JCSE Journal of Computing Science and Engineering

Invited Paper

Journal of Computing Science and Engineering,
Vol. 7, No. 3, September 2013, pp. 187-197

A Survey of Security Mechanisms with Direct Sequence Spread Spectrum Signals

Taeho Kang
Department of Computer Science and Engineering, Pohang University of Science and Technology (POSTECH), Pohang, Korea
darktoy@postech.ac.kr

Xiang Li
Department of Electrical and Computer Engineering, Cleveland State University, Cleveland, OH, USA
x.li110@csuohio.edu

Chansu Yu
Department of Electrical and Computer Engineering, Cleveland State University, Cleveland, OH, USA
Division of IT Convergence Engineering, Pohang University of Science and Technology (POSTECH), Pohang, Korea
c.yu91@csuohio.edu

Jong Kim*
Division of IT Convergence Engineering, Pohang University of Science and Technology (POSTECH), Pohang, Korea
jkim@postech.ac.kr

Abstract
Security has long been a challenging problem in wireless networks, mainly due to its broadcast nature of communication. This opens up simple yet effective measures to thwart useful communications between legitimate radios. Spread spectrum technologies, such as direct sequence spread spectrum (DSSS), have been developed as effective countermeasures against, for example, jamming attacks. This paper surveys previous research on securing a DSSS channel even further, using physical layer attributes—keyless DSSS mechanisms, and watermarked DSSS (WDSSS) schemes. The former has been motivated by the fact that it is still an open question to establish and share the secret spread sequence between the transmitter and the receiver without being noticed by adversaries. The basic idea of the latter is to exploit the redundancy inherent in DSSS's spreading process to embed watermark information. It can be considered a counter measure (authentication) for an intelligent attacker who obtains the spread sequence to generate fake messages. This paper also presents and evaluates an adaptive DSSS scheme that takes both jam resistance and communication efficiency into account.

Category: Ubiquitous computing

Keywords: Security and privacy; Hardware-dependent software and interfaces; Smart-environment computing

Open Access **http://dx.doi.org/10.5626/JCSE.2013.7.3.187** **http://jcse.kiise.org**

Received 12 June 2013, **Accepted** 4 July 2013
*Corresponding Author

 pISSN: 1976-4677 eISSN: 2093-8020

I. INTRODUCTION

Along with the growth of wireless communication systems, the demands for power efficiency for mobile devices and prompt security services for dynamic wireless environment have drawn considerable attention to physical layer security research. Spread spectrum technologies, such as direct sequence spread spectrum (DSSS), were originally developed for this purpose. DSSS spreads out the spectrum of the content signal with, for example, pseudonoise (PN) sequences to resemble white noise. Thus, the DSSS technique offers jamming resistance, interference rejection, message privacy and a number of other desirable properties [1]. For example, a jammer signal is not able to jam the wide-band signal, unless it knows the spread sequence, or the key and algorithm for generating the spread sequence [2]. Specifically with the interference rejection property, DSSS is widely adopted in commercial wireless network standards, such as IEEE 802.11 [3] and IEEE 802.15.4 [4], to provide robust communications. However, these standards make the PN sequences available to the public, and hence do not inherit one of the most important merits of DSSS. Many researchers have managed to complement the physical layer security for commercial DSSS systems, by extending the PN sequence set or manipulating chips in the PN sequences.

This paper surveys three key aspects of DSSS technique in the context of the mobile wireless environment.

First, like symmetric cryptographic keys in conventional network security mechanisms, it is not straightforward to establish the spread sequence between the transmitter and the receiver, without resorting to a fixed infrastructure. This constitutes a challenging research agenda establishing a DSSS channel with no prior negotiation on a shared spread sequence, namely keyless DSSS (Section IV).

Second, DSSS reduces the communication efficiency, because a wider bandwidth than necessary is needed to deliver the same amount of data bits, particularly when the jammer signal is stronger. On the other hand, the reduced communication efficiency can be compensated for by employing a more sophisticated modulation scheme, particularly when the user signal is stronger. Adaptive selection of the spread sequence length and modulation scheme can be performed, based on the jamming and channel conditions (Section V).

Third, one of the widely adopted security techniques in the physical layer is digital watermarking, in which a watermark signal can be embedded into or multiplexed with a content signal [5]. Many physical layer attributes, such as channel coding, modulation schemes and transmission power provide redundancy and randomness that are suitable for embedding watermark information [6]. One promising area in this direction is to utilize the inherent redundancy in DSSS signals to embed watermark information, which we call watermarked DSSS (WDSSS) (Section VI).

The rest of the paper is organized as follows. Section II explains DSSS, and Section III discusses the jamming and anti-jamming mechanisms, which are followed by discussions of the abovementioned three DSSS-based security mechanisms in Sections IV, V, and VI, respectively. The paper concludes with Section VII.

II. DIRECT SEQUENCE SPREAD SPECTRUM

Most of the security mechanisms for wireless networks depend on the intractability assumption and the corresponding computational complexity [7]. In DSSS techniques, it is channel bandwidth that complicates the process of decryption or decoding, because an original signal is spread into a wider bandwidth signal [8].

