial values of chaos generator at transmitter and receiver, respectively. The message is transmitted under AWGN channel with $SNR = 10$ dB. The received message is recovered completely. Considering a scenario that an attacker tried a key $\tilde{\mu}_0 = 0.2000000000000001$, Figure 13 shows that the recovered message is totally different from the message transmitted, which means the attacker is not able to decode the message. The difference between these two initial values is $\delta = \mu_0 - \tilde{\mu}_0 = |0.2 - 0.2000000000000001| = 1 \cdot 10^{-16}$. Identifying this difference requires 50 binary digits. The key space is thus expressed as 2^{50} for FM-CSK. In FM-DCSK, every bit duration is split into two time slots. In the first slot, a reference chaotic sequence is sent while in the second slot, a data-modulated time-delayed chaotic reference signal is sent. At the receiver, the reference sequence is correlated with the data modulated sequence to recover the transmitted bit. The avoidance of chaotic sequence recovery brings better performance against multipath fading effects. From the security point of view, the non-periodic nature reinforces the transmission security only for passive attacks. For active attacks, the spreading factor β could be used as a key, but the key space is small. In our experiments, the performance of FM-DCSK over a two-way Rayleigh fading channel is analyzed. The BER (Bit Error Rate) increases with β due to the increased noise power when β is large for a fixed E_b/N_0. $\beta = 20$ is selected for multipath Rayleigh/Rician channels for best performance; $\beta = 100$ is selected for AWGN channel. The key space is about 5 bits for fading channel and 7 bits for the AWGN channel. Furthermore, the parameters a and b can be considered as additional source for the secret keys.

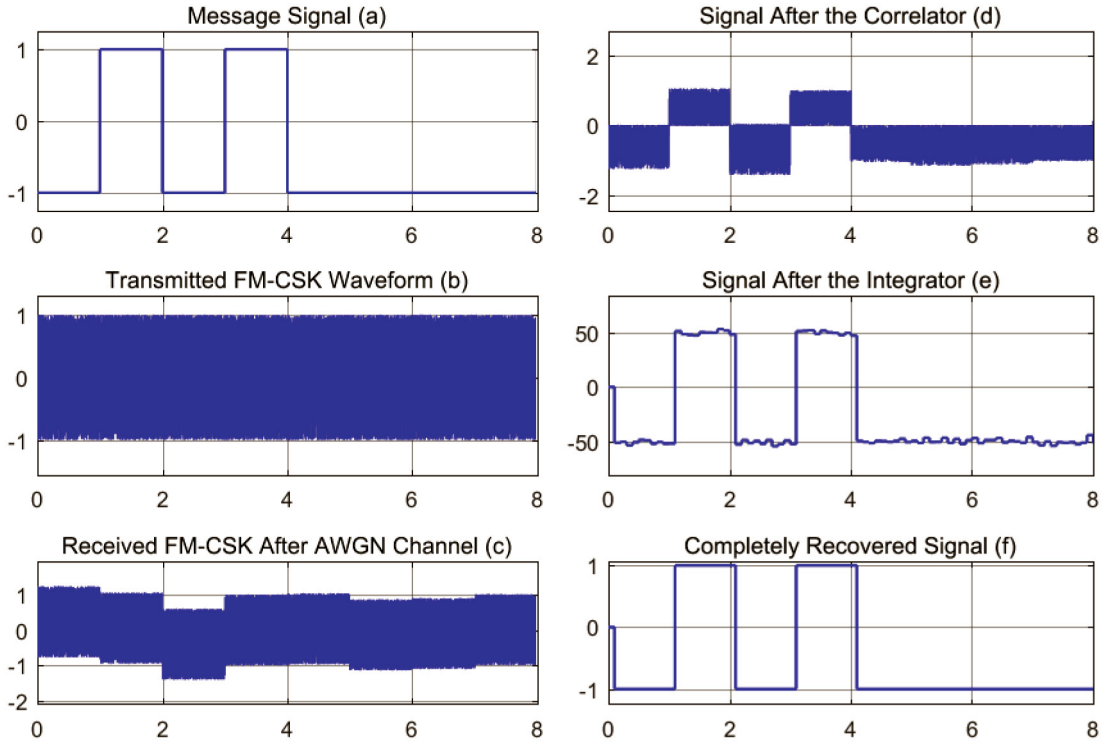


Figure 12. Legitimate user with the key $\mu_0 = 0.2$.

