Design of an OFDM Physical Layer Encryption Scheme

Junqing Zhang, Alan Marshall, *Senior Member, IEEE,* Roger Woods, *Senior Member, IEEE,* and Trung Q. Duong, *Senior Member, IEEE*

***Abstract*—This paper presents a new encryption scheme implemented at the physical layer of wireless networks employing orthogonal frequency-division multiplexing (OFDM). The new scheme obfuscates the subcarriers by randomly reserving several subcarriers for dummy data and resequences the training symbol by a new secure sequence. Subcarrier obfuscation renders the OFDM transmission more secure and random, while training symbol resequencing protects the entire physical layer packet, but does not affect the normal functions of synchronization and channel estimation of legitimate users while preventing eavesdroppers from performing these functions. The security analysis shows the system is robust to various attacks by analyzing the search space using an exhaustive key search. Our scheme is shown to have a better performance in terms of search space, key rate and complexity in comparison with other OFDM physical layer encryption schemes. The scheme offers options for users to customize the security level and key rate according to the hardware resource. Its low complexity nature also makes the scheme suitable for resource limited devices. Details of practical design considerations are highlighted by applying the approach to an IEEE 802.11 OFDM system case study.**

***Index Terms*—Communication system security, wireless networks, OFDM, physical layer, cryptography**

I. Introduction

The broadcast nature of wireless communications means that anyone within the physical communication range of a transmitter can receive the signal and potentially decode the transmissions. Therefore, wireless network security has been an important research area. Under the open systems interconnection (OSI) model, communication systems are partitioned into different protocol layers, such as physical layer, data link layer, etc. Communication security is conventionally handled by applying cryptographic schemes in upper layers (data link layer and above) [1], [2]. For example, Wi-Fi protected access (WPA) [3], [4] is designed to protect the media access control (MAC) layer, a sublayer of data link layer; transport layer security (TLS) protocol [5] is used to secure transport layer.

Although upper layer cryptography greatly improves the network security, wireless transmission still suffers from eavesdropping because these security mechanisms are implemented as independent functions in the communications protocol layers operating above the physical transmission [6]. This results in several vulnerabilities. For example, the underlying structures of user's data packet, such as the MAC address, are not encrypted and research has shown that it is possible to discover users' identities and the destinations/sources of their message [7]. This permits passive and active attacks, e.g., the attacker can analyze the network traffic by interpreting the MAC address and launch denial of service (DoS) attacks by flooding the legitimate receiver [8]. In addition, the physical layer header is transmitted in plaintext, which allows the eavesdropper to synchronize the wireless transmission, thus permitting the transmitted frames to be easily recovered (sniffed) and decrypted off-line.

In order to combat passive eavesdropping, a growing interest in moving the encryption to the physical layer has emerged to enhance the security of the wireless transmission [8]–[14], which is termed *physical layer encryption* (PLE) in this paper. It is implementable and can be offered as a complement to upper layer cryptographic schemes to enhance security of wireless communication.

PLE differs from physical layer security (PLS) schemes, which aim to achieve information-theoretic security by exploiting channel characteristics but not by encryption (see [15], [16] and references therein). For example, PLS can be achieved by introducing artificial noise [17], beamforming [18], and cooperative relay [19], etc. However, when it comes to the practical realization, there are many challenges such as complex implementation and unavailable eavesdroppers' channel state information [20], which prevent PLS schemes from protecting the commercial wireless systems.

Unlike upper layer encryption schemes, PLE schemes are closely related to the wireless communications medium through using different schemes to vary the ways of modulating the data. Orthogonal frequency-division multiplexing (OFDM) is one of the most popular wireless techniques due to its high spectral efficiency, robustness against inter-symbol interference (ISI) and fading, and efficient implementation. For many of these reasons, it has been adopted in wireless standards such as IEEE 802.11 a/g/n, IEEE 802.16 WiMAX, LTE, etc. Research has sought to improve the OFDM security level by employing PLE, such as constellation scrambling in

This work was supported by the Queen's University Belfast University Studentship, Newton Institutional Links Grant 172719890, Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22, and US-Ireland R&D Partnership USI033 'WiPhyLoc8' grant involving Rice University (USA), University College Dublin (Ireland) and Queen's University Belfast (Northern Ireland).

J. Zhang, R. Woods and T. Q. Duong are with the Institute of Electronics, Communications and Information Technology (ECIT), Queen's University Belfast, Belfast, BT3 9DT, UK. (email: {jzhang20, r.woods, trung.q.duong}@qub.ac.uk)

A. Marshall is with Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, UK. (email: Alan.Marshall@liverpool.ac.uk)

the frequency domain [8]–[10], data scrambling in the time domain [11], modulation symbols rotation [12], and noise enhanced constellation rotation [13], [14]. Whilst these schemes all make an OFDM system more secure, they have high key-to-data ratios which increase the computational complexity of the hardware design. Moreover in almost all of these schemes, the training symbol is sent in plaintext which permits eavesdroppers to easily recover the transmitted frames for subsequent decryption.

In this paper, a much more robust OFDM PLE scheme is proposed whereby the transmitted packets are completely unobservable to eavesdroppers. Our scheme involves subcarrier obfuscation and training symbol resequencing (SOTSR), which is a totally different approach from other methods. Obfuscation is achieved by reserving several OFDM subcarriers to transmit dummy data to randomize the encrypted data streams. Unlike other OFDM PLE schemes, the training symbol is resequenced to prevent an eavesdropper from synchronizing and estimating the channel to recover the physical frames. Thus, protection of the entire physical layer packet is achieved. Whilst the scheme is designed to be generically applicable to OFDM systems, an IEEE 802.11 OFDM protocol has been used as a case study. Our main contributions are:

- Obfuscation of the data at the subcarrier level by the transmission of dummy data in several OFDM subcarriers in order to make the data more random and secure. This also permits dynamic adjustment of the encryption parameters in order to customize the security level of a connection.
- Replacement of the training symbol with a more secure key sequence provides a new unique training symbol as the conventional training symbol will be resequenced in a way unknown to eavesdroppers, thus preventing them from synchronizing and estimating the channel. Legitimate users are still able to perform these functions normally, but eavesdroppers cannot locate and decode the data correctly. The feasibility and performance of training symbol resequencing is analyzed for the example of the IEEE 802.11 OFDM system.
- The scheme is designed to be much less computationally complex and thus particularly suitable for resource limited devices as the key rate can be varied to match hardware resources. It is usually low for most encryption parameters but here the security can be scaled according to the resource availability.
- A case study has been carried out by implementing the scheme according to IEEE 802.11 OFDM. We provide indications on how to interact with the existing modules in a communication protocol and how to apply effective protection to different data parts according to their specific structures and functions in the protocol.

The rest of paper is organized as follows. Section II introduces related work. Section III describes our OFDM PLE algorithm. A security analysis of the proposed scheme is presented in Section IV and a comparison with other OFDM PLE schemes is carried out in Section V by comparing them in terms of search space, key rate and complexity. A case study, implementation in IEEE 802.11 OFDM system, is presented in Section VI. Section VII concludes the paper.

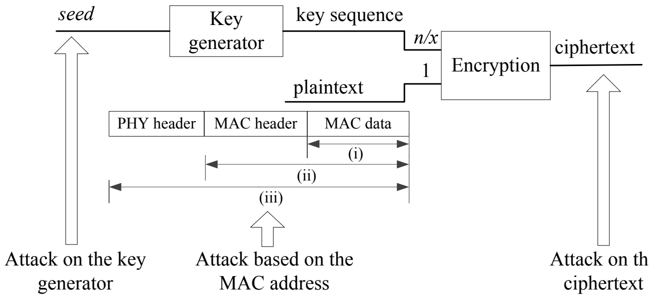


Fig. 1. Encryption schemes and security attacks. (i), (ii), and (iii) are different fields protected by MAC layer encryption schemes, most PLE schemes and our PLE scheme, respectively; n and x is key-to-data ratio for other PLE schemes and our scheme, respectively. The security analysis of these three attacks is presented in Section IV.

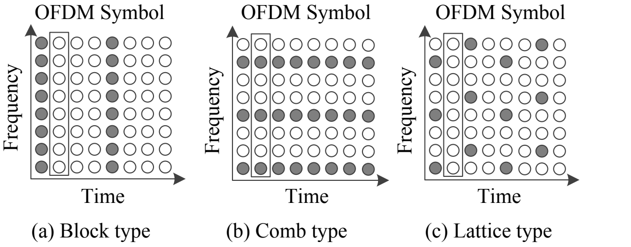
II. Related Work

Traditionally encryption is carried out at the MAC layer and above. As shown in Fig. 1, only the MAC data field (indicated by (i) in the diagram) is protected by the MAC layer encryption schemes and therefore cannot prevent passive and active attacks which target the MAC address as it is unencrypted. Moreover, MAC layer encryption does not prevent an eavesdropper from storing the data and decrypting it off-line. In order to address these vulnerabilities, it appears necessary to enhance security at the physical layer to protect data field (ii) or even (iii) indicated in Fig. 1.

