Research on Quantization Scheme in the Secret Key Extraction from Received Signal Strength

Chengzhi Yang, Ting Jiang

Beijing University of Posts and Telecommunications, Beijing, China

Beijing University of Posts and Telecommunications, Beijing, China

chengzhiyang@bupt.edu.cn,tingjiang1956@163.com

Keywords: secret key generation, quantization, RSS.

Abstract. In order to find an effective secret key generation scheme in wireless networks, many based on received signal strength methods have been proposed. However, the secret bit rates of existing schemes are relatively low. To resolve the problem of low generation rate, a vector quantization scheme is proposed in this paper where channel measurements are reused and every measurement can be quantified into two bits without increasing mismatching rate. Performance simulation results show that our proposed scheme improves the key generation rate almost twice at high entropy in comparison to the traditional schemes. At the same time, our scheme passes the randomness tests of the NIST test suite.

1. Introduction

Due to the open and shared nature of the wireless channels, a third-party eavesdropper can easily hear the message transmitted between two legitimate parties[1]. To ensure the safety and efficiency of the communication, secret key must be established to encrypt the message transmitted. Currently, many key generation methods exploring physical layer information have attracted intense research interest [2]. Received signal strength (RSS) is a very popular statistic of the wireless channel and can be used as the source of secret bits shared between a transmitter and receiver [3].Existing RSS-based quantization schemes have been extensively discussed in [4]. The typical quantization schemes include Aono et al.'s single threshold quantization algorithm [5], Mathur et al.'s two thresholds quantization algorithm [6], Jana et al.'s Adaptive Secret Bit Generation [7]. Aono et al.'s quantizer uses the median value of the RSS measurements as a threshold and drops any measurements that are close to the median value, which is suitable for the scheme of channel feature with deep fading [8] However, the method has high bit mismatch rates and low entropy. There is a modified version of this method in [6] namely Mathur's, where it drops the samples with RSS values that are less than q^- and greater than q^+, q^- is lower threshold and q^+ is upper threshold, it can effectively reduce the mismatching rate of key generation. But with more measurements are abandoned, the secret bit rate become lower. Based on Mathur's scheme, Jana et al.'s scheme named as Adaptive Secret Bit Generation (ASBG) [3, 7] uses a modified version of Mathur's quantizer in conjunction with two well-known information reconciliation [9,10]and privacy amplification techniques[11]. They extract multiple bits from a single RSS measurement. The bit rate become much higher after being quantified, however, it brings higher mismatching rate and as information reconciliation is a probabilistic technique, it might fail occasionally. In summary, the existing schemes that based on RSS values cannot generate secret bits at a high rate with low mismatching rate.

In this paper, a vector quantization method is proposed, it is based on Mathur's secret key extraction approaches and by reusing RSS measurements, which can greatly improve the bit rate at high entropy and keep low mismatch rate compared with existing quantization methods.

The rest of the paper is arranged as follows: Section 2 we describe the system model. Description and block diagram of vector quantization is provided in Section 3. In Section 4, the performance of the proposed method is analyzed, and Section 5 concludes the paper.

2. System Model

2.1 Channel Model

A typical physical layer key generation scenario is shown in Fig. 1. It contains three nodes: the communication pairs and an attacker. To simply the analysis, we assume Alice and Bob represent legitimate users, while Eve is on behalf of a potential adversary.

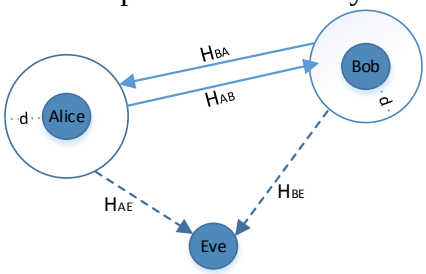

Fig. 1. A typical physical layer key generation scenario

To distinguish between the channel parameter of interest, and its value at a given time, we define the parameter by **h** and refer to its value as $h(t)$. To measure the parameter **h**, Alice and Bob must send known probe signals to Bob. Each party can then use the received signal along with the probe signal to compute an estimate $\hat{h}$ of **h**. However, typical commercial wireless transceivers are half duplex, i.e., they cannot both transmit and receive the signals simultaneously Thus, Alice and Bob must measure the radio channel in one direction at a time. As long as the time between two directional channel measurements is much smaller than the rate of change of the channel, Alice and Bob will have similar received signal. The received signal at Alice and Bob can be expressed as:

$$y_B(t) = x(t)h_{AB}(t) + n_{AB}(t) \quad (1)$$

$$y_A(t) = x(t)h_{BA}(t) + n_{BA}(t) \quad (2)$$

Where $x(t)$ is the known probe signal, n_{BA} and n_{AB} are the independent noise processes at Alice and Bob. Alice and Bob use the received signal to compute estimates of the channels, $\hat{h}_{AB}$ and $\hat{h}_{BA}$:

