A Novel Physical Channel Characteristics-based Channel Hopping Scheme for Jamming-resistant in Wireless Communication

Qiuhua Wang*[1], Hongxia Zhang[2], Qiuyun Lyu[1], Xiaojun Wang[1], And Jianrong Bao[3]

(Corresponding author: Qiuhua Wang)

School of Cyberspace, Hangzhou Dianzi University[1]
School of Communication Engineering, Hangzhou Dianzi University[2]
School of Information Engineering, Hangzhou Dianzi University[3]
No. 1158, 2nd Street, Jianggan District, Hangzhou 310018, P.R.China
(Email: wangqiuhua@hdu.edu.cn)

(Received Nov. 30, 2016; revised and accepted Mar. 11, 2017)

Abstract

Jamming is an effective denial-of-service (DoS) attack in wireless networks due to the open nature of radio propagation. In Jamming attack, the attacker purposely emits radio signals to corrupt the ongoing communication between the legitimate transmitter and receiver. Channel hopping is a feasible link-layer method for preventing jamming attack in wireless communications. In this paper, we propose a novel channel hopping scheme for jamming-resistant in wireless communication. In our proposed scheme, we explore the reciprocity, randomness and spatial uncorrelation of the wireless fading channel to generate random channel hopping sequences. We evaluate our channel hopping scheme through real-world experiments on 802.11a 5 GHz band. Experiment results show that our scheme is efficient and secure, and achieves higher channel agreement ratio with almost equally channel distribution.

Keywords: Channel Hopping; Channel Reciprocity; Jamming Attack; Quantization

1 Introduction

As wireless networks become increasingly popular, the security and reliability issues attract more and more attentions. Due to the broadcast and open nature of radio propagation, wireless networks are not only vulnerable to traditional attacks such as eavesdropping but also to jamming attacks [24]. Jamming is a very effective denial-of-service (DoS) attack, in which the attacker purposely emits radio signals to corrupt the ongoing communication between a pair of legitimate users [15, 28]. Jamming resistance is crucial for secure and reliable wireless communication.

The dominantly used approach to cope with jamming attacks is to employ physical layer techniques such as Direct Sequence Spread Spectrum (DSSS) [1] and Frequency Hopping Spread Spectrum (FHSS) [19]. These techniques use identical spreading codes or frequency hopping sequences known to both the sender and the receiver but unknown to jammers to achieve anti-jamming capability. To do this, both the sender and the receiver need to share secret keys (such as spreading codes in DSSS or frequency hopping sequences in FHSS) beforehand and keep them secret [3]. However, those spread spectrum techniques employ sophisticated physical-layer, which require more advanced and expensive transceivers and cannot be employed in most commodity wireless networks. Moreover, although the Frequency Hopping was available in the original 802.11 standard, it was not incorporated into the subsequent, more popular 802.11a, b and g protocols [16].

An alternative easy-performed method for anti-jamming is channel hopping (also known as channel surfing), in which legitimate transceivers quickly switch their communication channels to avoid jamming from attackers [8, 20, 23, 25].

The idea of channel hopping is motivated by frequency hopping. Channel hopping is similar to frequency hopping in that both of them change frequency during the communication. However, the difference between them is that, FHSS, unlike channel hopping, requires specialized antennas for transmitting and receiving signals. Channel hopping is a link-layer technology, it is much more feasible and easily used than FHSS and can be applied to the existing wireless devices without frequency hopping features [20]. Since there are multiple channels are available for next hopping, the key concern for channel hopping is to achieve the same channel selection between legitimate users.

Similar to FHSS, channel hopping also relies on a secret key shared by sender and receiver to control the channel selection. This secret key enables the communication parties to switch channels such that their transmission becomes unpredictable for a third party, thus reducing the probability of jamming. Without such a shared secret, it is impossible to establish effective anti-jamming communication between sender and receiver.

Until now, the requirement of shared keys has been fulfilled by out-of-band key pre-distribution on the devices. However, this approach suffers from scalability constraints in environments where a large number of users potentially take part in a pairwise communication, and may not even be feasible in highly dynamic network environments such as mobile ad hoc networks where two arbitrary parties usually do not have pre-shared secrets and they have to talk to each other beforehand to decide the channel switching sequence. Moreover, an attacker can compromise the pre-shared key and then jams the network. When those happen, the communication parties will have to agree on a new secret key in an ad-hoc manner using the wireless channel.