Fig. 1a shows a generic DSSS system model [9]. In a typical DSSS system, the transmitter first modulates the data signal with a carrier signal, and then spreads the modulated signal, by applying modulo-2 addition to it with a spreading signal. The spreading signal is generated from a PN sequence running periodically at a much higher rate than the original data signal. The spreading operation is shown in Fig. 1b. Each individual digit in the PN sequence is called a chip to be differentiated from the

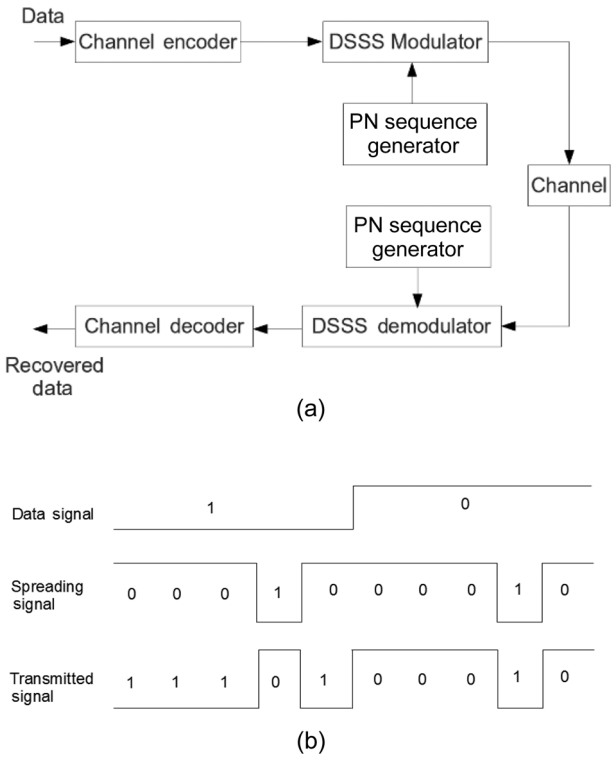

Fig. 1. (a) Direct sequence spread spectrum (DSSS) system model and (b) DSSS spreading operation; the pseudonoise (PN) sequence in this example is 00010.

bit in the data signal, and each period of the PN sequence is used to spread one data bit. Because the PN sequence is designed to resemble white noise, the spectrum of the original signal is spread out. Thus, the spectrum of the spread signal occupies a larger bandwidth than necessary and shows a lower power spectral density than that of the original signal.

Symmetrically, the receiver first performs a correlation process on the incoming signal, that is, it applies the modulo-2 addition to the incoming signal with a synchronized copy of the spreading signal. The receiver then obtains the underlying modulated signal, which is in turn demodulated to recover the original data signal. The duplicating modulo-2 addition provides interference rejection for the DSSS signal if the interference is narrow band, because modulo-2 addition of the narrow band interference with the spreading signal will spread out the power of the interference, and hence will increase the receiving signal-to-noise (SNR) of the signal of interest.

A longer spread sequence must be employed in order to enhance the jam resistance. However, it reduces the communication efficiency accordingly, because a wider bandwidth is utilized to deliver the same amount of data bits. The spread sequence can be generated in two different ways [8]: *PN sequence,* and *orthogonal code*. Two desirable features of the former are that auto-correlation is zero so that the synchronization at the receiver is easier, and that cross-correlation is zero too, so that multiple such codes can be used concurrently, like the *Gold sequence* in code division multiple access (CDMA). As for the latter, the cross-correlation is zero, but the auto-correlation is not. Thus, a tight synchronization is needed at the receiving end. *Walsh code* is a good example, which is used in CDMA, too.

III. JAMMING AND ANTI-JAMMING

Jamming is an unsophisticated technique that can effectively disrupt legitimate user's communication unless they are equipped with extremely sophisticated detection mechanisms and countermeasures. While DSSS has an anti-jamming capability, there also exist intelligent jamming strategies that effectively attack a DSSS channel.

A. Classification of Jamming Attack

There has been active research on developing effective jammer strategies. For example, [10] studied channel-oblivious and channel-aware jammers. Channel-oblivious jammers can jam deterministically at a specified rate (*periodic jammer*) or follow a certain distribution (*memoryless jammer,* following a Poisson process). The periodic jammer is useful when the jammer is not powerful enough to jam a wide band continuously. *Channel-aware jammers* monitor the channel and try to adjust their strategy according to the states of the legitimate stations in the neighborhood. For example, it stays quiet when the channel is idle, but starts transmitting radio signals when the channel becomes busy [11]. Consequently, a channel-aware (reactive) jammer targets the reception of a signal. In fact, jamming is not necessary when the channel is idle. Due to its reactive nature, it is harder to detect channel-aware jammers.

On the other hand, channel-oblivious jammers are easier to detect but at the same time easier to implement because they emit a radio signal constantly or regularly, without waiting for the channel to be idle. These jammers do not follow or abuse the underlying media access control (MAC) protocol by ignoring interframe spaces or congestion window mechanisms (like in 802.11 standards), and inject normal packets or random bit sequences so as to block all transmissions from legitimate nodes. It can also use normal packets rather than a random signal to disguise itself as a legitimate user. An advantage is that the detection is harder as normal packets are transmitted.

B. Jamming Characteristics

The main goal of a jammer is to interfere with wireless communications between legitimate mobile nodes. It achieves this goal by either blocking the source from sending its own packets or by blocking the receiver from receiving the legitimate packets. They are formulated as *packet send ratio* and *packet delivery ratio* (PSR and PDR), respectively [11], and are good indices to demonstrate the effectiveness of a jammer. PSR refers to the ratio of the number of packets that are successfully transmitted to the number of packets that are intended to transmit. Since a network interface has a limited size of packet buffer, packets will be dropped when they cannot be transmitted, decreasing the PSR. A low PSR means a highly congested network, or the presence of a jammer.

