ISBN 978-981-11-3671-9
Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering (WCSE 2017)
Beijing, *25-27 June*, *2017*, *pp. 935-939*
doi: 10.18178/wcse.2017.06.162

Power Analysis Attack on Jamming Assisted Key Agreement

Qiao HU [1 +] and Gerhard HANCKE [1]

[1] Department of Computer Science, City University of HK

Abstract. Physical layer key agreement is a trend in wireless communication. But physical layer key agreement schemes utilizing channel state to generate the key has quite low speed. iJam is a novel scheme utilizing assisted jamming signals to generate shared key with much higher speed. We propose a power analysis attack which can break iJam by analyzing the power difference of each received signal. Simulation results show that our attack breaks iJam in most time.

Keywords: physical layer key agreement, jamming, QAM.

1. Introduction

Physical layer security is a popular research area to improve the communication security of wireless networks with the presence of an eavesdropper. Secret key generation from randomness at the wireless physical layer is a hot topic. As this kind of key generation scheme is low cost, it is suitable for resources constrained devices which lack the computational capability for conventional encryption schemes. Also, these low-cost schemes do not need a trust third party to distribute cryptographic keys and keys for each communication are all different which promotes the security to a high level. The majority of papers try to establish the shared key between two devices with the characteristics of their wireless communication channel.

However, Jana Suman et. Al. [1] have proved that from the static environment the generated bits have very low entropy which means that the similarity among these extracted bits are high. To overcome this problem, a mobile environment with significant movement is a good solution. But this kind of movement is not suitable for indoor space. Shyamnath Gollakota [2] proposed a novel fast and channel independent scheme which could reach a fast key extracting speed with high entropy and without moving. This method is called iJam. Authors divide the message into several parts and send each part twice. The receiver will send noise to jam either the original part or the replicate part. The noise is a zero-mean data signal which can make it invisible to the eavesdropper when both noise and message are overlapped with each other. After the end of message transmission, the receiver will pick up unjammed parts to make up the original message. Then sender and receiver can generate the secret key from the message.

In this paper, we present an attack approach against iJam by distinguish whether a signal is jammed or not. The basic idea of our power analysis is as follows. After we receive a signal, we demodulate it and create a signal by modulating the previous demodulation result. The power difference between the received signal and corresponding recreated signal can be used to judge whether the received signal is jammed or not. We have validated that this attack can break iJam in theory. Also we conduct simulations to analyse two main factors that have impact on our attack, power ratio between the jamming signal and the data signal and signal to noise ratio of the background noise. The results of simulations show that our attack works well in most cases.

[+] Corresponding author.
E-mail address: qiaohu2-c@my.cityu.edu.hk.

2. Background and Related Work

2.1. Physical Layer Key Generation Scheme - iJam

The main flowchart of iJam is shown in Fig.1. Device Alice transmits data in several rounds. In each round, Alice first generates a random value and transmits it to Bob, then Alice transmits a duplicate data signal. Bob should receive two same signals. Before Alice transmitting, Bob has chosen one signal to jam. The jamming signal is generated in the same way as the data signal in Alice. If the values corresponding to the data signal and the jamming signal are all picked up from a zero-mean Gaussian distribution, then the signal mixed up by these two signals has Gaussian statistics. This means it is hard to distinguish the mixed signal from the data signal by comparing their variance. As Bob knows the jamming signals, he can easily ignore those jammed signals and concatenating the values resolved from the rest signals to form the shared key. But for the eavesdropper Eve, he can not distinguish whether a signal is jammed or not. He fails to get the shared key.

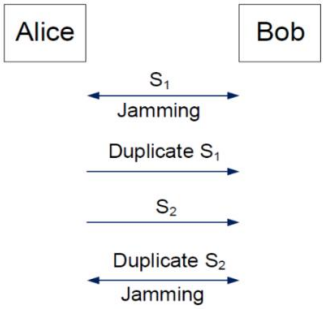

Fig.1: Flowchart of iJam

2.2. Related Work with iJam

The fundamental theory in iJam is physical layer key generation agreement [3-6]. This kind of agreement extracts the channel state information (CSI) from received signals and converts CSI into keys. CSI describes how the signal be affected by the environment during its propagation from the sender to the receiver. CSI varies all the time which makes it a secure way to generate random bits. However, CSI do not changes as fast as we want. We must wait more time for the variation of CSI to make sure that adjacent bits are uncorrelated.