All these observations lead to the following challenge: How can two users that do not pre-share any secret key achieve the channel hopping agreement securely over a wireless channel in the presence of a jammer? Only when two legitimate transceivers select the same channel at each time slot can they successfully communicate.

Some research works resort to Diffie-Hellman key agreement algorithm or public key encryption (e.g RSA) to establish a shared secret key over an insecure channel. However, unfortunately, all these schemes share some common limitations: (1) They have to split each DH/RSA message into multiple packets at the sender and reassemble them into meaningful DH/RSA messages at the receiver due to the constraint of wireless network packet size. This takes a long time (and sometimes is impossible) for these schemes to finish a DH/RSA key establishment in presence of jammers [9]. (2) Such methods consume significant amount of computing resources and power which might not be available in certain scenarios (e.g., wireless sensor networks). (3) More importantly, since they are based on the hardness of a mathematical problem, they are only computational secure.

Recently, exploiting wireless channel characteristics (e.g reciprocity, randomness and spatial uncorrelation) to generate a shared secret key between two legitimate users has become a promising technique for its high reliability, easy implementation, and low energy consumption [26]. It provides an excellent approach to the problem of key-establishment and can even achieve information theoretical secrecy [14]. However, almost all of these schemes need extra information reconciliation to correct the quantized bit errors between two parties [21]. If we try to adopt these approaches for channel hopping purpose directly, the extra communication overheads are considerable because information reconciliation needs many rounds information exchange and should be performed each time the channel switches. As a result, it will take a long time (and sometimes it may be impossible) for these schemes to finish information reconciliation in the presence of jammers.

In this paper, we propose a novel channel hopping scheme based on wireless channel characteristics which is effective and energy-efficient. Our method makes use of the inherent reciprocity, randomness and spatial uncorrelation of wireless fading channel. In typical wireless network environments, the wireless channel between two users, Alice and Bob, is reciprocal and varies randomly over time and space. Alice and Bob can measure some wireless channel characteristics (such as received signal strength indicator (RSSI) [4, 6, 10, 11, 14, 17], amplitude [13, 22] and phase [5, 12]. The channel reciprocity theory demonstrates that bidirectional wireless channel characteristics should be identical between two transceivers within the channel coherence time. We can use these measurements as shared random secrets to achieve the channel selection agreement.

In our approach, the information reconciliation procedure is eliminated, which greatly reduces the communication overheads and time cost. Therefore, our method is more energy efficient. Our approach only needs one-time extra information exchange which happens in the quantization phase.

Furthermore, due to the spatial uncorrelation of wireless channel, as long as the jamming attacker, Eve, is more than a half-wave-length away from Alice and Bob, the channel measurements she obtains will be independent to that between the legitimate ones. This means that the attacker can obtain no information about the channel characteristics between legitimate communicators because she experiences independent fading [2] and thus cannot measure the same channel characteristics as Alice and Bob [14]. To this extent, our channel hopping method provides a strong security.

We also conduct real-testbed experiments to evaluate our approach. The results show that with least information exchange, we can achieve a channel agreement ratio higher than 95 % and even 100%.

The rest of this paper is organized as follows. Section 2 introduces the network and adversary model used in our proposed scheme. Section 3 provides the detailed description of our proposed channel hopping scheme. Section 4 presents the experiment results and performance analysis. Finally, we conclude the paper in Section 5.

2 Network and Attack Model

We now outline the basic wireless network and jamming attack model that we use throughout this paper.

2.1 Network Model

Here we consider an ubiqitous Alice-Bob-Eve wireless communication scenario in Figure 1, in which Alice, Bob and Eve are geographically located at different positions. The legitimate users, Alice and Bob, want to transmit messages via wireless channel. An jamming-attacker, Eve, tries to jam the communication between Alice and Bob by sending random packets (or noise). Both Alice and Bob have multiple transducers that allow them to work on multiple channels. In our setting, Alice and Bob each sends data and ACK packets through the wireless channel from which they respectively measure the channel characteristic and construct the channel measurements, denoted by h_{ab} and h_{ba}. Due to the channel reciprocity, we have $h_{ab} \approx h_{ba}$ when they are conducted during the channel coherence time. Eve can estimate her channel to Alice or Bob, however, if Eve is more than λ / 2 (λ is the wavelength) away from Alice and Bob, she will experience independent channel variations, hence, her observations h_{ae} and h_{be} are sufficiently uncorrelated with h_{ab} and h_{ba} due to the spatial variations, e.g., $h_{ae} \neq h_{ab}$ and $h_{be} \neq h_{ba}$ [2].

