A SIMPLE LOCATION DEPENDENT KEY GENERATION METHOD BASED ON MULTIPLE ANTENNA FOR SECURING WIRELESS COMMUNICATION

MONAL S TELGOTE[1], PROF. A.K.PATHRIKAR[2]

[1](PG Student Department of E&TC, Savitribai Phule Women's Engineering College Aurangabad)

[2](Assistant Professor, Department of Electronics, Savitribai Phule Women's Engineering College Aurangabad)

[1]10monal@gmail.com, [2]anand_pathrikar@rediffmail.com

ABSTRACT—*Security is an important issue in wireless communication systems as the wireless channel is unguided. Cryptographic techniques in the wired communication may be used to secure the wireless communication, but the characteristics of radio channel are not exploited efficiently. This paper proposes a simple key generation method for securing wireless communication. It assumes that each terminal is equipped with multiple antennas; the method measures the special location relation between legitimate parties exploiting the technique of time difference of arrival. On the basis of the reciprocity principle, the result obtained by the two parties is identical; hence the same location-dependent key is separately generated. Since the completely identical result is impossible in practice due to the presence of noise and interference, a robust quantization technique is hence used. Simulation results show that the proposed method is effective to generate different keys in different locations and thus guarantees the wireless communication security.*

Keywords—Securing Wireless Communications, Key Generation, Location-Dependent Key, Channel Reciprocity, Multiple Antenna

I. INTRODUCTION

The development of wireless communications and wireless networks is very rapid in recent years, varieties of wireless applications continue to emerge. However, it is more difficult to secure wireless communications than wired communications as the wireless channel is unlimited. Securing the wireless communication is an extremely important aspect almost in every wireless communications system [1]. The classical cryptography is used to secure the wired communication. Two types of cryptographic techniques are used: public key cryptography and secret key cryptography. The transmitter converts the plaintext to encrypted message using public or private keys in the application layer. However, distributed parallel computing makes the public key cryptography become unsafe. Hence, the security of private keys determines the security of the systems for the secret key cryptography.

The classical cryptographic techniques in the wired communication can also be used to secure the wireless communication, but it is not the best method because the characteristics of radio channel are not exploited efficiently. In fact, the wireless channel is different from wired channel. The response of the wired channel can be seen as ideal within the bandwidth of the wired system, which means that different communicating parties always possess the same channel characteristics. However, the wireless channel is diverse since the existence of the multi-path and Doppler Phenomena. Therefore different communicating parties in the wireless communication usually have different channel characteristics (e.g. channel state information, Received Signal Strength Indication abbreviated as RSSI etc.). In addition, it is worth emphasizing that the principle of reciprocity holds in the wireless communication systems while the Time Division Duplex (TDD) is used [2]. Perfect security in wireless communication systems can be implemented by exploiting radio channel characteristics.

There are two ways to secure the wireless communication using wireless channel properties. One way is employing antenna array to make the eavesdropper's channel vary quickly while the legitimate user receives normally, hence the eavesdropper cannot demodulate correctly and then the secure communication is achieved [3], [4]. The other way is combining the key generation with physical layer characteristics and is first presented in [5].

Cryptographic techniques are used to secure wireless channel, but it is different from the classical cryptography for that the key generation depends on the characteristics of the radio channel. The communicators separately generate the identical key based on the principle of reciprocity to avoid the transmission of the key, and hence the probability of key leakage is decreased. However, it is impossible that the communicating parties always get the identical key due to the existence of noise, interference, and the slight difference of radio channels. Therefore, the channel characteristics separately obtained by communicators must be quantized properly to increase the probability of key agreement. It is obvious that the key space, which represents the number of available key, is decreased by quantizing; hence the probability of acquiring the identical key by different communicating pairs is increased simultaneously. There is a trade-off between the key agreement probability and the security.