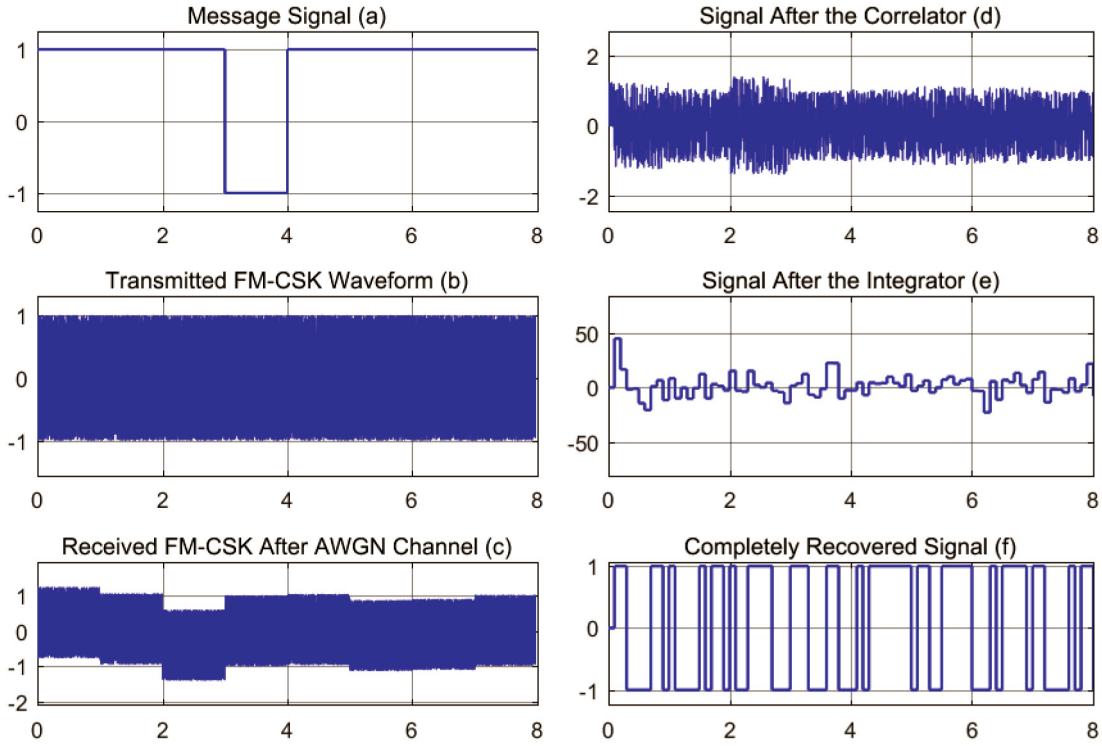


Figure 13. Attacker with a different key $\tilde{\mu}_0 = 0.2000000000000001$.

5.4. Security Protocol

Physical layer attacks on the security of communication networks can be divided into two basic types: passive attacks and active attacks. In passive attacks, the adversary does not provide input to the system, and has no access to the system. On the other hand, during active attacks the adversary uses a transmitter, actively interfering to the network. Let us use a three-node classic model shown in Figure 14 to illustrate a wireless connection with a potential eavesdropper. Here, a legitimate user (Alice) wishes to send a secret message to an intended receiver (Bob) in the presence an eavesdropper (Eve). The communication channel between Alice and Bob is called the main channel, while the one between Alice and Eve is named as wiretap channel. In the case of passive attacks, though Eve could capture the FM-DCSK signal, it is difficult for Eve to intercept it due to the non-periodic, pseudo-random, and wide-band feature of chaotic signals. The information is hidden in chaotic waveforms. The attacker is not even sure that communication is going on. The assumption we made here is that the attacker has no physical access to the IoT system. In considering remotely placed sensors/acuators, most devices are not physically protected and device hardware are designed for use by everyone. This gives potential attackers physical access to the system. For FM-DCSK, the exact knowledge of chaos based functions is not needed at the receiver. Once an attacker has access to the device, the message can be recovered. To protect against active attacks, a security protocol in switching modulation schemes/setting up transmission parameters is proposed. We could take advantage of channel secrecy capacity in transmitting spreading factor/initial condition. According to [18], the secrecy capacity C_s in Figure 14 is the difference between the main channel capacity C_m and the wiretap channel capacity C_w:

$$\begin{aligned} C_s &= \{0,\, C_m - C_w\} \\ &= B\left[\log(1+SNR_m) - \log(1+SNR_w)\right]^+ \end{aligned} \tag{11}$$

where $[x]^+ = \max\{0, x\}$. The secrecy capacity is the maximum secrecy rate that can be achieved by the legitimate users Alice and Bob given the presence of an eavesdropper, Eve. In order to obtain a secrecy capacity strictly positive, the quality of the main channel should be better than the wiretap channel, and a secure communication is possible. We chose to use this property of secrecy capacity and transmission rate in setting up the β for FM-DCSK and initial condition for FM-CSK. Both β and μ_0 are one piece of data information and low secrecy data rate is not a concern.

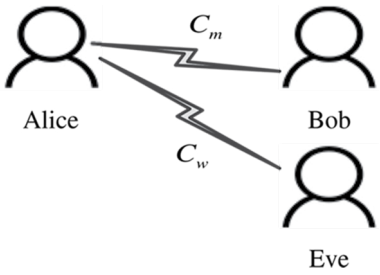


Figure 14. The wiretap channel.

As discussed in the previous section, the parameters in both FM-DCSK and FM-CSK could be adjusted online in enhancing transmission security. The following protocol is proposed in switching modulation schemes and setting initial values, or spreading factor β between transmitter and receiver:

1. Alice sends Bob a spreading factor β to be used in FM-DCSK modulation; the secure transmission is achieved by using the secrecy rate $R = C_s = C_m - C_w$;
2. Bob adjusts its FM-DCSK transmitter/receiver with β;
3. Alice and Bob start transmission via FM-DCSK modulation scheme at a rate $R >> C_s$, and a good throughput can be realized; the secure transmission is implemented in FM-DCSK waveforms;
4. If Bob's device is unprotected, Eve may copy the chaotic receiver; Bob sends the request for switching to FM-CSK modulation;
5. Alice and Bob switch to FM-CSK and update the key μ_0 and β at data rate C_s;
6. Alice and Bob switch back to FM-DCSK when channel condition worsened ($SNR <$ 10 dB).