If Alice and Bob communicate on a fixed channel, Eve, could identify the channel used for communication and then start to jam it indefinitely. Clearly, if the legitimates wish to continue communication, they must hop to a new channel. Let l represent the number of channels that can be utilized between legitimate users. For instance, l =12 in 802.11a when only non-overlapping channels are used for communication. The legitimate users may change channels over time. When such a channel change occurs, we say that the communication hops between channels.

2.2 Attack Model

Since we focus on message transmissions in the presence of a jammer, we only consider jamming attacks in this paper. Similar to the assumption in traditional channel hopping schemes [16, 20, 25], instead of considering a powerful attacker, we assume that Eve uses the same or similar hardware as legitimate users in terms of capability, energy capacity, and complexity, and the power-limited attacker can jam only one channel at a given time. One reason is that, to remain inconspicuous, the jammer would need to jam with conventional (802.11) hardware such as a single laptop with one or two wireless interfaces. In many cases, the attacker launches a jamming through a compromised node. Another reason for such assumption is that if a jammer is a high-power, broadband capable device, it can be easily detected by defenders since they violate the normal communication rules. Eve has the knowledge of the set of channels used by the sender and the receiver, and she chooses her jamming strategy depending upon the information that she obtains about the system.

3 Our Proposed Channel Hopping Scheme

Our method relies on the reciprocity of channel to achieve channel agreement, and spatial uncorrelation to prevent eavesdropping. Let $X^A = (x_1^A, x_2^A, ..., x_n^A)$ be the channel measurements recorded by Alice at time $t_1, t_2, ..., t_n$ respectively, and $X^B = (x_1^B, x_2^B, ..., x_n^B)$ be Bob′s channel measurements at time $t_{1'}, t_{2'}, ..., t_{n'}$, where $t_1 < t_{1'} < t_2 < t_{2'} < ...... < t_n < t_{n'}$, and x_i^u is the channel measurement value at time t_i or $t_{i'}$, $u = \{A, B\}$, $u = A$ represents Alice and $u = B$ represents Bob. According to the reciprocity of wireless channel, $x_i^A \approx x_i^B (1 \leq i \leq n)$, if they are obtained within the channel coherence time t_τ , i.e, $t_{i'} - t_i \ll t_\tau$. Since the channel variation is mainly caused by channel fading, it is random and unpredictable. Moreover, based on the location decorrelation property of the wireless channel, the attacker Eve cannot observe the same channel variations as the Alice-Bob channel if she is located several wavelengths away.

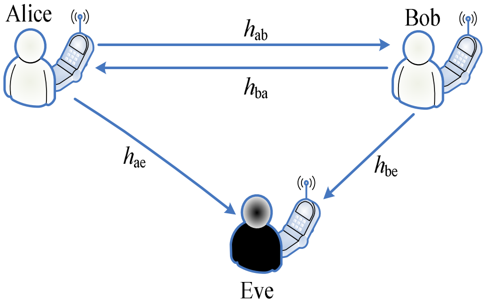

Figure 1: Wireless communication scenario.

3.1 Channel Hopping Protocol

Suppose that in the initial stage, Alice and Bob have obtained n channel measurements, $X^u = (x_1^u, x_2^u, ..., x_n^u), u = \{A, B\}$ prior to Eve′s arrival. Both Alice and Bob can use l channels, and their clocks are synchronized. Our protocol is described as follows.

1) Alice and Bob first quantize their channel measurements into binary bit sequences of length m respectively by performing channel quantization algorithm. Then they randomly permute the bit positions in their quantized sequences and obtain the random sequence $Q^u = (q_1^u, q_2^u, ..., q_m^u) \in \{0, 1\}^m$.

2) Alice and Bob divide their random sequence Q^u into blocks of length l denoted as

$$\begin{aligned} B_0^u &= (q_0^u, q_1^u, \cdots, q_{l-1}^u) \\ B_1^u &= (q_l^u, q_{l+1}^u, \cdots, q_{2l-1}^u) \\ \vdots &= \vdots \\ B_{\lfloor m/l \rfloor -1}^u &= (q_{(\lfloor m/l \rfloor -1)l}^u, q_{(\lfloor m/l \rfloor -1)l+1}^u, \cdots, q_{\lfloor m/l \rfloor l-1}^u). \end{aligned}$$

Then Alice and Bob compute a random channel selection sequence $CS^u = (CS_1^u, CS_2^u, ..., CS_{\lfloor m/l \rfloor -1}^u)$, respectively, where $CS_i^u = \{E_{B_i^u}(i) \mod l\}$, i is the packet sequence number, $B_i^u = (q_{il}^u, q_{il+1}^u, ..., q_{(i+1)l-1}^u), (0 \leq i \leq \lfloor m/l \rfloor - 1)$, and $E_K(\cdot)$ is an encryption function.

