An efficient emerging network and secured hopping scheme employed over the unsecured public channels

Aamir Shahzad\textsuperscript{1,2}, Kaiwen Zhang\textsuperscript{1}, René Jr Landry\textsuperscript{3}, Neal Xiong\textsuperscript{4} and Young-Gab Kim\textsuperscript{2}\textsuperscript{f}

Abstract
With the emergence of new smart technologies, including the Internet of Things, wireless media are playing an important role to connect numerous devices to fulfill the requirements of newly developed communication systems. The massive connectivity, therefore, made the wireless spectrum too crowded and gave several challenges to resisting against potential wireless jammers. Note that, the two main challenges that have always been a part of any communication system, especially in the case of wireless communication, are information security and information jamming. Carefully considering the given challenges, this study uses a new advanced anti-jamming approach, a modulation technique based on the frequency-hopping spread spectrum, which has notably high resistance accounted against various potential jammers. The objective of this study is two-fold. First, the physical channel properties are considered, and the random bits are transmitted, employing a cryptographic secured hoping-spread pattern, having a set of carrier frequencies, known at both sides of the transmission. Second, the hashing code is computed only for the key, and transmitted along the original hop-set, but with distinct frequencies set. The deployed practical anti-jamming approach, therefore, computed a high efficiency to examine the information secrecy well and primarily the connection availability even in the presence of the jammers. Moreover, this study considered and modeled a communication system and evaluated the proposed system’s performance, applying the theories of Shannon’s entropy and Wyner’s entropy (i.e. Wyner’s wiretap channel), to anticipate the system’s perfect secrecy, even in the worst case when jammer has unlimited computational capabilities.

Keywords
Physical layer security, information-theoretic security, encryption, hashing and perfect secrecy, anti-jamming, spread spectrum, frequency hopping, cipher system

Date received: 15 October 2019; accepted: 5 March 2020

Handling Editor: Cong Wang

Introduction
The demands to interconnect the devices through wireless media have been increasing day-by-day tremendously. Therefore, to transmit useful information over the physical channels requires reliable mechanisms that can resist under the circumstances of vulnerabilities, as various eavesdroppers and jammers are always residing to harm the communication systems.\textsuperscript{1,2} To fight against, as a part of physical layer security, the anti-jamming techniques have validly been deployed\textsuperscript{3} and

Corresponding author:
Young-Gab Kim, Department of Computer and Information Security, Sejong University, 209, Neungdong-ro, Gwangjin-gu, Seoul 05006, South Korea.
Email: alwaysgabi@sejong.ac.kr
are notably still a primary concern for today’s advanced wireless systems, such as cellular and military systems.\(^1\)\(^,\)\(^2\) Hence, due to the open nature and transmission over the weaker wireless channels, wireless systems have adequately been threatened with jammers and attack possibilities.\(^1\)\(^,\)\(^3\) The most common type of attack, as a broad category, at the physical layer, is categorized into active and passive attacks. The active attacks are mainly available in the form of jamming and interference, which principle targets are to obstruct the frequency bands by transmitting unwanted signals, and consequently, cause the transmission failures in most cases. Moreover, these attacks, therefore, have a potential effect on channel privacy and cause a more adverse impact on the quality of communication, hence weaken the required channel by establishing communication through intentional interference. On the other side, passive attacks are mainly caused by the utilization of wireless media properties and are further categorized as eavesdropping attacks and traffic inspection. Eavesdropping attacks are occurring to divulge almost the useful information resulting due to the open, unprotected nature of wireless channels. Traffic inspection is a kind of attack, mainly residing in wireless communication, which is caused by intelligently analyzing the given information continuously, and therefore affecting the normal traffic flow.\(^3\)\(^,\)\(^4\)

Traditionally, the jamming and anti-jamming techniques have extensively been implemented specifically for the military systems, where electron attack (EA) is a part of communications electron warfare (CEW), employing the jamming techniques to intercept the target system and its communication flow. Alongside this, the prevention solutions, or electronic defense (ED) solutions, also deployed widely against electronic attacks to degrading the harmful effects on the target system.\(^3\)\(^,\)\(^5\) For example, consider a jamming (or active attack) scenario that encompasses a communication pair of the legitimate transmitter (Tx) and an open, intended receiver (Rx), and an unauthorized entity as a jammer. Each time the signals are transmitted and propagating through a wireless channel to Tx, the signal quality is reduced due to the presence of noise, interference such as unintentional interference, and the consequences of multipath fading. The jammer is mainly residing close, or located distance far in a radius, toward the Rx; the signal propagation paths of legitimate transmitter Tx to receiver Rx and jammer to receiver Rx are usually individualized to each other. However, the jammer always has a goal to degrade the channel or to generate intentional interference to the Rx; therefore, the illegitimate established link between jammer and receiver is facing the deterioration, while signaling, because of the preceding channel effects.\(^5\)

Over the years, anti-jamming solutions have also been implemented for other wireless systems as part of wireless communication, including the valuable enhancements for the strategical military applications, where the primary goals of these techniques are to achieve the low probability of detection (LPD) and the low probability of interception (LPI).\(^5\) The LPD, as an anti-jamming solution, can be accomplished through the employment of a well-known anti-jamming technique called direct sequence spread spectrum (DSSS), which uses a larger frequency bandwidth to spread the desired original signals and targets to make the transmitted signals invisible to unknown entities that interrupt into the transmission. However, the LPI system states that the initially transmitted signals possibly have chances to be detectable during transmission but not easy to be intercepted by the unknown entities. For that, another predominated spread spectrum technique—frequency-hopping spread spectrum (FHSS)—has been employed in wireless communication systems; likewise, FHSS uses large radio frequency band and spreads the useful signals, followed by the hop sets that comprise distinct frequencies set shared between legitimate users of the communication system. Therefore, less probability of jamming, and as well, the lower expected signal-to-noise ratio (SNR), evaluates that the illegitimate user has minimal effects over the spread signals in transmission.\(^1\)\(^,\)\(^5\) Moreover, the useful signals that are transmitted can be hidden, from the unknown entities (such as eavesdroppers and jammers) through defined coordinated actions by employing Emissions Control (EMCON) as a part of emission control technology. EMCON solutions are vastly employed to limit the communication between legitimate nodes for a specific session; the information received continuously follows by the defined specific period, but usually, without acknowledgment of the receiver.\(^5\) In short, in literature, various subtle jamming techniques, and corresponding anti-jamming solutions, were implemented extensively;\(^6\)\(^,\)\(^6\) however, the relevant terms that to fully qualify and also to evaluate the success rates of communication, while employing these techniques, are achieved through the theoretical computations that have a high aspect in measurements.\(^6\)\(^,\)\(^7\)

As examined in previous studies,\(^8\)\(^–\)\(^10\) information security is still the main issue in wireless communication, the security mechanisms such as applying encryption, authentication, and security management,\(^11\)\(^–\)\(^13\) have some great security contributions against several vulnerabilities but are limited to applications at the physical layer.\(^4\) Therefore, among other solutions, information-theoretic security is one of the solutions employed to evaluate the wireless channel secrecy, considering as a part of physical layer security.\(^4\)\(^,\)\(^14\) Thereby, Shannon’s system has been still considered as a well-known approach targeting to achieve the perfect secrecy against the unbound computational power of illegitimate users of the communication system.
Shannon’s theory considered a noiseless cipher system in which the main goal was to secure the message \( M \) that was intended to be sent from a transmitter Tx to a legitimate receiver Rx. The encryption was computed on message \( M \) employing the secret key \( K_s \) shared between the Tx and Rx and further, the shared key \( K_s \) was assumed not to be known by the illegitimate entity of the communication system. In short, message \( M \) is encoded into a secure code, the intended message \( M \) secrecy was observed successfully, before transmitting to the receiver Rx; upon received, Rx used a similar secret key \( K_s \) to decode the secure code \( X \) in order to get the message \( M \). This approach is supposed to be secured in case the unknown entity has not succeeded in overhearing the information; therefore, the probability of intercepting the integrated information between the original message \( M \) and the secure code \( X \) was absolutely derived as zero, \( I(M; X) = 0 \). Employing Shannon’s entropy \( H \), the mutual information is defined as \( I(M; X) = H(M) - H(M/X) \), where the uncertainty of \( M \) is defined with entropy \( H(M) \). So that, \( H(M) = -\sum P(m) \log P(m) \), where \( P \) is defined to compute the probability of \( M \) by considering the value of \( m \), and further \( H(M/K_s) \) is the conditional entropy reported by the remaining uncertainty accounted in \( M \) after the secure code \( X \) is discovered. Therefore, considering \( I(M; X) = 0 \), the observed uncertainty \( H(M) \) and uncertainty \( H(M/X) \) of message \( M \) are statistically independent and are equal. Here is the condition; the perfect secrecy can be achieved in case the observed secure code \( X \) disclosed nothing about original message \( M \). In a situation where the eavesdropper has unlimited computation power; thus, the confidential information could have chances to be interfered by; here, the perfect secrecy can be attained by employing Shannon’s theory as \( H(K_s) \geq H(M) \).