Various OFDM PLE schemes have been proposed, which perform encryption in different stages of the physical layer. Tseng and Chiu [9], Khan *et al.* [8] and Zhang *et al.* [10] implement PLE by scrambling the constellation symbols in the frequency domain before the IFFT operation, whilst Li *et al.* [11] scrambles the data in the time domain after the IFFT operation. Dzung [12] adds rotation to the modulation symbols and encrypts the training symbol to prevent the attacker from synchronizing and estimating the channel. Ma *et al.* [13] and Reilly and Kanter [14], also encrypt the constellation symbols by converting to a much denser constellation; they introduce a small amount of random noise into each constellation symbol, making it more difficult for an adversary to demodulate the ciphertext.

These schemes have all acted to make OFDM transmission more secure, however, they still have limitations. Firstly, all the schemes encrypt one source data bit with one or more key bits; in the work of Reilly and Kanter [14], eight key bits per symbol are required for encryption and so the key-to-data ratio is always n ($n \geq 1$). The key bits are generated by a key generator, which uses a stream cipher or a chaotic map to generate the pseudorandom key sequence. The key-to-data ratio is a major factor when comparing encryption schemes for high data rate communications, because a higher speed key generator will generally be much more computational complex.

In addition, as shown in Fig. 1, most of the research [8]–[11], [13], [14] transmits the training symbol in plaintext



(a) Block type (b) Comb type (c) Lattice type

Fig. 2. Training symbol structures. The solid gray dots represent training symbol.

which allows an eavesdropper to perform synchronization and channel estimation just as legitimate users do. This means that the data is sniffable as the eavesdropper is then able to locate the data field in the recovered frame which has been the major issue with conventional OFDM PLE schemes. Dzung [12] encrypts both the training and data symbols by rotating them, but the author does not analyze the feasibility and performance in detail.

Several papers have proposed improving the security level by scrambling the data symbols in either the frequency or time domain [8]–[11]. This approach requires matrix operations: multiplication, determinant calculation and division, all of which introduce additional computational complexity which makes these schemes unattractive for low computation capability devices.

In this paper, a novel PLE scheme for OFDM systems is proposed, which makes the transmission more random by obfuscating the data at the subcarrier level and protecting the entire physical layer packet (iii) by resequencing the training symbol. The scheme has low complexity and the key-to-data ratio (x in Fig. 1) can be varied and usually made to be less than 1.

III. Subcarrier Obfuscation And Training Symbol Resequencing Scheme

A. Overview

In OFDM systems, the binary data is first coded and interleaved, then mapped to a complex data point, $X(n)$, by a mapping scheme, such as BPSK, QPSK, 16-QAM, 64-QAM, etc.. The complex data $X(n)$ is finally modulated to different subcarriers by IFFT operation, which can be written as

$$x(i) = \frac{1}{N_{\mathsf{IFFT}}} \sum_{n=0}^{N_{\mathsf{IFFT}}-1} X(n) e^{j2\pi ni/N_{\mathsf{IFFT}}}, \tag{1}$$

where N_{IFFT} is the IFFT size, $x(i), i = 0, 1, .., N_{\mathsf{IFFT}}-1$ forms a time domain OFDM symbol.

An OFDM system consists of data symbol and training symbol. The data symbol is modulated to transmit data while the training symbol is used for the synchronization and channel estimation. The training symbol may form a separate OFDM symbol, or be combined with the data symbol, depending on the training symbol structure, which is shown in Fig. 2.

The received signal in the frequency domain can be written as

$$R(n) = X(n)H(n) + W(n), \tag{2}$$

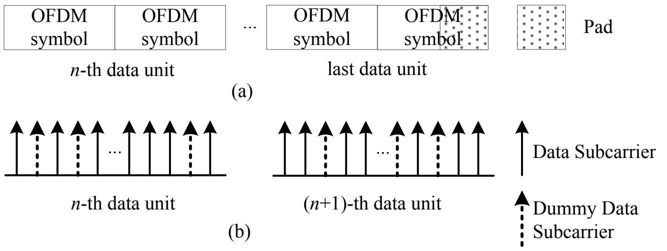


Fig. 3. Illustration of the data unit (a) Example of the data unit structure ($s = 2$); (b) Example of the dummy data subcarrier obfuscation ($s = 2$, $k = 3$)

where $H(n)$ and $W(n)$ are the channel and noise effect, respectively. The decoded signal can be written as

$$\widehat{X}(n) = \frac{R(n)}{\widehat{H}(n)}, \tag{3}$$

where $\widehat{H}(n)$ is the channel estimation.

In this paper, we propose to enhance the OFDM systems' security performance at the physical layer. The data part is randomized at the subcarrier level by reserving several subcarriers for dummy data transmission, i.e., some of the $X(n)$ are selected to obfuscate the data, as shown in Fig. 3. In addition, the training symbol is resequenced with a secure and random sequence. The entire physical layer packet of OFDM transmission is thus protected by subcarrier obfuscation and training symbol resequencing.

As the encryption information is shared between the legitimate users, the receiver can decode the signal as normal. However, an eavesdropper will be faced with significant challenges to decode the signal. First, as the training symbol is resequenced and kept secret to the eavesdropper, he/she cannot perform the synchronization and channel estimation correctly, i.e., $\widehat{H}(n)$ remains unknown to the eavesdropper. In addition, even though the eavesdropper could possibly get the channel estimation $\widehat{H}(n)$, after equalization, he/she would also have to remove the dummy data from $\widehat{X}(n)$ in order to reveal the real source data, and this requires further knowledge of the dummy reservation scheme being used at any time.

Fig. 4 shows the system block diagram of our proposed scheme. The white blocks represent the generic OFDM system and the gray blocks are added for encryption and decryption in our scheme. The same key generator with the stream cipher implemented inside is used in the transmitter and receiver to generate the key sequence. As the $seed$ and $[s, k]$ for the key generator are shared before the transmission using a secure channel, the transmitter and receiver can generate the same key sequence. These secret information, i.e., $seed$ and $[s, k]$, can be refreshed by the users according to the channel condition and security level that they intend to achieve.

B. Data Encryption and Subcarrier Obfuscation

1) Algorithm Description: The data part is encrypted and obfuscated in order to make the OFDM data symbols more random and secure. The source binary data is usually coded with a coding rate, R, and interleaved, and then modulated

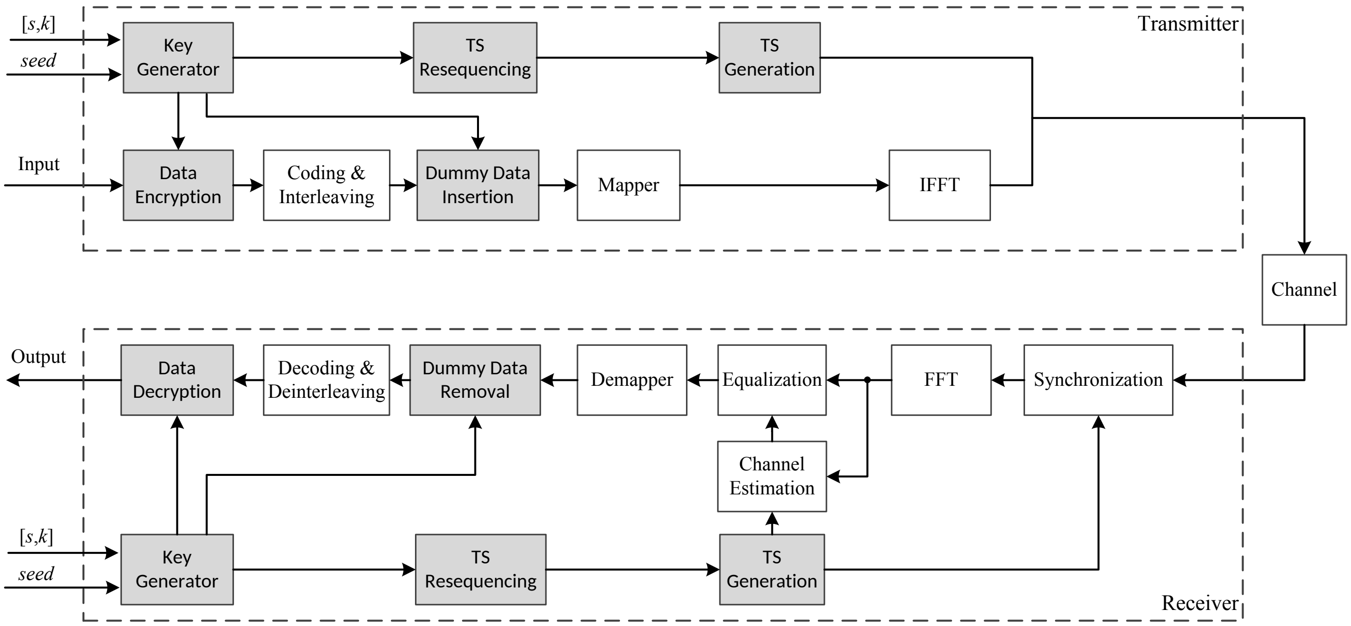


Fig. 4. The block diagram of the proposed OFDM PLE system. The gray blocks are added for encryption and decryption.

using a mapping scheme. The modulated complex points $X(n)$ are then passed to the IFFT module to form an OFDM symbol. The data with l_d bits can be modulated into

$$N_{\mathsf{OFDM}} = \lceil \frac{l_d}{N_d Rb} \rceil \tag{4}$$

OFDM symbols, where N_d is the number of the data subcarriers, b is the number of bits per subcarrier, determined by the mapping scheme, and $\lceil \cdot \rceil$ is the ceiling function.

