KEY ESTABLISHMENT TECHNIQUE FOR SECURE DIVERSIFIED WIRELESS NETWORK

Saleh Asadollahi  
MSc.IT and CA Department,  
Saurashtra University,  
Rajkot, Gujarat, India

Bhargavi Goswami  
MCA Department, Sunshine Group of Institutions,  
Rajkot, Gujarat, India

Ian Asare  
MSc.IT and CA Department,  
Saurashtra University,  
Rajkot, Gujarat, India

Abstract—With the rising use of Wireless network in recent years, the demand of security is increasing with time that researchers need to study on that. The Low computational requirement, less energy consumption and easy implementation are the cardinal design characteristics taken into consideration during the establishment of the key based on channel reciprocity technique. This method, by observing the wireless channel, attempts to establish a shared key for providing security to wireless network in diversified networking scenario. The pedestal of the raised technique are: I. The method of computing the wireless channel reciprocity into binary bits to form a secret way, II. The method of exploiting communication error and correcting mismatch bit by nodes to obtain key agreement and III. Take a tour on achievability and security issues related to this technique. This paper gives a helicopter view on raised research over channel reciprocity based key establishment technique, developed to eradicate some of these security issues in wireless network.

Keywords— Wireless network security, key establishment, diversified networking scenario

1. INTRODUCTION

We are witnessed how wireless network has been widely used due its advantage such as easier installation, more flexible configuration and lower maintenance cost. In wireless communication, devices communicate with any another devices and receive the signal through the open air within its power range and make a whole device network easily accessible. This schema introduces one of the major secure problem because it make wireless communication vulnerable to potential attackers, on the other hand shares a common secret key which can be used to encrypt and decrypt transmitted information to secure the communication against eavesdroppers or attackers. Traditional method uses a centralized trusted third party to generate, maintain, and distribute shared secret keys base on key pre-distributed and public key cryptography such as Deffie-Hellmen algorithm [1] that was due to complex computation and operation on large numbers which are not suitable to establish among wireless sensor nodes, which limit with battery life and computation capability. New approaches use channel reciprocity on wireless communication that focus on one or more physical layer characters such as Signal frequency-phase, Received Signal Strength (RSS) and Channel Impulse Response (CIR) which allows the transmitter and receiver to observe same channel simultaneously and establish shared secret key.

Therefore new techniques that overcome the drawback of traditional key establishment and increase achievement on fast and efficient shared key, have formed a fruitful area for research. In the following sections of this paper, we describe first, the techniques proposed to use different channel metric to establish shared key which is known as quantization. Second, we discuss and introduce methods to achieve agreement on final keys generated between two terminals. In the last part, we make discussion on feasibility and security of key establishment.

2. QUANTIZATION

The first and important part of key establishment is quantization. To obtain the secret key bits from channel variations, the channel values at a certain frequency base on specific channel metric must be sampled. Transmitter and receiver first mock-up the transmitted signal at certain frequency to determine a unique wireless channel, then quantization exploits particular thresholds to quantize the sampled values into binary bits. Current researches describe that using appropriate channel metric has a direct impact and efficiency on the quantization. We categorize and label RSS, CIR, and frequency-phase information as channel metric which can be used for purpose of quantization.

2.1 Received Signal Strength (RSS)

The most widely used channel metric in quantization is Received Signal Strength (RSS). This method measures the amplitude of receiver signal in the varying of different channel and uses two threshold, encode sampled values into binary sequence. Figure 1, presents
quantization use of RSS with two fixed threshold (0.3 and 0.6), the sample values will be encoded as 1 when it exceeds of high threshold of 0.6, or encoded as 0 when it smaller than the low threshold 0.3 and the values between the two threshold will be disregarded.

Using two fixed threshold makes quantization susceptible. Also active attackers can provide additional information to generate secret key by inserting or moving the intermediate object between the receiver and transmitter. To overcome these setbacks, several approaches are proposed and a method that has been introduced is Adaptive Secret Bit Generation (ASBG) which improves the performance of quantization. The basic idea behind ASBG is, sampled values are divided into several random blocks in which each block is quantized independently. Each block has its own threshold based on the current environment and standard deviation. This performance is adaptive to ASBG varying environment, however, quantization still suffers from random noise. The sample values between two thresholds are not used and drop but the random noise channel increase more secret bits. The method introduced in [8] reduce the effect of random noise channel using the relative difference between sample values. This method unlike ABGS which uses absolute signal amplitude, utilize relative different signal amplitude, it means quantizer performs the local average over every D sample value to eliminate the short-term fluctuation caused by the random noise. Also it increases the amount of secret key by using more threshold.

