A Study of Injection and Jamming Attacks in Wireless Secret Sharing Systems

Arsenia Chorti

▶ **To cite this version:**

Arsenia Chorti. A Study of Injection and Jamming Attacks in Wireless Secret Sharing Systems. International Worskhop on Communication Security WCS 2017: Proceedings of the 2nd Workshop on Communication Security, 2017, Lecture Notes in Electrical Engineering. hal-01686232

HAL Id: hal-01686232
https://hal.science/hal-01686232

Submitted on 17 Jan 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A Study of Injection and Jamming Attacks in Wireless Secret Sharing Systems

invited paper

Arsenia Chorti

Abstract Secret key generation (SKG) schemes have been shown to be vulnerable to denial of service (DoS) attacks in the form of jamming and to man in the middle attacks implemented as injection attacks. In this paper, a comprehensive study on the impact of correlated and uncorrelated jamming and injection attacks in wireless SKG systems is presented. First, two optimal signalling schemes for the legitimate users are proposed and the impact of injection attacks as well as counter-measures are investigated. Finally, it is demonstrated that the jammer should inject either correlated jamming when imperfect channel state information (CSI) regarding the main channel is at their disposal, or, uncorrelated jamming when the main channel CSI is completely unknown.

1 Introduction

The increasing deployment of wireless networks poses security challenges in next generation dynamic and decentralized networks, consisting of low cost, low complexity devices. Over the last two decades alternative/complementary means to secure data exchange in wireless settings have been investigated in the framework of physical layer security (PLS), addressing jointly the issues of reliability and secrecy. One of the most mature topics in PLS is the generation of secret keys via public discussion, based on either the so-called source model [1, 2] or the so-called channel model [3].

Single letter characterizations of the secret key capacity were derived in [1], while in [2] it was demonstrated that the secret keys can be generated without any information leakage to a passive adversary; in [4] these results have been extended to multiple terminals. Simple secret key generation (SKG) techniques have been proposed for wireless networks by exploiting the inherent correlation of the channel

Arsenia Chorti is with the School of Computer Science and Electronic Engineering, Wivenhoe Park, Colchester, CO4 3SQ, UK, email: achorti@essex.ac.uk

state information (CSI) between a pair of legitimate nodes due to reciprocity [5]. Furthermore, SKG processes over unauthenticated channels have recently been proposed [6–8], allowing to consolidate the proposed techniques with standard authenticated encryption (A.E.) schemes [9].

However, SKG systems are not robust against all types of active adversaries. Recently, in [10] the effect of denial of service attacks (DoS) in the form of jamming was demonstrated to substantially decrease SKG rates; with increasing jamming power the SKG rates were shown to asymptotically diminish. In this investigation the adversaries were assumed to inject constant jamming signals and have been shown to have a maximum impact on the SKG system when they were able to evaluate the channel state information (CSI) in the links between themselves and the legitimate nodes (partial CSI availability). However, neither the optimality of employing constant jamming signals nor the scenario of an adversary with imperfect estimate of the main channel CSI were addressed.

Furthermore, in [11] and it was shown that injection type of attacks allow an active adversary to act as a man in the middle (MiM) and potentially control (a large) part of the generated key. A simple heuristic approach to defend against injection type of attacks was presented in [12] by multiplying the received signals with independent zero-mean random signals, locally generated at the legitimate nodes. Although the proposed approach allows converting injection attacks to (potentially less harmfull) uncorrelated jamming attacks, the choice of the independent random signals was not optimized to maximize the SKG rates.

The limited literature on the impact of active adversaries on SKG systems reveals that a systematic analysis of these types of attacks is timely. In the present study, we begin with a review of joint SKG and crypto protocols in Section II. Next, we determine optimal signalling schemes for the pair of legitimate nodes in Section III, where we also investigate injection type of attacks. It is demonstrated that by employing a binary symmetric Bernoulli probing the legitimate nodes can reduce the injection attack to an uncorrelated jamming attack. Subsequently, jamming attacks are investigated in detail in Section IV, accounting for the worst case scenario in which a malicious node might obtain an imperfect estimate of the main channel CSI. This worst case scenario is essential in evaluating realistically the limitations of employing physical layer security techniques in next generation systems as argued in [13]. The conclusions of this work are presented in Section V.

2 Secret Key Generation Systems in the Presence of an Active Adversary

The SKG standard procedure typically encompasses three phases [2]:
1) Advantage distillation: The legitimate nodes exchange probe signals to obtain estimates of their reciprocal CSI and pass them through a suitable quantizer [14]. