2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)
August 28-29, 2018; Shahid Rajaee Teacher Training University - Tehran, Iran

Phase Jamming Attack: A Practical Attack on Physical layer-Based Key Derivation

S. Mohamad MirhoseiniNejad
School of Electrical Engineering
Iran University of
Science and Technology (IUST)
Tehran, Iran
sm_mirhoseini@elec.iust.ac.ir

Ali Rahmanpour
School of Electrical Engineering
Iran University of
Science and Technology (IUST)
Tehran, Iran
rahmanpour@alumni.iust.ac.ir

S. Mohammad Razavizadeh
School of Electrical Engineering
Iran University of
Science and Technology (IUST)
Tehran, Iran
smrazavi@ieee.org

***Abstract*—Key derivation from the physical layer features of the communication channels is a promising approach which can help the key management and security enhancement in communication networks. In this paper, we consider a key generation technique that quantizes the received signal phase to obtain the secret keys. We then study the effect of a jamming attack on this system. The jammer is an active attacker that tries to make a disturbance in the key derivation procedure and changes the phase of the received signal by transmitting an adversary signal. We evaluate the effect of jamming on the security performance of the system and show the ways to improve this performance. Our numerical results show that more phase quantization regions limit the probability of successful attacks.**

***Keywords*—Physical-Layer Security, Secret Key Generation, Jamming Attack, phase attack.**

I. Introduction

The broadcast nature of the wireless communication makes it insecure, which threats two security goals, i.e. data confidentiality and integrity. The traditional cryptography-based security approaches concern about computational complexity and expensive key management schemes. The physical layer security (PLS) is a developing approach, which provides the security and privacy in physical layer of network. Low computational complexity and provable security are among the advantages of the PLS in comparing with security approaches in higher layers [1]–[3].

PLS was first introduced in [4], which studies a wiretap channel and introduces the secrecy capacity as the security measure of the communication networks. Since then, several studies have extended the idea, such as [5] for Gaussian wiretap channels, [6] for fading channels and [2] for multiple-input multiple-output (MIMO) communication channels. The PLS approach attracts more attention in recent years, due to the uncertainty of traditional cryptography algorithms in upper layers.

The idea of deriving the secret keys using the randomness of communication channels was first introduced in [7]. Since then, many efforts have been dedicated to develop this method. For example, a key generation scheme is introduced in [8] which takes advantage of random fluctuation of the communication channels. Most of the proposed methods assume reciprocity-based approaches in which the channel is fixed during the key exchange [9]. A detailed description on the key exchange solutions in physical layer is discussed in [10]. The idea of deriving the secret keys from the received signal phase is a practical and relatively new method that utilizes the randomness nature of signal phase in the communication medium to generate the keys [11].

In spite of the advantages of the key generation methods in the physical layer, they are prone to physical layer attacks including active and passive attacks. If an attacker could manipulate the channel characteristics between the transmitter and receiver, then the key exchange algorithms become vulnerable and the generated key would be predictable by a smart attacker [12]. An active attacker, which deliberately changes the message signals and disrupts physical layer key exchange was first introduced in [13]. The disruptive jamming attack introduced in [14] is to minimize key derivation rate in the network. However, to the best of our knowledge, there is not any attempts in the literature, that study attacking a secure communication network, that utilizes received signal phase for secret key generation.

In this paper, we investigate the problem of jamming attack to a network that exploits the signal phase to generate the secret keys. This attack is different from typical jamming attacks as they disturb the information signal by using relatively high energy interference to disrupt the legitimate communication system. We consider one single-tone key derivation technique which is proposed in [11]. Then we show the effect of a phase jamming attack on this system in which the jammer tries to changes the phase of the received signal and disrupts the key generation process.

The paper is organized as follows: After presenting system model and key generation method in Section II, we analyze the phase jamming attack in Section III. In Section IV, we present our simulation results to evaluate the proposed jamming attack performance. Finally, the paper has been concluded in section V.

II. System Model and Key Derivation Scheme

A. System Model

Fig. 1 illustrates the model of communication network which encompasses a transmitter (Alice), a receiver (Bob) and a jammer (Mallory). The network is assumed to be static and the channel is reciprocal. Thus, the channel impulse response

978-1-5386-7582-3/18/$31.00

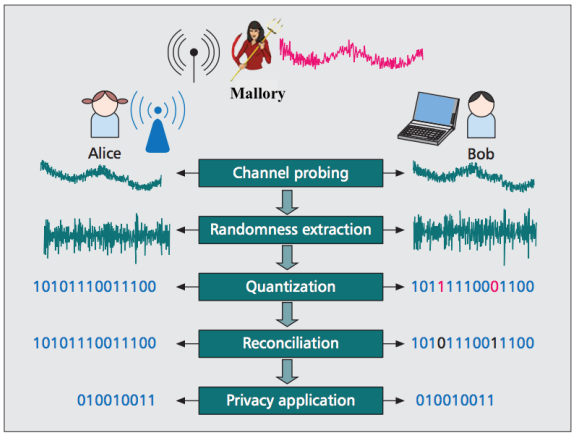

Fig. 1. Secret key generation model steps [10]

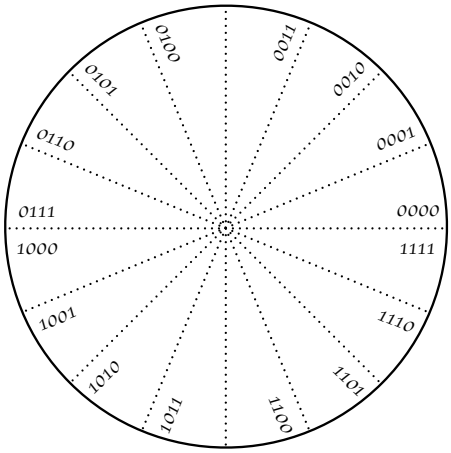

Fig. 2. Quantization regions with $Q = 16$

(CIR) is considered to be constant during the key generation phases. The jammer has a fading channel that is statistically independent from the main channel between Alice and Bob.

B. Key Generation Algorithm

In this section, we introduce the single-tone key generation algorithm proposed in [11] which utilizes the phase randomness properties of the main channel. For key derivation, first, Alice transmits a signal $x_A(t) = e^{j(2\pi f_c t+\phi_A)}$ to Bob, where f_c is the central frequency of the transmitted signal and the initial phase of the message is considered to be a random variable by uniform distribution (i.e. $\phi_A \sim U[-\pi, \pi]$). Bob receives the signal $y_{A,B} = e^{j(2\pi f_c(t-t_{A,B})+\phi_A+\theta)} + \eta_{A,B}(t)$, where $\eta_{A,B}(t)$ is the additive white Gaussian noise and θ denotes the phase response of the channel. Furthermore, the time delay between Alice and Bob is considered to be $t_{A,B}$. Bob then estimates $\phi_A + \theta$ as $\hat{\phi}_{A,B}$. He also, generates a random value ϕ_2 which is uniformly distributed over $[-\pi, \pi]$ to quantize the value of $S_1 = \hat{\phi}_{A,B} + \phi_B$. Next, the message $x_B(t) = e^{j(2\pi f_c t+\phi_B)}$ is transmitted to Alice by Bob. Alice receives the signal $y_{B,A} = e^{j(2\pi f_c(t-t_{B,A})+\phi_B+\theta)} + \eta_{B,A}(t)$. As a similar approach in Bob, Alice estimates $\phi_B + \theta$ as $\hat{\phi}_{B,A}$ and quantizes the value of $S_2 = \hat{\phi}_{B,A} + \phi_A$. The quantization scheme has been discussed in detail in [11]. It is important that the quantization regions of S_1 has to be similar to the quantization regions of S_2. Fig. 2 depicts the quantization regions for $Q = 16$, where Q is the number of quantization regions. In order to achieve a key agreement, the maximum allowed received phase differences between Alice and Bob is $2\pi/Q$. In the next section, we try to show the likelihood of key disagreement in the presence of an attacker.