RSS is a distance related parameter, it means that RSS is suitable for environment with rife of mobility. In other words, it doesn’t function effectively in a wireless network that consist of static nodes. This issue gives us another angle to target a new method for quantization in wireless channel which remain unchanged.

2.2 Frequency-phase based quantization method

Authors in [2, 9-11] proposed new methods based on channel Frequency-phase information for static wireless environment that is not correlated with distance between terminals. The authors of [2] bring together consecutive estimate of the channels frequency phase and exert multiple threshold to map each collected phase into particular binary bits to establish a secret key with high randomness.

The method introduced later in [11] uses a time-slotted round trip protocol to establish the secret key. In this method, receiver and transmitter separately select random frequency- phases that are equally distributed in a certain interval. After, both sides transfer signals in different time slots. Finally, quantizer uses multiple thresholds to quantize each estimated frequency-phase. In fact, the frequency-phase information is not associated with channel characteristics but it is also related to the initial choice made by the communicators.

In practice, the observed frequency-phase is divided into several zones where each zone has its own boundaries. If frequency-phases are close to the zone boundaries, wrong choice frequency-phase can be accrued. In this method, by determining a guard interval, if each frequency-phase fall in this guard interval will be discarded, the rest of procedure will be like the previous frequency-phase based method.

2.3 Channel Diversity

2.3.1 Single antenna based quantization

Frequency diversity scheme has been introduced by authors [3], measures the RSS values from a group of different channel frequency. In using the previous method, key generation rate is still quite limited and because they use single frequency with single antenna, they could just quantize one sample value at a time. It models the channel impulse response several times and computes the average to decrease the impact of random noise for each frequency. Multiple threshold is then used to quantize the average of the sampled channel impulse response into a binary bit sequence. The method proposed by authors [3] got achievement on a significant speed-up of the key generation.

However, value samples from different frequency which are correlated may interfere with each other and reduce the key generation security. To overcome this problem, Orthogonal Frequency Division Multiplexing (OFDM) is applied to minimize the interference. OFDM is a form of multicarrier modulation and is necessary for a receiver to receive the whole signal to be able to successfully demodulate the values sampled. OFDM modulates the data stream into multiple subcarriers with different frequencies that are orthogonal to each other and it makes quantization easy to estimate the channel taps on the frequency domain. Authors in [12] by exploiting the OFDM system can generate secret keys at a fast rate.

2.4 Multiple Antenna

New method [4, 13] has been proposed to explore the possibility of using multiple antenna besides using a single antenna to estimate the channel and generate the shared secret key. Authors in [4] introduced Multiple Antenna Key Generator (MAKG) by using multi-antenna diversity. It collects channel state information for each
pair antenna and is similar to RSS-based. quantizer applies several thresholds to convert the collected channel information into sequence bits. Assume each node has N antenna after channel estimation, each node can get N2 channel state information. It provides the generation of a long secret key with rich entropy.

In [13], like [12] it is based on frequency-phase quantization which uses diversity of Multiple-input and Multiple-output (MIMO) system and exploits guard interval to reduce bit error. The quantization of each channel is following the step described in [12]. In this method, like what is going on in [4], M2 channel can be estimated to collect a large number of binary bit for an M-input and M-output system which in effect increases the entropy of the final secret key.

It is obvious that generating a shared secret key by using current quantization method is still narrowed by certain issues. We expect and also hope in the future that quantization methods could be improved and get achievement in establishing a secret key in a short time. Figure 2 gives an illustration of key generation techniques in briefly.

Figure 2 the classification of wireless key generation base on Channel Reciprocity

3. RECONCILIATION AND PRIVACY AMPLIFICATION

Both receiver and transmitter should exploit the same quantization output based on channel reciprocity property. Due to its imperfect and random noise, a small number of mismatch bit between two outputs may be accrued. To obtain an identical final secret key. Reconciliation and privacy amplification is used to finding and correcting mismatch bit of quantization outputs. As figure 3 represents, two receivers and transmitters exchange the bits correcting information over a public channel in a reconciliation scenario. Accordingly, both devices use public channel and is therefore possible for eavesdroppers to explore part of the secret key by wiretapping the channel communication. On the other side, privacy amplification is used to eliminate shared information in increasing security and preventing an eavesdropper from learning the secret key.