The spread spectrum techniques have been widely considered to enhance the wireless systems performance (i.e. throughput rate) against various jammers (e.g. narrow and wideband jammers), hopping among distinct frequencies set while communication over wireless channels. These techniques are somehow much efficient in computation than other available anti-jamming schemes; where the useful signals are modulated using frequency patterns, the spread signals are assumed to be noise-like and are therefore very difficult to demodulate by the jammers, unless they do not have the spread codes. Because of the simplicity of wireless channels and having weaker channel secrecy, the jammers, therefore, used their computational powers to intercept successfully in between the transmission. For example, a jammer intends to place its antenna particularly directed toward the receiver and tries to demodulate the coming signals, hence getting the baseband signals successfully. A similar case may be possible while employing encryption schemes, for example, if the jammer has unlimited power to break the encryption codes using some potential cryptanalysis schemes, consequently it can obtain the original modulated bits. However, given the definition of Shannon, the perfect secrecy can be achieved in wireless transmission, if the unknown entity is not successful in deciphering the spread code, or the signals are similar to noise, or even the presence of inexhaustible computational power.

In this study, an intelligent step is taken to examine the security of wireless communication systems and its limitations at the physical layer; later a new integrated security approach, employing an integrated cryptography and spread spectrum solution, is proposed and implemented; this study concluded that there is enough security that can be achieved at the physical layer. The selection of the proposed security solutions has been made after comparison with other available algorithms, and finally, a perfect, lightweight security-integrated solution is selected; the information-theoretical security concepts (i.e. to attain perfect secrecy) are used in this study to ensure and prove the entire security system. To achieve that, the main objectives of this study are as follow:

1. The FHSS system is considered in this study, the spread code (or pseudorandom PN sequence) is generated, and then encryption is deployed on; the encrypted code is defined as spreading code for frequency hopping (FH). Later, the system’s perfect secrecy is examined based on information-theoretical security concepts.

2. To examine the perfect–perfect secrecy of the selective encryption key, the hashing function Sha-2 is applied, and thus, perfect–perfect secrecy is anticipated. To be more precise, the study goals are achieved, as a part of proposed security development, by ensuring that the security system attained perfect secrecy even in a case of potential jammer (or attacker) residing in a transceiver system.

The rest of the article is organized as follows: Section “Literature review” conducts a detailed survey on the available security and spread spectrum solutions. Section “Spread spectrum: an FH system” gives detail on spread spectrum systems, more specifically, focusing on FH systems. The study’s main problem statement is conducted in section “Problem statement.” Section “System model” describes the proposed system design and modeling, the cryptography module (CM) that validates the perfect secrecy and perfect–perfect secrecy of system; finally, the results are measured, and corresponding discussions are made. Section “Conclusion” concludes the overall study and gives the research directions for future developments.
Literature review

Code division multiple access (CDMA) scheme has widely been employed in wireless systems (e.g., 3G carriers), a multiple access method allowed several transmitters to communicate over a signal wireless channel simultaneously. As mentioned, CDMA technology inherently employed multiple users’ access, thereby has high chances of multi-user interferences. In standard CDMA systems, the code sequence is used to spread the desired signals over multiple symbols, and signals precluded through the arbitrary sampling, disordering the spread code with a pseudorandom sequence against jammers, making it not able to detect the baseband signals. However, the jammers can interrupt the transmitted signals if they are well-known about the real sequence code and the pseudorandom sequence, respectively. Hence, it is a common protection feature available, considering as a fragile method against various jammers (or attacks), in CDMA systems. In addition to this, a limitation might be part of CMDA systems, that is, the long code sequence that is mainly used in occupying 42 bits mask code computed through 42 bits linear feedback shift registers (LFSRs). Consequently, the mask code could have chances to be recovered by the jammer, as the total complexity \( C \) of recovery is just \( C(2^{42}) \), to detect and as well interrupt the useful signals. Moreover, an enhancement was made, prevention against multi-users interference and weaker security challenges, employing of secured DSSS approach for CMDA system; \( M \)-sequences were generated and spread securely to enhance the performance of the system, therefore highly protective against interference and attacks at the physical layer. For that, during communication, the spread code was transmitted over unsecured or weaker security channels—included an encryption key—therefore, the encrypted code was assumed as spread code and de-spread by a receiver that knows a similar key to get the original message. Likewise, another spread spectrum technique, called FHSS, has a better resistance against narrowband jammers and is much efficient in precluding against interferences but less efficient if the jammer successfully interrupted in, and used a similar technique to demodulate the spread signals. For example, a jammer, considering as a man-in-the-middle attack, which resides between the transmitter and receiver, is targeting to access the channel: the spread signals, the spreading method, and the PN sequence pattern. If that is possible, he or she targets to get a modulation scheme that employed to a pattern and later synchronizing himself as an authorized entity of the transceiver system. As a result, the jammer pretends himself as an authorized entity of system by successfully intercepting the receiving signals, for example, through masking as a real transmitter; therefore, he or she finally makes the legitimate receiver useless to get the real signals. To get the better system’s performance, or to make the wireless channel more protective, spread spectrum technology is highly demanded as a hybrid solution that utilizes the DSSS and FHSS together with advanced signal processing system. Therefore, the hybrid solution notably can better resist interference in the presence of jammers, multi-user radio frequency interference (RFI), and wireless fading channels. Meng et al. proposed a new anti-jamming solution for the FH system, which comprised of four main modules, such as recognition, suppression, suppression analyzing, and adaptive FH, which are required to build an integrated intelligent solution. In jamming recognition module, an algorithm was employed to make possible the recognition of jamming signals: first, the FH signals were erased on the desired jamming signals; second, the available bandwidth was analyzed, and narrowband jamming signals were discriminated from wideband jamming signals; and at the end, the required task for jamming recognition was performed well, through identifying and selecting the jamming type. In the jamming suppression module, the filtering techniques were identified not to be suitable to suppress the narrowband signals and tone jamming signals. However, FH and tone jamming signals are probably co-existence in the frequency domain; therefore, to settle down this issue through computing, the significant low jamming-to-signal ratio (JSR), essentially, the collective information confirmed that a hopping channel probably interfered with single tone jamming. Thereby, after filtering over-all measurements in the frequency domain, and the channel (or kurtosis) spectrum peak is low enough; thus, the FH signals get the chance to filter out to further perform the demodulation.

In section “Spread spectrum: an FH system,” a commonly used FH scheme is explained, considering a practical example of FH system, employing a two-way modulation scheme: a digital modulation scheme called multiple frequency-shift keying (MFSK), and frequency modulation scheme called FHSS, to spread the useful signals over the hopping bandwidth. Other useful components of the FH system are well described that to carry the transmission, for example, successful communication between transmitter and receiver, in the presence of anonymous narrowband jammer (that act as interference between transceiver system).