$$\hat{h}_{AB}(t) = h_{AB}(t) + z_{AB}(t) \quad (3)$$

$$\hat{h}_{BA}(t) = h_{BA}(t) + z_{BA}(t) \quad (4)$$

Where z_{AB} and z_{BA} represent the noise terms due to n_{BA} and n_{AB} after processing by the function that estimates **h**. However they can be highly correlated if Alice and Bob send probes to one another at a fast enough rate, Although Eve can overhear the probe signals sent by each user, the signals received by her are completely different:

$$y_{EA}(t) = x(t)h_{AE}(t) + n_{AE}(t) \quad (5)$$

$$y_{EB}(t) = x(t)h_{BE}(t) + n_{BE}(t) \quad (6)$$

Where h_{BE} denotes the channel between Bob and Eve. h_{AE} denotes the channel between Alice and Eve. According to communication theory, an entity that is at least $\lambda/2$ away from the network nodes experiences the fading statistically independent of the fading between the communicating nodes [2]. Therefore, despite possessing knowledge of the probe signal $x(t)$, Eve cannot use the received signals to compute meaningful channel estimates between Alice and Bob.

3. The Proposed Quantization Scheme

Because the channel estimates computed by Alice and Bob are consecutive random variables, it is necessary to quantize their respective sequences of channel estimates into same bit strings which is suitable as cryptographic keys. In this section, a vector quantization scheme is proposed to generate high-rate secret key.

3.1 Vector Quantization(VQ)

We assume that Alice and Bob get the sequence of RSS measurements R_a and R_b. The sequence length of RSS measurements is N, $R_a = [R_a[1], R_a[2], ..., R_a[N]]$ and $R_b = [R_b[1], R_b[2], ..., R_b[N]]$. $R_a[i]$ and $R_b[i]$ represent the i^{th} RSS measurement that Alice and Bob get from wireless channel, respectively. Alice and Bob calculate two adaptive thresholds q^+ and q^- independently such that: $q^+ = mean + a * std\_deviation$, $q^- = mean - a * std\_deviation$ Where $0 < a < 1$, a is an adjustable parameter for quantization. Alice and Bob exchange their sequence of RSS measurements through level-crossing algorithm and only keep the ones that they both decide not to drop. Level-crossing algorithm will be described later. We presume the remained list RSS measurements constitute a new sequence of RSS measurements $R_a' = [R_a'[1], R_a'[2], ..., R_a'[n]]$ and $R_b' = [R_b'[1], R_b'[2], ..., R_b'[n]]$ $(n \le N)$. We define:

$$
\begin{aligned}
V_a &= \{V_a[1], V_a[2], ..., V_a[n]\} \\
&= \{(R_a'[1], R_a'[1+delta]), (R_a'[2], R_a'[2+delta]), ..., (R_a'[n-delta], R_a'[n]), \\
&\quad (R_a'[n-delta+1], R_a'[1]), ..., (R_a'[n], R_a'[delta])\}
\end{aligned} \tag{7}
$$

$V_a[i] = (R_a'[i]\ R_a'[(i+delta)\%n])$, $1 \le i \le n$. $V_a[i]$ is a vector consists of two RSS measurements $R_a'[i]$ and $R_a'[(i+delta)\%n]$. $delta$ represents the index interval of two chosen measured values. We define the interval between $R_a'[(i+delta)\%n]$ and $R_a'[i]$ is t_g. $R_a'[(i+delta)\%n]$ is lagged to $R_a'[i]$ within an interval $[t_l, t_u]$. $[t_l, t_u]$ should follow principles as follows that t_l is larger than the channel coherence time to protect the variation is unpredictable and contains reasonable entropy, t_u should not be too large, otherwise, the large scale path loss may dominate the variation, which may lead to the variation to be predictable. If we set the interval t_g then $delta$ will be decided. The vector quantizer can be descripted as follows:

$$
Q(R'_a[i]) = Q(V_a[i]) = \begin{cases} 11 & R_a'[i] > q^+, R_a'[(i+delta)\%n] > q^+ \\ 10 & R_a'[i] < q^-, R_a'[(i+delta)\%n] > q^+ \\ 00 & R_a'[i] > q^+, R_a'[(i+delta)\%n] < q^- \\ 01 & R_a'[i] < q^-, R_a'[(i+delta)\%n] < q^- \end{cases}, \tag{8}
$$

In Mathur's quantizer, Alice and Bob extract a 1or a 0 for each RSS estimate if the estimate lies above q^+ or below q^-, respectively. But now, our scheme quantify every measurement into two bits(11,10,00 or 01) without decreasing the randomness of secret key by using two random RSS measurements. i.e $R_a'[i] > q^+$, $R_a'[(i+delta)\%n] > q^+$ the quantization result of $R_a'[i]$ is 11 while in Mathur's scheme just one bit as 1. The advantage of the proposed vector quantization is that we can make full use of RSS measurements. In the best case, the proposed modified quantizer can improve bit rates as much as two times than existing schemes.