The interest in physical-layer key generation schemes is keep growing to secure wireless communication. A key agreement scheme with multi-level quantization based on received signal strength indication (RSSI) using a variable directional antenna was developed in [6]. The approach presented for key generation in [7] is based on detecting deep fades of signal envelopes. A key distribution method is proposed in [8] that uses the ultra wideband (UWB) channel pulse response between two transceivers as a source of common randomness for the key agreement. Recently, some works have discussed methods of using the increased randomness available when the communicating nodes have multiple antennas. Reference [9] provided the theoretical security performance bounds for the communications using multiple antennas and proposes two practical methods for generating secret keys exploiting the increased randomness.

Experimental investigation of MIMO reciprocal channel key generation is performed in [10]. In [11], a practical key generation scheme for MIMO channels based on quantization performed on the blind channel estimation is presented.

However, most existing methods do not work well because different receivers located at different positions may obtain the same key with higher probability. For example, the RSSI parameter is very rough quantization for wireless channel, thus the probability of acquiring identical key by different communicating pairs is higher. For the methods based on the channel estimation, the phase in channel parameters is more important than the magnitude due to the existence of Automatic Gain Control (AGC) in radio channel. The key space is obviously limited since the phase is cyclic.

In this paper, a simple key generation method for securing wireless communication is proposed. It assumes that each terminal is equipped with two antennas at least; the method measures the special location relation between legitimate parties exploiting the technique of time difference of arrival. On the basis of the reciprocity principle, the result obtained by the two parties is identical; hence the same location-dependent key can be separately obtained. In practice, a completely identical result is impossible due to the presence of noise and interference, a robust quantization technique is hence used.

Simulation results show that the proposed method is effective to generate different keys in different locations and thus guarantees the wireless communication security.

II. The Proposed Method

In this section, the proposed method is described in details. For simplicity, it assumes that each node is equipped with two antennas shared one local oscillator, as shown in Figure 1. The symbols A1 and A2 denoted respectively the 1st and 2nd antenna of Alice, B1 and B2 are same as A1 and A2. The symbol1, 1 AB d is used to represent the electromagnetic wave propagation distance between A1 and B1, which includes the equivalent distance that generated by the delay of the transceiver channel and the process delay of the transceiver.

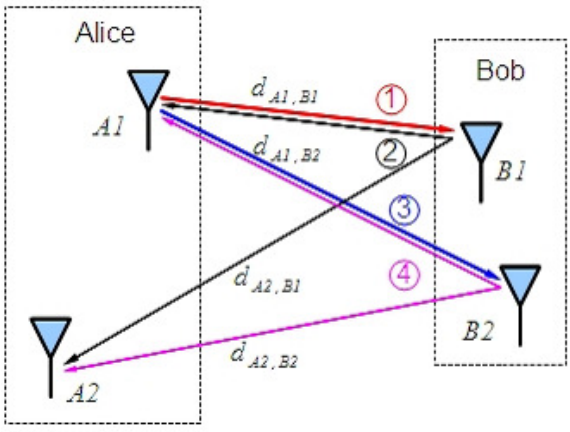

Figure 1.System Model

A. Obtaining identical channel characteristics separately

The entire procedure for key generation consists of four time slots, each slot contains three stages. The duration of this procedure should be less than or equal to the coherent time of the channel because of the channel reciprocity is required. The operations in every slot are the same except the antennas playing different roles. Therefore, only

the first slot is described in details, the remaining slots are same as slot 1. In addition, it assumes that there is no noise and interference for describing simplicity.

At the first stage in slot 1, Alice starts a timer at first, and then transmits a reference signal from the antenna A1.

$S(t)=cos(2\prod ft)$ (1)

Alice's antennas A1 and A2 switch to receive state when the reference signal has been transmitted. The antenna B1 waits for the reference signal.

At the second stage in slot 1, the antenna B1 receives the reference signal using the technique of correlation detection. The antenna B1 switches to transmit state after the reference signal is received, and transmits the same reference signal.