III. Phase Jamming Attack

In this section, we investigate the impact of a disturbance produced by an active attacker (jammer) in order to subvert the key agreement protocol described in the previous section.

We consider adversary to be a phase jammer. She is an active attacker which aims to change the phase of the exchanged signal between Alice and Bob to prevent a key agreement. The jammer transmits a jamming signal as

$$x_M(t) = Ae^{j(2\pi f_c t)}. \tag{1}$$

Consequently, Alice and Bob receive $y_{M,A}$ and $y_{M,B}$ signal, respectively, which are written as

$$\begin{aligned} y_{M,A}(t) &= A.e^{j(\omega_c(t-t_{M,A})+\theta_{M,A})} + \eta_{M,A}(t) \\ y_{M,B}(t) &= A.e^{j(\omega_c(t-t_{M,B})+\theta_{M,B})} + \eta_{M,B}(t) \end{aligned} \tag{2}$$

where $t_{M,A}$ and $t_{M,B}$ are the delay time of the received signals by Alice and Bob, respectively. $\theta_{M,A}$ and $\theta_{M,B}$ determine the phase response of $h_{M,A}$ and $h_{M,B}$, which are assumed to be the channel impulse response between jammer and Alice and between jammer and Bob, respectively. We assume that $\theta_{M,A}$ and $\theta_{M,B}$ are random variables with a uniform distribution in the range of $[-\pi, \pi]$ [15]. In this paper, we eliminate the path loss and signal distortion during the transmission for the sake of simplicity.

We denote by y_A and y_B the total received signals of Alice and Bob, respectively, which are

$$\begin{aligned} y_A(t) &= y_{B,A}(t) + y_{M,A}(t) \\ y_B(t) &= y_{A,B}(t) + y_{M,B}(t). \end{aligned} \tag{3}$$

.

Fig. 3 depicts the empirical probability density function (pdf) of the phase of received signals by Alice and Bob, which is distributed over $[-\pi, \pi]$ interval (for $A = 1$ and $SNR = 4dB$). The transmitted and initial phases (ϕ_A, ϕ_B, and $\theta_{A,B}$) are assumed to be zero, as these values are constant. With these assumptions, the variance of the distribution σ_r^2, equals to 1.25.

The jamming attack is called successful when she causes a key disagreement between Alice and Bob. The key disagreement occurs when the calculated phases (S_A and S_B) are not in a same quantization region, i.e. , $\lfloor \frac{S_A}{2\pi/Q} \rfloor \neq \lfloor \frac{S_B}{2\pi/Q} \rfloor$, where $\lfloor . \rfloor$ indicates the integer part function.

As the received signal follows a normal distribution with zero mean and variance of σ_r^2, the attack success probability (ASP) can be calculated as

$$ASP = \frac{1}{2} - \frac{1}{2} erf(\frac{\sqrt{2}\pi}{Q\sqrt{\sigma_r^2}}) \tag{4}$$

where $erf(x)$ is the error function of x, which is described as

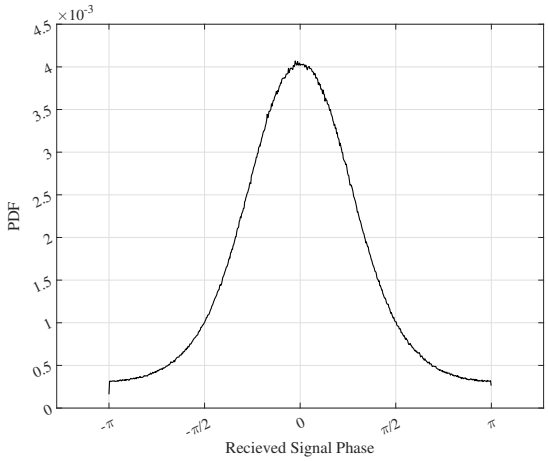

Fig. 3. The Empirical PDF of phase of received signals.