Table 1 Quantization Symbols And Meaning

symbols	meaning
R_a R_b	RSS measurements from channel
$mean$	mean value of RSS measurements
$std\_deviation$	standard deviation of RSS measurements
a	adjustable parameter for quantization
$delta$	The interval of two measured values for each vectors
$Q(\cdot)$	Quantizer

Table 1 describes the symbols used in vector quantization and the meaning of the symbols.

3.2 Level-crossing Algorithm

We now descript the level-crossing algorithm in details. At the first, it is assumed that the length of R_a and R_b is N .The purpose of the algorithm is to keep the measurements that Alice and Bob both decide not to drop and finally can generate cryptographic keys K_a and K_b $(K_a = K_b)$ .The procedure consists of the following steps:

- Step 1: Alice parse her RSS measurements R_a and drop RSS estimates that lie between q^+ and q^-, and maintain a list of indices to track the remained RSS estimates in the form of an array of indexes $L = \{l_1, l_2, \ldots, l_n\}$ .e.g. if $R_a[1] > q^+, q^- < R_a[2] < q^+, R_a[3] < q^-, \ldots.$ then $L = \{1, 3, \ldots\}$.
- Step 2: Alice finds the indexes in L where m or more successive RSS measurements above q^+ or below q^- and sends Bob the index of the RSS estimate lying the center of the excursion, as a List L' .e.g. $R_a(i) > q^+$ or $R_a(i) < q^-$ for some $i = i_{begin}, i_{begin+1}, \ldots, i_{end}$,then Alice sends Bob the index $i_{center} = \frac{i_{begin} + i_{end}}{2}$. m is a parameter that we can set by ourselves.
- Step 3: Alice sends the random subset of L' to Bob and for each index in L' ,Bob checks R_b whether contains at least $m-1$ RSS measurements above q^+ or below q^- centered around the index .if not, Bob will drop the index and only keep the indexes that has more than $m-1$ RSS measurements above q^+ or below q^- centered around it. The remained L' will be sent as a list $\hat{L}$ to Alice. i.e. for each index $\{l - \frac{m-2}{2}, \ldots, l + \frac{m-2}{2}\}$,whether $R_b[i] > q^+$ or $< q^-$, $l \in L'$.
- Step 4: Alice and Bob compute $Q(R_a)$ and $Q(R_b)$ respectively at each index in $\hat{L}$ as secret bits. Namely K_a and K_b.

4. Performance Evaluation

4.1 Simulation Parameters

In this section, the performance of the proposed vector quantization scheme is numerically analyzed by comparing with two existing secret key generation schemes in terms of secret bit rate and bit mismatch rate. Then, randomness of proposed vector quantization is tested. In Aono et al.'s method, a configurable parameter β is chosen and almost ten percent of the RSS measurements are abandoned. In Mathur et al.'s scheme, we choose α =0.2, $m = 2$ to ensure that most of measurements are used for bit extraction. Proposed vector quantization scheme chooses α =0.3, delta=10, $m = 3$ to keep a balance between the algorithm mismatch rate and secret bit rate. Other simulation parameters are listed in Table 2.

Table 2 Simulation Setup

Parameter	Value
Sampling time(T_s)	0.357us
Fading	Rayleigh
Doppler spectrum	Jakes
Carrier frequency(f_c)	2.4GHz
Coherence time (Tc)	3.75ms
Average path gain	-2dB

4.2 Experimental Results

The quality of the proposed method measured in terms of three metrics: secret bit rate, bit mismatch rate and entropy (randomness).

*Performance of Secret Bit Rate***:** Fig 2 shows the secret bit rate with signal-to-noise ratio (SNR). It can be clearly seen that the bit rates of vector quantization are always above 1 and almost two times greater than other two schemes' bit rates. The reason is that, in vector quantization, every measurement is quantified into two bits while the RSS measurements in Mathur's and Aono's quantization schemes are just a signal bit.