The special feature of FM-DCSK that it does not use carrier synchronization to perform the demodulation makes it even more robust against multipath fading effects. When channel condi-

tion is worsened, the modulation scheme is switched back to FM-DCSK, but with a new β.

6. Application of the Proposed Approach in IoT Device Authentication

Authentication is the process by which a trusted system verifies the identity of an untrusted device before granting it to access any data or resources. From the system point of view, an IoT device is all the same as a mobile device on which Pre-Shared Key (PSK) is widely used for device authentication. However, low-end IoTs bring new challenges. One of the challenges of low-end IoTs are the hardware and software differences that IoT devices have with respect to generic computing devices such as desktop and laptop computers and smartphones. Low-cost IoT devices usually have lower processing capabilities and cannot run endpoint security solutions that have been created for computers. Another challenge facing IoTs is that most devices are not physically protected aside being placed remotely. Thus, managing secrets may not be feasible.

A PUF leverages uncontrollable and intrinsic physical characteristic patterns of silicon devices due to process variations in manufacturing Integrated Circuits (IC). With each input, referred as a challenge, there is a unique output, referred as a response. The CRP mapping is unique and unpredictable. Even though the mask and manufacturing process are the same among different ICs, each IC is actually slightly different due to normal manufacturing variability. PUFs leverage this variability to derive "secret" information that is unique to the chip [8]. It offers an efficient alternative way to storing secret. Rather than physically being stored, the secret is derived from physical characteristics of an integrated circuit.

Delay based PUFs take advantage of hidden delay information in integrated circuits. Path delays in an IC are statistically distributed due to random manufacturing variations. Even with identical layout masks, the variations in the manufacturing process could cause significant delay differences among different ICs. A Ring Oscillator (RO) circuit in Figure 15 shows how path delay is measured. A RO circuit consists of odd number of inverters connected as in the Figure 15.

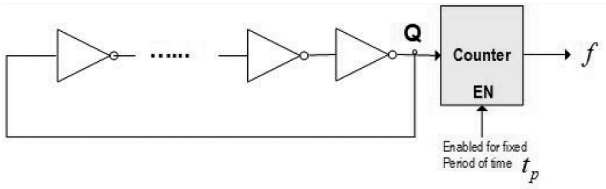


Figure 15. A Ring Oscillator.

The output Q oscillates between 0 and 1 at a frequency based on the circuit's delay as shown in Equation (12).

$$f = \frac{1}{2nt_{delay}} \tag{12}$$

Here, n is the number of inverters and t_{delay} is the propagation delay of each individual inverter. A counter is placed at the output of the RO to count the number of state changes within a fixed period of time t_p. The output of this counter at the end of a counting period reflects the frequency of the RO. The shorter the delay t_{delay}, the larger the f. The gate propagation delay and interconnection wire are mostly affected by process variations, which are unpredictable and unclonable. As a result, no two devices are the same. A RO PUF shown in Figure 16 is built based on the RO circuit. The path delay of each RO is measured by a counter placed at its output. The RO PUF contains 2^n identically laid out ring oscillators. Due to manufacturing variation, each ring oscillator oscillates with a different frequency, The n-bit challenge input selects any two ROs and their frequencies are compared to generate a 1-bit response "1" if $f_1 > f_2$, otherwise "0". To have an m-bit response, the 1-bit RO PUF circuit can be multiplicated m times; or the RO PUF can be used m times with different inputs. A specific challenge and its corresponding response form a challenge-response pair. A complete set of CRPs could be considered as a device DNA. As shown in Figure 16, PUF hardware uses simple digital circuits that are easy to fabricate. A secret is derived from complex physical characteristics of an IC rather than being stored in digital memory. As the PUF

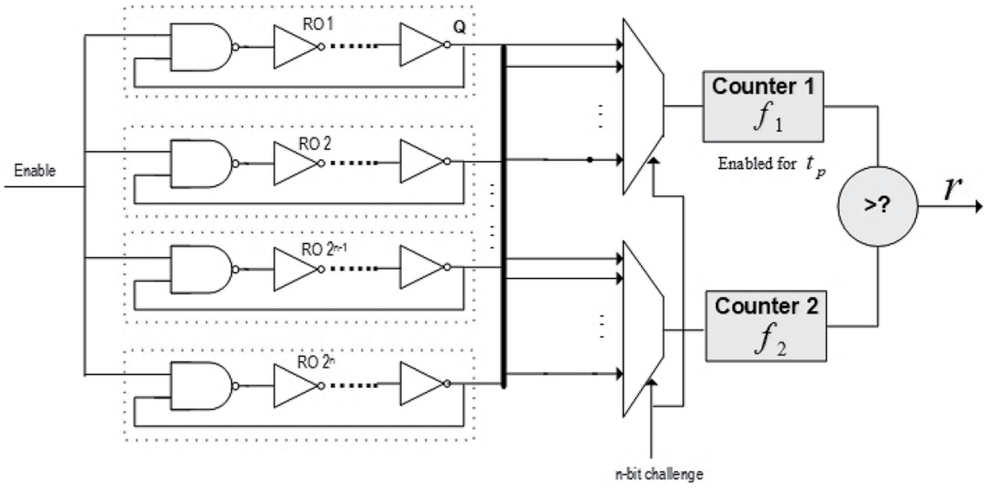


Figure 16. An RO PUF.

