ACCEPTED FROM OPEN CALL

PHYSICAL LAYER SECURITY IN WIRELESS NETWORKS: A TUTORIAL

YI-SHENG SHIU AND SHIH YU CHANG, NATIONAL TSING HUA UNIVERSITY
HSIAO-CHUN WU, LOUISIANA STATE UNIVERSITY
SCOTT C.-H. HUANG, CITY UNIVERSITY OF HONG KONG
HSIAO-HWA CHEN, NATIONAL CHENG KUNG UNIVERSITY

Active attacks

Denial of service attack

Resource consumption

Masquerade attack

Replay attack

Information disclosure

Massage modification

The authors offer a tutorial on several prevalent methods to enhance security at the physical layer in wireless networks. We will classify these methods based on their characteristic features into five categories.

ABSTRACT

Wireless networking plays an extremely important role in civil and military applications. However, security of information transfer via wireless networks remains a challenging issue. It is critical to ensure that confidential data are accessible only to the intended users rather than intruders. Jamming and eavesdropping are two primary attacks at the physical layer of a wireless network. This article offers a tutorial on several prevalent methods to enhance security at the physical layer in wireless networks. We classify these methods based on their characteristic features into five categories, each of which is discussed in terms of two metrics. First, we compare their secret channel capacities, and then we show their computational complexities in exhaustive key search. Finally, we illustrate their security requirements via some examples with respect to these two metrics.

INTRODUCTION

Wireless networks have become an indispensable part of our daily life, widely used in civilian and military applications. Security is a critical issue in wireless applications when people rely heavily on wireless networks for transmission of important/private information, such as credit card transactions or banking related data communications. Therefore, the ability to share secret information reliably in the presence of adversaries is extremely important. Adversaries may attempt to launch various attacks to gain unauthorized access to and modify the information, or even disrupt the information flows [1].

Most commonly used security methods rely on cryptographic techniques employed at the upper layers of a wireless network. With regard to a symmetric cryptographic technique (as depicted in Fig. 1), such as the Data Encryption Standard (DES), a common private key is normally shared by two users. If these two users do not have this private key, a secure channel is required for the key exchange. Instead of using an additional channel, the physical layer methods can be employed here to distribute secret keys, to supply location privacy and to supplement upper-layer security algorithms. The application of physical layer security schemes makes it more difficult for attackers to decipher transmitted information.

The existing physical layer security techniques can be classified into five major categories: theoretical secure capacity, and the power, code, channel, and signal detection approaches. It was suggested in [2] that perfect secrecy is achievable using physical layer techniques subject to the condition that the channels are unknown to unauthorized users or the channel of the unauthorized users is more noisy than that of the authorized users. While the traditional encryption techniques rely heavily on the upper-layer operations, it is interesting to know whether the physical layer can have some built-in security to assist the upper-layer security designs.

In this article, we give a tutorial on several existing prevalent methods to enhance security at the physical layer in wireless networks. We classify them into five major categories based on their characteristic features. Each of these methods will be evaluated and compared in terms of two performance metrics. First, we discuss their secret channel capacities, and then we investigate their computational complexities involved in exhaustive key search. Finally, we illustrate their security requirements with respect to these metrics using some practical examples.

The rest of this article is outlined as follows. Commonly used security attacks are reviewed and categorized. After we introduce the wireless communication model, we show some existing physical layer security approaches. A comparison of reliability, computational complexity, and secrecy channel capacity is made, followed by our conclusions and future work.

The work presented in this article was supported partly by National Science Council of Taiwan (NSC98-2219-E-006-011).

1536-1284/11/$25.00 © 2011 IEEE

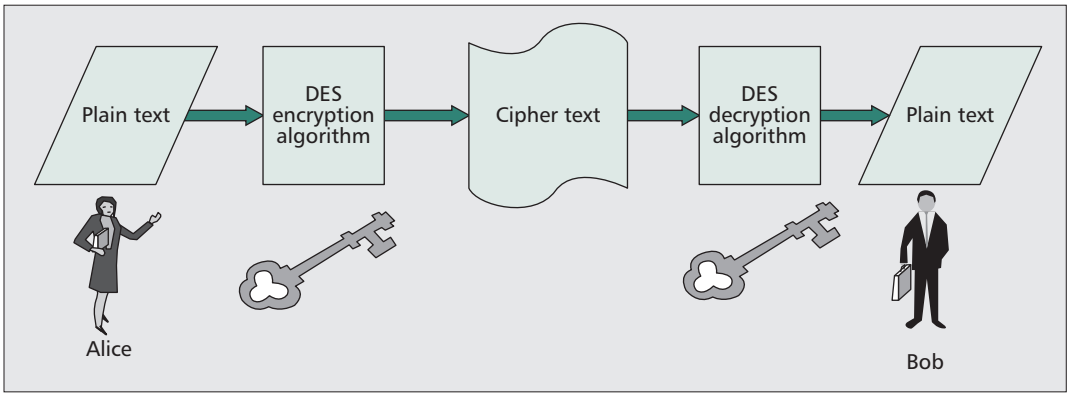

Figure 1. *The symmetric data encryption/decryption algorithm has been widely used in networks. This secret key cryptology operates in both transmission directions. Alice sends an encrypted message to Bob with a secret key. Bob may use the secret key to decipher the message. Because this message has been encrypted, even if the message is intercepted, the eavesdropper between Alice and Bob will not have the secret key to decipher the message.*

Security Attacks in Wireless Networks

In this section we summarize most commonly seen attacks in wireless networks, as listed in Fig. 2. Most attacks can be classified into two categories: passive and active [3]. Passive attacks do not disrupt network operation, and the adversary's objective is to steal transmitted information from wireless channels. Two types of passive attacks are often used, eavesdropping intrusion and traffic analysis.