3) Both Alice and Bob change their own channels according to the random channel selection sequence CS^u (which is unknown to anyone but the two parties involved).

4) Alice and Bob exchange their packet pair (DATA-ACK) with the sequence number i using channel CS_i^u. Once the communication begins, the channel characteristics are recorded and used to calculate the next round channel choice.

5) If Alice and Bob cannot achieve agreement on one channel (i.e.CS_i^A is not equal to CS_i^B), both of them go to the next channel represented by CS_{i+1}^u.

6) Once the current round channel selection sequence is used up, Alice and Bob jump to Step 1) to generate a new channel selection sequence based on the channel measurements obtained during the current round, and continue their next round communication according to the new computed channel selection sequence.

3.2 Quantization Algorithm

It is obvious that quantization is a crucial step in our proposed channel hopping scheme, and the choosing of the quantization algorithm has a great influence on the performance of our proposed protocol.

In the quantization stage, both Alice and Bob quantize their channel measurements into binary bit sequence based on particular thresholds. There are many proposals of channel quantization. The paper [27] summarizes some existing quantization methods and evaluates their performance. The difference in these quantization methods mainly results from their different choices of thresholds and the different number of thresholds they use. These quantization methods could generally be classified into two categories: Single-bit approaches and Multi-bit approaches [11]. Single-bit approaches quantize each channel measurement into at most one bit, while Multi-bit approaches quantize each channel measurement into multiple secret bits, k-bit ($k > 1$), but at a cost of higher bit error rate.

In tradition key generation based on the channel-characteristic, to achieve an identical shared key between two legitimate users, an information reconciliation protocol should be used to reconcile the bit errors. However, during information reconciliation phase, Bob and Alice must exchange reconciliation information on public channel several times, which is time and energy consumption. Even worse, information reconciliation leaks some information about the secret key which can be used by the attacker to guess portions of the extracted key, hence, a privacy amplification protocol will be further applied to solve this issue, which consumes more time and communication overheads.

Moreover, with the quantization bit error rate increasing, the subsequence information reconciliation will become more and more difficulty and the whole process of key generation may even be failure. That is because when the quantization bit error rate increases, the information reconciliation protocol has to be performed much more rounds to eliminate all errors, which will reveal more bits to the attacker. For example, when the bit error rate is 0.08 after the quantization phase, the Winnow information reconcile protocol should be performed 5 rounds to eliminate all errors with 57.13% information leaked. While when the bit error rate is 0.25, the Winnow information reconcile protocol should be performed 11 rounds with 96.77% information leaked [21]. So, the quantization approaches that exhibit high bit error rate are not useful in establishing a secret key.

In this paper, since we focus on designing a fast and energy efficient channel hopping protocol, we try to achieve channel agreement with high probability without using information reconcile and privacy amplification. This requires that the bit error rate of the quantization algorithm should be as low as possible. Our experimental result in Section 4.1 shows that with l=12, to achieve a channel agreement ratio higher than 95%, the bit error rate of the output of quantization should be lower than 0.4%. However according to our experiment results in Figure 2, none of multi-bit quantization approaches can achieve such low bit error rate. Therefore, in this paper, we choose to use two-threshold single-bit approach since it has lower bit error rate compared with Multi-bit approaches and other single-bit approaches [11].

The quantization algorithm used in this paper is described as follows.

1) Both Alice and Bob divide the channel measurement sequence into blocks of length j which is a configurable parameter.

2) For each block, they calculate two thresholds: the upper threshold q_+^u and the lower threshold q_-^u independently such that

$$q_+^u = \mu^u + \alpha \times \sigma^u. \quad (1)$$

$$q_-^u = \mu^u - \alpha \times \sigma^u. \quad (2)$$

where μ^u and σ^u represent the mean and the standard deviation of the measurement sequences in the ith block, and $0 < \alpha < 1$ is a parameter which can be tuned through experiments.