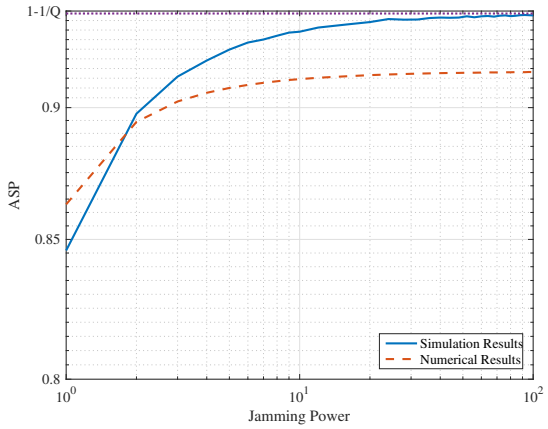

Fig. 4. Attack success probability versus the power of jammer.

$$erf(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{(-\phi^2)} d\phi. \tag{5}$$

While the mean of the received phase distribution is zero, it is expected that the received phase places in the first quantization region. Thus, the error occurs when $\phi < 0$ or $\phi > \frac{2\pi}{Q}$. While $\phi < 0$ represents the cumulative distribution function at point $\phi = 0$, which is equal to $\frac{1}{2}$. When the jamming signal gets a high power ($A \gg 1$), then the received signal has a uniform distribution. In this case, $ASP = 1 - \frac{1}{Q}$, which can be considered as the upper bound of the ASP.

IV. Simulation Results

In order to evaluate the jamming attack, we first examine the Eq. (4) by comparing the simulation and analytical results in two scenarios. Hence, we can demonstrate the impact of jamming power and SNR on the ASP. The system parameters are $Q = 16$, $SNR = 4dB$, and $A = 1$.

Fig. 4 represents the successfulness of attack in terms of the jammer power. The curves are approaching the limit value of $1 - \frac{1}{Q} = 0.9375$. The relationship between ASP and the number of quantization regions is illustrated in Fig. 5. Although increasing the value of Q is desirable for improving

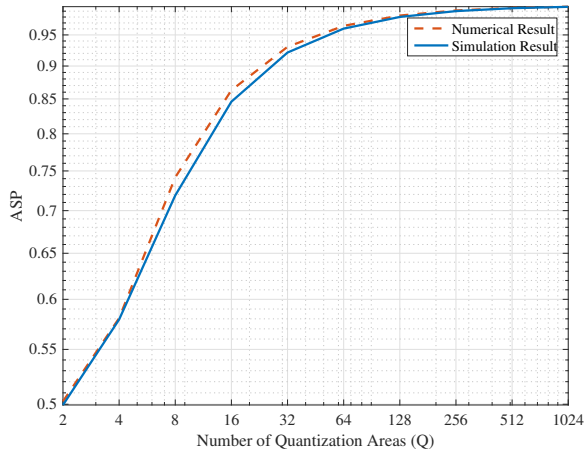

Fig. 5. Attack success probability versus Numbers of quantization regions.

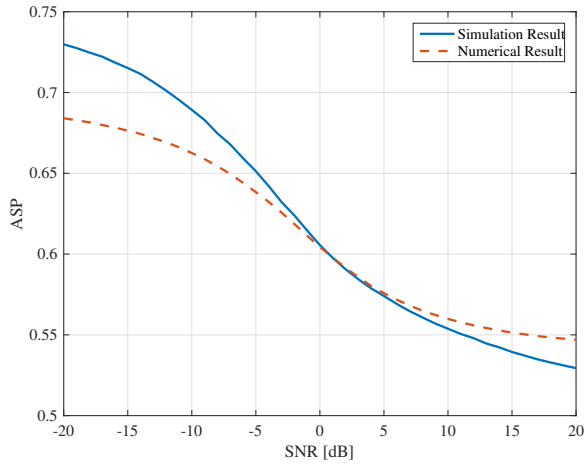

Fig. 6. Attack success probability versus SNR.

the key generation ratio, Fig. 5 suggests that in this condition, the key disagreement probability is grown, too.