On the other hand, active attacks can significantly interfere with normal network operations because an adversary often tries to alter the network data. The most common forms of active attacks include denial-of-service (DoS) attacks, masquerade and replay attacks, and information disclosure and message modification attacks.

DoS attacks: A DoS attack is an adversary's attempt to exhaust the resources available to its legitimate users. Jamming is also widely used to launch DoS attacks at the physical layer. Radio frequency jamming can be employed to invade the transmitted signal band. An adversary can utilize jamming signals (thereby disrupting the communications) to make the attacked nodes suffer from DoS in a specific region [1].

Masquerade attacks: In a masquerade attack, an intruder pretends to be a legitimate user and deceives the authentication system so as to usurp the system resource. A masquerade attack usually involves another form of active attack. For example, the authentication sequences can be captured, and therefore an invalid user can obtain privileges to access information illegally.

Information disclosure and message modification: A compromised node can act as an information leaker by deliberate disclosure of confidential information to unauthorized nodes. Information such as the amount and periodicity of the traffic between a selected pair of nodes and the changing traffic patterns can be valuable to the adversaries in many military applications.

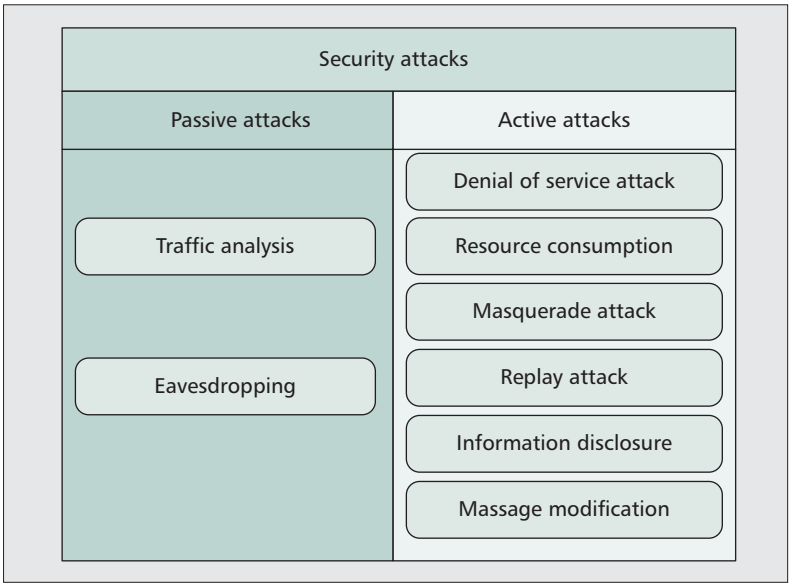

Figure 2. *Classification of the commonly used security attacks in wireless communications.*

Message modification refers to an attack in which an aggressor performs additions or deletions to the network communication content. For example, a message that says "Allow John Smith to read" may be modified as "Allow Fred Brown to read."

Eavesdropping intruders and traffic analysis: Eavesdropping is a way for an unintended receiver to intercept a message called an eavesdropper. A mobile communication session may contain confidential data. Thus, we have to prevent the eavesdroppers from learning the contents. Encryption is the most commonly used technique for masking the important contents. Eve might be able to intercept the transmitted signal but cannot obtain any critical information from it due to the encryption.

On the other hand, traffic analysis can also be used to determine the locations and identities of the communicating parties by intercepting and examining the transmitted messages. The traffic information may be useful for tracking the com-

A simple strategy to disrupt wireless communications is to interfere with communications directly by jamming the communication channel. In fact, intentionally interfering wireless communications is simple.

munication patterns of any two parties. Eavesdropping can be performed even if the messages are encrypted; hence, the malicious users can use the information gleaned from this type of attack for other forms of attack.

Wireless Network Security Requirements

In a wireless network, secured services should satisfy certain requirements discussed below [1]. The wireless communication medium is open to jamming (or interference) and eavesdropping attacks from intruders. For transmission security (TRANSEC) [4], a robustness function is widely used to encrypt data at the transmitter for different communication links, such as satellite links and mobile communication channels. TRANSEC usually provides a relatively weak capability of combating attacks. The robustness functions may also include low probability of intercept (LPI), low probability of detection (LPD), low probability of exploitation (LPE), and anti-jamming protection.

Authentication and Non-Repudiation

Authentication is used to confirm that a communication request comes from a legitimate user. Entity and data origin authentication are two types of authentication. Very often, the entity authentication is used to justify the identities of the parties in the communication sessions. The data-origin authentication focuses on confirming the identity of a data creator.

On the other hand, non-repudiation guarantees that the transmitter of a message cannot deny having sent the message, and the recipient cannot deny having received the message. Digital signatures, which function as unique identifiers for individual users, much like fingerprints, are widely used for non-repudiation purposes.

Confidentiality and Access Control

Confidentiality is the protection of transmitted data from passive attacks to prevent the access by, or disclosure to, unauthorized users. Confidentiality is related closely to data privacy, such as encryption and key management. The data sent by the transmitter must be accessible only to the intended receiver. Data encryption is a popular technique to ensure confidentiality. Even though an intruder might get hold of the data being sent, he/she may not be able to extract any useful information from it. The other aspect of confidentiality is the protection of traffic flows from any attacker's analysis. It requires that an attacker is not able to determine any information about the communication traffic, such as the source/destination location, transmission frequency, session length, or other characteristics of the traffic. As an alternative confidentiality mechanism, access control limits and governs the devices that have access to the communication links. Thus, each entity must be authenticated or identified beforehand to gain access to the communication links. However, because of the broadcast nature of the wireless communication medium, it is difficult to control access, and hence it is vulnerable to the eavesdropping.