Spread spectrum: an FH system

FHSS, a part of spread spectrum technology, has commonly been used as an anti-jamming solution for wireless communication systems, encompassing a hopping sequence pattern by which the carrier frequencies are changing periodically in transmission. For example, the
FHSS system employs a hopping set, let's suppose set $N$, that is, $N = \{f_1, f_2, f_3, f_4, \ldots, f_{i-1}, f_i\}$, which defines an order set $i$ to changing the carrier frequencies; however, FH is employed to define a number of symbols transmitting over one or more channels. Given carrier frequencies, during transmission, are hopping over available frequency bandwidth comprising a number of frequency channels called hopping band, mainly the employed hopping bandwidth is much larger than carrier frequency bandwidth or transmitted signals bandwidth. Thus, hopping set corresponding to the spread code defines the carriers to hop over predetermined frequency channels and comprised a large bandwidth; the carrier frequencies are periodically switching hop-to-hop in a time interval called hop interval, with a specified duration called hop duration $T_h$. In an FHSS system, the frequency synthesizer is used to convert available standard frequency to distinct frequencies; therefore, it is employed to synthesize the all-useful frequencies that are comprised into a hopset. A standard formulation $f_{hj} = xf_1 + yjf_R$, $j = 1, 2, 3, \ldots, N$, is a basic form of hopset containing a number of frequencies, where $x$ and $y_j$ are representing the rational numbers, respectively. $f_1$ defines the frequency of a hopset for spectral channel band, and the reference frequency is shown as $f_R$. The reference signal is a resulting source, or a tone signal, over the reference frequency generated from frequency operation, such as fed by the oscillator, to verify stability and accuracy of the resulting frequency from a synthesizer, similar to the reference signal.29,30 The frequency synthesizer is used to generate the FH pattern, each time the code generator resulting in bits, shown in Figure 1. So that, the FH signal is formed by scrambled together the original modulated signal, for example, angle modulation $\theta(t)$, and synthesizer pattern (resulted); thus, at the receiver end, for example, a sample $i$th hop signal is formulated in equation (1) as

$$S(t) = \sqrt{2S} \cos[2\pi f_j t + \theta(t) + \theta_i]$$

where $S$, $f_j$, and $\theta_i$ respectively are the average power, carrier frequency, phase angle of this $i$th hop signal. The frequency pattern from the transmitter is then synchronized with the receiver pattern generated through the synthesizer, which might offset with constant intermediate frequency; finally, after the mixing process, the dehopping is successfully performed. Later, the output of the mixer is then further passed to the bandpass filter in order to remove the extra frequency elements and the outage power of frequency channel and hence yielded the demodulated output.29

The dehopped signals, however, might get several chances of interference and multipath padding and have no prevention against white noise, as the hopping channel allows the signals to travel outer range of frequency channel.24,31 For that, providing the potentials against narrowband interference, practically the disassociate frequency channels are required, which are either contiguous or occupying unexploited spectral region.3,32 Few useful cases through spectral notching, the spectral channels region that are susceptible to interference and fading are mainly erased from predefined frequency’s hopset. The modulation technique called MFSK has commonly been employed with an FH technique, in which all the subchannels usually get impact, hence causing the possibility of interference. Whereas, for security purposes such as to verify the hopping pattern secrecy or/and uncertainty, the FH pattern must be generated and distributed in pseudorandom sequence in an order of frequencies set. Moreover, the pseudorandom sequence is generated in a multilevel sequence and has extended the period of time, lengthily linear span, and unpredictably distributed over specified frequency channels. The long period always is significant to preclude the anonymous jammers that are trying to capture and store the pattern period, and the larger linear span is useful in the case to add restrictions that discouraging the opponent to regenerates the pattern. Code, or pattern, generates a set of control bits typically composing a symbol that collected through a finite field incorporating set properties. Furthermore,

![Figure 1. A standard frequency hopping system.](image-url)
by affiliating a different frequency to each symbol collected, the FH pattern is produced to compute the more reliable, efficient, and more secure transmission; for that, control bits might subject to be encrypted through some cryptanalysis algorithms. Alongside, to be more efficient, control bits are required to be generated by employing the particular algorithm that might direct through: first, the security key, which always kept secure, the main source that provides security and further encompasses a bits set that changing irregularly according to time session; second, the time-of-day (TOD) composed of a bits set that formed through phasing the TOD counter, and its changing occurring correspond to changes of TOD clock. The possibility of changing in TOD might be in every second; however, the key only changing on daily basis; as defined, the employed algorithm is regulated through time-varying key; therefore, it could be beneficial in case the algorithm (i.e. control bits) add restrictions to avoid the key changing constantly in every particular defined time. The change in frequency occurred as a part of the code generator that controls the FH rate regulating by a system clock which operation rate notably much higher than TOD clock rate. Thereby, each time-frequency hopped is occurred, as per symbol, and is synchronized with symbol execution time that specified. Figure 2 illustrates the timing flows of FH employing of 8-ary FSK modulation scheme with its essential components.

In an FH system, for example, in order to compute the minimal number of pseudorandom noise (PN), chips that are needed in a frequency word encompasses a sequence of chips; so that, to formulate this given problem, the hopping bandwidth $H_{BW}$ and frequency step size $\Delta f$ are assumed as $H_{BW} = 600 \text{ MHz}$ and $\Delta f = 100 \text{ Hz}$, respectively. No of tones in hopping bandwidth, $H_{BW} = H_{BW}/\Delta f$

Adding values, $H_{BW} = 600 \text{ MHz}/100\text{Hz}$

$= 6 \times 10^6$, where $H_{BW} = (6e + 8)\text{Hz}$

Thus, no. of chips $= \left[\log_2(6 \times 10^6)\right] = 23 \text{ chips}$ (minimum)

For details, an example of an FH system is illustrated in Figure 2. The modulation scheme 8-ary FSK is employed with FH, that is, slow hopping, to perform modulation/demodulation at both sides—transmitter Tx and receiver Rx; the input information is composed in binary format with a data rate $R_D$ of 150 bits/s. Hence, the symbol rate $R_S$ is given as follows

$$R_S = \frac{R_D}{8-\text{ary FSK}} = \frac{150 \text{ bits/s}}{(\log_2 8)} = 50 \text{ symbols/s}$$

and the time duration of a symbol $T_S$ is computed as $T_S = 1/50 = 20 \text{ ms}$. Thereby, each time-frequency hopped is occurred, as per symbol, and is synchronized with symbol execution time that specified. Figure 2 illustrates the timing flows of FH employing of 8-ary FSK modulation scheme with its essential components.

In Figure 2, a binary data sequence is used, and the specified bits are joined together into three groups due to the 8-ary FSK modulation scheme to generate the symbols. In standard 8-ary FSK modulation system, the selective data band uses a fixed central frequency $f_0$, and at the same time, the central frequency $f_0$ is usually not the same for data band while using FH/MFSK system, as illustrated in Figure 2. So, this is only a

Figure 2. FH system using 8-ary FSK modulation.
Thereby, while moving toward the modern wireless systems of current age, the well-known techniques—channel coding and spreading techniques—somehow are limited to provide an inclusive security resistance. However, considering the useful properties of advanced cryptanalysis approaches examined to gain enough secrecy at the physical layer, which in short are the main objectives of this study. Therefore, we may say that the key encryption approaches are widely considered as effective approaches to analyze the perfect secrecy of the system by examining information theory concepts. However, these approaches are somehow infeasible in case the employed keys have a high probability of being stolen by an unknown system’s entity.

**System model**

In wireless communication systems, transmitting useful signals may have several issues; for example, transmission over an unsecured wireless channel is one of the major issues. Where, the potential jammers are always residing; for example, their intentions are to place antenna in the direction toward the target path to any legitimate entity of the transceiver system, the weaker channel and then target to get the desired useful signals by applying some jamming techniques, such as narrowband and wideband jamming solutions to demodulate the originally transmitted signals. For that given problem, a solution is proposed, that is, spread-spectrum techniques which have commonly been employed against the various jammers in wireless communication systems, and these solutions are working as mitigation techniques as well, to protect the baseband signals that transmit and prevent signals that might include interception through unauthorized system’s entities. Therefore, successful communication, without the interception from potential jammers, could be possible if the spreading code is always unknown (or obfuscating) by the unauthorized entities of the system. Thus, for the system secrecy estimation in the presence of potential jammers, primarily the M-sequence code (or shortly pseudorandom code) is one of the useful component, a part of spread spectrum systems, generated by and known to only the authorized entities (Tx and Rx) of the system and considered as a adequate solution to achieve channel secrecy. The cryptanalysis methods have been widely deployed to get the original signals in baseband, for example, the encrypted signals from the transmitter probably not decipher during transmission, so the channel is said to be a perfect secured channel.