We propose to encrypt the source data and obfuscate them by inserting dummy data in between the encrypted data. As the source data usually can be modulated over many OFDM symbols, we group s OFDM symbols as a data unit and reserve k subcarriers for dummy data, which is called an $[s, k]$ combination. An example of data unit structure and dummy data subcarrier obfuscation with $s = 2$, $k = 3$ is shown in Fig. 3. The locations of the dummy data subcarriers change for every data unit. Algorithm 1 describes the procedure for data encryption and subcarrier obfuscation applied to the data part.

Algorithm 1 Data encryption and subcarrier obfuscation

```
INPUT: data, $seed$, $[s,k]$, $b$, $R$
OUTPUT: data$_{enc}$
 1: $l_d = \mathsf{length}(\mathsf{data})$
 2: $N_{\mathsf{unit}} = \lceil \frac{l_d}{(N_d s - k)Rb} \rceil$
 3: $\mathsf{data} = \mathsf{pad}(\mathsf{data}, N_{\mathsf{unit}}(N_d s - k)Rb)$
 4: $[data_1, ..., data_i, ..., data_{N_{\mathsf{unit}}}] = \mathsf{data}$
 5: for $i \leftarrow 1\ to\ N_{\mathsf{unit}}$ do
 6:     $key = \mathrm{SC1}(seed, kb)$
 7:     $DummySubcLoc = \mathrm{SC1}(seed, k\lceil log_2(N_d s)\rceil)$
 8:     $DummyData = \mathrm{SC2}(seed2, kb)$
 9:     $DataSubcLoc = [1 : N_d s] - DummySubcLoc$
10:     $key2$ = expand($key$)        % $key2 = [key, ..., key]$
11:     $data2$ = xor($data_i$,$key2$)
12:     $data_{cod}$ = coding($data2, R$)
13:     $data_{int}$ = interleave($data_{conv}$)
14:     $data_{enc}(DataSubcLoc) = data_{int}$
15:     $data_{enc}(DummySubcLoc) = DummyData$
16:     $data_{enc}$ is passed to the remaining modules for further
        processing
17: end for
```

The source data is first padded with zeros to the length of $N_{\mathsf{unit}}(N_d s - k)Rb$ bits (line 3) and then the new data is divided into N_{unit} data groups, each of which has a length of $(N_d s - k)Rb$ bits (line 4).

For each data group, kb key bits and k dummy data subcarriers' locations (each with a length of $\lceil \log_2(N_d s)\rceil$) are generated by a stream cipher SC1 and kb dummy data bits are generated by another stream cipher SC2, in line 6, 7, and 8, respectively. In line 9, the data subcarriers' locations are generated by calculating the complementary set of dummy data subcarriers' locations. The key is expanded by replication to the length of the data group in line 10 and then XOR-ed with *i*-th data group in line 11.

Channel coding is usually adopted to correct wireless transmission errors. Therefore, if dummy data insertion occurs before coding, then the dummy data will be mixed with the data after coding and cannot be allocated to the specified subcarriers. In addition, the interleaver will permute the data so the dummy data will not be in the same subcarrier even if it is not encoded. Therefore, coding and interleaving are implemented before the dummy data insertion. The data unit is finally formed by allocating the encrypted data group and dummy data to their specified locations and then passed to the remaining modules for further processing.

After mapping, the data bits and dummy data bits are mapped to different subcarriers. Thus the data subcarriers are obfuscated by dummy data subcarriers, making the OFDM symbols random and presenting a challenge for the eavesdropper to sniff the data. Therefore OFDM symbols are encrypted and obfuscated at the subcarrier level.

At the receiver side, the dummy data is removed before the decoding, so that it will not affect the decoding of the encrypted data. Therefore $seed2$ is only generated in transmitter and does not need to be shared between the legitimate users.

Because k subcarriers are reserved to transmit the dummy data in every s OFDM symbols, the data throughput is decreased by

$$\alpha = \frac{k}{N_d s}. \tag{5}$$

In this paper, our scheme offers the potenial to make a tradeoff between the data throughput and security.

2) Benefits of Subcarrier Obfuscation: We obfuscate the OFDM transmission at the subcarrier level by insertion of the dummy data. This randomizes the analog waveform which makes it much harder for the eavesdropper to decode the signal. In addition, the subcarrier selection and dummy data insertion are feasible in hardware as the operations required are implementable and low cost. Finally, due to the introduction of the encryption parameters, the system's security level can be adjusted according to the hardware availability and security requirements. These benefits will be further discussed in detail through the rest of the paper.

C. Training Symbol Resequencing

The training symbol in OFDM standards is pre-defined sequences used to perform the time synchronization and channel estimation. For example, the long training symbol (LTS) used in IEEE 802.11 OFDM is defined as

$$\begin{aligned} \mathit{LTS} = \{&1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, \\ &-1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, \\ &1, 1, -1, 1, -1, 1, -1, -1, -1, -1, -1, 1, 1, \\ &-1, -1, 1, -1, 1, -1, 1, 1, 1, 1\}. \end{aligned} \tag{6}$$

Most OFDM PLE schemes use the same training symbol defined in the standard. However, the eavesdropper also has access to these sequences and then is able to synchronize to the transmitter and estimate the channel, which means he/she can decode and store the data for off-line decryption.

In order to enhance the security level of the OFDM system, we propose to resequence the training symbol by random sequences with N_t-bit binary data shared between legitimate users. The receiver has the new sequence to perform the synchronization and channel estimation while the eavesdropper can only have a random guess.

1) Feasibility Analysis: The content of the training symbol has been changed in our scheme. However, the subcarrier's carrier frequencies remain the same, therefore, the orthogonality of the OFDM system is not affected. We have shown in Section VI by a case study that the performance of synchronization and channel estimation is not impacted by the training symbol resequencing. Therefore, it is feasible to resequence the training symbol.

2) Security Against Blind Channel Estimation: Eavesdroppers may still use blind channel estimation to attempt to obtain the channel information in OFDM systems. However, statistical blind channel estimation suffers from slow convergence which makes it unsuitable for mobile environments while deterministic blind channel estimation is computationally complex which will present implementation challenges. The performance of blind channel estimation is greatly affected by the channel condition and is usually worse than training symbol-based methods [21]. Therefore, although the eavesdropper is still able to perform the blind channel estimation to get some information of the channel, he/she will have to spend a much longer time to successfully decode the signal. Classical encryption methods aim to achieve backward secrecy, which is not impacted by the blind channel estimation here.

IV. Attack and Security Analysis

Wireless communication is vulnerable to passive eavesdropping due to its broadcast nature. In this section, we use search space for the brute force attack to quantize the computational overhead for the eavesdropper, which is the same common tool used in security analysis for upper layer encryption schemes. However, PLE is different from upper layer schemes and introduces some new features. As shown in Fig. 1, there are three practical considerations for any PLE scheme:

- *The way that the key sequence is used to encrypt the plaintext*: PLE schemes use the key sequence differently by performing the encryption in different physical layer modulation stages, but other PLE work does not analyze the effect on the search space of the ciphertext. The *security level of the ciphertext* is termed to characterize the search space of the ciphertext, which is analyzed in Section IV-A.
- *The key generation algorithm adopted to generate the key sequence*: The search space for the key generator is the commonly used system's security level. The published schemes usually adopt a stream cipher or a chaotic map to generate random key sequence. Once the key generation method is determined, the system's security level is fixed as well. In our scheme, a stream cipher is also used to generate the key sequence, but the system's security level can still be customized, as explained in Section IV-B.
- *The data field that is to be protected*: Compared to upper layer encryption, PLE has provided further security as the MAC header is protected. However, most OFDM PLE schemes transmit the training symbol in plaintext, which makes the data linkable and detectable. In our proposed scheme, in addition to the data part, the training symbol is resequenced to make the system more secure.

The following security attacks and analysis are based on these three considerations.

A. Attack on the Ciphertext

In an attack on the ciphertext, an eavesdropper only knows the encryption algorithm and ciphertext, which means that he/she has the least amount of information to work with [22]. In our scheme, this attack involves an exhaustive key search by trying every possible key/subcarrier permutation until an intelligible translation of the ciphertext into plaintext is obtained.

1) Attack on the Data Part: If an eavesdropper has already obtained the ciphertext of the obfuscated data, he/she has to determine which subcarriers are carrying useful data, and then search the key bits for decryption. Assuming the eavesdropper already knows $[s,k]$, then the search space for one data unit, ss_{unit}, is given as

$$ss_{\mathsf{unit}} = C^k_{N_d s} 2^{kb}, \tag{7}$$

where $C^k_n = \frac{n!}{(n-k)!k!}$.

The dummy data subcarriers' locations change for every data unit, so the search space for the data part ss_{data} is given as

$$ss_{\mathsf{data}} = (ss_{\mathsf{unit}})^{N_{\mathsf{unit}}} = (C^k_{N_d s} 2^{kb})^{\lceil \frac{l_d}{(N_d s - k)Rb} \rceil}. \tag{8}$$

As the eavesdropper does not know $[s,k]$, he/she has to try the combinations one by one until the used $[s_0,k_0]$ is found, the search space ss_{data} becomes

$$\begin{aligned} ss_{\mathsf{data}} = &\sum_{s=1}^{s_0-1} \sum_{k=1}^{\lceil \alpha_{\max} N_d s \rceil} (C^k_{N_d s} 2^{kb})^{\lceil \frac{l_d}{(N_d s - k)Rb} \rceil} \\ &+ \sum_{k=1}^{k_0} (C^k_{N_d s_0} 2^{kb})^{\lceil \frac{l_d}{(N_d s_0 - k)Rb} \rceil}, \end{aligned} \tag{9}$$

where $s_0 \in [1, s_{\max}]$ and $k_0 \in [1, k_{\max}]$, $s_{\max}$, $k_{\max}$, and $\alpha_{\max}$ are the maximum values that s, k, and α could be, respectively.