On the other hand, PDR refers to the ratio of the number of packets that are successfully received to the number of packets that are transmitted. This can be measured at the transmitter, because it receives an ACK for each of the successful transmissions. However, PDR can also be measured at the receiver by calculating the number of packets that are successfully decoded to the number of packets that are received; i.e., it counts the packets that have been received and that pass the integrity check such as cyclic redundancy check (CRC). Either way, a low PDR means a strong interference or the presence of a jammer.

Detecting a jammer is challenging because there exist numerous intelligent jammer strategies. PSR and PDR mentioned above can be used as an indication of a jammer. Other MAC and PHY attributes, such as signal strength and carrier sensing time, can be used to detect a jammer when they exhibit abnormal distributions [11]. For example, when a node wishes to transmit, it senses

the channel following the underlying MAC algorithm, such as carrier sense multiple access (CSMA). It may declare the presence of a jammer if it does not have the opportunities to transmit its packet for an extended period of time while the channel is continuously intercepted by others, disrupting the fairness in a significant manner.

IV. KEYLESS SPREAD SPECTRUM COMMUNICATION

A. Secret Key Extraction

While the DSSS system supports confidentiality and authentication services, it is difficult to establish a spread sequence in secrecy. Recently, there has been active research on removing the dependency on the secret key at the cost of either increased communication delay or increased decoding delay. For example, they repeat the same message many times for synchronization [12, 13]. However, this is also useful in broadcast communication where a sender needs to share a secret key with multiple receivers [13, 14]. They include uncoordinated frequency hopping spread spectrum (FHSS) [12], uncoordinated DSSS [13], and randomized differential DSSS [14].

The essential idea is to establish a secret key by exploiting the wireless channel itself since it provides a unique opportunity for the sender and the receiver to create a shared secret information [15-17]. Note that the wireless channel is time-varying and location-specific but is also reciprocal [18, 19]. In [20], a new key extraction algorithm is presented, which does not require an authenticated channel. Since the channel fading at the location away more than $\frac{\lambda}{2}$ from the communicating peers is statistically independent from the peers, channel impulse responses between them are unique and decorrelated rapidly in space. These correlation observations result in a series of bits using the line-crossing algorithm, producing a shared secret information [20]. [17] presents the effectiveness of secret key extraction using received signal strength (RSS) variations, and found that the generated key does not hold a high enough entropy such that an adversary can possibly generate the same key. It proposes an adaptive approach where threshold values are determined adaptively based on the RSS mean and deviation. To make it work, the sender and the receiver accumulates a time series of measured RSS as they exchange packets.

B. Keyless DSSS

Those algorithms introduced in the previous section can be utilized to generate the spread sequence for DSSS without a prior negotiation between the transmitter and the receiver. However, there were studies in the literature that specifically target keyless DSSS. Several individual works considered expanding the PN sequence set used in a DSSS system [21-23]. In order to enhance the secrecy of the PN sequences, uncoordinated DSSS (UDSSS) [13] randomly picks the spread sequence from a public set. Because of randomly choosing the spreading sequence, attackers cannot know the next spreading sequence that the sender will use to modulate it. However, the sender needs to send a message several times (with different spreading codes) to increase the probability that the receivers get the message, even though they're not synchronized. And the receiver needs to sample the radio channel and to store it in a buffer, which will be applied with a subset of spread sequences for despreading. The advantage of UDSSS is the ability of communicating both unicast and broadcast under a jamming attack where the standard DSSS cannot. As a tradeoff, the throughput decreases and the latency increases because of sampling and trial-and-error to find the spreading sequence.

Both [21] and [22] also intended to improve the secrecy of the PN sequence. Their methods allow the transmitter and the receiver to generate an identical set of PN sequences with a prior negotiation, and the spreading and correlation processes share a code hopping scheme, which provide a dynamic synchronization between the PN sequences used in the transmitter and the receiver.

Randomized differential DSSS (RD-DSSS) [14] has been proposed to deal with broadcast communication in the presence of jammers. Similar to UDSSS, it uses a public set of spread sequences but modulates data using the correlation of two random spreading sequences. In other words, bit "0" is encoded using two different spreading sequences in the set, while bit "1" is encoded using two identical spreading sequences. Since the public set has been designed to exhibit low correlation (nearly or fully orthogonal) between any two different codes in the set, the receiver despreads the data by interpreting high correlation as "1" and low correlation as "0".

V. SPREAD SEQUENCE LENGTH AND COMMUNICATION EFFICIENCY ADAPTATION

A. Adaptive Modulation and Anti-Jamming Strategy

Adaptive selection of modulation scheme has been a heavily researched subject [24-26]. For example, IEEE 802.11a/g employs binary phase-shift keying (BPSK), quadrature phase-shift keying (QPSK), 16-QAM and 64-QAM, which achieve as much as 36, 72, 144, and 216 data bits per symbol, respectively [3]. Typically, the best modulation scheme and the corresponding data rate are determined based on a trial-and-error approach. In *auto-rate fallback* (ARF) [25], a node lowers its data rate (fewer data bits per symbol) if it experiences consecutive

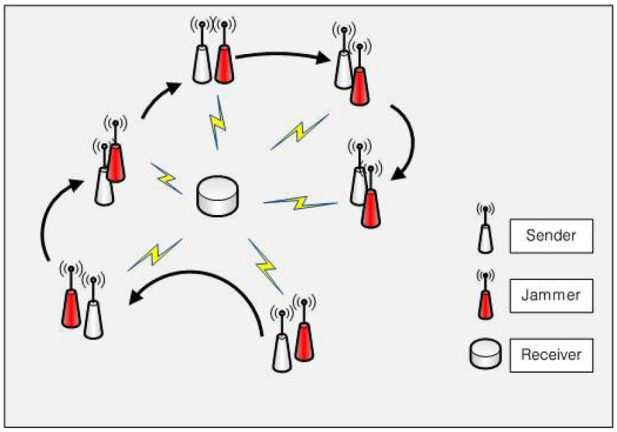

Fig. 2. Three-node scenario: the jammer chases after the sender.

transmission failures and increases its data rate (more bits per symbol) upon a number of consecutive transmission successes.