Integrity and Availability

In brief, integrity and availability are the trustworthiness and reliability of information. Integrity means the data that was sent by the source node should reach the destination node without being altered. It can be possible for a malicious node to alter the message during transmission. Integrity can even involve whether a person or an entity entered the right information, if the information reflects the actual circumstances, and whether, under the same circumstances, identical data would have been generated.

The availability can be defined as follows. Communication should remain fully operational when a legitimate user is communicating. It must be robust enough to tolerate various attacks during any authorized transmission, and should be able to provide guaranteed transmissions whenever authorized users require them.

Resistance to Jamming

A simple strategy to disrupt wireless communications is to interfere with communications directly by jamming the communication channel. In fact, intentionally interfering with wireless communications is simple. A jammer may broadcast an interference signal on a broad spectral band to disrupt legitimate signal reception. According to the reaction of jammers, jamming interference can be classified into two types: active (constant) jammers and reactive jammers.

Active (constant) jammers send out random bits or a radio signal continuously into the channel and therefore block the communications of users, making the prevention of such interference a big challenge. A reactive jammer is idle until it senses transmission activities occurring in the channel; then it transmits jamming signals to interrupt the ongoing transmission. Since the jammer must detect transmission activities before issuing its jamming signal, the transceiver may improve its own low probability of detection (LPD) to avoid jamming attacks.

A persistent and powerful adversary can always jam all data transmissions by transmitting high-power white noise over the entire frequency spectrum. Although such availability threats are powerful, they can be addressed through many physical layer security schemes.

Resistance to Eavesdropping

The broadcast nature of the wireless medium makes it hard to eliminate unauthorized access to wireless networks. Hence, it is very easy to eavesdrop on it in general. A typical secrecy problem in a wireless communication system involves three nodes: the transmitter, the receiver, and the eavesdropper. The transmitter wants to communicate with the intended receiver but does not want to let the eavesdropper learn its secret message. The eavesdropper is assumed to be passive; hence, its location is unknown to the transmitter and receiver. Perfect secrecy, as defined by Shannon in [5], is achieved when the transmitter delivers a positive information rate to the legitimate receiver and ensures that the eavesdropper cannot obtain any information.

The most common way to maintain confidentiality is to use a cipher to encrypt each transmit-

ted data stream, which can only be decrypted at the intended receiver using a private shared key. Another widely used approach to maintain confidentiality is to force the transmitter and receiver to adopt some information hiding measures to prevent unauthorized detection of any transmission activities, which could be used, for example, to determine the geographical location of the transmitter. Information hiding is a method to embed private messages into a background signal or noise process.

Physical-Layer Security Approaches

In this section, we introduce schemes that could be used to achieve physical layer security against different attacks. We can classify the existing physical layer security methods into five major categories: theoretical secure capacity, channel, coding, power, and signal detection approaches.

Theoretical Secure Capacity

In recent years, the fundamental issues of secure channel capacity have drawn much attention in the information theory community [6–8]. Most of these works focused on the study of so-called secrecy capacity, that is, the maximum rate achievable between the legitimate transmitter-receiver pair subject to the constraints on information attainable by the unauthorized receiver. In Wyner's original work [6], he showed for that discrete memoryless channels the perfect secrecy capacity is actually the difference of the capacities for the two users. A similar result has been generalized to Gaussian channels by Leung *et al.* [9].

The authors in [10] considered a full channel state information (CSI) case, where the transmitter has access to the channel gains of the legitimate receiver and the eavesdropper. The secrecy capacity under this full CSI assumption is adopted as an upper bound for the secrecy capacity when only the CSI of the legitimate receiver is known at the transmitter. The authors in [10] also proposed a low-complexity on/off power allocation strategy that achieves near optimal performance with only the main channel CSI. More specifically, this scheme was shown to be asymptotically optimal as the average signal-to-noise ratio (SNR) goes to infinity. The proposed scheme was shown to attain the secrecy capacity of the full CSI assumption. All of the aforementioned studies have shown that channel fading has a positive impact on secrecy capacity and rate adaptation based on the channel CSI.

The authors in [11] extended their previous work [12] by considering the presence of imperfect CSI. Based on an information-theoretic formulation of the problem, in which two legitimate partners communicate over a quasi-static fading channel and an eavesdropper observes their transmissions through a second independent quasi-static fading channel, the important role of fading was characterized in terms of the average secure communication rates and outage probability. The authors in [11] developed a secure communication protocol that adopts the following four-step procedure to ensure wireless information-theoretic security:

- Common randomness via opportunistic transmission
- Message reconciliation
- Common key generation via privacy amplification
- Message protection with a secret key

Finally, a set of security measures for assessing average secure key generation rates was established, and it was shown that the protocol is effective in secure key renewal even in the presence of imperfect CSI.