Additionally, because s and k can be adjusted, the search space is much larger than the search space of fixed s and k, which makes the scheme more secure.

2) Attack on the Training Symbol: Assuming the eavesdropper has synchronized to the transmitter, he/she will have to try 2^{N_t} times to find the new sequence during channel estimation. However, the eavesdropper does not know the start of the physical layer packet, he/she can only have a random guess. Assuming that the eavesdropper find the start of the packet after N_a attempts, the total search space ss_{TS} is given as

$$ss_{\mathsf{TS}} = N_a 2^{N_t}. \tag{10}$$

3) Ciphertext Attack Summary: In order to decrypt the physical layer packet, an eavesdropper will have to acquire knowledge of the new training symbol and then decrypt the data part. As the eavesdropper does not know which training symbol the legitimate users are using, the attack on the training symbol is a ciphertext only attack. So for the entire physical layer packet, the search space of our SOTSR scheme is

$$\begin{aligned} ss^{\mathsf{SOTSR}}_{\mathsf{PLE}} &= ss_{\mathsf{TS}} \times ss_{\mathsf{data}} \\ &= N_a 2^{N_t} (\sum_{s=1}^{s_0-1} \sum_{k=1}^{\lceil \alpha_{\max} N_d s \rceil} (C^k_{N_d s} 2^{kb})^{\lceil \frac{l_d}{(N_d s - k)Rb} \rceil} \\ &+ \sum_{k=1}^{k_0} (C^k_{N_d s_0} 2^{kb})^{\lceil \frac{l_d}{(N_d s_0 - k)Rb} \rceil}). \end{aligned} \tag{11}$$

B. Attack on the Key Generator

In an attack on the key generator, the eavesdropper tries to break down the key generator with an N_s-bit *seed* stream cipher using an exhaustive key search. The search space is

$$ss'_{\mathsf{KG}} = 2^{N_s}. \tag{12}$$

In our proposed scheme, besides obtaining the *seed* for the key generator, an eavesdropper also has to attempt N_a times to locate the start of the data symbols and find out $[s,k]$ in order to carry out the decryption correctly. For every *seed*, the eavesdropper has to try $N_a sk$ times, the total search space ss_{KG} can be given as

$$ss_{\mathsf{KG}} = N_a sk 2^{N_s}. \tag{13}$$

As s and k are preshared between transmitter and receiver, the width of s and k are determined by $s_{\max}$ and $k_{\max}$, respectively. So the security improvement is at a cost of adding $(\lceil \log_2 s_{\max} \rceil + \lceil \log_2 k_{\max} \rceil)$ more bits to the secret information sharing between transmitter and receiver. This secret information increase is postulated worthwhile. For example, for $s_{\max} = 16$, $k_{\max} = 128$, $s = 4$, $k = 4$, $N_a = 1$, and $N_s = 80$, the shared secret information is increased by $\frac{\lceil \log_2 16 \rceil + \lceil \log_2 128 \rceil}{80} = 13.75\%$. However the search space ss_{KG} is enhanced by $1 \times 4 \times 4 = 1600\%$, which dramatically increases the eavesdropper's required computational overhead. Also it is worth noting that due to the training symbol resequencing, the system is N_a times more secure, without adding any overhead to the secret information sharing.

For most other encryption schemes, after the key generation algorithm is determined, the security level of the system is fixed as well. In our scheme, the system's security level can still be customized by changing the values of s and k, which is another reason to make these values adjustable. This feature is quite useful, as most encryption schemes will adopt off-the-shelf key generation algorithms, but our scheme can still offer some options after the key generation algorithm is selected.

It seems that the value of ss_{KG} is much smaller than the value of $ss^{\mathsf{SOTSR}}_{\mathsf{PLE}}$. However, the attack on the key generator is more complicated than the attack on the ciphertext. The attack on the ciphertext involves trying different key sequences to determine some readable plaintext by only knowing the ciphertext. But the attack on the key generator is to try different seeds for the key generator and then use the generated key sequence to decrypt the ciphertext. In addition, the information known by the eavesdropper and the purpose of the attack is also different for these two attacks. Therefore, these two search spaces are not comparable.

C. Attacks Based on the MAC Address

Encryption schemes implemented at MAC layer leave the MAC header unprotected, making the system vulnerable to attacks based on the MAC address. The proposed encryption scheme is implemented at the physical layer, so the entire MAC packet is encrypted, including the MAC header. Moreover due to our training symbol resequencing, the eavesdropper cannot perform synchronization and channel estimation correctly in real-time, and therefore does not know where the

MAC header is. Thus the system is very robust to attacks based on the MAC address.

V. Performance Evaluation and Comparison

In this section, comparison with other OFDM PLE schemes is carried out by evaluating the performance of search space, key rate and complexity. The search space is one of the most critical metrics for any encryption scheme as it determines the raw processing power (brute force) required by an eavesdropper, while the key rate and complexity determine how easy the scheme is to implement.

A. Search Space

Search space is not the final parameter describing the computational complexity for the brute force attack, which also depends on the computation overhead required for each round of the attack. As PLE schemes protect the data at different modulation stages, the eavesdropper may carry out part of the receiving procedure and then be faced to decrypt the data, as illustrated in Fig. 5. When the training symbol is unchanged, the eavesdroppers can detect the signal arrival and only need to store one complete received waveform. The eavesdropper then can carry out part of the receiving procedure and search for the right key. For example, for modulation symbols rotation-based schemes, the eavesdropper can perform the procedure as far as to the FFT operation then it will be faced to guess the correct angle for each constellation symbol. Conventional XOR encryption happens at the first stage of the physical layer modulation by XOR-ing the source binary data with key sequence so it does not randomize the transmitted waveform, thus the eavesdropper can perform the entire receiving procedure. However, in our scheme, due to the training symbol resequencing, the eavesdropper is not able to perform synchronization and channel estimation correctly, he/she will then have to store all of the received signal waveform, and be always required to repeat the entire receiving procedure when trying each possible key sequence. This significantly increases the computational overhead for the eavesdropper. However, it is difficult to quantize the number of the computational operations for each round of the attack, therefore, we still use search space to analyze the security level of the system as it provides a quantitative description of numbers of the attempts required.

1) Search Space of the Entire Packet: Conventional encryption is implemented in the upper layers, e.g., MAC layer. The search space for MAC layer encryption by exhaustive key search is denoted as ss_{MAC}. All the OFDM PLE schemes add further protection to the MAC packet, i.e., the data part of the physical layer packet. The search space can be written as

$$ss_{\text{total}} = ss_{\text{PLE}} \times ss_{\text{MAC}} \tag{14}$$

For most OFDM PLE schemes, only the data part are protected, the search space can be written as

$$ss_{\text{PLE2}} = ss_{\text{data}} \tag{15}$$

In Dzung's work [12], the author encrypts the training symbol by rotating it based on the key stream. When the eavesdropper tries to find the encrypted training symbol, as he/she knows the standard training symbol, it is a known plaintext attack. This means the eavesdropper obtains the ciphertext and also knows the corresponding plaintext. The search space for the entire packet is

TABLE I
Search space of the data part for different PLE schemes

ss_{data}	ss^{scr}_{data}	ss^{rot}_{data}
1.18×10^{141}	$(48!)^{34}$	2.47×10^{173}

TABLE II
System Setting

l_d	N_d	R	b	$[s_0, k_0]$	α	α_{max}	N_{bps}
800	48	1/2	1	$[4, 4]$	2%	10%	2

$$ss_{\text{PLE3}} = ss_{\text{TS}} + ss_{\text{data}}. \tag{16}$$

While the training symbol encryption adds some additional protection to the system, the improvement is quite limited. Our scheme's search space is much larger, which means it is much more secure. Compared to the encrypted training symbol scheme, our scheme even has a slightly simpler training symbol generation method. This is because we used the sequence from the key generator as the training symbol directly without any encryption operations required.

2) Search Space of the Data Part: All the PLE schemes enhance the system's security by protecting the data part of the physical layer packet. The search space of the data part ss_{data} for our scheme has been given in (9).

Scrambling-based PLE schemes [8]–[11] rearrange the data positions by a scrambling matrix S. For each OFDM symbol, there are $N_d!$ different permutations. Therefore, the search space of the entire data part can be given as

$$ss^{scr}_{\text{data}} = (N_d!)^{\lceil \frac{l_d}{N_d R b} \rceil}. \tag{17}$$

Modulation symbols rotation-based schemes [12]–[14] rotate the constellation symbols by an angle determined by the number of bits per modulation symbol, N_{bps}, e.g., in the work of Reilly and Kanter [14], 8 bits are used for each rotation, thus $N_{bps} = 8$. For each constellation symbol, there are $2^{N_{bps}}$ possible choices. Thus, for the entire packet, the search space can be written as

$$ss^{rot}_{\text{data}} = (2^{N_{bps}})^{\lceil \frac{l_d}{N_d R b} \rceil N_d}. \tag{18}$$

The search space increases with the data length. An example of the search space of the data part for different PLE schemes are given in Table I while the system setting is shown in Table II. Assuming the eavesdropper is equipped with a powerful machine which can process 1 million decryptions per microsecond [22], it will take the eavesdropper 3.74×10^{121} years to crack our scheme! This is achieved only at a tradeoff of 2% decrease in the bandwidth.