3) Each measurement value $x_i^u (1 \le i \le n)$ is mapped to a binary bit via a quantizer $Q^u(\cdot)$ as shown in Figure 3, such that measurements below q_-^u are encoded as bit 0; measurements above q_+^u are encoded as bit 1, while measurements within the interval $[q_-^u, q_+^u]$ are discarded.

$$Q^u(x_i^u) = \begin{cases} 1, & if\ x_i^u > q_+^u \\ 0, & if\ x_i^u < q_-^u \\ e, & otherwise \end{cases} \quad (3)$$

where e is an undefined state. The superscript u stands for user and may refer to either Alice, in which

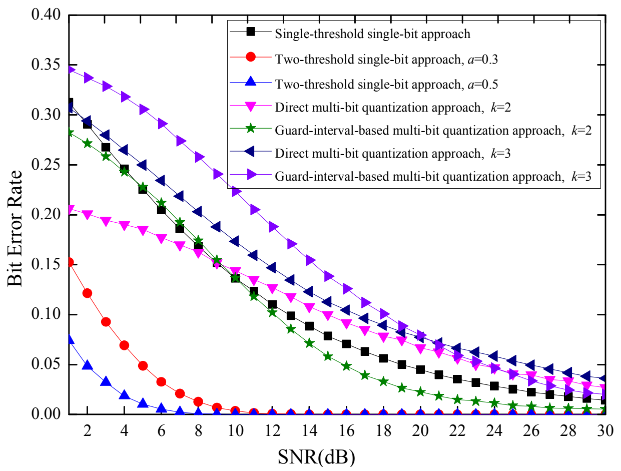

Figure 2: Bit error rate of different quantization approaches.

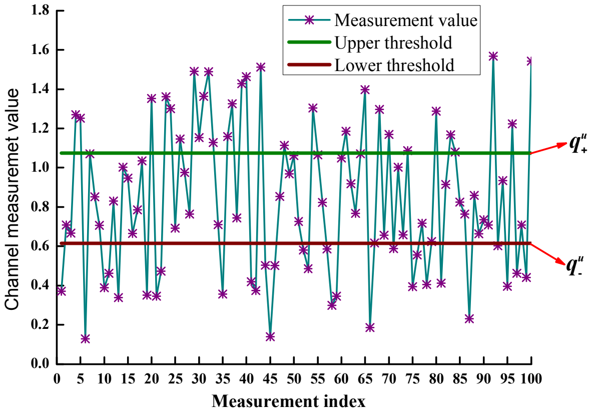

Figure 3: Bit error rate of different quantization approaches.

case the quantizer function is $Q^A(\cdot)$, or to Bob, for which the quantizer is $Q^B(\cdot)$.

4) Alice and Bob maintain a list of indexes of discarded values and exchange it with each other so that they only keep the ones that they both decide not to drop.

4 Experiment Results and Performance Analysis

In this section, we first describe our experiment settings, and then present the results and the performance of our scheme.

In our experiment, we make use of the most popular channel characteristic parameter, RSSI, as the indicator of the channel because its reading is readily available in the existing wireless infrastructures. Most of the current of-the-shelf wireless cards, without any modification, can measure it on a per packet/frame basis. RSSI can be read during the preamble stage of receiving an 802.11 frame. The variation over time of the RSS caused by motion and multipath fading, can be quantized and used for generating channel agreement sequences.

It should be noted that our approach is also applicable to any other parameters of channel characteristic, such as amplitude or phase, etc.

4.1 Experiment Setup

We conducted our experiments on three laptops (acting as Alice, Bob and Eve) equipped with in-built Intel PRO/Wireless 3945ABG network cards in a real indoor environment. Alice is configured as an access point (AP mode) and remains stationary, while Bob acts as a client (Station mode) and moves randomly at a speed of about 1m/s . Eve is configured to monitor mode and sits next to Alice, only about 30 centimeters away. Alice records the RSSI values of data packets from Bob, and Bob records the RSSI values of the corresponding MAC layer ACK packets from Alice. These data and ACK packets are all for data communication between Alice and Bob.

We perform experiments on 802.11a 5 GHz band because it has more non-overlapping channels (12 non-overlapping channels in the 802.11a) than 802.11b/g. We note that this experiment setting favors the jammer, as she only needs to scan 12 channels in order to detect the used channel between legitimate users. The jammer is guaranteed a direct hit once he locates the channel with traffic. In our experiments, the residence time that the legitimate communication stays fixed in a particular channel is 100 ms.

4.2 Channel Hopping Approach

As introduced in Section 2.1, after the legitimate users communicate on a single channel for a short period or once a communication channel is jammed, they must jump to another new channel to continue the communication. According to the jamming attack style, there are two most efficient hopping approach for jamming: the reactive hopping and the proactive hopping.