As discussed in the Introduction section, a certain scenario allows the employment of such a more sophisticated modulation scheme, which has the potential to compensate for the reduced communication efficiency due to the redundant use of bandwidth as in DSSS. The jammer scenario is a command-and-control scenario, where the jammer chases the transmitter in order to effectively analyze and jam the legitimate communication as shown in Fig. 2. Both the sender and the receiver monitor the communication channel, and they can adaptively change the modulation scheme and the spread sequence length based on the condition of the communication link.

The objective is for the sender and the receiver to communicate at or below the required jam resistance (bit error rate [BER] performance of 10^{-6}). They desire to acquire the maximum communication efficiency (high data rate, R_b), but at the same time the minimum spread spectrum bandwidth (W_{ss}). In other words, the sender and the receiver monitor the channel condition. If the channel condition is good, they try to increase the data rate (R_b) by changing the modulation scheme to a more sophisticated one. When a higher data rate is not available, they decrease the spread spectrum bandwidth (W_{ss}) to increase the communication efficiency. In contrast, if the channel condition is bad, they try to increase the spread spectrum bandwidth first, by using a longer spread sequence. Otherwise, they change the modulation scheme to decrease the data rate for the required jam resistance. Please refer to [27] for more details.

B. Performance Evaluation

We have investigated the implementations of the abovementioned adaptation scheme in the context of Universal Software Radio Peripheral (USRP; Ettus Research, Mountain View, CA, USA) [28], and GNU Radio [29].

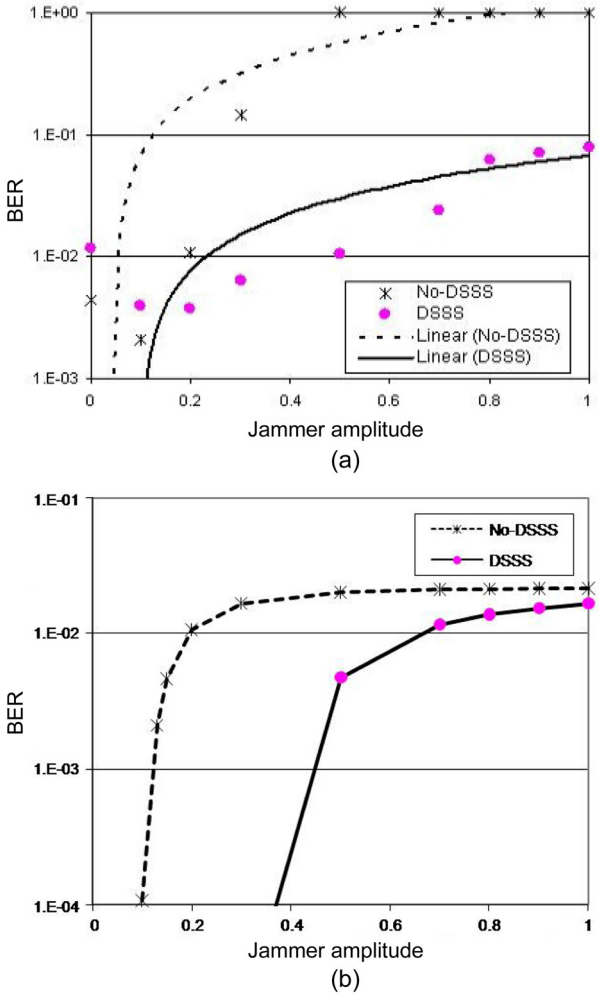

Fig. 3. Bit error rate (BER) versus jammer amplitude; the spread sequence length can be adapted depending on the jammer condition, including its amplitude. (a) Experimental results and (b) theoretical results. DSSS: direct sequence spread spectrum.

The core of the USRP is a motherboard with two high-speed analog to digital converters (ADCs) and digital to analog converter (DACs), and a Xilinx Spartan field programmable gate array (FPGA). The ADCs/DACs are connected to the daughterboards, while the FPGA is connected to a host purpose computer running GNU Radio via a Gigabit Ethernet interface. We used the implementation of 802.11b from BBN Technologies Company [30]. Pulse jammer is used with a pulse width of 220 μsec and the period of 10,000 μsec. Fig. 3a compares the BER performance of DSSS and no-DSSS with varying jammer amplitude. The figure includes trend lines as well in order to mask experiment errors, which is typical in practical experiments, and thus to better capture the general trend of the experiment results. According to the chart, the BER increases with the jammer's amplitude as expected. It is important to contrast it with the theoretical results in Fig. 3b, which exhibit a similar pattern. Note that the