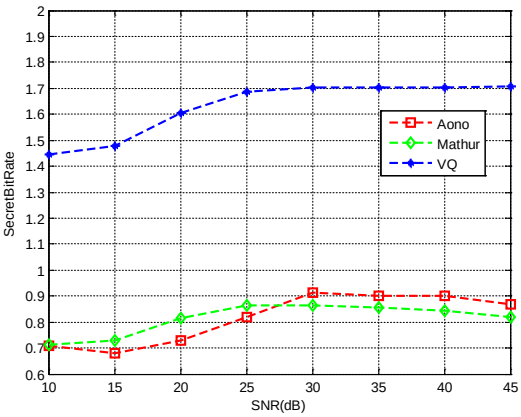

Fig. 2. Secret bit rate of Mathur's scheme, Aono's scheme and VQ

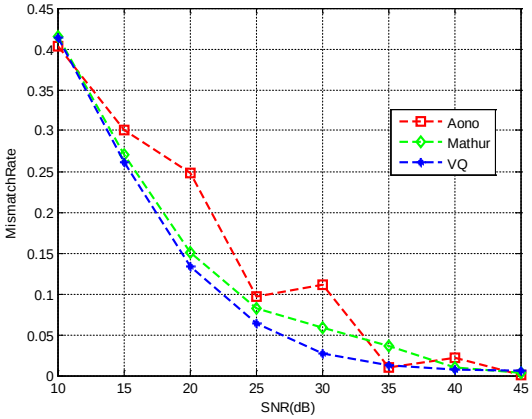

Fig.3. Bit mismatch rate of Mathur's scheme Aono's scheme and VQ

Performance of Key Bit Mismatch Rate: The bit mismatch rate is shown in Fig 3. The mismatch rate between vector quantization and Mathur's scheme is slightly different. It proves that the bit error is kept low in our scheme. On the other hand, Aono's scheme achieves the highest mismatch rate as some of measurements are too close to quantified threshold. In fact, vector quantization can always find a secret key for the SNRs larger than 40 dB.

Entropy(Randomness Test):

Table 3 the NIST Statistical Test Suite Result of VQ

Parameter	P-value
Frequency	0.74
Block Frequency	0.53
Cumulative sums (Rev)	0.69
Cumulative sums(Fwd)	0.36
Runs	0.35
Longest run of ones	0.74
FFT	0.4
Approx. Entropy	0.55
Serial	0.53,0.43

In this test, the SNR is fixed in 25 dB. To pass a randomness test, the p-value for that test must be greater than 0.01. It is clear that our scheme can pass the randomness tests of the NIST test suite [12]. We undertake 20 tests and find the entropy of vector quantization is high ranging from 0.954 to 0.999.

5. Conclusions

In order to increase the secret bit generation rate from the received signal strength (RSS), a vector quantization scheme has been developed in this paper. Through making full use of RSS measurements, our scheme improves the key generation rate almost twice at high entropy without increasing the mismatching rate compared with the existing ones.

For future work, we intend to test our scheme in different real environment scenarios, and use Channel Impulse Response (CIR) as the measurement of the wireless channel characteristic to improve the accuracy of measurement.

Acknowledgments

This work was supported by National Science Foundation of China (61171176).The authors would like to thank the anonymous reviewers for their thoughtful and constructive remarks that are helpful to improve the quality of this paper.

References

[1]. Limmanee A, Henkel W (2010) Secure physical-layer key generation protocol and key encoding in wireless communications. GLOBECOM Workshops IEEE: 94-98

[2]. Ren K, Su H, Wang Q (2011) Secret key generation exploiting channel characteristics in wireless communications. Wireless Communications IEEE 18(4): 6-12

[3]. Premnath S N, Jana S, Croft J, et al. Secret key extraction from wireless signal strength in real environments[J]. Mobile Computing, IEEE Transactions on, 2013, 12(5): 917-930.

[4]. Guillaume R, Mueller A, Zenger C T, et al. Fair comparison and evaluation of quantization schemes for phy-based key generation[C]//OFDM 2014; 18th International OFDM Workshop 2014 (InOWo'14); Proceedings of. VDE, 2014: 1-5.

[5]. T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. IEEE Transactions on Antennas and Propagation,53(11):3776–3784, Nov. 2005.

[6]. S. Mathur, W. Trappe, N. B. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In ACM MOBICOM Conference, Sept. 2008.

[7]. Jana S, Premnath S N, Clark M, et al. On the effectiveness of secret key extraction from wireless signal strength in real environments[C]. In: Proceedings of the 15th Annual International Conference on Mobile Computing and Networking. ACM,2009: 321–332.

[8]. Babak A, Alejandra M, Bulent Y et al (2007) Robust key generation from signal envelopes in wireless networks. Proceedings of the 14th ACM conference on Computer and communications security. ACM:401-410.

[9]. Gilles B, Louis S (1994) Secret key reconciliation by public discussion. Lecture Notes in Computer Science 765: 410–423.

[10]. G. Brassard and L. Salvail. Secret key reconciliation by public discussion.Lecture Notes in Computer Science,765:410–423, 1994.

[11]. R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. InSTOC, 1989.

[12]. NIST. A statistical test suite for random and pseudorandom number generators for cryptographic applications, 2001.