In this study, a new integrated security design includes three main security paradigms: cryptography, physical layer security, and the information theory for perfect secrecy; therefore, to set forth a security

Problem statement

In wireless systems, the massive connectivity of devices, and communication over weaker protective channels, the protection against various jammers is a major consideration. Several well-known solutions have been employed mainly at the application and data link layers; the ultimate target is to fight against the wireless system vulnerabilities and attacks, but there are limitations to implement at the physical layer. To be advanced, the security developments, such as channel coding schemes, spread-spectrum approaches, and the information-theoretical security, respectively, are accounting prominent developments, probably considering as the best among others, toward the physical layer security. However, none of one has evaluated a complete solution to the given security problem, excluding the information-theoretical security, toward physical layer security, which precludes the communication from stronger jammers that might have unlimited computation resources. In addition, most common methods employed at the physical layer were not very effective; it could be a case that the system was not designed with the consideration of acknowledgment paradigms. The strong channel established corresponding to a weak channel by the non-legitimate user could grab the original signals, and thus, the transmitter has no awareness at all about the interruption of the illegitimate entity in the system. For that, advanced security designs at the physical layer, the cryptanalysis solutions have also been implemented in the literature, but are considered as difficult implementations due to complexity of mathematical modeling for physical layer security. Although, almost all available cryptography solutions deployed for various communication systems are evaluated the best, regardless of massive complexities that are accounting during computations.
development for the general systems design and modeling are required. In Figure 3, the proposed integrated security system is illustrated, including a wiretap channel for intended jammer (or eavesdropper $J_{Eve}$) active assumed to be at the physical layer in transceiver system, a legitimate transmitter $T_{Alice}$ and a legitimate receiver $R_{Bob}$ are also active to communicate with each other. For communication, a traditional wireless system is considered using standard FHSS for precluding the communication against jammers and MFSK modulation. However, this study has no focus to well detail the FHSS and MFSK modulations because the goal is not to do something with modulation schemes, the objective is to employ these modulations schemes to get the proposed system’s objectives. Thus, in short, the main study target is to add a new CM, which is design encompassing the encryption, hashing, and comparator module, a new design module that may be considered as a part of the FH system. For that, three physical channels, such as

1) $Ch_{main}$: (Alice $\rightarrow$ Bob),
2) $Ch_{FB}$: (Bob $\rightarrow$ Alice), and
3) $Ch_{WT}$: (Eve $\rightarrow$ Bob)

are used, which carry the desired/undesired information signals in the transceiver system. In detail, the channel, $Ch_{main}$, is legitimated main channel between the transmitter $T_{Alice}$ and receiver $R_{Bob}$; the second channel called feedback (FB) channel, $Ch_{FB}$, is an authenticated channel between the receiver $R_{Bob}$ and transmitter $T_{Alice}$, which is established each time (distinct from other channels) as a channel for synchronization and confirmation and FB purposes about the signals that are transmitted by $T_{Alice}$ and then received by $R_{Bob}$. Thereby, $R_{Bob}$ and $T_{Alice}$ are well synchronized with each other—and will give the confirmation if the confirmation bit is set—upon delivery of each signal. The third channel is an illegitimate channel, or wiretap channel, between $J_{Eve}$ and $R_{Bob}$. Thus, there is no FB channel, $\neg Ch_{FB}$: (Eve $\rightarrow$ Alice), between $J_{Eve}$ and $T_{Alice}$ and vice versa. Therefore, it is considering as a way that makes $J_{Eve}$ identification clear in legitimated transceiver system, if the confirmation bit was enabled and, there will be no confirmation at all.

Here, a standard system, that is, 8-ary FSK modulation system, detailed in section “3” of this article is extended to 16-ary FSK modulation system. The required hopping sequence, or simply the PN sequence ($PN_{Seq}$), which is supposed to be known by both legitimated entities (i.e. transmitter and receiver) of the system, is generated using LFSRs. In Figure 4, a four-state LFSRs are employed to generate the 15 possible output values; however, r-state PN sequence, or
maximum sequence, can be generated using $m = 2^r - 1$, where the maximum number of states directly depending on the value of $r$ (as an input value). For the output sequence, Figure 4 illustrates a four-state register used to store and shifting the binary numbers using exclusive-OR function or modulo-2 adder, an FB pathway, and clock pulses that used to control the shift register overall processing. It is noted that, in Table 1, the PN sequence is truly a random sequence, as it has been conducted and verified by three main properties of randomness: Balance, Run, and Correction.

The output sequence generated using LFSRs, that is, four-state registers labeled as [R1 R2 R3 R4], is defined alternatively as $PN\_Seq = \{(St)_0, (St)_1, (St)_2, \ldots, (St)_{15}\}$, wherein sequence $(St)_0$ and $(St)_1$ are representing the sequence in order of 0’s and 1’s, respectively. For FH system, hopping bandwidth $HBW$ and frequency step size $Df$ is 400 and 25 kHz, respectively, and the corresponding bits-pattern is given using LFSRs. Furthermore, FH sequence ($H\_Seq$), $H = Seq = [f_0, f_4, f_2, f_0, \ldots, f_3, f_1]$, a period in which original signals are modulated with carrier frequencies one after another, is generated followed through bits-pattern and the step (time) in order of 0–15. So, in order to preclude the transceiver system from external jammers or/and attackers, that is, eavesdropping and a man-in-the-middle attack, for that, the spreading code or $PN\_Seq$ is said to be transmitted securely using encryption (a mechanism), which is a significant way to enhance the security of an FH system.

For security enhancement, suppose that $H\_Seq$ is logically defined and proportional to $PN\_Seq$, an output sequence finally generated from $4^4$ LFSRs. Thus, the $PN\_Seq$ encompassing a binary sequence (of 0’s and 1’s) is encrypted with a key that is randomly generated, and its length is at least larger or equivalent to the length of the message, for example, $PN\_Seq$ in our case. Here, we only use the truly random secret key, generated using a non-proprietary key generator (software), and the size of the key is exactly similar to the size of $PN\_Seq$. As it was stated by Debbah et al.\(^7\) [Shannon entropy], the perfect secrecy can be achieved if and only if the probability (or entropy) of the secret key is larger than the entropy of secret message. In this work,

**Table 1.** A four-state using LFSR H-pattern.

| Step (time) | m-bit/symbols | CFs  | H-pattern [R1 R2 R3 R4] | Output sequence | H-Seq |
|------------|---------------|------|------------------------|-----------------|-------|
| 0          | 0000          | 25 kHz | [1000]                | 0               | $f_8$ |
| 1          | 0001          | 50 kHz | [0100]                | 0               | $f_4$ |
| 2          | 0011          | 75 kHz | [0010]                | 0               | $f_2$ |
| 3          | 0100          | 100 kHz | [1001]               | 1               | $f_9$ |
| 4          | 0101          | 125 kHz | [1100]               | 0               | $f_{12}$ |
| 5          | 0110          | 150 kHz | [0110]               | 0               | $f_6$ |
| 6          | 0111          | 175 kHz | [1011]               | 1               | $f_{11}$ |
| 7          | 1000          | 200 kHz | [0101]               | 1               | $f_5$ |
| 8          | 1001          | 225 kHz | [1010]               | 0               | $f_{10}$ |
| 9          | 1011          | 250 kHz | [1101]               | 1               | $f_{13}$ |
| 10         | 1100          | 275 kHz | [1110]               | 0               | $f_{14}$ |
| 11         | 1101          | 300 kHz | [1111]               | 1               | $f_{15}$ |
| 12         | 1110          | 325 kHz | [0111]               | 1               | $f_7$ |
| 13         | 1111          | 350 kHz | [0011]               | 1               | $f_5$ |
| 14         | 1111          | 375 kHz | [0001]               | 1               | $f_1$ |
| 15         | 1111          | 400 kHz | [1000]               | n/a             | n/a   |

LFSR: linear feedback shift registers.
therefore, to achieve the perfect secrecy of a given system, mainly to secure the spread code, one-time padding (OTP) algorithm has been employed. Let us assume that the spreading code or PN_Seq is just a message that contains 15 bits in binary format, \( PN_{Seq} = [0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1] \) depicted in Table 1, and the key is formatted equally in binary, \( SC = [1 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1] \); thus the encryption/decryption function is computed using OTP as:

| 0 0 0 1 0 0 1 1 0 1 0 1 1 1 | (PN_Seq) |
| 1 1 1 0 1 0 0 1 0 1 0 1 0 1 0 | (Key) |
| 1 1 1 1 1 0 1 0 0 0 0 0 0 0 1 0 | (Encryption) |
| 0 0 0 1 0 0 1 1 0 1 0 1 1 1 | (Decryption) |