taps into the random variation during an IC fabrication process, the secret is extremely difficult to predict or extract [12]. As such, PUF has become a promising innovative primitive for device security such as authentication especially for resource constrained IoT devices. In most PUF based authentication methods [7] [14] [15] [16], the challenge and response are transmitted in clear format. To protect against man-in-the-middle attacks, challenges are never reused. This requires that the PUF should have an exponential number of challenge response pairs. This, in turn, will increase hardware overhead, which is a critical issue for some simple IoT devices. Another assumption made here is that model building based on the collected CRPs is impossible. However, there are a number of techniques with proven capability in building numerical models of PUF devices based on the collected CRPs including machine learning, linear programming or algebraic methods. The vast majority of IoT nodes maybe deployed in remote environments with little or no protection; therefore gaining access to these devices for CRPs collection can be relatively easy [16]. Implementing cryptographic functions will add significant area overhead and most IoT sensor nodes cannot afford it. The devices that might utilize our proposed chaotic based PUF authentication process are unattended devices such as wireless sensor nodes, actuators deployed for infrastructure monitoring, and environmental monitoring [19].

Figure 17 shows our proposed authentication process. As discussed in the previous section, the communication between IoT gateway and network server is through backhaul communication technology using standard IP connections, and security could be provided by contemporary cryptography. The security challenge is in the path from edge device to IoT gateway, as shown in Figure 17. In our proposed approach, PUF is embedded in each IoT device. The trusted server keeps pre-recorded CRPs for each edge device. Before sending/receiving data, each IoT edge device will be verified. The trusted server randomly selects a challenge and send it over the untrusted cloud to the IoT gateway. Due to the constrained resource in the edge device, the transmission of the challenge from gateway to edge device is in plain format. To protect from man-in-the middle attack, the proposed security approach is applied to communication between gateway and edge device.

Figure 18 shows the chaotic transmission system to be implemented in the edge device. There are three parts in the system: chaos signal generater, transmitter, and receiver. In the experiment, CRPs are randomly generated by Bernoulli distribution. The CRPs binary sequence is converted to a bipolar one for easy implementation of FM-DCSK. The spreading factor β = 100 is used for the AWGN channel with channel condition *SNR* = 10 dB. The transmission of the 32-bit challenge is shown in Figure 19 as follows: (a) shows the 32-bit PUF

challenge data; (b) shows the FM-DCSK signal waveform after the AWGN channel, which has the 32-bit challenge hidden in it; (c) shows the FM-DCSK signal after the Integrator; (d) shows the completely recovered 32-bit challenge. The PUF 32-bit challenge is disguised in the FM-DCSK waveform as shown in Figure 19 (b).

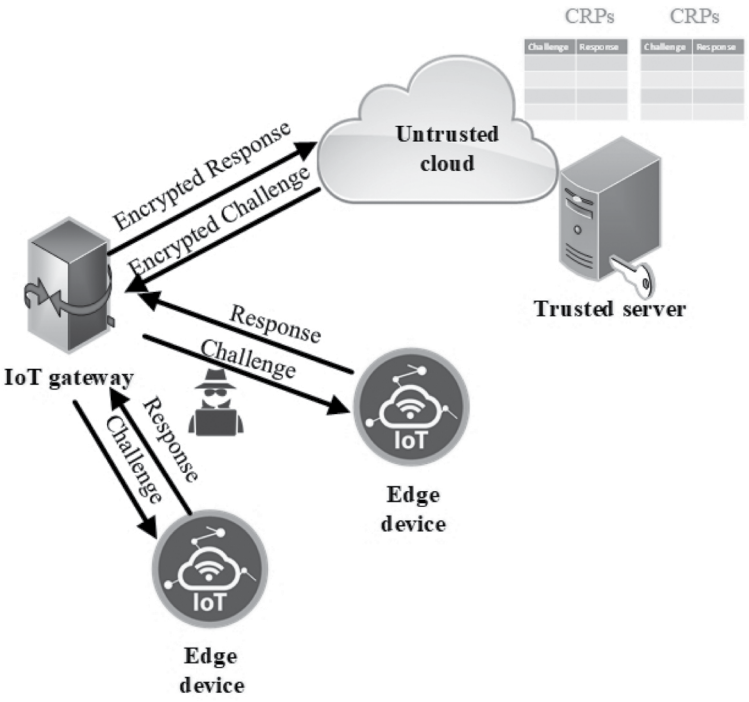


Figure 17. The IoT authentication process.

