Ad Hoc Networks 64 (2017) 22–31

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

On the using of discrete wavelet transform for physical layer key generation

Furui Zhan, Nianmin Yao*

School of Computer Science and Technology, Dalian University of Technology, Dalian, China

ARTICLE INFO

Article history:
Received 23 October 2016
Revised 27 April 2017
Accepted 14 June 2017
Available online 15 June 2017

Keywords:
Key generation
Wireless channel reciprocity
Discrete wavelet transform
Gray code

ABSTRACT

For key generation between wireless transceivers, key generation leveraging channel reciprocity is a promising alternative to public key cryptography. Several existing schemes have validated its feasibility in real environments. However, in some scenarios, channel measurements collected by the involved transceivers are highly correlated but not identical, i.e., measurement sequences of these transceivers have too many discrepancies, which makes it difficult to extract the shared key from these measurements. In this paper, we propose a scheme to achieve secret key generation from wireless channels. During the proposed scheme, to reduce the amount of the referred discrepancies and further achieve efficient key generation, the involved transceivers separately apply a compressor based on the discrete wavelet transform (DWT) to pre-process their measurements. Then, multi-level quantization is implemented to quantify the output of DWT-based compressor. An encoding scheme based on gray code is employed to establish bit sequence and ensure that the resulting bit mismatch rate can be further reduced so that efficient information reconciliation can be implemented. Accordingly, the shared key between these transceivers can be derived after information reconciliation. Finally, 2-universal hash functions are used to guarantee the randomness of the shared secret key. Several experiments in real environments are conducted to validate the proposed scheme. The results demonstrate that the proposed scheme is available to generate shared secret keys between transceivers even though their measurement sequences have too many discrepancies.

1. Introduction

The intrinsic open broadcast nature of wireless communication makes most wireless applications susceptible to various attacks. Accordingly, security of wireless communication is critical. Almost all security mechanisms are implemented based on key generation. Traditional solution for establishing key is achieved by public key cryptography, which is generally based on the unproven assumptions of the hardness of some problems, such as integer factorization and discrete logarithm. However, a public key encryption system can be broken if the adversary has enough computing power. Moreover, such method consumes too many resources and might require a key management center.

In contrast, key generation leveraging wireless channel reciprocity is considered as a promising alternative to public key cryptography [1]. This method can be used to dynamically establish shared secret keys between transceivers. Theoretically, key generation from wireless channel is achieved by channel reciprocity and temporal channel variations [2]. Channel reciprocity ensures that two transceivers who simultaneously measure the communicating channel can derive the same channel state. Then, the channel state can be applied as their shared secret for establishing key. Therefore, channel reciprocity is the basis of key generation. In contrast, temporal channel variations reflect the variation of channel states and determine the randomness of the generated key, i.e., temporal channel variations affect the efficiency of key generation. Moreover, in typical multipath environments, the channel fading rapidly decorrelates over distances of the order of half a wavelength. As a result, it is possible to extract shared secret keys from the channel between legitimate transceivers even under the eavesdropping of adversaries.

Several schemes were proposed to establish keys from wireless channels [3]. Typically, these schemes consist of four components: channel probing, quantization, information reconciliation and privacy amplification. During channel probing, different statistics can be used to exploit the channel state, such as channel state information (CSI), channel impulse response (CIR) and received signal strength (RSS). In contrast to other statistics, most existing schemes extracted keys from RSS, since RSS can be easily de-

* Corresponding author.
E-mail address: lucos@dlut.edu.cn (N. Yao).

http://dx.doi.org/10.1016/j.adhoc.2017.06.003
1570-8705/

rived from the off-the-shelf devices without any modification. After channel probing, each involved transceiver collects a sequence of channel measurements.

To convert channel measurements into bits, the involved transceivers separately quantify their measurements with the same process. Generally, source coding might also be used to generate the bit sequence if multi-level quantization is implemented. The number of bits assigned for each quantization bin is required to be no less than $\log_2\lceil level \rceil$, where *level* denotes the level of quantization. Accordingly, the quantization level and code length together determine the number of the generated bits. The implementation of quantization might lead to entropy loss since different input values might fall into the same quantization bin and be marked as the same symbol. In addition, quantization and encoding also affect the bit mismatch rate between two generated bit sequences, i.e., the randomness of the shared key and the efficiency of key generation might be affected.

Each involved transceiver can generate a bit sequence from their measurements after the implementation of quantization (and encoding). However, these bit sequences might have some mismatches caused by discrepancies between measurement sequences of different transceivers. These mismatches can be corrected by information reconciliation, which can be achieved by Cascade [4] or error correcting code (ECC), such as the LDPC code [5] and BCH code [6]. During information reconciliation, transceivers have to exchange some information, which leads to the leakage of information. Consequently, a shared bit sequence can be established as the shared key and some information on the shared key might be leaked to the adversary.