In Fig. 6, the ASP is demonstrated in terms of SNR. As it is seen, the Eq. 4 is no longer valid in large and small SNR values. This is because the received phase does not follow a normal distribution in these situations. Fig. 7 illustrates the distribution of received phase for different SNR values. The received phase contains a uniform distribution over $[-\pi, \pi]$, for small SNRs and over $[-\pi/2, \pi/2]$ for large SNR values. Fig. 6 suggests that the Eq. 4 is acceptable in SNRs between about $-5dB$ to $10dB$.

V. Conclusion and Future Works

In this paper, we evaluated a jamming attack against a signal phase approach for key generation. The results suggest that the attack is less successful in high SNR environments. Moreover, the key agreement approach is more vulnerable against the jamming by choosing larger number of quantization regions (Q), in order to increase the key generation rate. In fact, there is a trade off between key generation rate and its vulnerability.

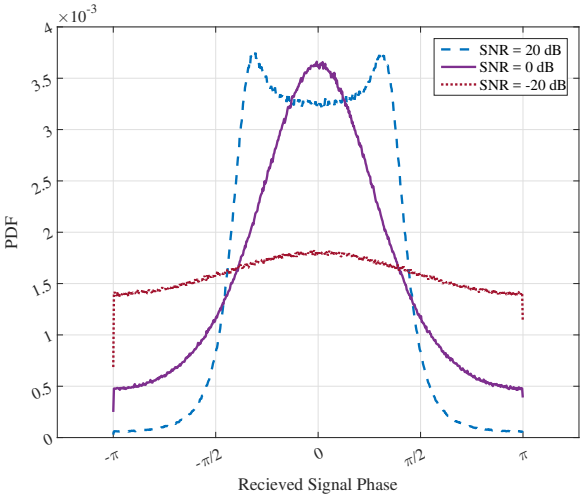

Fig. 7. PDF of Received signal Phase in different SNR values.

REFERENCES

[1] S. MirhoseiniNejad, V. T. Vakili, and D. Abbasi-Moghadam, "Secure resource allocation for the SISO-OFDM wiretap channel," *IET Communications*, vol. 11, no. 18, pp. 2702–2712, 2017.

[2] A. Rahmanpour, V. T. Vakili, and S. M. Razavizadeh, "Enhancement of physical layer security using destination artificial noise based on outage probability," *Wireless Personal Communications*, vol. 95, no. 2, pp. 1553–1565, July 2017.

[3] D. Abbasi-Moghadam and S. M. Mirhoseini-Nezhad, "Energy detector in ultra wideband systems using phase compensation technique," *Wireless Personal Communications*, vol. 79, no. 3, pp. 1609–1620, Dec 2014.

[4] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[5] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[6] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[7] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, no. 4, pp. 207–212, 1996.

[8] 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*, vol. 53, no. 11, pp. 3776–3784, Nov 2005.

[9] N. Döttling, D. Lazich, J. Müller-Quade, and A. S. de Almeida, "Vulnerabilities of wireless key exchange based on channel reciprocity," in *Information Security Applications*, 2011.

[10] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, June 2015.

[11] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *INFOCOM, 2011 Proceedings IEEE*. IEEE, pp. 1422–1430.

[12] 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 *Proceedings of the 15th annual international conference on Mobile computing and networking*. ACM, 2009, pp. 321–332.

[13] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," pp. 235–252, 2012.

[14] M. Zafer, D. Agrawal, and M. Srivatsa, "Limitations of generating a secret key using wireless fading under active adversary," *IEEE/ACM Transactions on Networking (TON)*, vol. 20, no. 5, pp. 1440–1451, 2012.

[15] J. N. Laneman and G. W. Wornell, "Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2415–2425, Oct 2003.