Cooperative jamming scheme is adopted by iJam to increase the speed of key generation. Cooperative jamming schemes [7-10] utilize jamming signal to hide the data signal from the eavesdropper but still allows the legitimate communication. To achieve this target, the receiver transmits the jamming signal to degrade the capacity of eavesdropper-sender channel and eliminates the degradation on sender-receiver channel by removing the known jamming signal out from received mixed signals.

iJam can generate keys fast, but is it secure? Steinmetzer. D. et. al. [11] proposed multi-eavesdropping attack to break iJam by exploiting signal diversity on signals received from different antennas at different places. But if the sender and the receiver are very close to each other, multi-eavesdropper may lose the ability to separate mixed signals.

3. Adversary Model

In our adversary model, there are three entities: two legitimate participants, Alice and Bob, and an eavesdropper Eve. Alice and Bob generate their shared key using iJam. Eve is a single eavesdropper with single antenna. All these entities are work with the same 802.11 protocol. Eve knows all the details of iJam but have no knowledge about the instantly generated jamming signals by Alice and Bob. We assume that he can at any place and have no resource constraint which means the power of the attack signal can be as high as the attacker want.

4. Jamming Detection

4.1. Theory Analysis

iJam described in previous section utilizes cooperative jamming signals to confuse the attacker Eve. It works well when we only consider the variance of the signal, how about other aspects like energy? We propose a jamming detection scheme in which a single attacker with single antenna can distinguish the jammed signal from the data signal by comparing the power differences of received signals and original signals. Original signals is generated by the data recovered from corresponding received signals. This power difference comes from a common modulation scheme used in iJam, Quadrature amplitude modulation (QAM). QAM modulates data by following equation:

$$\mathrm{s(t)} = I \cdot g(t) \cdot \cos(2\pi f t) - Q \cdot g(t) \cdot \sin(2\pi f t) \quad (1)$$

g(t) is the impulse signal, f is the carrier frequency. I is short for In-Phase and Q is short for Quadrature. QAM determines the values of I and Q by the values of data. We illustrate an example of 16-QAM in Fig.2. We can see that four bits data correspond to a pair of I and Q. To demodulate the signal, we only need to get the values of I and Q. We can put these new pairs of I and Q in Fig.2. For each new point, the nearest point that belongs to the original 16 points represents the corresponding four bits data contains in this new point.

To be simple, we assume there exists no background noise and no channel fading here. So if only Alice transmits data signal, all new points should at the same places of those original 16 points. There should be no power difference between received signals and original signals. But if Bob starts jamming, things are different. We show the possible range of I and Q of received jammed signals in Fig.3. In this figure, we assume that the power of the data signal and the jamming signal are the same. The asterisks and pluses represent original 16 points and new points from received signals separately. For each point, we calculate its power difference by following equation:

$$\mathrm{Pow\_Dif} = \int_0^T |(I_n - I_o)g(t)\cos(2\pi f t) - (Q_n - Q_o)g(t)\sin(2\pi f t)|dt \quad (2)$$

I_n and Q_n means the values of I and Q of the new point. T is the total time of one symbol period. I_o and Q_o means the values of I and Q of the original point corresponding to the new point in demodulation process.