The use of multiple antennas has drawn a lot of attention in wireless communication research. The first study of the problem was presented by Hero [13]. The main contribution of this article is that a proper exploitation of space-time diversity at the transmitter can also enhance information security and information-hiding capabilities. Different from the approach adopted in the wire-tap channels, the authors in [13] introduced the constraints of LPD, and low probability of intercept (LPI), considering a scenario where the transmitter and receiver are both informed of their CSI while the eavesdropper has no knowledge of its own. More generally, this work also compared the capacity limits for both informed/uninformed transmitter and informed receiver scenarios subject to LPI and LPD constraints. In [14], a single-input multiple-output (SIMO) wiretap channel was considered. The authors in [14] presented a single letter characterization of the secrecy capacity of a SIMO channel with colored Gaussian noise by transforming the channel into a scalar Gaussian wiretap channel using the standard techniques of communications theory. The derived result is proper to study the impact of slow fading on the secrecy capacity of the channel, and to know how the use of multiple receive antennas could improve the performance of the communication system. For more results on the secrecy in multi-input multi-output (MIMO) communication, please refer to [15, 16].

In summary, information-theoretic security is an average-information measure. The system can be designed and tuned for a specific level of security, but it may not be able to guarantee security with probability one. Furthermore, it requires knowledge about the communication channel that may not be accurate in practice. A few systems (e.g., quantum key distribution) have been deployed, but the technology is not available widely due to its implementation cost.

Channel Approaches

The following three methods have been proposed to increase security based on exploitation of the channel characteristics: radio frequency (RF) fingerprinting, algebraic channel decomposition multiplexing (ACDM) precoding, and randomization of MIMO transmission coefficients.

RF Fingerprinting — The RF fingerprinting system proposed by [17] consists of multiple sensor systems that capture and extract RF features from each received signal; an intrusion detector processes the feature sets and generates a dynamic fingerprint for each internal source identifier derived from a few packets. This RF fingerprinting system monitors the temporal evolution of

Information-theoretic security is an average-information measure. The system can be designed and tuned for a specific level of security, but it may not be able to guarantee security with probability one. Furthermore, it requires knowledge about the communication channel that may not be accurate in practice.

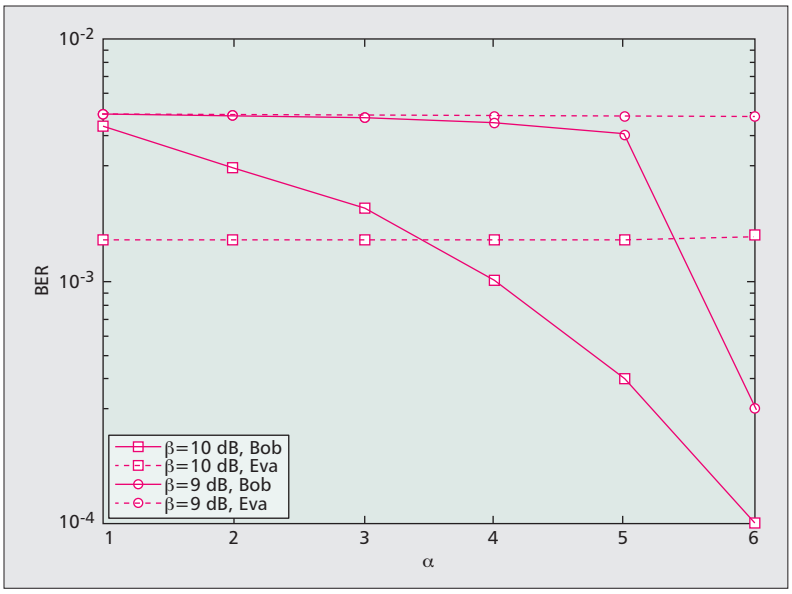

Figure 3. *Bit error rate performance of a legitimate receiver (Bob) and an eavesdropper (Eva) when artificial noise is added at the transmitter. The horizontal axis α gives the ratio of the variance of the artificial noise to that of the legitimate receiver's channel noise. The curves were generated for different values of β, which is the ratio of the energy per bit to artificial noise.*

each fingerprint and issues an intrusion alert when a strange fingerprint is detected, thus helping distinguish an intruder from a legitimate user.

ACDM Precoding — The authors of [18] introduced the ACDM precoding scheme, in which the transmitted code vectors are generated by singular value decomposition (SVD) of the correlation matrix, which describes the channel characteristic features between the transmitter and the intended receiver.

The transmitted message is sent in terms of symbol blocks and then modulated by a unit-energy complex code vector in order to provide high-data-rate communication over dispersive multipath channels. Owing to the difference in the multipath structure of the transmitter-receiver channels, even intruders, which have a perfect knowledge of the transmission code vectors and their own channel responses, cannot achieve their objectives to acquire the true messages due to the difference in the locations of the intruders and the legitimate user.

Randomization of MIMO Transmission Coefficients — In [19], a method was proposed to achieve perfect secrecy by randomizing the MIMO transmission coefficients. The transmitter generates a diagonal matrix dependent on the impulse response matrix of the transmitter-receiver channel. This diagonal matrix has the unique properties that make the matrix undetectable to the intruders but easily detectable to the intended receiver. This method reduces the signal interception capability of the intruder and leads to a blind deconvolution problem due to the redundancy of MIMO transmissions.

Figure 3 shows the bit error rate (BER) performance of Bob (a legitimate receiver) and the eavesdropper with respect to α, the ratio of the variance of the artificial noise to that of the legitimate receiver's channel noise for different β, where β is the ratio of the energy per bit to the artificial noise. A 4 × 4 random MIMO system with binary phase shift keying (BPSK) modulation is adopted. The BER performance of both receivers improves as α increases, but the eavesdropper's performance is kept almost constant with respect to ratio β, while the BER for Bob improves as α increases. If the legitimate receiver's channel noise is given, the ratio a can be increased by increasing the variance of the artificial noise, while simultaneously increasing bit energy such that their ratio, β, stays unchanged. The artificial noise can thus be adjusted with the aid of experimental data, such as those shown in Fig. 3, to choose an operating point that maximizes the performance gain between the legitimate and eavesdropper receivers.