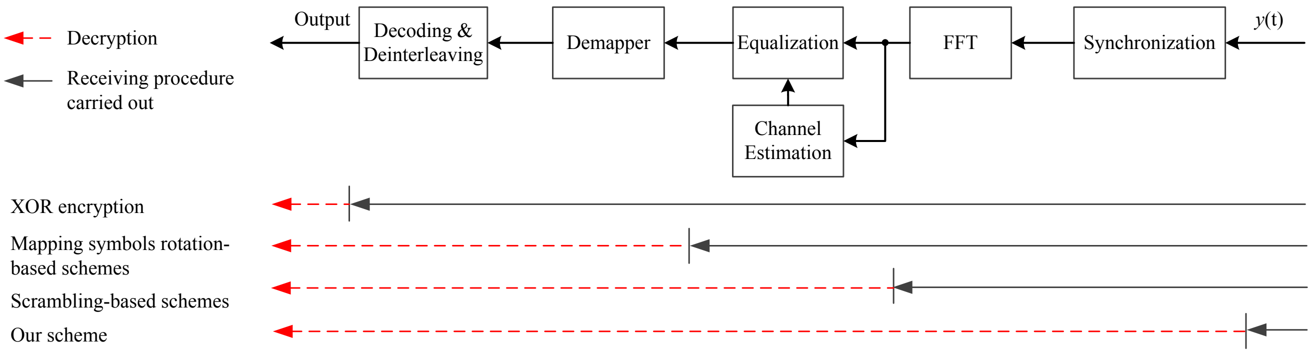


Fig. 5. Illustration of the decryption processes.

B. Key Rate

The key rate is an essential factor in encryption. Key sequence is generated by stream cipher or chaotic map. A higher key rate requires more computational complexity to realize. Wireless technologies are used widely in mobile devices which are sensitive to hardware and power. The output speed of the key generator can become a major system bottleneck whenever a mobile device attempts high data rate encrypted communications.

In wireless communications, the system will adjust the coding rate and mapping scheme according to the channel's *SNR* to maintain a low bit error rate (BER), leading to different data rate. For example, there are four mapping schemes used in IEEE 802.11 OFDM, i.e., BPSK, QPSK, 16-QAM, and 64-QAM, so the value of b could be 1, 2, 4, and 6, respectively. The coding rate R of IEEE 802.11 OFDM could be 1/2, 2/3, 3/4. The data rate, *DR*, can be given as

$$\mathit{DR} = \mathit{DR}_{\min} b \frac{R}{1/2} = 2\mathit{DR}_{\min} R b, \tag{19}$$

where $\mathit{DR}_{\min}$ is the minimum data rate of the system when it is coded with a rate of $R = 1/2$ and BPSK mapped. For the simplicity of analysis, $\mathit{DR}_{\min}$ is normalized to 1.

The n_k-bit key is required to encrypt n_d-bit source data. The key-to-data ratio can be defined as the ratio between them, and is also a ratio between the key rate, *KR*, and the data rate *DR*, which is given as

$$\eta = \frac{n_k}{n_d} = \frac{\mathit{KR}}{\mathit{DR}}. \tag{20}$$

In our scheme, the key-to-data ratio can vary with $[s, k]$. Key bits with a length of $k(\lceil \log_2(N_d s)\rceil + b)$ can encrypt $(N_d s - k)Rb$ data bits, thus the key-to-data ratio of our SOTSR scheme is given as

$$\eta^{\mathsf{SOTSR}} = \frac{k(\lceil \log_2(N_d s)\rceil + b)}{(N_d s - k)Rb}. \tag{21}$$

The key rate can be calculated as

$$\mathit{KR}^{\mathsf{SOTSR}} = \mathit{DR}\eta^{\mathsf{SOTSR}} = \frac{2k(\lceil \log_2(N_d s)\rceil + b)}{(N_d s - k)} \mathit{DR}_{\min}. \tag{22}$$

In scrambling-based PLE schemes [8]–[11], if the index of the scrambling matrix is generated by a stream cipher, for each subcarrier index, it needs $\lceil \log_2(N_d)\rceil$ bits. The key bits required for the entire matrix are at least $\lceil \log_2(N_d)\rceil N_d$. Therefore, the minimum key-to-data ratio of scrambling-based schemes can be written as

$$\eta^{scr} = \frac{\lceil \log_2(N_d)\rceil N_d}{N_d Rb} = \frac{\lceil \log_2(N_d)\rceil}{Rb}. \tag{23}$$

And the key rate is given as

$$\mathit{KR}^{scr} = \mathit{DR}\eta^{scr} = 2\lceil \log_2(N_d)\rceil \times \mathit{DR}_{\min}. \tag{24}$$

In modulation symbols rotation-based schemes [12]–[14], the key sequence is used to generate the rotation angle. The key-to-data ratio of their system can be given as

$$\eta^{rot} = \frac{N_{bps}}{Rb}. \tag{25}$$

The key rate of these schemes can be calculated as

$$\mathit{KR}^{rot} = \mathit{DR}\eta^{rot} = 2N_{bps} \times \mathit{DR}_{\min}. \tag{26}$$

Key rates of different schemes are shown in Fig. 6, with an OFDM system running at a coding rate $R = 3/4$ and 64-QAM mapping scheme ($b = 6$). For scrambling-based schemes, $\mathit{KR}^{scr} = 12$; for modulation symbols rotation-based schemes, $\mathit{KR}^{rot} = 4$ when $N_{bps} = 2$ and $\mathit{KR}^{rot} = 16$ when $N_{bps} = 8$. Our scheme can be configured to have a smaller key rate by adjusting the values of s and k. It is also worth noting that the key rate of our scheme is usually smaller than the data rate, which means the key-to-data ratio η^{SOTSR} is smaller than 1.

As our scheme can adjust the key rate by changing the encryption parameters, the security can be scaled according to the hardware availability, thus it is especially useful for resource limited devices. With larger s and k, the search space will be higher and the system will be more secure. For example, as shown in (13), ss_{KG} increases linearly with s and k. However, the security improvement is at a cost of more keys, and thereof more computational resources, as larger s and k result in higher a key rate.

C. Complexity

It is important to consider the hardware implications of any change both in terms of the hardware increase and the impact on the propagation delay which will affect the speed of operation. A coarse computational complexity estimation

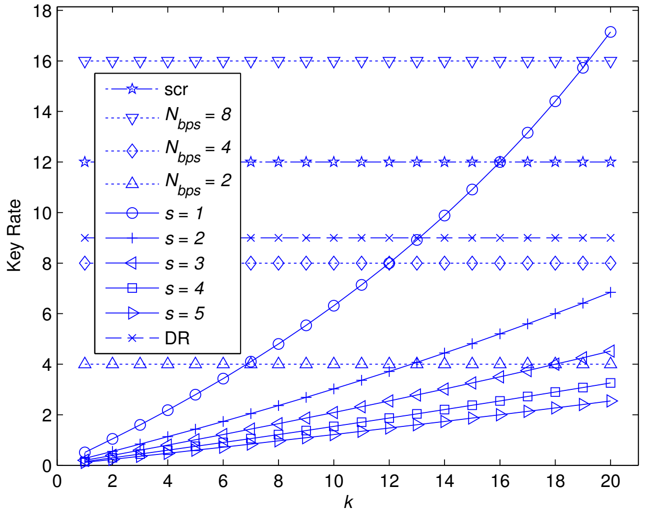


Fig. 6. Data rate, key rate of scrambling-based schemes, modulation symbols rotation-based schemes and our scheme with different encryption parameters $[s, k]$, $b = 6$, $R = 3/4$, $DR_{\min} = 1$, $N_d = 48$.

has been carried out and our scheme is much less computationally complex, compared to some other published OFDM encryption schemes.

As the data encryption and subcarrier obfuscation of the data part, i.e., Algorithm 1, is the most time consuming process in our scheme, therefore, only the complexity of Algorithm 1 is considered here to simplify the analysis. The encryption complexity of our SOTSR scheme is given by

$$\begin{aligned}\psi^{\mathsf{SOTSR}} &= M_1 + N_{\mathsf{unit}} M_2\\ &= M_1 + \lceil \frac{l_d}{(N_d s - k) Rb} \rceil M_2\\ &\approx M_1 + \frac{M_2}{(N_d s - k)} \frac{l_d}{Rb},\end{aligned} \tag{27}$$

where M_1 and M_2 are the operation numbers introduced by our scheme outside and inside the loop of Algorithm 1 (i.e., lines 1 to 4 and lines 6 to 16, respectively). In our scheme, the operation required for decryption process is similar to the operation in the encryption process, so the decryption has almost the same complexity.