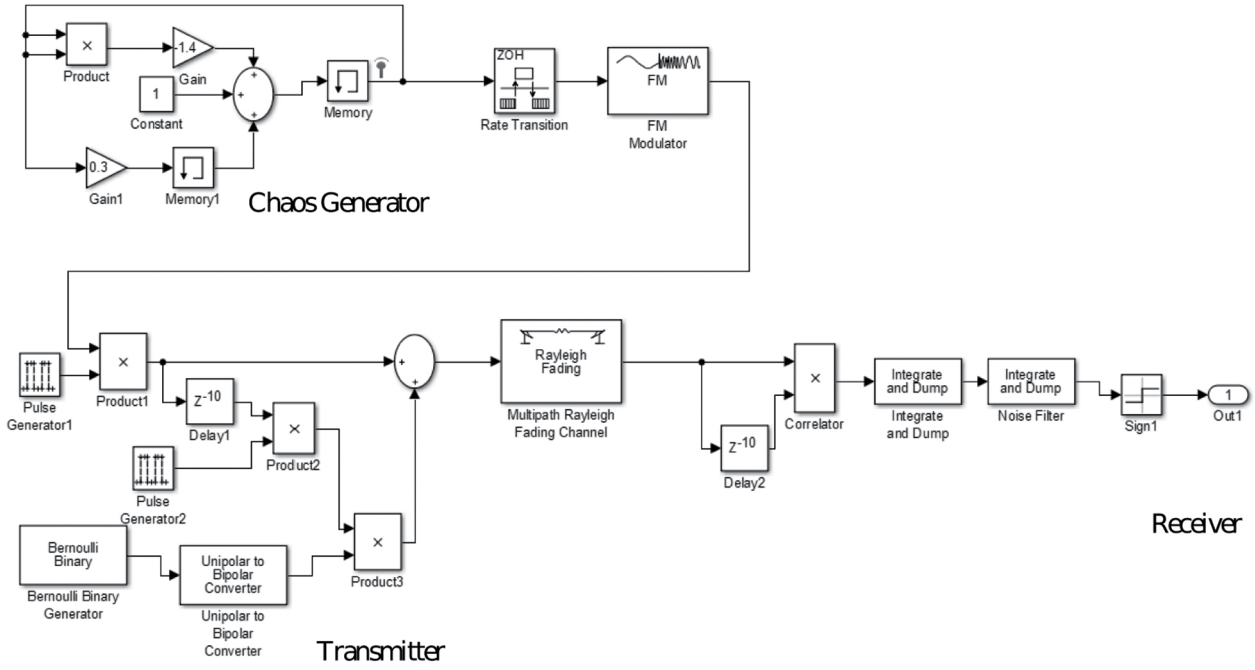


Figure 18. The chaotic transmission system.

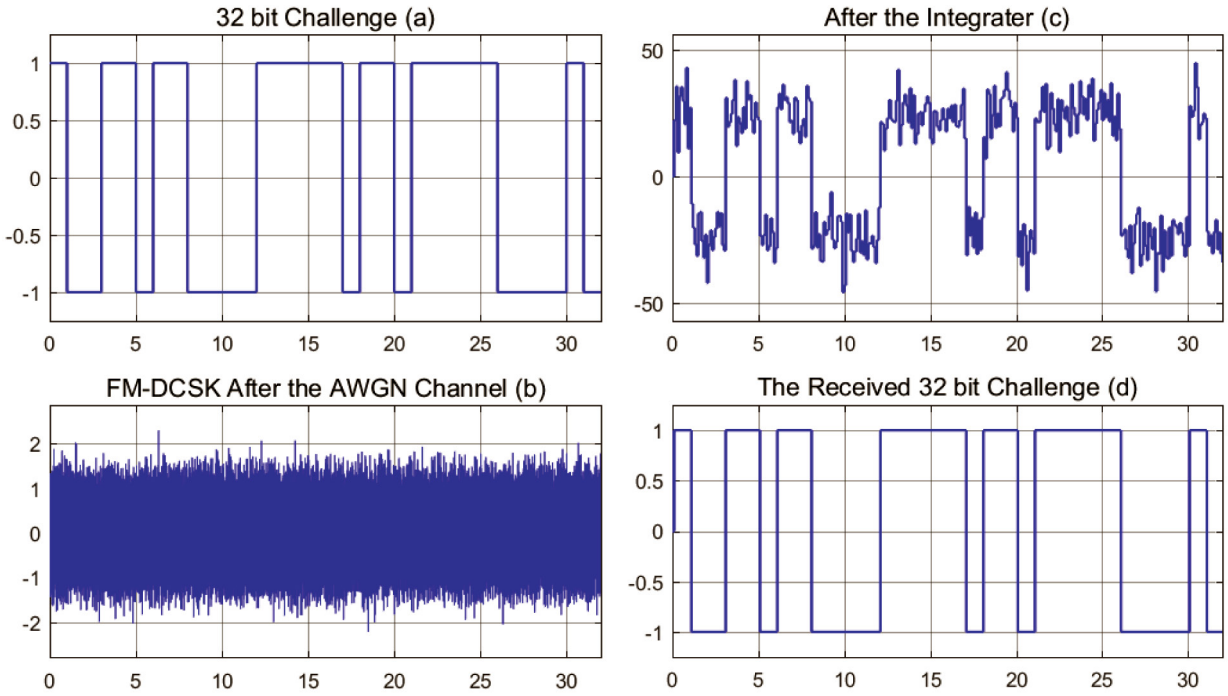


Figure 19. The transmission of 32-bit CRP ($\beta = 100$) by FM-DCSK under AWGN channel.