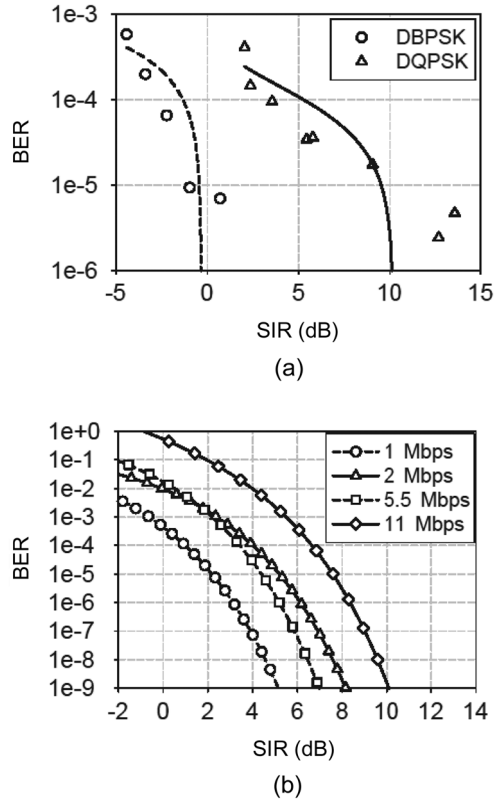

Fig. 4. Bit error rate (BER) versus signal amplitude; the modulation scheme can be adapted depending on the channel condition, including the signal strength or signal-to-noise and signal-to-interference ratio (SNR/SIR). (a) Experimental results and (b) theoretical results. DBPSK: differential binary phase shift keying, DQPSK: differential quadrature phase shift key.

BER ranges in Fig. 3a and b are not the same, which is due to the complex wireless propagation phenomenon in reality.

On the other hand, Fig. 4 shows the BER curve for several modulation schemes (data rates). In Fig. 4b, the SNR/signal-to-interference (SIR) requirement for the target BER of, for example, 10^{-5} is 2.2, 5.2, 6.4, and 7.6 dB, for 1, 2, 5.5, and 11 Mbps, respectively. In other words, users are not allowed to use a high data rate under a bad channel condition or a communication in the distance. Combining this with Fig. 3, there is a tradeoff between jam resistance and the communication efficiency considering the 3-node scenario in Fig. 2. Please refer to [27] for more results.

VI. PHY LAYER WATERMARKING

A. Watermarked DSSS

The goal for designing a WDSSS technique is to embed secret information in the PN sequences of the DSSS technique, so as to complement the physical layer security for a DSSS system with publicly known PN sequences. Two fundamental premises for WDSSS techniques are the error correcting capability of PN sequences and the correlation procedure of the DSSS receiver. The error correcting capability of PN sequences implies coding redundancy in good communication environments. The coding redundancy can consequently be exploited to carry additional information without requiring extra bandwidth.

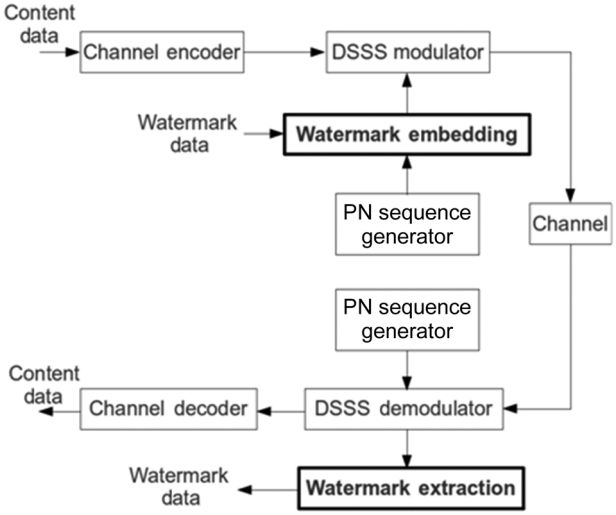

Fig. 5. Watermarked direct sequence spread spectrum (DSSS) system model. PN: pseudonoise.

A WDSSS technique consists of two major operations, watermark embedding and extraction, which are placed in a transmitter and an *aware receiver*, respectively. A WDSSS system model is shown in Fig. 5. A watermark embedding processing block and an extraction processing block are added in the classic DSSS signal processing paths. In the transmitter, the watermark embedding block flips chips in the PN sequence at positions indicated by the watermark information, and then the modified PN sequence is used to spread the content bit. In the aware receiver, the demodulator correlates incoming signals with the original PN sequence, and determines content data bit values by comparing the correlation results with a threshold. The unmatched chip positions are then passed to the watermark extraction processor, which in turn translates the position information into watermark data bits. On the other hand, in an *unaware receiver* without the watermark extraction block, the demodulator can still recover the content bit values based on the correlation results, but ignores the specific positions of error chips since it does not examine the individual chips.

B. WDSSS Approaches

There has been specific work devoted in physical layer

watermarking research, combining the watermarking technique with various physical layer properties. Goergen et al. [31] generated the watermark signal from a finite length synthetic FIR channel response. [32] proposed to generate the watermark signal from the application of a robust Hash function on the content signal and a secret key, and then superimpose the watermark signal onto the content signal at a lower power level. Two physical layer watermarking techniques were proposed in [33], applied to the payload or the cyclic time of an orthogonal frequency-division multiplexing (OFDM) signal. The first method spreads modulated watermark bits with a Gaussian distributed PN sequence, and then superimposes them onto the OFDM payload data with a low power level. The second method uses positive and negative cyclic time shifts to represent Manchester encoded watermark bits.

Another physical layer watermarking method proposed in [34] embeds a watermark signal in the *M*-ary phase-shift keying (M-PSK) modulation scheme. The principle behind the design is that different values of *M* result in different phase differences between the reference points on the M-PSK constellation maps, and that the M-PSK demodulator decodes symbols by matching them to the reference points within minimum phase difference. The author then utilized a fraction of the phase difference of the content signal to embed the watermark signal.