The given encryption/decryption function using OTP examined the perfect secrecy of the spreading code; furthermore, this study mainly focused on the weaknesses and the probability of key that the key might be stolen by the illegitimate entity of the system, while communication over weaker wireless channels. In fact, the perfect secrecy was successfully computed and verified using OTP; but in some situations, for example, the probability of the key is less secured against some powerful jammers. Therefore, the key secrecy is another challenge, which is the second main contribution of this study. For simplicity, let us suppose that the entropy of key non-confidentiality is somehow higher against jammers, and the legitimate receiver of the system is unaware of this unpredicted situation. To ensure the key secrecy, that is, perfect–perfect secrecy, which is mainly computed through the integrity function at both sides of transmission, the cryptography hashing function is the best choice. Unlike OTP, the hashing algorithm (i.e. SHA-2) always generates a fixed size output secured code, that is, 32-bit and 64-bit words, against any input length message. The strong secrecy that is computed through the OTP algorithm has been widely proved, so, for perfect–perfect secrecy, we assumed that both key and hashing secured code are similar in size, for example, like OTP. This is just an assumption that logically interrelates the defined term perfect–perfect secrecy with perfect secrecy has been examined using OTP, and alongside evaluated that spreading code integrity can be possible using hashing algorithm. However, this statement is truly based on an assumption defined, so the reality is still far challenging to be achieved. In the section below, the channel entropy is simply explained and examined, and the useful basic terminologies are given in Table 2.

**Preliminaries: channel entropy**

**Definition 1.** The system is supposed to be secured if the mutual information \( I \) between \( M_T \) and \( X_T \) in the presence of a jammer \( J_{Eve} \) is defined a value that approaches absolute zero

\[
I(M_T; Y_R) = 0
\]

And using Shannon’s theory, the entropy \( H \) of mutual information \( I \) is defined as

\[
I(M_T; Y_R) = H(M_T) - H\left(\frac{M_T}{Y_R}\right)
\]

where \( M_T \) are original data signals and the encoded message \( X_T \) transmitted from \( T_{Alice} \) and then, received by the legitimate receiver \( R_{Bob} \) and as well by \( J_{Eve} \) over wiretap channel \( Ch_{WT} \).

**Definition 2.** The entropy of a random variable \( M_T \) is defined as

\[
H(M_T) = - \sum_{m \in M} p_{M_T}(m) \log p_{M_T}(m)
\]

For random variable \( M_T \), entropy is applied to make a realization about the uncertainty, thus if \( M \), some alphabet defines probability with which \( M_T \) carries on ‘m’, computes a value approach to zero, then the total entropy of \( H(M_T) \) is defined as zero

\[
M_{def} p_{M_T}(m) = 0
\]

\[
\Rightarrow H(M_T) = - \sum_{m \in M} 0 \log(0) = 0
\]

**Definition 3.** Suppose the value of \( Y_R \) is observed, then the remaining conditional uncertainty in a random variable \( M_T \) is computed by \( H(M_T/Y_R) \):

\[
\frac{H(M_T)}{Y_R} = \sum_{y \in Y} p_{Y_R}(y) H(y)
\]

\[
= \left\{ \sum_{y \in Y} p_{Y_R}(y) H(y) \right\} H\left(\frac{M_T}{Y_R}\right) = y; M_{def} p_{M_T}(m)
\]

Thus, concluding that, the uncertainty \( H(M_T) \) of the transmitted message \( M_T \) is equal to the measured conditional uncertainty \( H(M_T/Y_R) \) while the \( Y_R \) formed

\[
\text{Inf}(M_T; Y_R) = H(M_T) - H\left(\frac{M_T}{Y_R}\right) = 0 \& \&
\]

\[
\text{Inf}(M_T; Y_R) = \text{Inf}(Y_R; M_T) = 0 \quad \text{(symmetric property; Definition 1)}
\]

**Definition 4.** Generalizes the system security using Wyner’s wiretap channel, considering the noisy communication channel, assume that the receiver receives the message \( M_R \) in the presence of Eve using wiretap channel, after decoding, that is
Probability, $\mathbb{P} = \{M_R \neq M_T\} \Rightarrow 0$, and $\Rightarrow \infty$

$M_T$ is the message being sent, after encoded into $X_n^{M_T}$ having a length and correspondingly $X_T$ is encoded message, $M_T \Rightarrow X_T$, through the computing of $Y_n^{M_T}$ a receiver received after passing over the noisy channel. Furthermore, Eve also get some value (unknown Probability, $\mathbb{P}$) computed of $Z_n^{M_T}$ passing over the noisy channel, where she is connected legitimately. Means that the secret code having length “n” possibly utilizes the channel “n” times, and for other, the legitimate receiver can get the channel output at $Y_n^{M_T}$ and the eavesdropper at $Z_n^{M_T}$. Such that

$$X_n^{M_T} = \{X_1^{M_T}, X_2^{M_T}, \ldots, X_n^{M_T}\}$$

Similarly, $Y_n^{M_T} = \{Y_1^{M_T}, Y_2^{M_T}, \ldots, Y_n^{M_T}\}$ and $Z_n^{M_T} = \{Z_1^{M_T}, Z_2^{M_T}, \ldots, Z_n^{M_T}\}$

Thus, $\text{Inf}(M_T; X_T)$ according to the Wyner’s wiretap channel model, for secrecy condition, both the encoding/decoding outputs are contented and, with a minimal rate of error (probability).

$\mathbb{C} = \max_{p_M} \text{Inf}[X_T; Y_R]$  

**Definition 6.** A message $M_T$ assumed to be secure if encrypted with a secret key $K_{ss}$ forms $X_T$, and then the perfect secrecy is defined as

$$\mathbb{H} \left( \frac{M_T}{X_T} \right) = \mathbb{H}(M_T)$$

It means that, $X_T$ leaks no information about the message $M_T$.

**Definition 7.** Perfect secrecy can be achieved if ciphertext provides no information about the message $M_T$ and secret key $K_{ss}$, and $\mathbb{H}(K_{ss}) \geq \mathbb{H}(M_T)$, thus we also define a perfect–perfect secrecy for $K_{ss}$ using hashing

$$\mathbb{H} \left( \frac{K_{ss}}{X_H} \right) = \mathbb{H}(X_H)$$

It means, $X_H$ leaks no information about key $K_{ss}$, and $X_H$ provides perfect–perfect secrecy for $K_{ss}$.

**Definition 8.** FB, through an authenticated FB channel, is replied, a way to examine information secrecy by the setting of bits $(0, 1)$ is

### Table 2. System terminologies.

| No. | Terminologies | Description |
|-----|---------------|-------------|
| 1.  | $(T_{Alice}; R_{Bob}; J_{eaves})$ | (A legitimate transmitter; a legitimate receiver; jammer: eavesdropper) |
| 2.  | Channels (Chmain: ChFB: ChWT) | Three channels (Chs) are employed to carry the information: (1) main, (2) feedback, and (3) wiretap |
| 3.  | $M_T$ | Spreading code or message $M$ from the transmitter |
| 4.  | $f_{\text{MFSK}}(M_T) = X_{\text{MFSK}}$ | Modulation applied on message $M_T$ |
| 5.  | $\text{Cry}(E) = f_Z[K_{ss}(PN\_ Seq)] = X_{PN}$ | Cryptography encryption function, encryption $E$ is performed on $PN\_ Seq$ using the secret session key $K_{ss}$ |
| 6.  | $f_{\text{FB}}(X_{\text{MFSK}}) = X_{\text{FB}}$ | Frequency hopping (modulation) applied and got value $X_{\text{FB}}$ transmitted to the main channel |
| 7.  | $\text{Cry}(H) = f_Z[K_{ss}] = X_H$ | Cryptography hashing function, hashing is performed on key $T_{Alice}(K_{ss})$ using the SHA-2 algorithm |
| 8.  | $X_{\text{FB}(H)}$ | Gathered, $X_{FB}$ and $X_{FB}$, as $X_{FB(H)}$ while passing over the Chmain |
| 9.  | $Y_R = X_{\text{FB(H)}}$ | While received, after passing the Chmain, at $R_{Bob}$ |
| 10. | $Z_f = X_{\text{FB}(H)}$ | While received, after passed the ChWT, at $J_{eaves}$ |
| 11. | $f_{\text{WT}(M_T; X_{\text{FB}(H)})} = P(M_T; X_{\text{FB}(H)})$, where $(M; X_{ss})$ are unknown values. | A wiretap channel, $f_{\text{WT}}$ is computed by an eavesdropper; to grab the information about $(M_T; X_{FB(H)})$, with some probability of success |
| 12. | $f_{\text{FB}}(X_{FB}) = [X_{FB}\text{setbit}(0, 1)]$ | The feedback, while $X_{FB}$ received, if set bit enabled |
| 13. | $\text{Cry}(H) = f_Z[K_{ss}] = Y_H$ | At $R_{Bob}$, cryptography hashing function, hashing is performed on key $R_{Bob}(K_{ss})$ using the Sha-2 algorithm |
| 14. | $\text{Cry}(H) = f_Z[K_{ss}] = Y_H$ | Cryptography hashing comparator CP function $f_Z$, computed some value as $(XH)_h$ |
| 15. | $\text{Cry}(D) = f_D[K_{ss}(PN\_ Seq)] = Y_{PN}$ | Cryptography decryption function, decryption $D$ is performed on $PN\_ Seq$ using the secret session key |
| 16. | $Y_{\text{FB}}$ | Frequency hopping demodulated output |
| 17. | $f_{\text{MFSK}}(Y_{\text{FB}}) = Y_{FB} = M_R$ | MFSK demodulated output |