- Reactive hopping approach [24, 25]: the legitimate users hop to a new channel only after they have detected the presence of a jammer on the current channel they are using.

- Proactive hopping approach [7]: the legitimate users hop channels for every t seconds without attempting to detect the presence or the absence of the jammer on the current channel and hopping channel.

The advantage of the reactive hopping is the least hop number per unit time, while the proactive approach switches hop more often than is necessary. However, the advantage of the proactive hopping is that since channel hopping takes place for every t seconds it is difficult for the jammer to identify the current channel. It is robust when appropriate t value is chosen [7]. Moreover, in the proactive hopping, the legitimate users dont need to detect the presence of a jammer. In fact, obtaining an accurate estimate of a channel's status in a short period of time is not easy. For example, the DOMINO system [18] as reported requires several seconds to make an accurate determination of a greedy station. In our experiment, we make use of the proactive hopping approach. Alice and Bob switch their channel every 100 ms.

It should be noted that when a pulsing, fast-switching attacker appears, channel hopping can work in conjunction with other approaches such as the packet fragmentation and the redundant encoding to defend against this type of jamming [23].

4.3 Channel Hopping Agreement Ratio and Distribution of Channel Selection

We simulate the performance of our proposed channel hopping scheme with different quantization parameter α. The experimental results are shown in Figure 4. It is clear that larger value of α leads to a higher probability of channel agreement rate. When $\alpha = 0.3$, our channel hopping method can achieve a channel agreement ratio higher than 97%. When α =0.45, the channel agreement ratio of our method can even achieve 100%.

We also evaluate the channel selection distribution of our proposed scheme. The experiment results are draw in Figure 5. From Figure 5, we can see that the hopping probability on each channel is almost equally distributed.

Additionally, our approach eliminates the information reconciliation cost and only needs one time extra information exchange in the quantization phase. Therefore, our proposed channel hopping scheme is an effective one and is more energy efficient.

4.4 Security

As for the security, on the one hand, Eve′s channel measurements do not provide her any useful information about the measurement sequences X^A and X^B due to the spatial uncorrelation. On the other hand, the transmission of position indexes over the public channel in the quantization phase does not reveal any information about the quantized bits to Eve either. This is because they contain position indexes only, whereas the generated quantized bits depend upon the values of the channel measurement at those indexes. Further, this guarantees that Eve cannot use his observations to infer the values of the channel measurement of Alice or Bob at those indexes

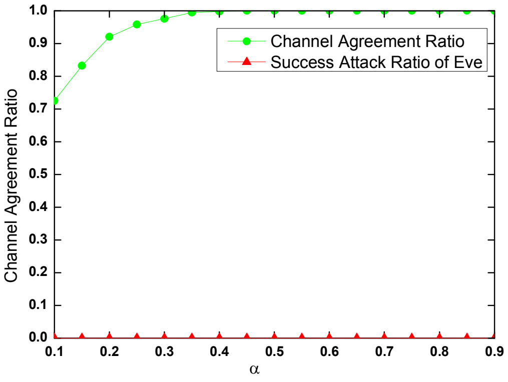

Figure 4: Channel agreement ratio and Eve's successful attack ratio as a function of quantization parameter α