Figure 3 changing the data during reconciliation within public channel

3.1 Reconciliation

Both devices should exchange certain information to get agreement on a shared key. Reconciliation is used to correct mismatch bit with a minimum amount of exchange information in a public channel. Authors in [5] represent a simple schema of reconciliation by used of [n, k, 2t+1] error-correction coed to correct mismatch bits, where n defines the length of code word, k is the length of the code and t shows the maximum number of bit errors that the code can correct. A practical way in [16] proposed during the key establishment is that both devices get agreement on random permutation to transpose their quantization output. Also permutation makes communicators able to transpose the mismatched bits. Then, both devices divide their transposition result into multiple blocks, the size of each block should be considered less than or equal to 1. At the end of this method, both devices compare their block parity. Regarding the result, agreement on the corresponding block will be achieved and they use binary search to correct the mismatch bits. The methods used in [16] is a typical way to achieve reconciliation that discloses only a small amount of bits quantized from the wireless channel.

The method in [26] achieves improvement compared to [16] by use multiple passes to correct the mismatch bits which each passes uses different block sizes and permutation. The operation of each pass is same as defined in [16].

3.2 Privacy Amplification

Last part named Privacy Amplification will be exploited after reconciliation to eliminate mismatch bits to extract shared secret key, enhance the security and amplify the difficulty for eavesdropper to guess the secret key. Authors in [6, 15, and 17] by reducing the length of secret key achieve these aim. The theory of reconciliation and privacy amplification are still unidentified in real scenario and under-explored. Authors in [6] based on different eavesdropper model assume that two terminals are able to communicate through both public and private channels. In this theory eavesdroppers can take three model into consideration, 1) An eavesdropper has complete access to the public channel
and private channel with just bit of error, 2) eavesdroppers do not have complete access to public channel but can catch an amount of information by private channel and, 3) eavesdropper can catch the public channel also private channel. Regarding to these eavesdropper models by use of a function g : (0,1)^n \rightarrow (0,1)^{\gamma}, which can extirpate the leaking information on both public and private channel by extenuating the final secret key size from n bit to r bit, where r<n.

4. FEASIBILITY, SECURITY AND NEW TECHNIQUES OF KEY EXTRACTION

Channel reciprocity, special decorrelation and key extraction rate are three factors that affect the feasibility and security of key extraction. Key generation based on correlated randomness has been noted theatrically in [7] and [13]. It is shown that two terminals through the public channel where eavesdroppers take third party can obtain a secret key with two essential component. First, channel reciprocity and second spatial decorrelation are two important component to establish a secure transmission. Authors in [23] describe and analyze how to get initial secret key based on properties of channel reciprocity. It considers K(a) and K(b) as two terminal that if K(a) and k(b) are collected together within a short time duration, channel reciprocity ensure a high correlation between K(a) and k(b) which means an increasing in k(a) will result in an increasing in K(b), in another words these two terminal can use high correlated channel estimate to achieve the initial secret key.

**TABLE 1 CONTRAST OF DIFFERENT QUANTIZATION METHODS**

<table>
<thead>
<tr>
<th>Received signal strength (RSS)</th>
<th>Frequency-phase based quantization method</th>
<th>Channel diversity based quantization method</th>
<th>Feasibility</th>
<th>Mismatch bit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Single antenna</td>
<td>Multiple antenna</td>
<td>Easy to implement</td>
<td>Use average value to reduce the impact from the channel</td>
</tr>
<tr>
<td></td>
<td>Need to send multiple frequencies</td>
<td>Need extra hardware</td>
<td>Frequency-phase estimation is not trivial</td>
<td>Use guard interval to decrease the bit mismatch</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

Second, as discussed earlier it is important to ensure that the two terminals are independent of each other with a special decorrelation. As a perspective of security, secret keys that have been obtained from different channel should be distinct with high probability. This affair makes eavesdropper binding to keep certain distance of transmitter and receiver to ensure an uncorrelated link.

Thirdly, further channel reciprocity and special decorrelation, key generation rate is very important to the security strength of secret keys. To obtain this improvement, building a fast and secure link between two terminals is required. The theory in [34] describes achievement on key generation rate relies on the channel condition. It shows that the capacity of channel between two terminals must be larger than the capacity between the eavesdropper. Table 1 shows the summary of these quantization method.

5. CONCLUSION

In this paper, we have reviewed the present research on channel reciprocity based key establishment from three angles. First and most importantly, we described the current quantization techniques, which provide initial information of wireless channel by converting the unique wireless channel features into binary bits. Also, we talked on reconciliation and privacy amplification techniques, which generate shared secret key with minimum information leakage in present of eavesdropper. Lastly, we discussed the feasibility, security issue in this research area. Table 1 shows the comparision of different quantization methods.

Regarding wireless channel characteristics such as easy implementation, low energy consumption and high reliability to generate secret key is becoming a great area for research and introduce key generation protocols seems a challenge in the future. In addition, the key generation rate and mismatch bits introduced by channel asymmetry are still an issues which should be solved.

6. REFERENCE

secure pairing using ambient wireless signals. In proceeding of ACM Mobisys, New York, NY, USA.