Scrambling-based PLE schemes [8]–[11] require matrix operations, including matrix multiplication, determinant, division, inversion, which have a high computation complexity. For example, matrix inversion has a complexity of $O(N_{\mathsf{mat}}^3)$, where N_{mat} is the matrix size which for OFDM, will represent the same as IFFT/FFT size N_{IFFT}. For a data packet with the same length l_d, there will be $\lceil \frac{l_d}{N_d Rb} \rceil$ OFDM symbols. For each OFDM symbol, the data is scrambled in either frequency or time domain, so there will be $\lceil \frac{l_d}{N_d Rb} \rceil$ rounds of encryptions and decryptions. Scrambling-based schemes need to calculate the inverse of the scrambling matrix in the decryption process. If we consider the computational complexity of matrix inversion only, the decryption complexity of scrambling-based schemes is written as

$$\psi^{scr} = \lceil \frac{l_d}{N_d Rb} \rceil O({N_{\mathsf{IFFT}}}^3) \approx \frac{O({N_{\mathsf{IFFT}}}^3)}{N_d Rb} l_d. \tag{28}$$

As there are some guard bands in OFDM, $N_d \leq N_{\mathsf{IFFT}}$. For example, in IEEE 802.11 OFDM, the IFFT/FFT size is 64, but only 48 of the inputs are used for data subcarriers. Thus we have

$$\psi^{scr} \geq \frac{O(N_d^3)}{N_d} \frac{l_d}{Rb}. \tag{29}$$

Modulation symbols rotation-based schemes [12]–[14] perform the encryption by multiplying the constellation symbols with a factor generated from the key sequence. The complexity can be given as

$$\psi^{rot} = \lceil \frac{l_d}{N_d Rb} \rceil N_d \approx \frac{l_d}{Rb}. \tag{30}$$

Multiplication is not at bit level but at data values, which could make the implementation relatively more complex. However, the overall complexity of modulation symbols rotation-based schemes is not high as it only introduces a multiplication.

Note that in our scheme, all the operations are non-complex, so the factor of $\frac{l_d}{Rb}$ in ψ^{SOTSR} is much smaller than its factor in ψ^{scr}, i.e., the complexity of scrambling-based schemes [8]–[11], which means our scheme has a lower complexity and thus is more suitable for resource limited devices. The gray modules in Fig. 4 are introduced for encryption and decryption which cost extra hardware. All the operations in our scheme occur before mapping and thus at the bit level, which makes for a comparatively more hardware efficient solution. The encryption process only requires XOR and bit stuffing while the decryption process only requires XOR and bit removal. XOR is used in conventional XOR encryption as well. The additional resource for bit stuffing and bit removal consists of multiplexers and control circuits, which is not a big overhead. *TS Resequencing* module does not require extra hardware as it uses the sequence from the *Key Generator* directly. *TS Generation* transforms the resequenced training symbol from frequency domain to time domain, which requires an IFFT module or could be designed to share the IFFT module in the data stream modulation. Therefore, the extra hardware introduced by our scheme is relatively small. The implementation of our scheme is left for the future work by when a detailed design will be undertaken and circuit area will be precisely computed.

D. Summary

In this section, we evaluated and compared the performance of different PLE schemes in terms of search space, key rate and complexity. As summarized in Table III, the overall performance of our scheme outperforms other PLE schemes.

In this paper, we proposed to protect the entire OFDM physical layer packet by subcarrier obfuscation of the data part and the training symbol resequencing, which work together to enhance the security of the OFDM transmission.

Data part is the main part of the OFDM physical layer packet, which is protected by subcarrier obfuscation. As analyzed in Section IV-A and Section V-A2, subcarrier obfuscation does not compromise the security of the ciphertext. In addition, the introduction of two adjustable parameters, s and k, offers us the capacity to customize the search space of

TABLE III
PERFORMANCE COMPARISON OF DIFFERENT PLE SCHEMES

	Our Scheme	Scrambling-based Scheme	Modulation Symbols Rotation-Based Scheme
Search Space (ss_{data})	High	High	High
Key Rate (*KR*)	Usually low, adjustable	High	Usually high, adjustable
Complexity (ψ)	Low	High	Low

ciphertext (11), the search space of key generator (13), and the key rate (22). Finally, subcarrier obfuscation is a relatively low complexity technique, which is suitable for resource limited devices.

There are usually much less training symbol subcarriers than data subcarriers. In terms of the contribution to the search space, training symbol resequencing may seem to be less essential than subcarrier obfuscation. However, as analyzed in Section V-A, the training symbol resequencing can randomize the physical transmission, which makes it much more difficult for the eavesdroppers to carry out the synchronization and channel estimation correctly. In addition, this technique does not require complicated implementation, therefore, the security improvement is achieved in a very effective way. Finally, training symbol resequencing is independent of subcarrier obfuscation and can be implemented with other data part protection schemes such as modulation symbols rotation-based schemes and scrambling-based schemes.

VI. CASE STUDY: IMPLEMENTATION IN IEEE 802.11 OFDM SYSTEM

Other research has reported their proposed schemes in a generalized manner, without reference to particular wireless systems or consideration to the protocol details. However PLE is dependent on the transmission scheme used, e.g. structure of training symbol, format of the physical layer packet, etc. Therefore, a case study is carried out here by implementing our encryption scheme according to the IEEE 802.11 OFDM protocol, in order to offer some insights on how our encryption scheme interacts with the transmission protocol.

IEEE 802.11 OFDM is widely used in commercial electronic devices. Although MAC layer encryption schemes such as WEP and WPA provide some protection, it still remains vulnerable to attacks [23]. Therefore, we propose to enhance the security performance by applying our PLE scheme to the standard.

The algorithm is prototyped using MATLAB simulation. The model is implemented according to the IEEE 802.11 OFDM protocol and is the same as shown in Fig. 4. It demonstrates that as long as the synchronization and channel estimation are correctly performed, the encryption and decryption of the data part will not impact the BER. In this section, first the related IEEE 802.11 OFDM protocol is introduced. The SIGNAL field, DATA field and LTS are protected differently due to their specific structure. The reason that short training symbol (STS) is not encrypted is also explained.

A. IEEE 802.11 OFDM Protocol

The frame format of IEEE 802.11 OFDM physical layer convergence protocol (PLCP) protocol data unit (PPDU), i.e., the physical layer packet, is shown in Fig. 7. It consists of the PLCP preamble, the SIGNAL field and the DATA field. The PLCP preamble is composed of ten identical STS t_1, t_2, $\ldots$, t_{10} and 2.5 LTS GI2, T_1, T_2, whose structure is the block type as shown in Fig. 2(a). The STS is used for automatic gain control (AGC), signal detection and coarse frequency synchronization etc., whilst the LTS is used for data symbol alignment and channel estimation. In the time domain, each STS is 16 samples and each LTS is 64 samples.

The bit assignment of the SIGNAL field is shown in Fig. 7. The RATE subfield defines the coding rate R (1/2, 2/3 or 3/4) and mapping scheme (BPSK, QPSK, 16-QAM or 64-QAM) used for the DATA field while the LENGTH subfield indicates the number of octets in the PLCP service data unit (PSDU). The SIGNAL field is always mapped with BPSK and uses convolutional coding at rate $R = 1/2$. The DATA field contains the SERVICE subfield, PSDU, the Tail bits and the Pad bits. The PSDU is the MAC frame passed from MAC layer requesting the physical layer to transmit. The DATA field is convolutionally encoded and mapped using the parameters defined in the SIGNAL field.

B. Data Encryption and Subcarrier Obfuscation

The data part of the PPDU consists of SIGNAL and DATA field, which are protected differently due to their specific structures.

1) SIGNAL Field Encryption: The SIGNAL field is used to decode the DATA field as it contains the coding rate, mapping scheme and length information of the DATA field. The SIGNAL field is always convolutionally coded with a rate of $R = 1/2$ and BPSK mapped. In order to make the system more secure, a 24-bit key is generated to encrypt the SIGNAL field using an XOR operation. As the SIGNAL field forms a complete OFDM symbol after convolutional coding and mapping, no dummy data is inserted into the SIGNAL field thus ensuring minimal change to the current protocol.

2) DATA Field Protection: DATA field is the main data part of the PPDU and protected using our proposed data encryption and subcarrier obfuscation scheme. When the DATA field is modulated, the number of OFDM symbols is:

$$N_{\mathsf{OFDM}} = \lceil \frac{8N_{\mathsf{PSDU}} + 16 + 6}{N_d Rb} \rceil, \tag{31}$$

where N_{PSDU} is the number of bytes in the PSDU, $N_d = 48$ in IEEE 802.11 OFDM.

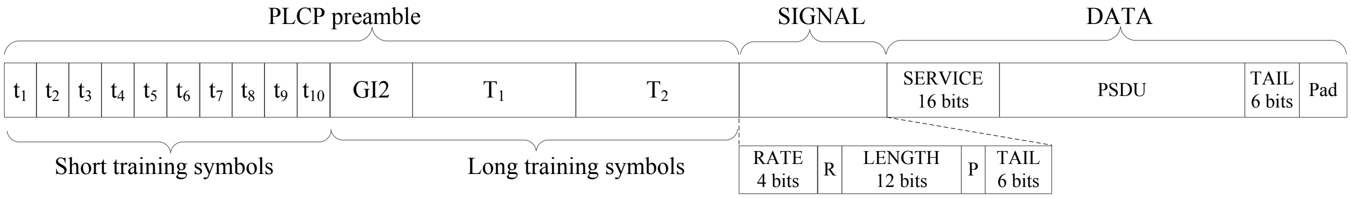


Fig. 7. IEEE 802.11 OFDM PPDU frame format [24] (For simplicity, guard interval of the OFDM data symbols is not shown in the figure)

As the LENGTH subfield in the SIGNAL field is 12 bits, theoretically the PSDU can be up to 4095 bytes long. According to the standard, the fragmentation threshold is 2346 bytes [24], which limits the maximum MAC frame size. The mean MAC packet length is 1500 bytes; when the DATA field is modulated using 64-QAM with 3/4 coding rate, there are approximately $\lceil \frac{1500\times 8+16+6}{48\times 3/4\times 6} \rceil = 56$ OFDM symbols. Thus when the DATA field is modulated using a lower order mapping scheme and a smaller coding rate, there will be more OFDM symbols. Therefore, it is feasible to group several OFDM symbols together to form a data unit.