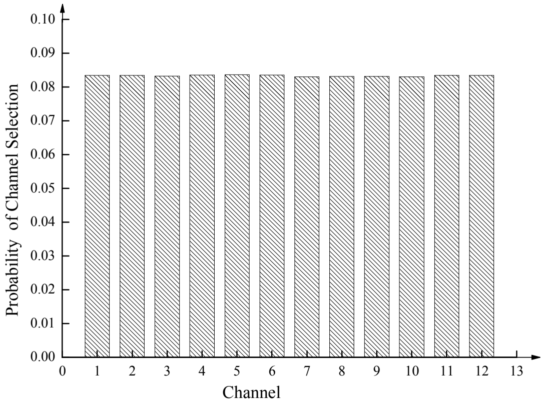

Figure 5: Distribution of channel selection

Eve can perform two kinds of Jamming attacks: predictive jamming and reactive jamming [7, 3]. If Eve chooses to use the predictive jamming, she has two possible strategies. The first is random Jamming. Eve sends jamming signal on a random channel. In this case, the probability of Eve selecting the correct channel at random is $1/l$. In our experiments, $l = 12$, and Eve′s random attack successful probability is about $1/12 = 8.33\%$ (Of course, the more channels legitimate users have, the lower probability Eve can achieve). By itself, this gives a relatively high chance of success to the attacker. However, successful jamming one message gives no advantage for the next, since legitimate users will be on a different, unknown channel. If Eve is more intelligent, she may use the same method as Alice and Bob to select channel. Eve can also collect the RSSI sequences by eavesdropping the communication between Alice and Bob, and then computes the channel hop sequences following the same steps as our method. We tested the probability that Eve successfully computes the channel that Alice and Bob will hop to. The experimental results are also shown in Figure 4. From the results, Eves successful attack probability is almost 0, which is even much lower than the random attack. This demonstrates that our proposed scheme is also resistant to more sophisticated jammers. Our experiment results also verify that the channel fading is a random shared secret between Alice and Bob, and Eve almost obtains no useful information by eavesdropping.

On the other hand, if Eve chooses to use the reactive jamming attack, she needs to scan all channels first and then launches attacks on the channel that legitimate users are using. The time to scan each channel and the radio start-up cost in a new channel of 802.11 devices is typically tens of milliseconds [24]. In our experiments, since Alice and Bob switch their channel every 100 ms, it is impossible for Eve to complete scanning before Alice and Bob switch their channels.

Hence, our proposed scheme is secure and causes no loss of secrecy.

5 Conclusions

In this paper, we focus on how to protect legitimate transmission from jamming attack by having the legitimate users hop among channels to hide the transmission from the jammer. We propose a novel channel hopping scheme for jamming-resistance based on wireless channel characteristics. We evaluate the proposed scheme through real-world experiments in terms of the channel agreement rate, distribution of channel selection and security. The experiment results show that our proposed scheme can work reliably with high efficiency and that it achieves higher channel agreement rate with almost equally channel distribution. Moreover, our scheme is light-weight and easy-implementable on the current wireless devices. In the future, we will focus on achieving channel hopping agreement without extra information exchange.

Acknowledgments

This work was done when Qiuhua Wang visited the Department of Electrical & Computer Engineering, Syracuse University. The authors would like to thank Dr. Yingbin Liang for her constructive comments and helpful suggestions. This work was partially supported by National Natural Science Foundation of China (No.61401128, No.61471152), Zhejiang Province Natural Science Foundation (No. LQ14F020010), Project of Zhejiang Provincial Key Enterprises Institute Construction and Project of Zhejiang Provincial Smart City regional synergy innovation center and the China Scholarship Council (CSC).

References

[1] A. Alagil, M. Alotaibi, and Y. Liu, "Randomized positioning dsss for anti-jamming wireless communications," in *International Conference on Computing, Networking and Communications (ICNC'16)*, pp. 1–6, 2016.

[2] G. D. Durgin, *Space-time Wireless Channels*, Prentice Hall PTR, New Jersey, USA, 2003.

[3] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *International Journal of Ad-Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, 2014.

[4] R. Guillaume, F. Winzer, and A. Czylwik, "Bringing phy-based key generation into the field: An evaluation for practical scenarios," in *The 82nd IEEE Vehicular Technology Conference (VTC Fall'15)*, pp. 1–5, 2015.

[5] J. Huang and T. Jiang, "Dynamic secret key generation exploiting ultra-wideband wireless channel characteristics," in *IEEE Wireless Communications and Networking Conference (WCNC'15)*, pp. 1701–1706, 2015.

[6] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *International Conference on Mobile Computing and Networking (MOBICOM'09)*, pp. 321–332, 2009.

[7] K. Karunambiga, A. C. Sumathi, and M. Sundarambal, "Channel selection strategy for jamming-resistant reactive frequency hopping in cognitive wifi network," in *International Conference on Soft-Computing and Network Security (ICSNS'15)*, pp. 1–4, 2015.

[8] S. M. Khattab, D. Mosse, and R. G. Melhem, "Modeling of the channel-hopping anti-jamming defense in multi-radio wireless networks," in *International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services (MOBIQUITOUS'08)*, pp. 1–5, 2008.

[9] A. Liu, P. Ning, H. Dai, and Y. Liu, "Usd-fh: Jamming-resistant wireless communication using frequency hopping with uncoordinated seed disclosure," in *IEEE International Conference on Mobile Adhoc and Sensor Systems (IEEE MASS'10)*, pp. 41–51, 2010.

[10] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *The 31st Annual IEEE International Conference on Computer Communications (IEEE INFOCOM'12)*, pp. 927–935, 2012.

[11] Y. Luo, L. Pu, Z. Peng, and Z. Shi, "Rss-based secret key generation in underwater acoustic networks: Advantages, challenges, and performance improvements," *IEEE Communications Magazine*, vol. 54, no. 2, pp. 32–38, 2016.