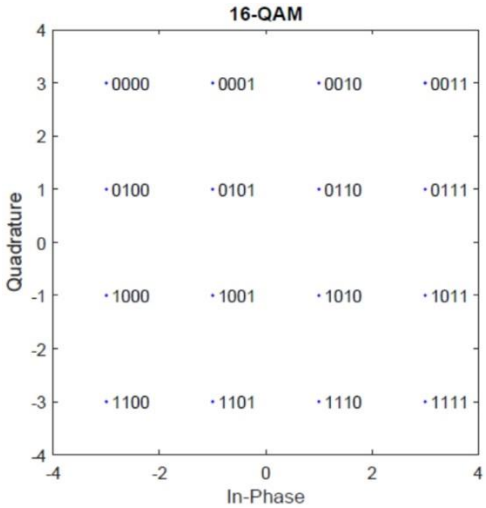

Fig.2: Constellation Diagram of 16-QAM

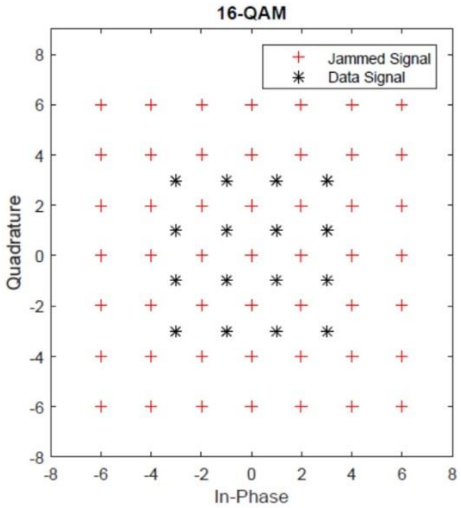

Fig.3: Constellation Diagram of Jammed Signal

During the signal generation period, the probability of choosing each one of the 16 original points is 1/16. So for the jammed signal, there are 256 combinations of the data signal and the jamming signal. The probability of each combination is 1/256. We calculate the power differences of these combinations and the result is shown in Fig.4. X-axis represents the power ratio of the power difference to the average power of the data signal.

This figure tells us that most power differences are only 20% of the average power of the data signal. But the rest power differences are quite high. According to Fig.4, the average power difference of the jammed signal is 40%, which is quite higher than the zero power difference of the data signal. It is an easy job to distinguish the jammed signal.

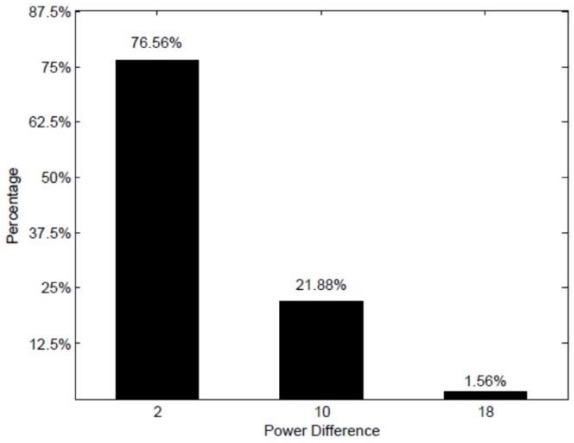

Fig.4: Distribution of Power Difference

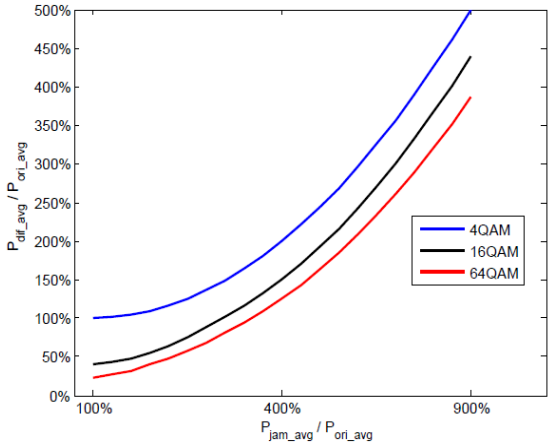

Fig.5: Impact of the Power of the Jamming Signal on the Attack

4.2. Simulation on Jamming Detection

We have proved that our attacker can distinguish the jammed signal from the data signal in the assumption of no background noise, no fading and similar power. First, we show the result of the impact of the power of the jamming signal in Fig.5. The values at X-axis represent the power ratio of the average power of the jamming signal to the average power of the data signal. Y-axis tells us the power ratio of the power difference of the jammed signal to the power difference of the data signal. Fig.5 shows that with the increasing power of the jamming signal, the power difference of the jammed signal increases which means it is easier for the attacker to distinguish the jammed signal.

To make our attack more practicable, we conduct simulation on the impact of noise on our attack. In the simulation, we following the 802.11 which is adopted in iJam, choosing 2.4G Hz as the carrier frequency. We record all signals under different SNR.

The result of noise impact simulation is shown in Fig. 6. X-axis represents the SNR of background noise to the data signal. Y-axis means the power ratio of the power difference of the jammed signal to the power difference of the data signal. If the value of the power ratio is around 1 or less than 1, it means the attacker should make mistake on distinguish jammed signals. From Fig. 6 we can observe that for 16-QAM and 64-QAM, our attack works with SNR less than 0 dB, while for 4-QAM, the work range increases 2 dB.