As the chaos sequence is a non-periodic and pseudo-random signal, it is difficult for an attacker to intercept the hidden message. The security is directly implemented at modulation level without any additional cost in software and hardware. The CRP could be reused, which further reduces cost in having a large number of CRPs. The spectrum of the transmitted DCSK in Figure 20 shows that the original signal only occupies half of the central lobe. It also indicates that the Henon map has a very good feature of broadband signal. The spreading factor plays an important role in security: a large β can ensure harder prediction of the spreading sequence. For multipath fading channels such as Rayleigh and Rician ones, the increase of β decreases FM-DCSK performance in our experiments. According to [13], this might be due to the increased noise power (with large β) overwhelming any gain in symbol detection. Thus, $\beta = 30$ is used in testing the proposed chaotic communication system under Rayleigh fading channel and $\beta = 20$ for Rician channel. Figure 21 shows the performance for transmitting the 32-bit PUF challenge under a Rayleigh fading channel with maximum Doppler shift $f_{D,\,max} = 10$ Hz, and two-way delay vector $[0,\ 2e-6]$ s. Figure 22 shows the performance under a Rician channel. The parameters for the Rician fading channel are: $K_{r,\,k} = [1,\ 1]$, delay vector $[0,\ 2e-6]$(s), Doppler shift of line-of-sight component vector $f_{d,\,LOS,\,k} = [5,\ 5]$(Hz), maximum diffuse Doppler shift 5 Hz. As described in [8], FM-DCSK has a potentially low sensitivity to multipath because the demodulation is performed without carrier synchronization and the transmitted signal is a wide-band signal which cannot be completely canceled by a multipath-related null. The special feature of FM-DCSK that it does not use carrier synchronization to perform the demodulation makes it even more robust against multipath.

Another important advantage of applying chaos-based systems is its easy implementation. Chaotic signals are much easier and faster to generate using a simple circuit. The use of all nonlinear operation excursion of electronic and optical components avoids the rather complicated and energy consuming measures to overcome nonlinearities in traditional communication schemes. For example, LoRa uses chirp spread spectrum modulation, a spread spectrum technique where the signal is mod-

ulated by chirp pulses (frequency varying sinusoidal pulses). To keep linearity, energy consuming measures are needed. However, the chaos-based system itself is non-linear, and no such complicated measures are needed. While in conventional SS communication systems the broadband signals are generated using pseudo-random sequences to spread signals in frequency, in chaos based schemes the bare fact that a chaos-generating device is running is sufficient to generate broadband signals. Hence, reduction in hardware cost is obtained. Furthermore, chaotic dynamics could be controlled by a low power signal [5]. This makes the proposed method the best candidate for IoT security.

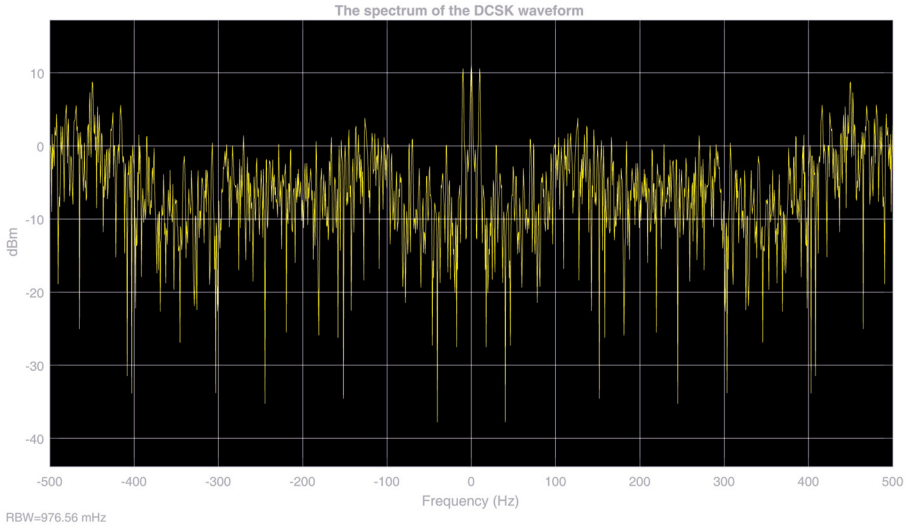


Figure 20. The spectrum of the DCSK signal.

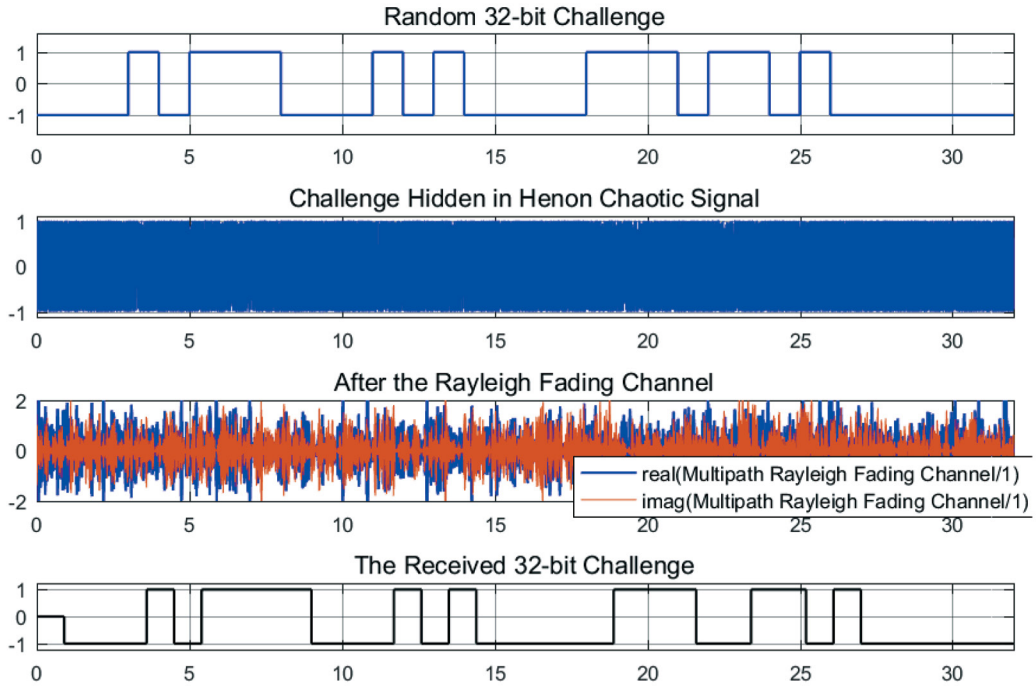


Figure 21. 32-bit PUF CRP transmission under Rayleigh channel ($\beta = 30$).