Code Approaches

The main objective of code approaches is to improve resilience against jamming and eavesdropping. The code approaches include the use of error correction coding and spread spectrum coding.

Error Correction Coding — In a conventional cryptographic method, a single error in the received ciphertext will cause a large number of errors in the decrypted plaintext after channel decoding. In order to address this problem, a combination turbo coding and advanced encryption standard (AES) cryptosystem was proposed in [20]. This scheme uses the encrypted turbo codes to set up a secure communication session based on the pseudo-random number generation algorithms for selecting N bits from M turbo encoded bits. Depending on the channel condition, this method can be adopted to choose the number of redundant bits required to protect the information in order to achieve high efficiency. The main advantages of secure turbo code include higher-speed encryption and decryption with higher security, smaller encoder/decoder size, and greater efficiency.

Spread Spectrum Coding — Spread spectrum is a signaling technique in which a signal is spread by a pseudo-noise (PN) sequence over a wide frequency band with frequency bandwidth much wider than that contained in the frequency ambit of the original information. Spread spectrum is an effective solution to achieve physical layer security. Techniques like this have been most widely used for attaining LPI and LPD. Direct-sequence spread-spectrum (DSSS) has been widely used to spread the transmitted data over multiple frequencies [21]. Frequency-hopping spread-spectrum (FHSS) continuously changes the central frequency of a conventional carrier several times per bit duration (i.e., in a fast hopping system) in accordance with a randomly selected channel so that it is extremely difficult to illegally monitor the spread spectrum signals.

The main difference between conventional cryptographic systems and spread-spectrum systems lies in their key sizes. Traditional crypto-

graphic systems can have a very large key space. However, in a spread-spectrum system, the key space is limited by the range of carrier frequencies and number of different sequences.

Code-division multiple access (CDMA) has been developed for secure communications. In direct-sequence CDMA (DS-CDMA) systems, all users share the same channel by using different spreading codes to distinguish their signals. First, the signal from the transmitter is spread using a code sequence. Then the spread signal is scrambled using a PN sequence so as to be hidden in noise to prevent the communications being detected by an intruder.

Therefore, the use of relatively long PN scrambling sequences is pivotal to the physical layer security of CDMA systems if the channelization codes chosen for this purpose happen to be Walsh codes as they are easy to generate. In [22], a method was proposed to enhance the physical layer security of CDMA systems by using AES operation to generate the scrambling sequences. The AES specifies three key sizes (128, 192, and 256) so that the AES-CDMA method can raise the security level to guard against the exhaustive-key-search attacks.

In this subsection an interesting topic, designing some special spreading sequences that are particularly suited to implementing a secure CDMA system, is discussed. Research on this topic is still widely open as it involves extensive knowledge of both information/security theory and physical layer architecture expertise.

Power Approaches

Data protection can also be facilitated using power approaches. The usual schemes in these approaches involve the employment of directional antennas and the injection of artificial noise, as explained below.

Directional Antennas — As beam width is inversely proportional to peak gain in a directional antenna, directional transmission can improve spatial reuse and enlarge geographical coverage. In [23], networking conditions using directional antennae and omnidirectional antennae were compared under various jamming conditions. If an omnidirectional antenna is used, a node in the coverage range of a jammer would not be able to receive data successfully. However, if a directional antenna is used, the node would still be able to receive data from the directions not covered by the jamming signals. Therefore, the employment of directional antennas can improve wireless network capacity, avoid physical jamming attempts, and enhance data availability.

Artificial Noise Scheme —In [24], a method was suggested to ensure perfectly secure communications. This method showed that perfect secrecy can be achieved when the intruder's channel is noisier than the receiver's channel. In this method, artificial noise is generated using multiple antennas or the coordination of helping nodes, and is injected into the null-subspace of the intended receiver's channel (i.e., MIMO channel). Artificial noise is utilized to impair the intruder's channel, but it does not affect the intended receiver's channel since the noise is generated in the null-subspace of the legitimate receiver's channel, as shown in [24]. It was also shown that relying on artificial noise, secret communications can be achieved even if the intruder enjoys a much better channel condition than the intended receiver.

In this subsection, we have briefly introduced data protection facilitation using power approaches. First, if a directional antenna is used, the node would still be able to receive data from the directions not covered by the jamming signal. Second, if artificial noise is used, secret communication can be achieved. However, the shortcoming of using directional antennae is their bulky size, which increases with the increase in angular resolution of the antenna array. This is an open problem needing to be solved.

Signal Design Approaches

Inspired by the work done in [25], a method was proposed in which discriminatory channel estimation is performed by injecting artificial noise (AN) to the left null space of the legitimate receiver's channel to degrade the estimation performance of the eavesdropper. By exploiting the channel feedback information from the legitimate receiver at the beginning of each communication stage, a multistage training-based channel estimation scheme was proposed in [26] to minimize the normalized mean squared error of channel estimation at the legitimate receiver subject to a constraint on the estimation performance attainable by the non-legitimate receiver. For example, we may consider a network that consists of a multiple-antenna transmitter and several single-antenna receivers (i.e., for the legitimate receiver and the eavesdropper). The approach to discriminate in channel estimation to achieve secure communication requires the transmitter's knowledge of the channel to the legitimate receiver from feedback. The quality of the channel estimation obtained by the eavesdropper is constrained due to the use of AN, while the channel estimation at the legitimate receiver can be refined after each stage. Therefore, quality of service (QoS) discretion can be attained by using high-order modulations or high-rate error correction codes for information data broadcasting.