However, high SNR may cause high bits error rate in normal communication. We show the result of the impact of SNR on bits error rate in Fig. 7. X-axis represents the SNR of background noise to the data signal. Y-axis means bits error rate. This figure shows that for 16-QAM and 64-QAM, bits error rate is quite high when the SNR is high enough to against our attack. Both error rates are larger than 20% which means the normal communication fails. For 4-QAM, when SNR is around 2 dB, the error rate is about 5% which the normal communication can tolerate. But the normal communication fails if the SNR increasing to around 10. It means that the power of the noise has negative impact on our attack, but our attack works in most times.

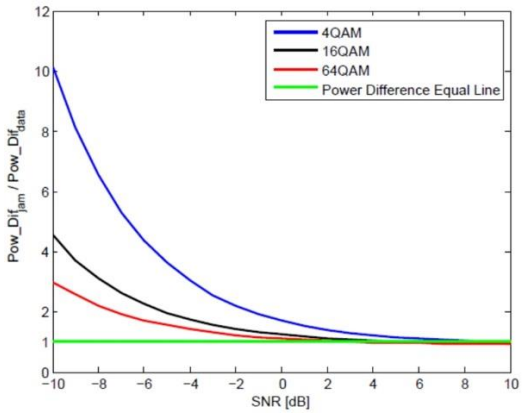

Fig.6: Impact of Background Noise on the Attack

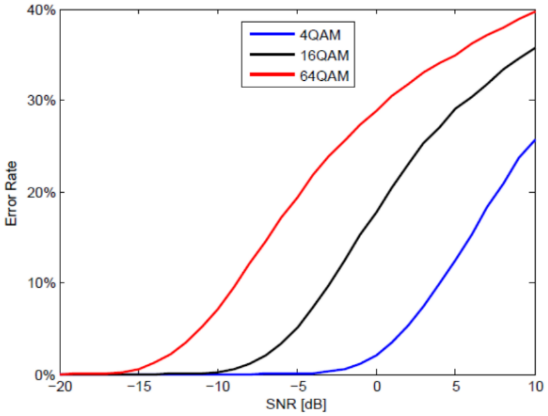

Fig.7: Bits Error Rate under Different SNR

5. Conclusion

In this paper, we propose an attack which can break iJam by power difference analysis. Our simulation result shows that this attack works well in most time. Next step is to test our attack in real environment.

6. References

[1] Jana, S., Premnath, S.N., Clark, M., Kasera, S.K., Patwari, N. and Krishnamurthy, S.V., 2009, September. On the effectiveness of secret key extraction from wireless signal strength in real environments. In Proceedings of the 15th annual international conference on Mobile computing and networking (pp. 321-332). ACM. A. Gray. Modern Differential Geometry. CRE Press, 1998.

[2] Gollakota, Shyamnath, and Dina Katabi. "Physical layer wireless security made fast and channel independent." INFOCOM, 2011 Proceedings IEEE. IEEE, 2011.

[3] Azimi-Sadjadi, Babak, et al. "Robust key generation from signal envelopes in wireless networks." Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007.

[4] Mathur, Suhas, et al. "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel." Proceedings of the 14th ACM international conference on Mobile computing and networking. ACM, 2008.

[5] Zeng, Kai, et al. "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks." INFOCOM, 2010 Proceedings IEEE. IEEE, 2010.

[6] Liu, Hongbo, et al. "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks." INFOCOM, 2012 Proceedings IEEE. IEEE, 2012.

[7] Liu, Yupeng, Jiangyuan Li, and Athina P. Petropulu. "Destination assisted cooperative jamming for wireless physical-layer security." IEEE transactions on information forensics and security 8.4 (2013): 682-694.

[8] Dong, Lun, et al. "Cooperative jamming for wireless physical layer security." Statistical Signal Processing, 2009. SSP'09. IEEE/SP 15th Workshop on. IEEE, 2009.

[9] Nandakumar, Rajalakshmi, et al. "Dhwani: secure peer-to-peer acoustic NFC." ACM SIGCOMM Computer Communication Review. Vol. 43. No. 4. ACM, 2013.

[10] Zhang, Bingsheng, et al. "PriWhisper: Enabling Keyless Secure Acoustic Communication for Smartphones." IEEE Internet of Things Journal 1.1 (2014): 33-45.

[11] Steinmetzer, Daniel, Matthias Schulz, and Matthias Hollick. "Lockpicking physical layer key exchange: weak adversary models invite the thief." Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2015.