MFSK: multiple frequency-shift keying.
\[ f_{VB}(X_{FH}) = [X'_{FH} \text{ set bit}(0, 1)] \]
\[ \Rightarrow \text{Set bit}(t) = \begin{cases} 
0, & \text{no confirmation require} \\
1, & \text{confirmation require} 
\end{cases} \]

**CM**

The proposed CM is developed, considering the wireless physical layer security design, based on the actual FHSS modulation. For a given FHSS system, as described, the spreading code or PN\_Seq was generated using linear-feedback shift registers (LFSRs); thus to implement and to examine the spreading code secrecy, the PN-Seq has to be encoded using the secret session key \( K_{ss} \), that is

\[ E(M) = X_T = K_{ss}\{PN\_Seq\} \quad (2) \]

where \( PN\_Seq \) is generated as a maximum sequence, \( m = 2^r - 1 \). Meaning that, the encoded form of \( PN\_Seq \), as \( E(M) \), is treated as spreading code of FH system. The \( K_{ss} \) is generated with a session that is random in reality and shared securely between \( T_{Alice} \) and \( T_{Bob} \), through a defined channel \( Ch_{main} \), prior to FH modulation. Thereby, to perform FH, the spreading code, that is, \( E(M) \), has to be synchronized between \( T_{Alice} \) and \( T_{Bob} \), prior to the transmission; thus, in case of the synchronization failure issues, \( T_{Bob} \) will only receive \( X_{FH} \) signals similar to the noise-like signals. However, only possible to get the spreading code is through decoding function \( D(X_T) \), that is,

\[ D(X_T) = Y_R = K_{ss}[E(M) = K_{ss}\{PN\_Seq\}] \]

As the key, \( T_{Alice} (K_{ss}) = T_{Bob} (K_{ss}) \) is statistically generated and distributed in the absences of the certificate authority (CA) and the key distribution center (KDC) to perform encryption/decryption function. For each transmission, the key is processed with a session that is always in random to avoid jammer \( J_{Eve} \). For example, if the secret key has a session of 28 s, and at the receiver, the spreading code or \( E(M) \) is unsuccessfully decoded using the same key. Then, a new key will be requested, with a new session, to decode the \( E(M) \).

The second main challenge, a statement that information of secret key can be leaked while communicating over an open and weak wireless channel, is addressable by verifying the integrity of key that is used at the receiver site. Therefore, this study has considered a cryptography SHA-2 hashing function as a potential solution to this problem. Suppose \( H \) is a hashing algorithm, and \( f_H \) is a hashing function applied on key, the hashing value of the key is then computed as \( T_{Alice} : Cry(H) = f_H[K_{ss}] \). This operation is done before passing of spread code toward the frequency synthesizer, which is used to convert the conventional frequencies to distinct required frequencies, shown in Figure 3, at both ends of the transceiver system. Thus, the transceiver system has been fully configured and setup with CM; the computed hash code \( Cry(H) \) is sent toward the legitimate receiver \( R_{Bob} \), along with spread code as \( E(M) \), readable by legitimate receiver \( R_{Bob} \) prior to passing through the hash comparator function. As a consequence, the jamming \( J_{Eve} \) will not able to change (or alter) the reception of the data signals that transmitted from \( T_{Alice} \), for that, she has to compute the hashing code similar to the intended receiver, which is almost impossible; then, she is able to make alternation into the data signals that surly also impossible for her. At the receiver side, to get the spreading code that is transmitted from \( T_{Alice} \), \( R_{Bob} \) computes first the hash value of spread code, \( Cry(H) = f_H(K_{ss}) \), before converting to the desired hopset frequencies through the synthesizer. At the same time, the unknown receiver \( J_{Eve} \) has a probability to interrupt in-between the communication via wiretap channel, to get the original transmitted spread code along with hash value, after spending much effort with high-level system computations. However, it depends on the computation probability of whether she should be able to get something valuable or not. In short, in the presence of unlimited resources, targeting via wiretap channel \( J_{Eve} \), are somehow useful to get the information, but not reliable because the information that computed will not be much sufficient to attack or continuously attack over the legitimated channel between \( T_{Alice} \) and \( R_{Bob} \). As the transceiver system is fully setup with high secrecy paradigms in mind at the physical layer only, using a CM and a secured acknowledgment channel in between \( T_{Alice} \) and \( R_{Bob} \), so the \( J_{Eve} \) finally do not have a high-level probability to interrupt the transmission. Therefore, in the case of a legitimate receiver, \( R_{Bob} \), successfully able to computed the hashing value \( Cry(H) \), using a hashing function \( f_H \), that is, \( R_{Bob} : Cry(H) = f_H(K_{ss}) \); means that, the \( K_{ss} \) integrity has been verified, and same key employed to decode the spread code, such that

\[ D(X_T) = K_{ss}[R_{Bob}][K_{ss}][T_{Alice}][PN\_Seq] \quad (3) \]

From the above equation, we may conclude that this study has been well contributed to prove and achieve the system secrecy, mainly communicating over the weaker open channels. Through information-theoretical concepts, the goals are to achieve and anticipate the high secrecy against powerful jammers that intercepting in transmission via wiretap channel. To be clear, this study considered the jammers as potential system’s eavesdroppers, or illegitimate entities, intercepting the signals through the wiretap channel \( Ch_{WT} \). The following mathematical computations, or lemmas, solely demonstrate the study contributions slightly close to reality; however, overall study work is conducted using simulation.
Furthermore, for testing the proposed CM and analyzing its performance over the wiretap channel, this study setups and considers the jammers applying through jamming techniques. These jammers are considered as an alternative to potential eavesdroppers, or man-in-the-middle attacks because the main target is to examine the secrecy of spreading code, $T_{\text{Alice}} : M_T = T_{\text{Bob}} : M_R$, while communicating over weaker wireless channels.

**Lemma 1.** $M_T$ is the desired message in bits order being spread through defining spread code that is encrypted with the secret session key, $K_{ss}$, generated as symmetric and distributed between the nodes. Such that

$$M_T \xrightarrow{f_{\text{FSK}}} X_{\text{FSK}} \xrightarrow{f_{\text{H}}} X_{FH}$$

$X_{PN}$ is the output value, after encrypted with $K_{ss}$, and used as spread code for spread the desired signal over frequencies defined in the hopping pattern. Thus, if $f_E$ exist for $X_{PN}$ then $f_D$ is formulated as

$$\text{Cry}(D) = f_D[X_{PN}] = Y_{PN}$$

At $R_{\text{Bob}}$, the same key $K_{ss}$ which was deployed to authenticate the PN code is sent from the legitimate transmitter $T_{\text{Alice}}$; moreover, the integrity of $K_{ss}$ is also a requirement thus verified by computing $X_H$ using $f_H$ (Lemma 2).