[12] M. G. Madiseh, S. He, M. L. McGuire, S. W. Neville, and X. Dong, "Verification of secret key generation from uwb channel observations," in *IEEE International Conference on Communications (ICC'09)*, pp. 593–597, 2009.

[13] S. Mathur, Miller R, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: Proximity-based secure pairing using ambient wireless signals," in *The 9th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'11)*, pp. 211–224, 2011.

[14] S. Mathur, W. Trappe, and N. Mandayam, "Radio-telepathy: extracting a secret key from an unauthen-

ticated wireless channel," in *International Conference on Mobile Computing and Networking (MOBICOM'08)*, pp. 128–139, 2008.

[15] B. Mihajlov and M. Bogdanoski, "Analysis of the wsn mac protocols under jamming dos attack," *International Journal of Network Security*, vol. 16, no. 4, pp. 304–312, 2014.

[16] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *IEEE International Conference on Computer Communications (INFOCOM'07)*, pp. 2526–2530, 2007.

[17] S. N. Premnath, S. Jana, J. Croft, and P. L. Gowda, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917–930, 2013.

[18] M. Raya, J. Hubaux, and I. Aad, "Domino: A system to detect greedy behavior in IEEE 802.11 hot spots," in *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'04)*, pp. 84–97, 2004.

[19] Y. R. Tsai and J. F. Chang, "Using frequency hopping spread spectrum technique to combat multipath interference in a multiaccessing environment," *IEEE Transactions on Vehicular Technology*, vol. 43, no. 2, pp. 211–222, 1994.

[20] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," *International Journal of Production Economics*, vol. 172, pp. 76–94, 2016.

[21] Q. Wang, X. Wang, Q. Lv, X. Ye, Yi Luo, and L. You, "Analysis of the information theoretically secret key agreement by public discussion," *Security and Communication Networks*, vol. 8, no. 15, pp. 2507–2523, 2015.

[22] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrow band fading channels," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 9, pp. 1666–1674, 2012.

[23] A. D. Wood, J. A. Stankovic, and G. Zhou, "Deejam: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks," in *IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON 2007, Merged with IEEE International Workshop on Wireless AdHoc and Sensor Networks*, pp. 60–69, 2007.

[24] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of The 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (ACM MobiHoc'05)*, pp. 46–57, 2005.

[25] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," in *The Workshop on Wireless Security*, pp. 80–89, 2004.

[26] J. Zhang, T. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, no. 3, pp. 614–626, 2016.

[27] C. T. Zenger, J. Zimmer, and C. Paar, "Security analysis of quantization schemes for channel-based key extraction," in *Workshop on Wireless Communication Security at the Physical Layer*, pp. 267–272, 2015.

[28] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

Biography

Qiuhua Wang received her B.S. and M.S. degrees in communication engineering from Liaoning Technical University, Fuxin, China, in 2000 and 2003, respectively. She received her Ph.D. degree in Communications and Information systems from Zhejiang University, Hangzhou, China, in 2013. Now, she is an Associate Professor of the School of CyberSpace, Hangzhou Dianzi University. Her current research interests include information security, security issues in wireless networks, key management and physical layer security, etc.

Hongxia Zhang received her B.S. degree in Electronic and Information engineering from Shandong University of Technology, Zibo, China, in 2015. She is currently pursuing the M.S. degree in Communication Engineering. Her research interests include key generation and physical layer security.

Qiuyun Lyu received her B.S. and M.S. degrees in Computer Science and Technology from Chang'an University, Xi'an, China, in 2000 and 2003, respectively. Now, she is an Associate Professor of the School of CyberSpace, Hangzhou Dianzi University. Her current research interests include information security and privacy, security issues in wireless networks.

XiaojunWang received his B.S. and M.S. degrees in Communication and Information system from University of Electronic Science and Technology of China, Chengdu, china, in 1997 and 2000 respectively. Now, he is a teacher of the School of CyberSpace, Hangzhou Dianzi University. His research interests include information security, vulnerability analysis and software security.

Jianrong Bao received his B.S. degree in Polymer Materials & Eng., and the M.S.E.E. degree from Zhejiang University of Technology, Hangzhou, China, in 2000 and 2004, respectively. He received his Ph.D. E.E. degree from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2009. He is with the school of Information Engineering, Hangzhou Dianzi University, Hangzhou, China. His research interests include space wireless communications, communication signal processing, information security & channel coding, etc.