A Novel Secret Key Generation Method in OFDM System for Physical Layer Security

Wang Dong, Southeast University, Nanjing, China
Hu Aiqun, Southeast University, Nanjing, China
Peng Linning, Southeast University, Nanjing, China

ABSTRACT

In this paper, a novel physical layer key generation method for extracting secret key from mutual channel information in orthogonal frequency division multiplexing (OFDM) systems has been proposed. Firstly, a well-designed data extraction process has been introduced to reduce the redundancy and inconsistency of channel state information (CSI). After that, a new quantization method using gray code is proposed. Furthermore, an associated method is designed to reduce key error rate (KER). With these improvements, higher key generation rate (KGR) can be obtained compared to existing methods. Finally, available secret keys have been generated after information reconciliation and privacy amplification. The proposed method has been analyzed and verified in long term evolution advanced (LTE-A) systems and the generated secret keys have passed randomness test.

KEYWORDS
KER, Key Generation, KGR, LTE-A, OFDM, Physical Layer Security, Quantization

1. INTRODUCTION

In recent years, wireless physical layer security has received more and more attention. The model of physical layer security was first established by Shannon (1949), it mainly includes two branches: security schemes without key leaded by Wyner (1975) and secret key based secrecy schemes leaded by Maurer (1993). The basic idea of secret key based secrecy schemes is to use the uniqueness and randomness of wireless communication link to convert channel mutual information of between authorized users into a shared key, encrypt the data and achieve the secure communication. As eavesdropper cannot obtain the same channel information as authorized user, it can hardly generate the identical key. How to effectively extract secret key from the common information has become the focus of physical layer security.

Orthogonal frequency division multiplexing (OFDM) technology has been widely used in wireless communication systems. Due to the diversity of channel information, key generation methods in OFDM systems have received wide attention. The generalized features, such as received signal strength (RSS) and bit error rate (BER), can be used to extract secret key. For example, the work in (Kitano et al., 2007) generates keys from BER of received signal, and uses an intermediate value of BER as a quantization threshold. A key generation method for wireless local area network systems is studied in (Yasukawa et al., 2008), the quantization threshold is determined by sorting RSS value of a period of time, which makes the probability of quantization value is basically the same. Because RSS and BER are both generalized channel information, the key generation rate (KGR) obtained by these methods is relatively low.
OFDM technology uses multi-carrier transmission, which can conveniently obtain the channel state information (CSI) on each subcarrier in channel estimation process. These large numbers of common random information provide favorable conditions for obtaining higher KGR (Liu et al., 2012; Liu et al., 2013). However, in order to effectively use this advantage, it still needs to solve some problems. Firstly, CSI contains a large amount of redundant information, which will reduce the randomness of key. Secondly, due to the influence of RF device asymmetry, time division duplex (TDD) transmission characteristics and environmental noise, channel reciprocity will be destroyed. A discrete cosine transform method has been studied in (Yasukawa et al., 2008) to reduce the redundancy. In addition, an adaptive multi-bit quantization method has been adopted to generate the secret key. In order to improve channel reciprocity, a low-pass filter has been designed to reduce the noise in (Zhang et al., 2015). A channel gain compensation method has been proposed to reduce the effect of the asymmetry of radio frequency circuit in (Liu et al., 2013).

In all of the secret key generation methods, it is necessary to quantize channel information. The selection of quantization method is related to the key generation efficiency. A suitable quantization method can be used to maximize the use of these channels information. At present, the primary quantization methods mainly include single threshold quantization (Aono et al., 2005), double threshold quantization (Mathur et al., 2008), multi bit quantization (Jana et al., 2009) and cumulative distribution function based quantization (Patwari et al., 2010), etc. The key sequence generated in the quantization process can be called a candidate key. In order to generate an available key, it still needs to carry out information reconciliation and privacy amplification.

In this paper, we propose a novel key generation method in OFDM system. We introduce the data extraction to reduce data redundancy and inconsistency. A new quantization method is designed, which adopts the direct quantization and associate with low round operation. Compared with the quantization methods mentioned above, this method can effectively improve the key generation efficiency. In the aspect of information reconciliation, we remove the inconsistent bits based on cyclic redundancy check (CRC) check method. The randomness of key is improved by 8b/10b encoding and sequence interleaving.

The rest of this paper is organized as follows. Section 2 gives a description of the system model. In Section 3, the proposed key generation method is introduced in detail. In Section 4, we present and discuss the simulation results. The paper is summarized in Section 5.

2. SYSTEM MODEL

Alice and Bob are authorized users, where exist a wireless communication link between them. Alice and Bob generate the secret key according to the common channel information, and then use the key to encrypt communication data. Eve is a non-active attack eavesdropper, which can obtain all the information from Alice or Bob. Eve also knows the key generation method. However, Eve is outside of the Alice’s (or Bob’s) coherent distance (coherent distance is represented by \( d \) in Figure 1). Therefore, Eve cannot obtain the same channel information as Alice or Bob, it can’t generate the identical key. The system model is shown in Figure 1.

3. PROPOSED KEY GENERATION METHOD

Alice and Bob establish a TDD wireless communication link. Firstly, the channel frequency response (CFR) is obtained by channel estimation in Alice and Bob. Secondly, Alice and Bob extract the CFR data separately, it includes two stages: stage 1, coarse data extraction, in order to remove redundant data; stage 2, fine data extraction, in order to reduce CFR deviation between Alice and Bob, so as to improve channel reciprocity. And then, the extracted CFR data are quantized into binary code directly, and continue to convert into gray code. This process is called direct quantization. Through the above process, the residual error is mainly distributed in the low bits of each quantization value. Therefore,
Fuzzy QoS Based OLSR Network
[www.igi-global.com/chapter/fuzzy-qos-based-olsr-network/72416?camid=4v1a](www.igi-global.com/chapter/fuzzy-qos-based-olsr-network/72416?camid=4v1a)

Hybrid Trust Structure in Self-Organizing Networks
[www.igi-global.com/article/hybrid-trust-structure-self-organizing/4041?camid=4v1a](www.igi-global.com/article/hybrid-trust-structure-self-organizing/4041?camid=4v1a)

Global Regulations in Content Industries: The Google Privacy Policy as a News Gatekeeping Factor
[www.igi-global.com/article/global-regulations-in-content-industries/204575?camid=4v1a](www.igi-global.com/article/global-regulations-in-content-industries/204575?camid=4v1a)