**Lemma 2.** $K_{ss}$ is a symmetric session key employed to secure $PN_{\text{Seq}}$, at both sites of $C_{\text{man}}$, thus for $K_{ss}$ secrecy, a fixed code $X_{H}$ is computed and defined as

$$\exists T_{\text{Alice}} : M_T \xrightarrow{f_T} \text{Cry}(H) = f_H[H(K_{ss})] = X_H$$

$$\exists R_{\text{Bob}} : Y_{PN} \xrightarrow{f_H} \text{Cry}(H) = f_H[H(K_{ss})] = Y_H$$

Both the computed values ($X_H, Y_H$) are compared and verified, employing comparator hashing function $f_{CP}$, which further prove the secrecy of $K_{ss}$ by examining the probability that jammer existed (Definition 7)

$$\text{Cry}(CP) = f_{CP}(X_H: Y_H) = (XY)_H$$

**Lemma 3.** For perfect secrecy, employing CM, assumed that: finite message set $(X_T)_v = \{(x_T), 0 \leq i \leq v\}$, finite ciphertext (of PN) set $(X_{PN})_u = \{(x_{PN}), 0 \leq l \leq u\}$, and finite hashing (of a key) set $(X_H)_w = \{(x_H), 0 \leq k \leq w\}$.

$\Rightarrow \mathbb{H}[(X_T)_v] = \mathbb{H}[(X_{PN})_u], \text{ here } X_T$ is assumed as $X_{FH}$

1. In given set $(X_T)_v$, for any $(X_T)_v$ : The entropy is defined, as $\mathbb{H}[(X_T)_v]$, to show that $(X_T)_v$ is transmitted.
2. For the given ciphertext $(X_{PN})_u$ : The entropy is defined, as $\mathbb{H}[(X_T)_v/(X_{PN})_u]$, to show that $(X_T)_v$ was transmitted.

Thus, $\mathbb{H}[(X_T)_v] = \mathbb{H}[(X_T)_v/(X_{PN})_u]$ is conditionally true for perfect secrecy because both statements are equal. Similarly, to anticipate the perfect–perfect secrecy of $K_{ss}$, entropy is defined as $\mathbb{H}[(X_T)_v](X_{FH})_v$, $X_T$ is assumed as $X_{FH}$

1. In given set $(X_T)_v$, for any $(X_T)_v$ : The entropy is defined, as $\mathbb{H}[(X_T)_v]$, to show that $(X_T)_v$ is transmitted.
2. For the given hashing $(X_H)_w$ : The entropy is defined, as $\mathbb{H}[(X_T)_v/(X_H)_w]$, to show that $(X_T)_v$ was transmitted.

$\Rightarrow \mathbb{H}[(X_{FH})_v] = \mathbb{H}[(X_{FH})_v/(X_{PN}:X_H)(w,u)]$, here $X_T$ is replaced with $X_{FH}$

Let us suppose that, for some finite number as $v = w = 3$, thus sets are given:

1. $(X_T)_v = \{(x_T)_3, 0 \leq i \leq 3\}$
2. $(X_{PN})_u = \{(x_{PN})_3, 0 \leq l \leq 3\}$
3. $(X_H)_w = \{(x_H)_3, 0 \leq k \leq 3\}$

$\Rightarrow \mathbb{H}[(X_{FH})_v] = \mathbb{H}[(X_{FH})_v/(X_{PN}:X_H)(w,u)]$

$= \mathbb{H}[(X_{FH})_v] = \begin{bmatrix} 1 \ 1 \\ 3 \ 3 \end{bmatrix}$

**Secrecy presumptions**

**Presumption 01.** Based on the aforementioned definitions and lemmas, we may say that the proposed approach (i.e. CM) was contributed significantly to anticipate the perfect secrecy of the system, even in the case of potential jammers (active using Wiretap channel). The perfect secrecy was successfully achieved through the key encryption scheme. Note that, to examine the perfect secrecy of a random message that is transmitted in the unsecured channel, the used key length is must be large or equal to the length of the message or plain text size. However, in the case of large-sized plaintext, the size of the used key must be larger or equal to the size of the selective payload; otherwise, it is impossible to achieve the processing and perfect secrecy in some scenarios. Nevertheless, depending on the conditions and the corresponding analytical
conducted before, the system design assumed to be a perfectly secure system.

**Presumption 02.** On the other side, the goal to ensure the secrecy of the key itself that is used to examine the perfect secrecy of the system or wireless channel secrecy, the hash was computed on the key that is deemed to be symmetric. The successful deployment, therefore, assumed to provide the secrecy of the key uncertainties might be residing in illegitimate transmission. So the system may be considered not only under perfect secrecy paradigms but also under perfect–perfect secrecy paradigms.

In the below section, results are measured and discussed to demonstrate the study significances, through simulation, which may consider a far from real-time measurements. However, real-time development is the future goal of this study.

**Results and discussion**

This study employed the FH technique, a technique that has been commonly used in wireless systems to protect the communication against jammers (or narrowband jammers) and deployed a CM and the information-theoretic security solution to validate the secrecy of information that transmitted is over the unsecured open physical channels. The FHSS technique inherently used PN code to spread the desired signals among the selective frequencies; in short, it is a safeguard for communication against jammers, or system eavesdroppers, as the signals are always transmitted employing distinct frequencies that defined in the hopping set and are known by transmitter and receiver. Therefore, PN code has high importance to gain security, hence this study developed a CM to ensure the PN code secrecy. The proposed solution was successfully implemented and validated the perfect secrecy by employing the key encryption method and further validated the perfect–perfect secrecy by computing the hashing code of the key. So that, the CM has been accounted as an inclusive module to validate the perfect secrecy and as well the perfect–perfect secrecy at the same time.

The given overall measurements are conducted using a CM, a number of times spreading codes were generated and transmitted between $T_{Alice}$ and $T_{Bob}$, and $J_{Eve}$ using wiretap channel $Ch_{HT}$. Meaning that, the system performances have been measured based on successful experiments those distributed according to the defined scenarios and compared to finally examine the effectiveness of the proposed CM, through careful comparison with the existing FH system having security limitations directly connected with its spreading code. So that, the entropy $H$ of spreading code was measured using given lemmas, and the demonstrated the PN_Seq secrecy that individually computed while running over the normal communication (without wiretap channel) and in the presence of a jammer $J_{Eve}$ (with a wiretap channel). At the end, overall conducted results are compared to compute the system precision and to demonstrate the analytical contributions of this study.

In Figure 5, only successful experiments are randomly selected among other several experiments, the computed results show the exchanging of information (or PN_Seq) between the transmitter and receiver. Suppose that the information transmitted from the transmitter was enclosed in a packet contained a random bits order and was always distinct in size for each successful measurement. So, the blue line shows a number of packets (i.e. a PN_Seq order), and the parallel orange line along shows the throughput or transmission gain at the receiver site. As examined, there are few differences while comparing both performances that might

![Figure 5. Computed results over normal transmission.](image-url)
be because of some unknown wireless medium impairments. However, overall transmission gain over each transmission does not look very different from the original once each time. The exact information loss, that is, bits loss, are illustrated in Figure 6.

Furthermore, in Figure 6, the wiretap channel is established to conduct the measurements based on the collective final results of information loss, the main target is to get overall transmission gain at the receiver side and further validate the system performances in the presence of jammer(s). Hence, it is further helpful to acquire and compare the total loss of information while transmitting in the presence of anonymous jammers interception, illustrated in Figure 7. Alongside, in Figure 8, the red color marker over each measurement demonstrates the key status either successfully operated representing in the form of red marker or leakage over the wiretap channel representing through red filled symbol or marker.

In Figure 9, information secrecy is examined, through the employed key and key secrecy employed through hash value, to conclude the secrecy levels—perfect-secrecy and perfect–perfect secrecy of system—the red plus (+) symbol visualizes perfect secrecy at each measurement, while the green plus (+) symbol visualizes perfect–perfect secrecy. The results of Figure 9 are equally computed in the presence of a wiretap channel. Finally, Figure 10 illustrates system efficiency, the mean assessment of overall equivalent measurements for both employed scenarios—normal channel and wiretap channel. Consequently, we may say that the proposed system has a resistance against the jammers.