C. LTS Resequencing

The frequency domain value of the LTS in IEEE 802.11 OFDM is shown in (6), which is a 52-bit long sequence modulated by BPSK. The time domain values of the LTS can be calculated by applying an IFFT operation to the frequency domain values. In order to make the OFDM transmission unrecoverable to the eavesdropper, the LTS is resequenced with a 52-bit key sequence, rather than using the sequence defined in the standard. This sequence may be changed from system to system for even greater security. As the legitimate receiver has the same new LTS sequence as the transmitter, he/she can synchronize and estimate the channel correctly while the eavesdropper can only have a random guess, thus providing an additional level of security. In this section, we show that the LTS resequencing still retains the functionality to allow the normal synchronization and channel estimation.

1) Effect on Data Symbol Alignment: The LTS is used to identify the start of the data symbols at the physical layer packets by calculating the cross correlation coefficient, C_{lts}, using the expression below:

$$C_{\mathsf{lts}}(n) = \sum_{i=0}^{N_{\mathsf{LTS}}-1} r(n+i)lts(i)^*, \tag{32}$$

where $r(n+i)$ is the received signal, $lts(i)$ is the time domain LTS, N_{LTS} is the length of the LTS, and $(\cdot)^*$ is the conjugate operation [25]. When $C_{\mathsf{lts}}(n)$ reaches its maximum value, which is proportional to the value of $\sum_{i=0}^{N_{\mathsf{LTS}}-1} |lts(i)|^2$, then n is the index of the start of the LTS and $n+128$ is the start of the data symbols (the two LTSs' length is 128). An eavesdropper does not have any knowledge of the new *lts*, so he/she cannot correctly identify the start of the data and therefore can only have a random guess.

As the LTS is BPSK modulated in the frequency domain, resequencing it will only change the sign of its elements. Thus the resequenced LTS, $LTS_{\mathsf{new}}(n)$, can be written as

$$\mathit{LTS}_{\mathsf{new}}(n) = (-1)^t \mathit{LTS}(n),\ t = 0, 1, \tag{33}$$

where $\mathit{LTS}(n)$ is the frequency domain LTS in the standard.

According to Parseval's theorem, we have

$$\sum_{i=0}^{N_{\mathsf{IFFT}}-1} |x(i)|^2 = \frac{1}{N_{\mathsf{IFFT}}} \sum_{n=0}^{N_{\mathsf{IFFT}}-1} |X(n)|^2, \tag{34}$$

where $X(n) = \sum_{i=0}^{N_{\mathsf{IFFT}}-1} x(i)e^{-j2\pi in/N_{\mathsf{IFFT}}}$, $n = 0,\ 1,\ ...,\ N_{\mathsf{IFFT}}-1$.

Then

$$\begin{aligned}\sum_{i=0}^{N_{\mathsf{IFFT}}-1} |\mathit{lts}_{\mathsf{new}}(i)|^2 &= \frac{1}{N_{\mathsf{IFFT}}} \sum_{n=0}^{N_{\mathsf{IFFT}}-1} |\mathit{LTS}_{\mathsf{new}}(n)|^2 \\ &= \frac{1}{N_{\mathsf{IFFT}}} \sum_{n=0}^{N_{\mathsf{IFFT}}-1} |(-1)^t \mathit{LTS}(n)|^2 \\ &= \sum_{i=0}^{N_{\mathsf{IFFT}}-1} |\mathit{lts}(i)|^2,\end{aligned} \tag{35}$$

where $\mathit{lts}_{\mathsf{new}}(i)$ is the new time domain LTS. Thus, although the LTS is resequenced, the value of $\sum_{i=0}^{N_{\mathsf{LTS}}-1} |\mathit{lts}(i)|^2$ will remain the same, and so will the maximum value of $C_{\mathsf{lts}}(n)$.

Some simulation results of the symbol alignment performance when the system uses the standard LTS and resequenced LTS are shown in Fig. 8. As there are 2.5 LTSs in the preamble, the index of the first peak is the start of the LTS. Both systems have two clear peaks and the peaks of the LTS resequenced system match those of the standard LTS system, indicating that LTS resequencing does not impact the performance of the symbol alignment.

The value $C_{\mathsf{lts}}(n)$ is compared with a threshold to detect the appearance of the maximum correlation coefficient and hence detect the start of the data symbols. However, as it is shown in the above analysis and simulation, the maximum correlation coefficient will stay the same so the threshold value does not require dynamic adjusting. The legitimate user can perform the data symbol alignment correctly with the knowledge of the resequenced LTS.

2) Effect on Channel Estimation: The LTS is also used to estimate the channel. The least-square (LS) channel estimation method is used widely due to its simplicity [21], which is also adopted in our model. The mean-square error (MSE) of the LS channel estimation is inversely proportional to the *SNR*, which is not affected by the content of the training symbol,

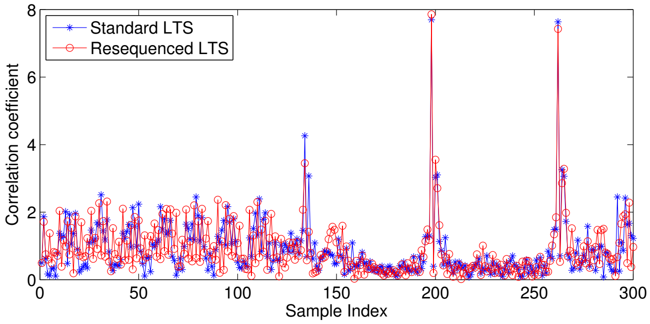


Fig. 8. Data symbol alignment using standard LTS and resequenced LTS, in the same environment with the same channel impulse response and noise, *SNR* = 10 dB

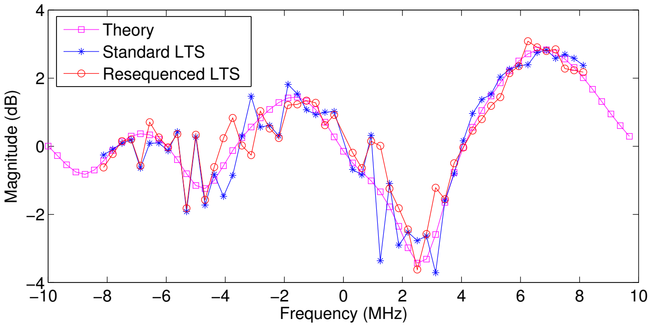


Fig. 9. Channel estimation using standard LTS and resequenced LTS, in the same environment with the same channel impulse response and noise, *SNR* = 10 dB. Theory curve is calculated by applying FFT operation to the channel impulse response.

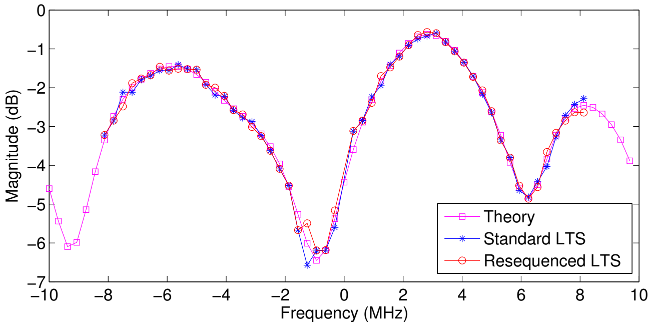


Fig. 10. Channel estimation using standard LTS and resequenced LTS, in the same environment with the same channel impulse response and noise, *SNR* = 30 dB. Theory curve is calculated by applying FFT operation to the channel impulse response.

as shown in Fig. 9 and Fig. 10. Therefore LTS resequencing will not impact channel estimation.

D. STS Encryption

The STS is not encrypted or resequenced in our proposed scheme. The STS is used for signal detection, AGC and coarse frequency offset estimation, etc. in IEEE 802.11 OFDM. The receiver carries out these functions based on the periodicity of the STS and through calculation of the delay and autocorrelation of the received signal, that is

$$C_{\mathsf{sts}}(n) = \sum_{i=0}^{N_{\mathsf{win}}-1} r(n+i)r(n+i+N_{\mathsf{STS}})^*, \qquad (36)$$

where N_{STS} is the length of the STS, N_{win} is the length of the search window, and $C_{\mathsf{sts}}(n)$ is the autocorrelation coefficient [25].

The receiver does not have to know the time domain and/or frequency domain values of the STS to calculate $C_{\mathsf{sts}}(n)$. As long as the 10 STSs are the same, the receiver can perform the delay and autocorrelation correctly, and so can the eavesdropper.