Comparison of Physical Layer Security Schemes

In the previous section, several approaches to increase security on the physical layer have been discussed for wireless communications. Table 1 provides a brief summary for most popular physical layer security schemes in terms of their resistance against attacks and their security requirements. Of those schemes, some make use of the inherent characteristics of the channels, and they work depending on a variety of assumptions to ensure security. The assumptions include that an unauthorized user has a much worse channel than that of an intended user, or has no idea about the spreading codes or channel characteristics. Secrecy can be achieved while these assumptions are valid; otherwise, secrecy may not be obtained. In order to address these prob-

As beam width is inversely proportional to peak gain in a directional antenna, directional transmission can improve spatial reuse and enlarge geographical coverage.

In encrypted transmissions, normally an intruder is unable to obtain correct information without the secret key. In this case, the number of possible keys is related closely to the security level; the larger the number, the higher the security level will be.

Security scheme	Resisted attacks	Achieved security requirement
RF fingerprint [17]	Eavesdropping, resource consumption, masquerade	Authentication confidentiality
Rand MIMO [19]	Eavesdropping	Confidentiality
AES CDMA [22]	Eavesdropping	Confidentiality
ACDM [18]	Eavesdropping	Confidentiality
FHSS	Jamming, eavesdropping, traffic analysis	Availability confidentiality
Pseudo-chaotic DS/SS [21]	Eavesdropping, traffic analysis	Confidentiality
Artificial noise [26]	Eavesdropping	Confidentiality

Table 1. *Comparison of different attack methods and their security schemes.*

Approach	Method	Number of secret keys	Time required at 10^6 decryptions/ms
RF fingerprint	24-bit DES	1.7×10^8 keys	8.4 milliseconds
IS-95 CDMA	42-bit LFSR	4.4 × 1012 keys	2.2 seconds
AES CDMA	128-bit AES	3.4×10^{38} keys	5.4×10^{18} years
Rand-MIMO	Random matrix	3.4×10^{38} 4 × 4 matrix	5.4×10^{18} years

Table 2. *Required decryption time comparison.*

lems, we introduce two metrics to compare these physical layer security approaches: secret channel capacity and computational complexity.

Secret Channel Capacity

In this subsection we evaluate the secret channel capacity [19] of each method. The LPI is an important factor in physical layer security, as it guarantees confidentiality in wireless transmissions without relying on extra upper-layer data encryption.

One of the fundamental issues for physical layer security is the secret channel capacity. This secrecy is defined as information-theoretic secrecy; that is, an intruder will acquire no more information than a random guess from the communications during a transmission to an intended receiver at some given positive information rate. Information-theoretic secrecy is in fact equivalent to perfect secrecy according to information theory.

A comparison of the secret channel capacity (or normalized throughput) of the different methods is made in Fig. 4. Thus, the secret channel capacity can be used to measure the confidentiality and availability of transmitted data.

Computational Complexity

In encrypted transmissions, normally an intruder is unable to obtain correct information without the secret key. In this case, the number of possible keys is closely related to the security level; the larger the number, the higher the security level. In other words, the existence of many keys makes it difficult for an intruder to decrypt secure data by an exhaustive key search. Table 2 makes a comparison among different approaches with respect to the computational complexity of resisting brute force attacks (decryption using the exhaustive key search). A larger key size makes it more difficult for an eavesdropper to decrypt the message, but the computational complexity will become a serious challenge to receivers since they have to decrypt all messages (even if those incoming messages have been changed by jamming or tampered with by illegitimate users). Therefore, we recommend using data authentication to distinguish signals received from intended and unintended users. Alternately, anti-jamming and error correction codes can be employed to preserve data integrity.

In Fig. 4, we compare the normalized throughput for physical layer security systems implemented by FHSS and DSSS. Both systems use BPSK for their modulations. Interference in one channel has no effect as long as it is kept below a given interference-to-signal ratio (ISR) limit of the demodulator: –5 dB when $N = 50$ and $J = 2$ (the curve marked by circles), and 0 dB in case of $N = 50$ and $J = 10$ (the curve marked by crosses), where J is the number of jammed channels out of the N channels available. Beyond this limit, the interference controls the demodulator on that channel, and the desired communication interference is not present on the remaining channels (thus, normal communication proceeds), and the throughput

falls to $(N - J)/N$. For DSSS scheme. Two configurations are used for the performance evaluation. The first is a DSSS system (the curve marked by diamonds), which uses a 15-chips/data bit spreading code. The other is a DSSS system, which uses 127 chips/bit (the curve marked by squares). It is observed that the FHSS scheme can provide higher normalized throughput when the ISR is higher than that of the DSSS scheme. However, the DSSS scheme is preferred at a relatively low ISR region as the normalized throughput of DSSS is higher than FHSS at low ISR. The reason for the much larger degradation of normalized throughput for DSSS compared to FHSS is the soft-bounded nature of DS spreading in contrast to the hard-bounded nature of FH spreading.

Conclusions and Future Work

In this article, issues in physical layer security for wireless networks have been discussed in a tutorial manner. Numerous existing physical layer security approaches have been introduced and compared in terms of their abilities to improve security in wireless transmissions. We have also shown the effectiveness of some physical layer security schemes via illustrations. Two important metrics, secret channel capacity and computational complexity, have been used to compare the performance of different approaches. It should also be noted that due to hardware complexity, the low-cost implementation of most physical layer security schemes is still beyond the capability of current microelectronics technologies.