**Conclusion**

The proposed study is a significant step in computing and examining the secrecy of wireless communication systems, and the secrecy is directly linked with the physical layer. After the depth analysis and based on the potential available security issues related to the spread-spectrum techniques, the CM is proposed and
implemented. The CM is an inclusive security module, comprised of encryption and hashing systems, whose development provided a well-examined PN_Seq secrecy as a part of the FH system. Moreover, the proposed system is successfully applied and validated with information-theoretical security approaches, and consequently, the perfect secrecy and perfect–perfect secrecy are well anticipated. This study provides further future research directions to enhance the security at the physical layer, to fight against the vulnerabilities and jamming attacks, and to deploy in other applications or systems that using various random codes to transmit the desired information. This study will be very useful to integrate with the existing conventional designs of the wireless systems, such as Bluetooth, Wi-Fi, CDMA systems, and so on, to ensure secrecy at a high level.

Declaration conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.
Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (grant no.2019-0-00231, Development of artificial intelligence based video security technology and systems for public infrastructure safety).

ORCID iDs
Aamir Shahzad https://orcid.org/0000-0003-0265-545X
Young-Gab Kim https://orcid.org/0000-0001-9585-8808

References
1. Ebrahimzadeh A and Falahati A. Frequency hopping spread spectrum security improvement with encrypted spreading codes in a partial band noise jamming environment. *J Inf Secur* 2013; 4: 1–6.
2. Zheng P, Peterson LL, Davie BS, et al. *Wireless networking complete*. San Francisco, CA: Morgan Kaufmann Publishers Inc., 2009.
3. Grover K, Lim A and Yang Q. Jamming and anti-jamming techniques in wireless networks: a survey. *Int J Ad Hoc Ubiqu Co* 2014; 17: 197–215.
4. Fang W, Li F, Sun Y, et al. Information security of PHY layer in wireless networks. *J Sensors* 2016; 2016: 1230387.
5. Dabcevic K. *Intelligent jamming and anti-jamming techniques using cognitive radios*, PhD Thesis, Programme in Computational Intelligence, University of Genoa, Genoa, 2015.
6. Motlagh NH. *Frequency hopping spread spectrum: an effective way to improve wireless communication performance* (Advanced trends in wireless communications). London: INTECH Open Access Publisher, 2011.
7. Debbah M, El-Gamal H, Vincent Poor H, et al. Wireless physical layer security. *PNat Acad Sci USA* 2010; 2009: 1–2.
8. Barros J and Rodrigues MRD. Secrecy capacity of wireless channels. In: *Proceedings of the IEEE international symposium on information theory*, Seattle, WA, 9–14 July 2006, pp.356–360. New York: IEEE.
9. Bassily R, Ekrem E, He X, et al. Cooperative security at the physical layer: a summary of recent advances. *IEEE Signal Proc Mag* 2013; 30(5): 16–28.
10. Chen Z, He M, Liang W, et al. Trust-aware and low energy consumption security topology protocol of wireless sensor network. *J Sensors* 2015; 2015: 716468.
11. Tafaroji M and Falahati A. Improving code division multiple access security by applying encryption methods over the spreading codes. *IET Commun* 2007; 1(3): 398–404.
12. Shahzad A, Lee M, Kim HD, et al. New security development and trends to secure the SCADA sensors automated transmission during critical sessions. *Symmetry* 2015; 7: 1945–1980.
13. Shahzad A, Lee M, Lee C, et al. The protocol design and new approach for SCADA security enhancement during sensors broadcasting system. *Multimed Tools Appl* 2015; 75: 14641–14668.
14. Yener A and Ulukus S. Wireless physical-layer security: lessons learned from information theory. *P IEEE* 2015; 103(10): 1814–1825.
15. Shannon CE. Communication theory of secrecy systems. *Bell Syst Tech J* 1949; 28(4): 656–715.
16. Renna F, Laurenti N and Poor HV. Physical-layer secrecy for OFDM transmissions over fading channels. *IEEE T Inf Foren Sec* 2012; 7(4): 1354–1367.
17. Bloch M and Laneman JN. On the secrecy capacity of arbitrary wiretap channels. In: *Proceedings of the 46th annual Allerton conference on communication, control, and computing*, Urbana-Champaign, IL, 23–26 September 2008, pp.818–825. New York: IEEE.
18. Tugnait JK and Li T. Blind detection of asynchronous CDMA signals in multipath channels using code-constrained inverse filter criterion. *IEEE T Signal Proces* 2011; 49(7): 1300–1309.
19. Leukhin A, Moreno O and Tirkel A. Secure CDMA and frequency hop sequences. In: *Proceedings of the tenth international symposium on wireless communication systems*, Ilmenau, 27–30 August 2013. New York: IEEE.
20. Darnell M and Yung HM. Security considerations in frequency hopping radio systems. In: *Proceedings of the IEEE colloquium on security and cryptography applications to radio systems*, London, 3 June 1994, pp.111–113. New York: IEEE.
21. Wang Z, Fok MP and Prucnal PR. Physical encoding in optical layer security. *J Cyber Secur Mobil* 2012; 1: 83–100.
22. Mansour I, Chalhoub G and Quilliot A. Security architecture for wireless sensor networks using frequency hopping and public key management. In: *Proceedings of the IEEE international conference on networking, sensing and control (ICNSC)*, Delft, 11–13 April 2011. New York: IEEE.
23. Prashanth BU and Pandurangaiyah Y. Generation of secret key for physical layer to evaluate channel characteristics in wireless communications, 2013, https://arxiv.org/ftp/arxiv/papers/1308/1308.1206.pdf
24. Meng XY, Tao R and Jia LN. An intelligent anti-jamming frequency hopping system. In: *Proceedings of the first international conference on pervasive computing, signal processing and applications*, Harbin, China, 17–19 September 2010, pp.1053–1056. New York: IEEE.
25. Popper C, Strasser M and Capkun S. Anti-jamming broadcast communication using uncoordinated spread spectrum techniques. *IEEE J Sel Area Comm* 2010; 28(5): 703–715.
26. Shen F, Wang J and Wang J. An anti-interference method for spread spectrum system based on amplitude domain processing. In: *Proceedings of the IEEE international conference on mechatronics and automation*, Changchun, China, 9–12 August 2009, pp.3589–3594. New York: IEEE.
27. Olama MM, Ma X, Kuruganti TP, et al. Hybrid DS/FFH spread-spectrum: a robust, secure transmission technique for communication in harsh environments. In: *Proceedings of the military communications conference*, Baltimore, MD, 7–10 November 2011, pp.2136–2141. New York: IEEE.
28. Hanawal MK, Abdel-Rahman MJ and Krunz M. Game theoretic anti-jamming dynamic frequency hopping and rate adaptation in wireless systems. In: Proceedings of the 12th international symposium on modeling and optimization in mobile, Hammamet, Tunisia, 12–16 May 2014, pp.247–254. New York: IEEE.

29. Torrieri D. Principles of spread-spectrum communication systems. New York: Springer, 2015.

30. Sklar B. Digital communications, vol. 2. Upper Saddle River, NJ: Prentice Hall, 2001.

31. Borah DK and Hart BT. Frequency-selective fading channel estimation with a polynomial time-varying channel model. IEEE T Commun 1999; 47(6): 862–873.

32. Giorgetti A, Chiani M and Win MZ. The effect of narrowband interference on wideband wireless communication systems. IEEE T Commun 2005; 53: 2139–2149.

33. Kumar PV. Frequency-hopping code sequence designs having large linear span. IEEE T Inform Theory 1988; 34(1): 146–151.

34. Cong L and Songgeng S. Chaotic frequency hopping sequences. IEEE T Commun 1998; 46(11): 1433–1437.

35. Zhang J, Duong TQ, Marshall A, et al. Key generation from wireless channels: a review. IEEE Access 2016; 4: 614–626.

36. Dinca LM and Hancke G. User-centric key entropy: study of biometric key derivation subject to spoofing attacks. Entropy 2017; 19: 70.

37. Yu L, Wang M and Qiao X. A novel hybrid spread spectrum system and anti-jamming performance analysis. Procedia Engineer 2012; 29: 1325–1330.

38. Harrison WK. Physical-layer security: practical aspects of channel coding and cryptography. Doctoral Thesis, Georgia Institute of Technology, Atlanta, GA, 2012.

39. Quan H, Zhao H and Cui P. Anti-jamming frequency hopping system using multiple hopping patterns. Wireless Personal Communications 2015; 81: 1159–1176.

40. One-Time Pad. http://web.engr.oregonstate.edu/~rosulekm/crypto/chap1.pdf