Typically, transceivers apply the same privacy amplification process to eliminate the leaked information during information reconciliation and guarantee the secrecy of the shared secret key. Some schemes have been proposed to achieve privacy amplification by universal hash functions [7] or extractors [8]. After privacy amplification, a highly random bit sequence shared by these transceivers can be generated as their shared secret key.

Actually, when we implement key generation in real environments, many interferences might produce the referred discrepancies, e.g., asymmetric noises, various channel interferences, hardware differences. Moreover, most of the current communication systems are half-duplex, i.e., the transceiver can only either transmit or receive message at any given time. Therefore, the involved transceivers cannot simultaneously measure the communicating channel. In practice, the communication system can ensure that both transceivers measure the channel within the coherence time. As a result, these transceivers can derive the same or approximately the same channel state. Measurement sequences of different transceivers might be highly correlated but have many discrepancies. As mentioned above, the referred discrepancies significantly affect the efficiency of key generation. In some scenarios where too many discrepancies are produced, key generation might be even unavailable.

In this paper, a practical key generation scheme based on wireless channel reciprocity is proposed, which can be used to generate shared secret keys between transceivers even when their measurements have too many discrepancies. The proposed scheme consists of five components: channel probing, pre-processing, quantization & encoding, information reconciliation and privacy amplification. After collecting sufficient measurements during channel probing, the involved transceivers separately apply a compressor based on the discrete wavelet transform (DWT) to pre-process their measurements. Then, multi-level quantization in junction with source coding is implemented to convert the output of DWT-based compressor to bits. To further reduce the bit mismatch rate, an encoding scheme based on gray code is applied to generate the bit sequence. During information reconciliation, the interactive Cascade is applied to correct bit errors between these bit sequences and extract the shared key. Finally, transceivers use same 2-universal hash functions to eliminate the leaked information and guarantee the randomness of the shared secret key. To validate the proposed scheme, several experiments in real mobile environments are conducted. During each experiment, RSS measurements from heterogeneous devices are extracted as their shared randomness sources for establishing the secret key. The results of experiments show that measurement sequences of the involved transceivers have many discrepancies when they are equipped with different wireless cards. Furthermore, the results also demonstrate that the implementations of pre-processing and encoding scheme can reduce the bit mismatch rate and the proposed scheme can be used to generate keys in complicated scenarios where measurement sequences of different transceivers have too many discrepancies.

The reminder of this paper can be summarized as follows: Section 2 introduces several key generation schemes based on wireless channel reciprocity. In Section 3, system and adversary models are described. Then, we illustrate the proposed key generation scheme in Section 4. In Section 5, performance evaluation of the proposed scheme is conducted. Finally, this paper is concluded in Section 6.

2. Related work

Several schemes were proposed to generate secret keys from wireless channels. In these schemes, different statistics were used to exploit the channel state as their shared secret, such as RSS and CSI.

As a coarse measurement of wireless channels, RSS has been used in many schemes to generate shared secret keys. In [9], a level-crossing algorithm was proposed to extract secret keys from RSS and CIR. In this scheme, 2-level excursion-based quantization was implemented to convert measurements to bits and ensure that the probability of key disagreement was extremely low. In [10], an adaptive key generation scheme was proposed, which has similar processes to [9]. The key difference from [9] was that measurements were divided into blocks and the quantizer was customized according to each block. Besides, a multi-bits key generation scheme based on gray code was also introduced in this work. The results of comprehensive experiments showed that channel variations significantly affect the efficiency of key generation and multi-bits scheme can generate secret keys from RSS at a high rate. In [11,12], the finite impulse response (FIR) filter was used to preprocess measurements. However, the complexity of this scheme was high since the Karhunen-Loève transform (KLT) was also implemented during key generation. Besides, several schemes also used different methods to extract secret keys from RSS in different scenarios [13,14]. Moreover, a group key generation scheme was proposed in [15], which ensured that members can establish the group key by transmitting the differences of RSS measurements among them.

Recently, CSI becomes a new popular statistic for key generation. Comparing with RSS, CSI has more information on wireless channel. Therefore, efficient key generation can be implemented by CSI. In [16], a method for extracting secret keys from multipath fading randomness was proposed. In this work, both CSI and RSS were used to validate the proposed key generation method. The results of analysis demonstrated that the key generation rate from CSI was far higher than RSS. Besides, in [17–19], several schemes were also designed to achieve key generation from CSI. In summary, RSS and CSI are mostly used statistics to achieve key generation from wireless channels. As mentioned above, CSI has more information on wireless channels and generate the shared secret key at a higher rate than RSS. However, RSS can be easily derived from almost all of the off-the-shelf devices without any modifica-