Other WDSSS schemes are found in [35-37], managing to construct a covert channel on top of plain DSSS communications by manipulating the PN sequences. For example, the coding redundancy in PN sequences is exploited to assign a certain amount of chips in a PN sequence to represent secret data [35]. The proposed work in [36] presented the encoding scheme of embedded data bits to minimize the effect of embedded signal on the content signal. The encoding scheme is to expand each original PN sequence into a cluster of PN sequences that are closer to the corresponding original PN sequence than to any other PN sequences in the original set. The cluster is then used to represent embedded data bits. The work introduced in [37] is based on [35] and adopts the Hamming distance method used in [36]. They provided additional discussion in terms of error correcting capability in the codeword design, and suggested the utilization of all chip position combinations to carry secret information and to recover the secret information through the altered chip positions information. Thus, the size of the covert communication alphabet is equal to the sum of combinations of each possible number of altered chips. They further deduced an optimal number of altered chips for the purpose of interference resistance.

Table 1. Maximized minimum distance method: a set of modified pseudonoise (PN) sequences for the 11-chip Barker sequence (00011101101) with 3 flipped chips

Watermark bit value	Modified PN sequence	Flipped positions	Total embedding capability (bits)
0	01001100101	9, 7, 3	1
1	00010101000	6, 2, 0	

C. Watermark Embedding Methods

A typical WDSSS technique embeds watermark information by flipping chips on designated positions, and thus it is important to establish a mapping relationship between the watermark data bits and the chip positions in the PN sequence. One simple method is to exhaustively use all combinations of chip positions to represent watermark data bits. For a PN sequence of length *n*, if *m* chips can be flipped, the number of position combinations is $\binom{n}{m}$. Thus, the number of watermark bits that can be represented by one modified PN sequence is $\left\lfloor log_2\binom{n}{m} \right\rfloor$. Because one PN sequence is equivalent to one content data bit, this embedding method can provide a much higher watermark data rate than the content data rate.

The Maximized Minimum Distance Method chooses code words with inter-code Hamming distance less than or equal to a certain limit to guarantee optimal error correcting capability. Table 1 shows a set of modified PN sequences for the 11-chip Barker Sequence with 3 flipped chips. The resulting set has a minimum distance of 6.

The subsequence method is another one. It divides the PN sequence into several subsequences, flips one chip in each subsequence, and then combines flipped chips together to represent a watermark value. Table 2 shows an example of the subsequence embedding method to flip up to 4 chips in the 11-chip Barker Sequence. This method also can provide security for the watermark information, because the subsequence dividing scheme is a shared secret between the transmitter and the aware receiver. As

Table 2. Subsequence watermark embedding method for 11-chip pseudonoise sequence

Flipped chips	Starting position	Ending position	Embedding capability (bits)	Total embedding capability (bits)
1	0	7	3	3
2	0	3	2	4
	4	7	2	
3	0	1	1	5
	2	5	2	
	6	9	2	
4	0	1	1	5
	2	3	1	
	4	5	1	
	6	9	2	

shown in Table 2, this method provides high embedding capability. However, this method does not provide error-correcting capability for the watermark signal, because the minimum distance is 2 in the sets of modified PN sequences.

D. Performance Evaluation

The performance of a digital communication system is usually evaluated by the BER. The BER of the WDSSS content signal is related to the BER of the underlying DSSS signal. This paper implements the DSSS spreading operation after the differential encoding in the transmitter, and places the DSSS correlation process before the differential decoding in the receiver; therefore, the actual transmitted and received signal is modulated and demodulated with BPSK. In order to be consistent with the measured experimental results, the theoretical BER is converted into packet error rate (PER): $PER = 1 - (1 - BER)^{8s}$, where s is the packet size in bytes, which is set to 1520 in the experiments of this paper. The theoretical PERs of DSSS signal and WDSSS content signal with various chip flipping options are plotted in Fig. 6a. To maintain PER of less than 10% [3], the required SNR increases 1.25 dB for 1-chip flipping, increases another 1.5 dB for 2-chip flipping, increases another 2 dB for 3-chip flipping, and increases another 3.1 dB for 4-chip flipping. On average, the extra SNR required for each additional flipped chip is 1.96 dB.

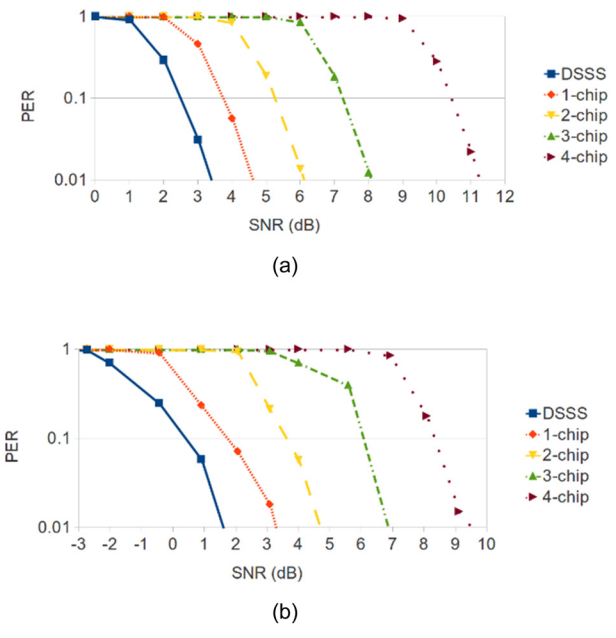

Fig. 6. Packet error rate (PER) of direct sequence spread spectrum (DSSS) signal and watermarked DSSS content signals; a good channel represented by a high signal-to-noise (SNR) allows users to flip more chips in the pseudonoise sequence, embedding more watermark information. (a) Theoretical PER and (b) experimental PER.