Indeed, the work presented in this article could be extended in many interesting directions, as summarized below.

Multi-user information-theoretic security: Most of the current work on information-theoretically secure communications is related to the wiretap channel model, and little attention has been devoted to information-theoretic security of wireless networks where multi-user security is important. To generalize the results obtained from secure point-to-point communications to secure network communications is a challenging topic for further investigation. The notions of feedback, cooperation, and trust are of paramount importance in multi-user scenarios and are not yet well understood.

Cross-layer protocols for physical layer security: The implementation of physical layer security in a real system will be part of a layered approach, and the design of protocols that combine traditional cryptographic techniques with physical layer techniques is an interesting research direction. A key portion of this research is the definition of relevant metrics that would make it possible to assess the performance of these hybrid schemes.

Experimental validation: A more extensive study of the hardware requirements for physical layer security is required to evaluate the weakness of realistic systems. In cryptographical systems, hardware devices inevitably present security vulnerabilities that have not been taken into account by the theoretical models used in most security research work.

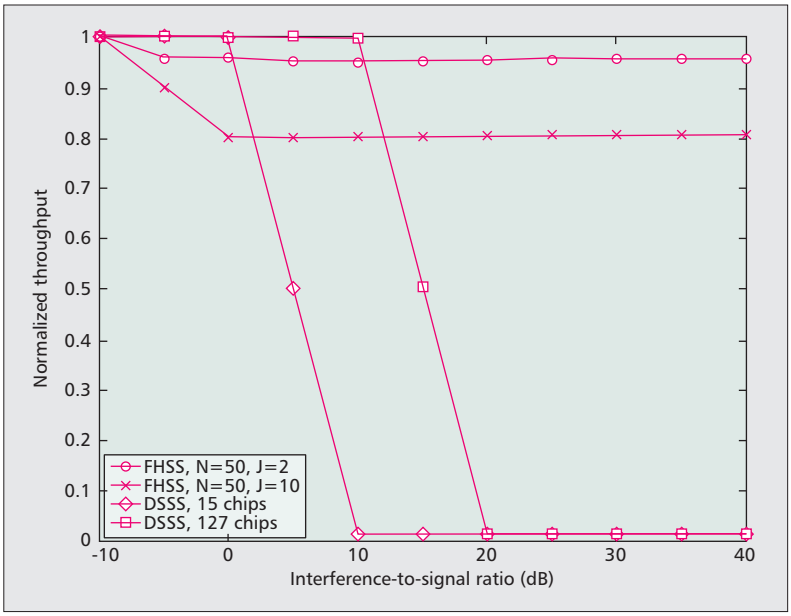

Figure 4. *Normalized throughput comparison for FHSS and DSSS techniques.*

Acknowledgments

The authors would like to thank the editors and anonymous reviewers for their invaluable comments on the article. Their comments have been very constructive, helping us to improve the quality of the article.

References

[1] C. S. R. Murthy and B. S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*, Prentice Hall PTR, 2004.

[2] A. D. Wyner, "The Wiretap Channel," *Bell System Tech. J.*, vol. 54, 1975, pp. 1355–87.

[3] W. Stallings, *Cryptography and Network Security Principles and Practices*, Prentice Hall PTR, 2006.

[4] B. E. White, "Layered Communications Architecture for the Global Grid," *IEEE MILCOM 2001,* 2001, pp. 506–11.

[5] Op cit, Wyner.

[6] A. Khisti and G. W. Wornell, "Secure Transmission with Multiple Antennas: The MIMOME Wiretap Channel," 2008, submitted to *IEEE Trans. Info. Theory*.

[7] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," *IEEE Int'l. Symp. Info. Theory*, 2008, pp. 524–28.

[8] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian Wire-Tap Channel," *IEEE Trans. Info Theory*, 1978, pp. 451–56.

[9] P. K. Gopala, L. Lai, and H. E. Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Trans. Info. Theory*, 2008, pp. 4687–98.

[10] M. Bloch *et al.*, "Wireless Information-Theoretic Security," *IEEE Trans. Info. Theory*, 2008, pp. 2515–34.

[11] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels," *IEEE Int'l. Symp. Info. Theory*, 2006, pp. 356–60.

[12] A. O. Hero, "Secure Space-Time Communication," *IEEE Trans. Info. Theory*, 2003, pp. 3235–49.

[13] P. Parada and R. Blahut, "Secrecy Capacity of SIMO and Slow Fading Channels," *IEEE Int'l. Symp. Info. Theory*, 2005, pp. 2152–55.

[14] Z. Li, W. Trappe, and R. Yates, "Secret Communication via Multi-Antenna Transmission," *Conf. Info. Sci.and Sys.*, 2007, pp. 905–10.

[15] A. Khisti *et al.*, "On the Gaussian MIMO Wiretap Channel," *IEEE Int'l. Symp. Info. Theory*, 2007, pp. 2471–75.

[16] A. A. Tomko, C. J. Rieser, and L. H. Buell;, "Physical-Layer Intrusion Detection in Wireless Networks," *IEEE MILCOM 2006*, pp. 1–7.

[17] C. Sperandio and P. Flikkema, "Wireless Physical-Layer Security via Transmit Precoding Over Dispersive Channels: Optimum Linear Eavesdropping," *Proc. MILCOM 2002*, 2002, pp. 1113–17.