At the third stage in slot 1, the Alice's Antennas A1 and A2 received the reference signal that transmitted by B1. By measuring the time difference of the reference signal arriving at A1 and A2, Alice can get the distance difference as shown in equation (2) since A1 and A2 shared the same local oscillator. The technique is so-called time difference of arrival (TDOA) [12].

$\mathbf{D}\text{ali\_dif1} = \boldsymbol{d}_{A1,B1} - \boldsymbol{d}_{B1,A2}$ (2)

When A2 received the reference, Alice stops the timer, and can compute the summation of distance using the elapsed time as follows.

$\mathbf{D}\text{ali\_sum1} = \boldsymbol{d}_{A1,B1} + \boldsymbol{d}_{B1,A2}$ (3)

$\mathbf{D}_{\text{ali\_dif1}}$,$\mathbf{D}_{\text{ali\_sum1}}$ denotes the first distance difference and summation that Alice obtained respectively.

The operations in slot 2 is similar to slot 1, the only difference is the antenna B1 is substituted with the antenna B2.Therefore, Alice can get the second distance difference and summation as follows:

$\mathbf{D}\text{ali\_dif2} = \boldsymbol{d}_{A1,B2} - \boldsymbol{d}_{B2,A2}$ (4)

$\mathbf{D}\text{ali\_sum2} = \boldsymbol{d}_{A1,B1} + \boldsymbol{d}_{B1,A2}$ (5)

As same as Alice, Bob also can get the similar distance differences and summations through slot 3 and slot 4, as shown in the equations (6)~(9).

$\mathbf{D}\text{bob\_dif1} = \boldsymbol{d}_{A1,B1} - \boldsymbol{d}_{B1,A2}$ (6)

$\mathbf{D}\text{bob\_sum1} = \boldsymbol{d}_{A1,B1} + \boldsymbol{d}_{B1,A2}$ (7)

$\mathbf{D}\text{bob\_dif2} = \boldsymbol{d}_{A1,B2} - \boldsymbol{d}_{B2,A2}$ (8)

$\mathbf{D}\text{bob\_sum2} = \boldsymbol{d}_{A1,B1} + \boldsymbol{d}_{B1,A2}$ (9)

Alice sums the two distance summations and gets

$D_{ali\_sum} = D_{ali\_sum1} + D_{ali\_sum2}$ (10)

$= d_{B1,A1} + d_{B1,A2} + d_{B2,A1} + d_{B2,A2}$ (11)

The first distance difference minus the second one, Alice has

$\mathbf{D}\text{ali\_dif} = \left| \mathbf{D}\text{ali\_dif1} - \mathbf{D}\text{ali\_dif2} \right|$ (12)

$= \left| \boldsymbol{d}_{A1,B1} - \boldsymbol{d}_{B1,A2} - (\boldsymbol{d}_{A1,B2} - \boldsymbol{d}_{B2,A2}) \right|$ (13)

Similarly, Bob can get

$D_{bob\_sum} = D_{bob\_sum1} + D_{bob\_sum2}$ (14)

$= d_{B1,A1} + d_{B1,A2} + d_{B2,A1} + d_{B2,A2}$ (15)

If the inconsistency of RF circuits between different transceivers can be neglected, then $\boldsymbol{d}_{A1,B1} = \boldsymbol{d}_{A1,B2}$, $\boldsymbol{d}_{A1,B2} = \boldsymbol{d}_{A1,B2}$, etc. hold. Thus we have

$D_{ali\_sum} = D_{bob\_sum} \approx D_{bob}$ (16)

$D_{ali\_dif} = D_{bob\_dif} \approx D_{dif}$ (17)

The distance summation denoted by sum D and the distance difference denoted by dif D can be separately obtained by Alice and Bob. Hence, the identical keying variables are acquired by the communicating pairs without transmission. It should be noted that the distance summation and difference are dependent with the special location relation between Alice and Bob. Thus, the key is location-dependent.