The corresponding experimental results are shown in Fig. 6b. Because the estimated SNR values used in the experiments are different from the actual SNR values from the USRP2 platform, there is an approximate 2 dB SNR difference between the theoretical results and the experimental results. Except for this SNR offset, the experimental results show that to maintain the acceptable 10% PER, the required SNR increases 1.45 dB for 1-chip flipping, increases another 1.85 dB for 2-chip flipping, increases another 2.4 dB for 3-chip flipping, and increases another 2.25 dB for 4-chip flipping. On average, the extra SNR required for each additional flipped chip is 1.99 dB, which is similar to the theoretical result. Please refer to [38] for more details.

VII. CONCLUSION AND FUTURE WORK

With the increasing use of wireless communication, it is becoming more important to provide secure and robust communications in the presence of attackers. This paper surveys several physical layer techniques based on DSSS. Since it is still hard to establish a shared spread sequence between the sender and the receiver, Section IV discusses previous work in addressing this issue.

This paper also presents an adaptive scheme for modulation and anti-jamming capability, where the sender and the receiver adaptively change the modulation scheme and spread sequence length with changing channel condition. Since they experience the same channel, this can be used to independently deduce the same spread sequence length, which is an additional hurdle for the jammer, as it experiences a different channel. This is the main theme in Section V. In the future, we will develop a complete adaptation algorithm that makes a prudent tradeoff between communication efficiency and jam resistance.

Another important agenda in this paper is the WDSSS in Section VI. The WDSSS technique flips chips at designated positions in the PN sequence to convey authentication information. Thus, it provides additional physical layer security to the DSSS system without requiring extra bandwidth. A literature survey is followed by theoretical analysis as well as experimental results on the performances of the WDSSS. The impact of flipped chips on the performance of content signal was quantitatively measured, and indicated that, for the 11-chip PN sequence, an approximately 2 dB extra SNR is required for each additional flipped chip.

Considering that the performance of the WDSSS system is closely related to the channel quality, an adaptive chip flipping options scheme can be designed to balance the content signal quality and the watermark signal throughput. With this scheme, the chip flipping option gets increased when the channel quality reaches a set of thresholds, and gets decreased when the channel quality

deteriorates. Note that the watermark signal gives priority to the content signal so that the system performance can be maintained at an acceptable level.

AKNOWLEDGMENTS

This research was supported in part by the Basic Science Research Program (2010-0029034) and World Class University program (R31-10100), both of which are through the National Research Foundation of Korea, funded by the Ministry of Education, Science, and Technology.

REFERENCES

1. J. S. Lee and L. E. Miller, *CDMA Systems Engineering Handbook*, Norwood, MA: Artech House Inc., 1998.
2. M. Simon, J. Omura, R. Scholtz, and B. Levitt, *Spread Spectrum Communications Handbook*, New York, NY: McGraw-Hill, 1994.
3. Institute of Electrical and Electronics Engineers (IEEE), "IEEE Standards for local and metropolitan area networks, part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications," IEEE Standard 802.11-1997, 1997.
4. Institute of Electrical and Electronics Engineers (IEEE), "IEEE Standard for information technology: local and metropolitan area networks, specific requirement, part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (WPANs)," IEEE Standard 802.15.4-2006, 2006.
5. I. J. Cox, M. L. Miller, and A. L. McKellips, "Watermarking as communications with side information," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1127-1141, 1999.
6. R. L. Olesen, P. R. Chitrapu, B. A. Chiang, R. D. Herschaft, J. E. Hoffmann, S. H. Shin, A. Reznik, and J. D. Kaewell, "Watermarks/signatures for wireless communications," US Patent 11 032 780, 2005.
7. W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.
8. W. Stallings, *Wireless Communications and Networks*, Upper Saddle River, NJ: Prentice Hall, 2002.
9. J. G. Proakis, *Digital Communications*, 4th ed., Boston, MA: McGraw-Hill, 2001.
10. E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the performance of IEEE 802.11 under jamming," in *Proceedings of the 27th IEEE Conference on Computer Communications*, Phoenix, AZ, 2008, pp. 1265-1273.
11. W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Urbana-Champaign, IL, 2005, pp. 46-57.
12. M. Strasser, C. Popper, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, CA, 2008, pp. 64-78.
13. C. Popper, M. Strasser, and S. Capkun, "Jamming-resistant broadcast communication without shared keys," in *Proceedings of the 18th Conference on USENIX Security Symposium*, Montreal, Canada, 2009, pp. 231-248.
14. Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: jamming-resistant wireless broadcast communication," in *Proceedings of the 29th IEEE Conference on Computer Communications*, San Diego, CA, 2010.
15. L. C. Baird, W. L. Bahn, M. D. Collins, M. C. Carlisle, and S. C. Butler, "Keyless jam resistance," in *Proceedings of the IEEE SMC Information Assurance and Security Workshop*, West Point, NY, 2007, pp. 143-150.
16. J. Croft, N. Patwari, and S. K. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors," in *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*, Stockholm, Sweden, 2010, pp. 70-81.
17. S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction using wireless signal strength in real environments," in *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*, Beijing, China, 2009, pp. 321-332.
18. S. Mathur, W. Trappe, and N. Mandayam, C. Ye, and A. Reznik, "Secret key extraction from level crossings over unauthenticated wireless channels," in *Securing Wireless Communications at the Physical Layer*, R. Liu and W. Trappe, editors, New York, NY: Springer, 2010, pp. 201-230.
19. H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Communication Letters*, vol. 4, no. 2, pp. 52-55, 2000.
20. S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, San Francisco, CA, 2008, pp. 128-139.
21. F. Hermanns, "Cryptographic CDMA code hopping (CH-CDMA) for signal security and anti-jamming," in *Proceedings of the 6th European Workshop on Mobile/Personal Satcoms*, Noordwijk, Netherlands, 2004.
22. B. Muntwyler, V. Lenders, F. Legendre, and B. Plattner, "Obfuscating IEEE 802.15.4 communication using secret spreading codes," in *Proceedings of the 9th Annual Conference on Wireless On-demand Network Systems and Services*, Courmayeur, Italy, 2012.
23. C. Popper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp. 703-715, 2010.
24. Z. Ji, Y. Yang, J. Zhou, M. Takai, and R. Bagrodia, "Exploiting medium access diversity in rate adaptive wireless LANs," in *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking*, Philadelphia, PA, 2004, pp. 345-359.
25. A. Kamerman and L. Monteban, "WaveLAN-II: a high-performance wireless LAN for the unlicensed band," *Bell Labs*