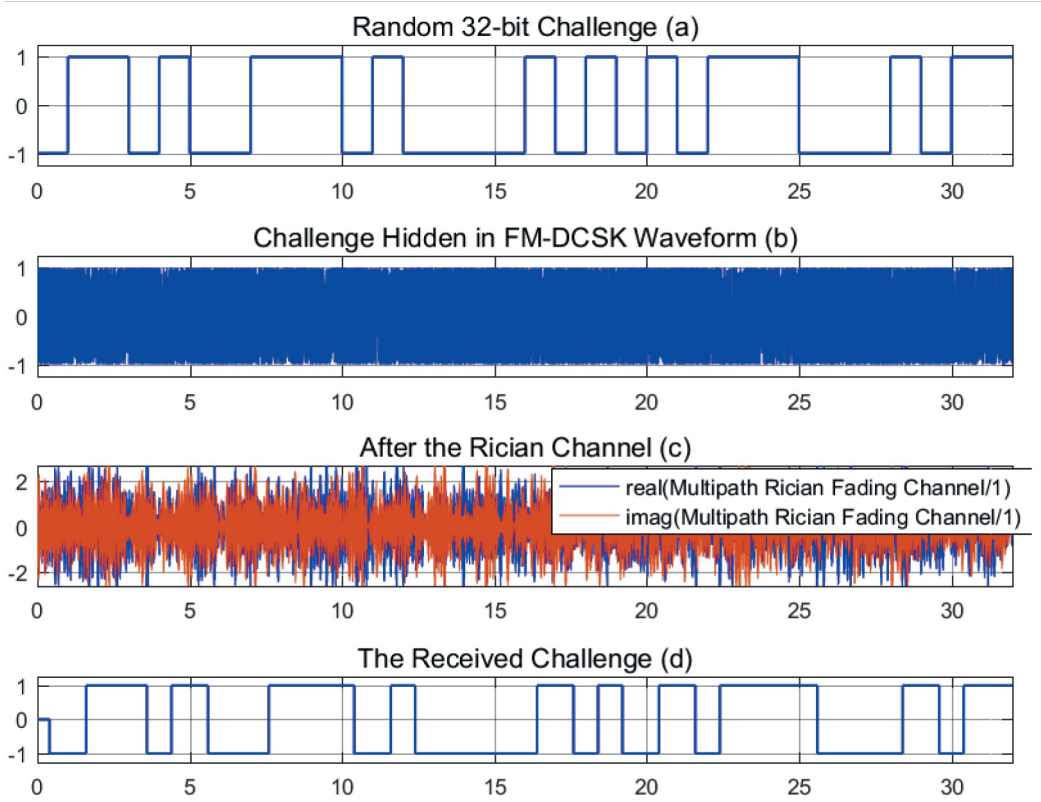


Figure 22. 32-bit PUF CRP transmission under Rician channel ($\beta = 20$).

7. Conclusions and Future Work

Securing IoT devices over the last mile is challenging due to both software and hardware limitations of simple devices. In this paper, we proposed and implemented FM-DCSK and FMCSK transmission systems that address the channel characteristics as well as the need to secure transmissions in spite of these limitations. The simulation results show that FM-DCSK has high resistance to interference and more immunity against multipath effects, which is a big concern in long distance wireless communication. Security is directly implemented at waveform level in both FM-DCSK and FM-CSK via hiding data in chaotic carrier signals–LPI is observed. By using the initial condition as a key in FM-CSK and the spreading factor as a key in FM-DCSK, transmission security is reinforced due to sensitivity of the chaotic function to its initial condition and non-periodic nature. Security performance is analyzed in terms of key space and statistical property of the chaos signal. This approach is applied in the proposed PUF based IoT authentication. In contrast to conventional communication systems that require modulators, source encoders, channel encoders and filters, the proposed approach can be implemented using only one subsystem which provides all the basic processing. All the above features make it a promising approach for providing physical layer security for IoTs in the last mile.

References

[1] LoRa Alliance, *A Technical Overview of LoRa® and LoRaWAN*, 2015 LoRa Alliance. https://www.tuv.com/content-media-files/master-content/services/products/1555-tuv-rheinland-lora-alliance-certification/tuv-rheinland-lora-alliance-certification-overview-lora-and-lorawan-en.pdf

[2] W. Trappe, "The Challenges Facing Physical Layer Security", *IEEE Communications Magazine*, pp. 16–20, 2015. http://dx.doi.org/10.1109/MCOM.2015.7120011

[3] CISCO, *Securing the Internet of Things: A Proposed Framework*, 2017. https://blogs.cisco.com/sp/securing-the-internet-of-things-a-proposed-framework

[4] J. Yu and Y.-D. Yao, "Detection Performance of Chaotic Spreading LPI Waveforms", *IEEE Trans. Wireless Communications*, vol. 4, no. 2, pp. 390–396, 2005. http://dx.doi.org/10.1109/TWC.2004.842948

[5] J. M. V. Grzybowski *et al.*, "Chaos Based Communication Systems: Current Trends and Challenges", in: *Applications of Chaos and Nonlinear Dynamics in Engineering – Vol. 1, Understanding Complex Systems*, Springer-Verlag Berlin Heidelberg, pp. 203–230, 2011.