B. Quantization and consistency test

However, it is impossible that the communicating parties always get the identical key due to the existence of noise, interference, and the slight difference of RF channels. Therefore, the channel characteristics separately obtained by communicators must be quantized properly to increase the probability of key agreement. Many a quantization method have been presented in many papers. A simple quantization method is used in this paper.

A ruler as a basic unit is properly selected to measure the distance summation and difference. The ruler size is dependent with the communication system. The simulation in this paper employs the wavelength of the reference signal as the ruler. We use the ruler to divide the distance summation and the distance difference. The quotients are used as the keys.

If the remainder is greater than 0.75, the corresponding quotient increased by one. Thus the keys generated. Since Alice and Bob don't know if the generated keys are identical, a consistency test method is necessary. Alice generates an original random sequence with cyclic redundancy check (CRC), then encrypts the sequence with its keys and transmits the encrypted sequence. Bob gets the random sequence using its keys. The generated keys are identical if CRC passed.

Iii.Problems Of Implementation

Some problems of implementation are discussed in this section.

A. Key Space

The complexity of the key obtained using the method in section II is not enough. The complexity can be increased by employing the following methods.

1) Spatial method: If the communicators are with more antennas, then we can increase the complexity of the key by using the method repeatedly for different antenna pairs.

2) Frequency method: If the bandwidth of communication system is greater than the coherent bandwidth of the channel, then we can increase the complexity of the key by using the method repeatedly with different reference signal frequency.

3) Temporal method: We can use the method repeatedly at different time, as long as the time interval between two successive measurements is greater than the coherent time of the channel.

4) Mobility: The movement of the communicating parties results in the varied location, then the generated keys are different.

B. Environmental effects: LOS , NLOS and multi-path

Non-light-of-sight (NLOS) environment makes the eavesdroppers have no chance to guess the keys by existing positioning methods.

In the light-of-sight (LOS) environment, the generated keys are monotonous, thus the possibility of crack is increased In order to solve this problem, we can make diversification by introducing artificial delays.

The reference signal is a sine signal; the linear combination of different paths still is a sine signal with the same frequency. Hence, the method of correlation detection is still available. If the multi-paths are separable, then the first arrival is detected.

Iv. Simulation Results

In order to test the method in this paper, two simulation experiments are performed using MATLAB. One is for testing the key agreement probability between the legitimate parties, the other is for test the key agreement probability between the different communicating pairs. The communicators are located in an area of 60 times 45 square meters, as shown in Figure 2. The locations of Alice's antennas are random located at the area of []25, 35 [0, 5] ×.Bob's antennas must locate in an area of 1 times 1 square meters.

In experiment 1, Alice's position is fixed and Bob randomly chooses a location within the experimental range. The simulation is performed in Gaussian channel and the range of signal-to-noise ratios (SNR) are 1-20dB. 50000 simulations are performed at each SNR.

In experiment 2, Alice and Bob's positions are fixed as in Figure 2. Another user named Eve randomly chooses a location within the experimental range. At each SNR, Eve locates at 50000 different positions. Then, the probability of key agreement between Bob and Eve is tested.