Technical Journal, vol. 2, no. 3, pp. 118-133, 1997.
26. C. Yu, K. G. Shin, and L. Song, "Maximizing communication concurrency via link-layer packet salvaging in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 4, pp. 449-462, 2007.
27. C. Yu, T. Kang, X. Li, and J. Kim, "Fisheye: modulation and spread code adaptation," Cleveland State University, Cleveland, OH, Technical Report, 2013.
28. Ettus Research, Universal Software Radio Platform (USRP), http://www.ettus.com/.
29. GNU Radio Project, http://gnuradio.org/redmine/projects/gnuradio/wiki.
30. BBN 802.11b Receiver, https://www.cgran.org/wiki/BBN80211.
31. N. Goergen, T. C. Clancy, and T. R. Newman, "Physical layer authentication watermarks through synthetic channel emulation," in *Proceedings of the IEEE Symposium on New Frontiers in Dynamic Spectrum*, Singapore, 2010, pp. 1-7.
32. P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38-51, 2008.
33. J. E. Kleider, S. Gifford, S. Chuprun, and B. Fette, "Radio frequency watermarking for OFDM wireless networks," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, Montreal, Canada, 2004, pp. 1520-6149.
34. B. Lebold, "Physical layer watermarking of binary phase-shift keyed signals using standard GNU radio blocks," master's thesis, Oklahoma State University, Stillwater, OK, 2011.
35. T. Kho, "Steganography in the 802.15.4 physical layer," UC Berkeley, Berkeley, CA, Technical Report, 2007.
36. A. M. Mehta, S. Lanzisera, and K. S. J. Pister, "Steganography in 802.15.4 wireless communication," in *Proceedings of the 2nd International Symposium on Advanced Networks and Telecommunication Systems*, Mumbai, India, 2008, pp. 1-3.
37. E. Zielinska and K. Szczypiorski, "Direct sequence spread spectrum steganographic scheme for IEEE 802.15.4," in *Proceedings of the 3rd International Conference on Multimedia Information Networking and Security*, Shanghai, China, 2011, pp. 586-590.
38. X. Li, "Physical layer watermarking of direct sequence spread spectrum signals," master's thesis, Cleveland State University, Cleveland, OH, 2013.

Taeho Kang

Taeho Kang received his B.S. degree in computer science and engineering from Pohang University of Science and Technology (POSTECH), Korea, in 2009, and is now an M.S.-Ph.D. integrated program student at POSTECH. In 2007, he had an internship program at Lappeenranta University of Technology in Finland. His major areas of interests are mobile systems, wireless communication, data mining and machine learning.

Xiang Li

Xiang Li received her M.S. degree in Electrical Engineering in 2013 at Cleveland State University, Cleveland, OH, USA, and B.E. degree in Computer Science and Technology at Beijing University of Posts and Telecommunications, Beijing, China, in 2001. Her research interests include security over wireless networks, digital signal processing and software defined radio systems.

Chansu Yu

Chansu Yu received his B.S. and M.S. degrees in electrical engineering from Seoul National University, Korea, in 1982 and 1984, respectively, and Ph.D. degree in computer engineering from Pennsylvania State University in 1994. He is currently a professor in the Department of Electrical and Computer Engineering at Cleveland State University (CSU), Cleveland, Ohio. Before joining CSU, he was on the research staff at LG Electronics. He has been on the program committee or organizing committee of many conferences and workshops, including co-chair of the IEEE Percom Workshop on Pervasive Wireless Networking during the last eight years, and co-chair of the 2013 Fourth International Conference on the Network of the Future. He has authored/coauthored more than 110 technical papers and book chapters in the areas of mobile networks, performance evaluation, and parallel and distributed computing, and is a senior member of the IEEE.

Jong Kim

Jong Kim received his B.S. degree in electronic engineering from Hanyang University, Korea, in 1981, M.S. degree in computer science from Korea Advanced Institute of Science and Technology, Korea, in 1983, and Ph.D. degree in computer engineering from Pennsylvania State University in 1991. He is currently a professor in the Division of IT Convergence Engineering, Pohang University of Science and Technology, Korea. From 1991 to 1992, he was a research fellow in the Real-Time Computing Laboratory of the Department of Electrical Engineering and Computer Science, University of Michigan. His major areas of interest are fault-tolerant computing, parallel and distributed computing, and computer security. He is a member of the IEEE.