Moreover, the OFDM system's transmission power is much larger than the noise power, so the eavesdropper can detect the signal arrival by the increase in the received signal's power. Therefore, in any case it is difficult to prevent the eavesdropper from detecting the signal in OFDM transmission systems. However, transmitting the STS in plaintext (as is currently the case) does not compromise the system's security very much, because the eavesdropper will still have to decrypt the subsequent LTS, the SIGNAL and the DATA fields as described above.

E. Summary

In this section, we implemented our encryption scheme to the IEEE 802.11 OFDM system, and presented the design considerations of how to apply the scheme to a specific communication protocol. For example, special attention has been paid to the SIGNAL field and STS due to their special data structure and usage.

As the above analysis shows, the training symbol resequencing does not interrupt the normal synchronization and channel estimation process, and the DATA field is suitable to be protected by data encryption and subcarrier obfuscation. Therefore, our encryption scheme is applicable for IEEE 802.11 OFDM systems and provides additional security enhancement at the physical layer.

VII. Conclusion

A new OFDM PLE scheme using subcarrier obfuscation and training symbol resequencing is proposed in this paper. The OFDM transmissions are more random due to subcarrier obfuscation through the insertion of dummy data transmitted in several subcarriers. Two encryption parameters, s and k, are introduced for the subcarrier obfuscation. Although the key sequence is used differently from the conventional PLE schemes, it is shown that this does not compromise the security level by analyzing each of the search spaces using an exhaustive key search. In the proposed scheme, the encryption parameters can be made adjustable, and it is shown that this greatly improves the security level at a cost of a relatively small overhead of the secret information sharing between transmitter and receiver. Another key feature of our scheme is the resequencing of the training symbol which means the protection of the entire physical layer packet. This obscures and encrypts both the packet contents and the location of the

MAC frame, totally preventing the system from the attacks based on the MAC address.

Our proposed scheme has a good performance in terms of search space, key rate and complexity. The search space is large enough to resist brute force attack. The key rate can be varied by adjusting the encryption parameters and usually can be made small. Using a coarse computational complexity estimation, it is shown how the scheme has a low complexity and therefore is especially suitable for resource limited devices. A case study has been carried out to IEEE 802.11 OFDM system to show the design consideration to apply a general OFDM encryption scheme to a specific communication protocol. The practical hardware implementation of the scheme will be the focus of our future work.

References

[1] L. Chen, J. Ji, and Z. Zhang, Eds., *Wireless Network Security: Theories and Applications*. Springer, 2013.

[2] Y. Zou, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances and future trends," pp. 1–31, 2015. [Online]. Available: http://arxiv.org/abs/1505.07919

[3] K. J. Hole, E. Dyrnes, and P. Thorsheim, "Securing Wi-Fi networks," *Computer*, vol. 38, no. 7, pp. 28–34, Jul. 2005.

[4] A. H. Lashkari, M. M. S. Danesh, and B. Samadi, "A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i)," in *Proc. 2nd IEEE Int. Conf. on Computer Science and Information Technology (ICCSIT)*, Beijing, China, Aug. 2009, pp. 48–52.

[5] T. Dieks and E. Rescorla, "The Transport layer security (TLS) protocol," Internet Requests for Comments, RFC Editor, RFC 5246, Aug. 2008. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5246.txt

[6] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun. Mag.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[7] F. Armknecht, J. Girao, A. Matos, and R. L. Aguiar, "Who said that? Privacy at link layer," in *Proc. 26th IEEE Int. Conf. on Comput. Commun. (INFOCOM)*, Anchorage, Alaska, USA, May 2007, pp. 2521–2525.

[8] M. A. Khan, M. Asim, V. Jeoti, and R. S. Manzoor, "On secure OFDM system: Chaos based constellation scrambling," in *Proc. Int. Conf. on Intelligent and Advanced Syst. (ICIAS)*, Kuala Lumpur, Malaysia, Nov. 2007, pp. 484–488.

[9] D. Tseng and J. Chiu, "An OFDM speech scrambler without residual intelligibility," in *Proc. IEEE Region 10 Conf. (TENCON)*, Taipei, Oct. 2007, pp. 1–4.

[10] L. Zhang, X. Xin, B. Liu, and Y. Wang, "Secure OFDM-PON based on chaos scrambling," *IEEE Photon. Technol. Lett.*, vol. 23, no. 14, pp. 998–1000, Jul. 2011.

[11] H. Li, X. Wang, and W. Hou, "Secure transmission in OFDM systems by using time domain scrambling," in *Proc. 77th IEEE Veh. Technology Conf. (VTC Spring)*, Dresden, Germany, Jun. 2013, pp. 1–5.

[12] D. Dzung, "Data encryption on the physical layer of a data transmission system," U.S. Patent 7 752 430B2, Jul. 6, 2010.

[13] R. Ma, L. Dai, Z. Wang, and J. Wang, "Secure communication in TDS-OFDM system using constellation rotation and noise insertion," *IEEE Trans. Consum. Electron.*, vol. 56, no. 3, pp. 1328–1332, Aug. 2010.

[14] D. Reilly and G. Kanter, "Noise-enhanced encryption for physical layer security in an OFDM radio," in *Proc. IEEE Radio and Wireless Symp. (RWS)*, San Diego, CA, USA, Jan. 2009, pp. 344–347.

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

[16] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.

[17] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[18] A. Mukherjee and A. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[19] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[20] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

[21] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM Wireless Communications with MATLAB*. Wiley-IEEE Press, 2010.

[22] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 4th ed. Prentice Hall, 2006.

[23] E. Tews and M. Beck, "Practical attacks against WEP and WPA," in *Proc. 2nd ACM Conf. on Wireless Network Security (WiSec)*, Zurich, Switzerland, Mar. 2009, pp. 79–86.

[24] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 2012.

[25] B. Bloessl, M. Segata, C. Sommer, and F. Dressler, "An IEEE 802.11 a/g/p OFDM receiver for GNU radio," in *Proc. 2nd Workshop on Software Radio Implementation Forum (SRIF)*, Hong Kong, Aug. 2013, pp. 9–16.

Junqing Zhang received the B.Eng. and M.Eng. degrees in electrical engineering from Tianjin University, China in 2009 and 2012, respectively, and the Ph.D. degree in electronics and electrical engineering from Queen's University Belfast, U.K. in 2016. He is currently a Post-Doctoral Research Fellow with Queen's University Belfast. His research interests include physical layer security, cryptography and OFDM.

Alan Marshall (M'88-SM'00) has spent over 24 years working in the telecommunications and defense Industries. He has been a Visiting Professor in network security at the University of Nice/CNRS, France, and an Adjunct Professor for Research at Sunway University Malaysia. He is currently the Chair in Communications Networks at the University of Liverpool, where he is also the Director of the Advanced Networks Group. He has formed a successful spin-out company Traffic Observation & Management (TOM) Ltd., specializing in intrusion detection and prevention for wireless networks. He has authored over 200 scientific papers and holds a number of joint patents in the areas of communications and network security. His research interests include network architectures and protocols; mobile and wireless networks; network security; high-speed packet switching, quality of service & experience architectures; and distributed haptics. He is a fellow of The Institution of Engineering and Technology. He is a Section Editor (section B: Computer and Communications Networks and Systems) for the Computer Journal of the British Computer Society, a member of Editorial Board of the Journal of Networks (JNW), and on the program committees of a number of IEEE conferences.

Roger Woods (M'95-SM'01) received the B.Sc degree (Hons.) in electrical and electronic engineering and the Ph.D. degree from the Queen's University Belfast in 1985 and 1990, respectively. He is currently a Full Professor with Queen's University Belfast, and has created and leads the Programmable Systems Laboratory. He has co-founded a spin-off company, Analytics Engines Ltd., which looks to exploit a lot of the programmable systems research. His research interests are in heterogeneous programmable systems and system level design tools for data, signal and image processing and telecommunications. He holds 4 patents and has authored over 200 papers. He is a member of the IEEE Signal Processing and Industrial Electronics Societies and is on the Advisory Board for the IEEE SPS Technical Committee on the Design and Implementation of Signal Processing Systems. He is on the Editorial Board for the ACM Transactions on Reconfigurable Technology and Systems, the Journal of VLSI Signal Processing Systems and the IET Proceedings on Computer and Digital Techniques. He acted as General Chair for the 2014 Asilomar IEEE Conference on Signals, Systems, and Computers and is on the program committees of a number of IEEE conferences.

Trung Q. Duong (S'05-M'12-SM'13) received the Ph.D. degree in telecommunications systems from the Blekinge Institute of Technology, Sweden in 2012. Since 2013, he has been with Queen's University Belfast, U.K., as a Lecturer (Assistant Professor). He has authored or co-authored 190 technical papers published in scientific journals and presented at international conferences. His current research interests include cooperative communications, cognitive radio networks, physical layer security, massive MIMO, cross-layer design, mm-waves communications, and localization for radios and networks.

Dr. Duong received the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, and the IEEE International Conference on Communications (ICC) 2014. He is currently a recipient of the Royal Academy of Engineering Research Fellowship. He currently serves as an Editor of the IEEE Transactions on Communications, IEEE Communications Letters, IET Communications, Wiley Transactions on Emerging Telecommunications Technologies, and Electronics Letters. He has also served as the Guest Editor of the special issue on some major journals including IEEE Journal in Selected Areas on Communications, IET Communications, IEEE Wireless Communications Magazine, IEEE Communications Magazine, EURASIP Journal on Wireless Communications and Networking, EURASIP Journal on Advances Signal Processing.