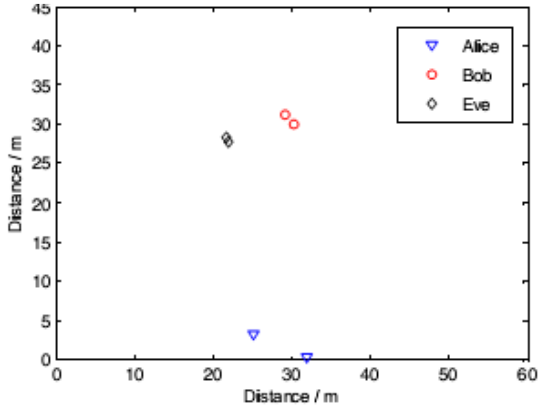

Figure 2.Experimental Scenarios

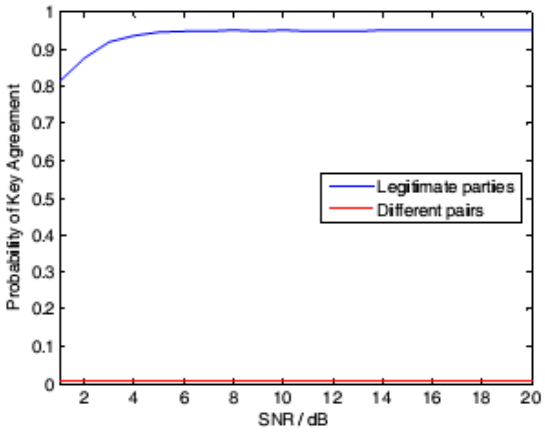

Figure 3.Experimental result

The simulation results are showed in Figure 3. The probability of key agreement between communicating parties is higher enough. The probability is greater than 94% when the SNR is equal or greater than 5dB. While the probability of key agreement between different communicating pairs is very low, it's always less than 1%.

V.CONCLUSIONS

In this paper, a simple location-dependent key generation method for securing wireless communication with multiple antennas is proposed. The method measures the special location relation

between legitimate parties. Based on the reciprocity principle, the same location-dependent key can be separately obtained by legitimate parties. Simulation results show that the proposed method is effective to generate different keys in different locations and thus guarantees the wireless communication security.

There are many aspects need to investigate, such as quantization method, the design of the reference signal, the key generation in LOS environment and the field experiments.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China (Grant No. 60772095, 60971113, 61071125, and 61071216) and the Foundation for Innovative Research Groups of the National Natural Science Foundation of China (Grant No. 60921003).

REFERENCES

[1] M Shin, J Ma, A Mishra, et al., "Wireless network security and interworking," Proceeding of the IEEE, vol. 94, no. 2, pp. 455-466, Feb. 2006.

[2] J. G. Proakis, Digital Communications, 3rd ed., New York, USA: McGraw-Hill, 2000.

[3] X. Li, J. Hwu, E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," Journal of Communications, vol. 2, no. 3, pp. 24-32, Mar. 2007.

[4] P. Mu, Q. Yin, W. Wang, "A security method of physical layer transmission using random antenna arrays in wireless communication," Journal of Xi'an Jiaotong University, Vol. 44, No. 6, pp. 62-66, Jun. 2010.

[5] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable Communications, vol. 43, no. 1, pp. 3-6, Jan. 1995.

[6] S. Yasukawa, H. Iwai, and H. Sasaoka, "A secret key agreement scheme with multi-level quantization and parity check using fluctuation of radio channel property," in Proc. ISIT'08, 2008, p. 732.

[7] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, et al., "Robust key generation from signal envelopes in wireless networks," in Proc. ACM CCS '07, 2007, p 401.

[8] R. Wilson, D. Tse and R. A. Scholtz,, "Channel identification: secret sharing using reciprocity in ultrawide band channels," IEEE Transactions on Information Forensics and Security, vol. 2, no. 3, pp. 364 -375, Sep. 2007.

[9] J. W. Wallace, C. Chen, and M. A. Jessen, "Key generation exploiting MIMO channel evolution: algorithms and theoretical limits," inProc. EuCAP'09, 2009, p. 1499.

[10] J. W. Wallace and R. K. Sharma, "Experimental investigation of MIMO Reciprocal Channel Key Generation," inProc. ICC'10, 2010, p.1.

[11] S. S. Shetty and R. P. Ramachandran, "Blind channel estimation based robust physical layer key generation in MIMO networks," inProc. ISCAS'10, 2010, p.2522.

[12] R. O. Schmidt, "A new approach to geometry of range difference location," IEEE Transactions on Aerospace and Electronic Systems,vol. AES-8, no. 6, pp. 821-835, Nov. 1972.

.