[18] X. Li and E. Ratazzi, "Mimo Transmissions with Information-Theoretic Secrecy for Secret-Key Agreement in Wireless Networks," *IEEE MILCOM 2005*, 2005, pp. 1353–59.
[19] D. Abbasi-Moghadam, V. T. Vakili, and A. Falahati, "Combination of Turbo Coding and Cryptography in Non-Geo Satellite Communication Systems," *Int'l. Symp. Telecommun.*, 2008, pp. 27–28.
[20] Y. Hwang and H. Papadopoulos, "Physical-Layer Secrecy in AWGN via a Class of Chaotic DS/SS Systems: Analysis and Design," *IEEE Trans. Sig. Proc.*, 2004, pp. 2637–49.
[21] T. Li *et al.*, "Physical Layer Built-In Security Analysis and Enhancement of CDMA Systems," *IEEE Military Commun. Conf.*, 2005, *MILCOM 2005*, pp. 956–62.
[22] G. Noubir, "On Connectivity in Ad Hoc Network Under Jamming Using Directional Antennas and Mobility," *2nd Int'l. Conf. Wired and Wireless Internet Commun.*, 2004, pp. 54–62.
[23] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Trans. Wireless Commun.*, 2008, pp. 2180–89.
[24] S. Goel and R. Negi, "Secret Communication in Presence of Colluding Eavesdroppers," *IEEE MILCOM 2005*, 2005, pp. 1501–06.
[25] T. H. Chang, Y. W. P. Hong, and C. Y. Chi, "Training Signal Design for Discriminatory Channel Estimation, *IEEE GLOBECOM*, 2009.
[26] Csiszar and J. Korner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Info. Theory*, 1978, pp. 339–48

Biographies

YI-SHENG SHIU (g9564551@oz.nthu.edu.tw) received his M.S. degree in communication engineering from National Tsing Hua University, Hsinchu, Taiwan, R.O.C., in 2009. His research is focused on wireless communication systems.

SHIH YU CHANG [M'06] (shihyuch@cs.nthu.edu.tw) received his B.S.E.E. degree from National Taiwan University, Taipei, in 1998 and his Ph.D. degree in electrical and computer engineering from the University of Michigan at Ann Arbor in 2006. Since August 2006 he has been a faculty member of the Department of Computer Science, National Tsing Hua University, Taiwan. His research interests include wireless communications and wireless networks. He is very active in IEEE ComSoc. He has been on the technical program committees for ICC 2008, GLOBECOM 2008-2009, IWCMC 2008. He also constantly participates in technical paper reviews for numerous IEEE journals in communications, computer science, networking, and so on.

HSIAO-CHUN WU [M'00, SM'05] (wu@ece.lsu.edu) received a B.S.E.E. degree from National Cheng Kung University, Taiwan, in 1990, and M.S. and Ph.D. degrees in electrical and computer engineering from the University of Florida, Gainesville, in 1993 and 1999, respectively. From March 1999 to January 2001 he worked for Motorola Personal Communications Sector Research Laboratories as a senior electrical engineer. In January 2001 he joined the faculty in the Department of Electrical and Computer Engineering, Louisiana State University, Baton Rouge, Louisiana. From July to August 2007 he was a visiting assistant professor at Television and Networks Transmission Group, Communications Research Centre, Ottawa, Canada. From August to December 2008 he was a visiting associate professor at the Department of Electrical Engineering, Stanford University, California. He has published more than 130 peer-refereed technical journal and conference articles in electrical and computer engineering. His research interests include the areas of wireless communications and signal processing. He is an IEEE Distinguished Lecturer. He currently serves as an Associate Editor for *IEEE Transactions on Broadcasting*, *IEEE Signal Processing Letters*, *IEEE Communications Magazine*, *International Journal of Computers and Electrical Engineering*, *Journal of Information Processing Systems*, *Physical Communication*, and *Journal of the Franklin Institute*. He used to serve as an Associate Editor for *IEEE Transactions on Vehicular Technology*. He has also served for numerous textbooks, IEEE/ACM conferences, and journals as a technical committee member, symposium chair, track chair, or reviewer in signal processing, communications, circuits, and computers.

SCOTT CHIH-HAO HUANG [M'09] (shuang@cs.cityu.edu.hk) received his B.S. degree in mathematics from National Taiwan University, and his Ph.D. degree in computer science from the University of Minnesota, Twin Cities. He used to be with the Computer Science Department, City University of Hong Kong. In August 2010 he joined the faculty of the Electrical Engineering Department, National Tsing Hua University. His research interests include wireless ad hoc/sensor network, security, communication theory, algorithms, and combinatorial optimization.

HSIAO-HWA CHEN [S'89, M'91, SM'00, F'10] (hshwchen@ieee.org) is currently a Distinguished Professor in the Department of Engineering Science, National Cheng Kung University, Taiwan. He obtained his B.Sc. and M.Sc. degrees from Zhejiang University, China, and a Ph.D. degree from the University of Oulu, Finland, in 1982, 1985, and 1991, respectively. He has authored or co-authored over 400 technical papers in major international journals and conferences, six books, and more than 10 book chapters in the areas of communications. He has served as general chair, TPC chair, and symposium chair for many international conferences. He has served or serves as an Editor or/and Guest Editor for numerous technical journals. He is the founding Editor-in-Chief of Wiley's *Security and Communication Networks Journal* (www.interscience.wiley.com/journal/security). He was the recipient of the best paper award at IEEE WCNC 2008 and a recipient of the IEEE Radio Communications Committee Outstanding Service Award in 2008. He is a Fellow of IET and BCS.