[6] K. Wrona, "Securing the Internet of Things: A Military Perspective", in *Proc. of the IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015, pp. 502–507. http://dx.doi.org/10.1109/WF-IoT.2015.7389105

[7] M. Naveed *et al.*, "Physical Unclonable Functions for IoT Security", in *Proc. of the 2016 ACM*, 2016. http://dx.doi.org/10.1145/1235

[8] G. Kolumban *et al.*, "Chaotic Communications with Correlator Receivers: Theory and Performance Limits", in *Proc. of the IEEE,* vol. 90, no. 5, pp. 711–732, 2002. http://dx.doi.org/10.1109/JPROC.2002.1015003

[9] G. Kolumban *et al.*, "FM-DCSK: A Robust Modulation Scheme for Chaotic Communications", *IEICE Trans. Fundamentals,* vol. E81-A, no. 9, pp. 1798–1802, 1998.

[10] M. C. Jeruchim *et al.*, *Simulation of Communication Systems*, Second Edition, New York, Kluwer Academic/Plenum, 2000.

[11] A. Mukherjee *et al.*, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey", *IEEE Communications Survey and Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014. http://dx.doi.org/10.1109/SURV.2014.012314.00178

[12] C. Herder *et al.*, "Physical Uncolonable Functions and Applications: A Tutorial", in *Proc. of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014. http://dx.doi.org/10.1109/JPROC.2014.2320516

[13] Y. Xia *et al.*, "Performance of Differential Chaos-Shifting-Keying Digital Communication Systems Over a Multipath Fadding Channel with Delay Spread", *IEEE Transactions on Circuits and Systems-II Express Briefs*, vol. 51, no. 12, pp. 680–684, 2004. http://dx.doi.org/10.1109/TCSII.2004.838329

[14] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation", in 2007 44th ACM/IEEE Design Automation Conference (DAC), pp. 9–14, 2007.

[15] T. Idriss, H. Idriss and M. Bayoumi, "A PUF-based Paradigm for IoT Security", in *Proc. of the IEEE 3rd World Forum on Internet of Things (WF-IoT)*, 2016, pp.700–705. http://dx.doi.org/10.1109/WF-IoT.2016.7845456

[16] B. Halak *et al.*, "Overview of PUF-based Hardware Security Solutions for the Internet of Things", in *Proc. of the 2016 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2016. http://dx.doi.org/10.1109/MWSCAS.2016.7870046

[17] J. M. V. Grzybowski, M. Eisencraft, and E. N. Maceau, *Applications of Chaos and Nonlinear Dynamics in Engineering*, Springer-Verlag, vol. 1, 2011. http://dx.doi.org/10.1007/978-3-642-21922

[18] M. Bloch and J. Barros, *Physical-layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[19] H. Zhao and L. Njilla, "Hardware Assisted Chaos-based IoT Authentication", in *Proc. of the IEEE International Conference on Networking, Sensing and Control*, 2019. http://dx.doi.org/10.1109/ICNSC.2019.8743151

Received: October 2021
Revised: -
Accepted: February 2022

Contact addresses:
Hong Zhao
Fairleigh Dickinson University
Teaneck
New Jersey
United States
e-mail: zhao@fdu.edu

Paul Ratazzi
Air Force Research Laboratory
Rome
New York
United States
e-mail: edward.ratazzi@us.af.mil

Hong Zhao received the PhD in electrical and computer engineering from New Jersey Institute of Technology in 2004. She is a professor of electrical engineering at Fairleigh Dickinson University, NJ, USA. Her research focuses on various aspects of broadband communications and computer security including network traffic/performance/security analysis and modeling, and hardware trojan detection. Dr. Zhao serves as Vice Chair of the IEEE North Jersey Section. She received VFRP (Visiting Faculty Research Program) award from AFRL (Air Force Research Lab) in 2014-2016, SFFP (Summer Faculty Fellowship Program) award in 2017-2021 from AFOSR (Air Force Office of Scientific Research), Visiting Professor Award from Ministry of Science and Technology Taiwan in 2015, and 2015 IEEE Region 1 award for Outstanding Support for the Mission of the IEEE, MGA, REGION 1 and Section.

Paul Ratazzi received the BSc degree in electrical engineering from Rensselaer Polytechnic Institute (RPI) in 1987, the MSc degree in electrical engineering from Syracuse University in 1992, the MSc degree in management from RPI in 2006, and the PhD degree in electrical and computer engineering from Syracuse University in 2016. He is currently technical advisor to the Information Warfare Division of the Air Force Research Laboratory Information Directorate in Rome, NY, USA. Dr. Ratazzi is also an adjunct professor with the Department of Network and Computer Security, SUNY Polytechnic Institute, where he teaches secure protocols and computer security in the graduate program.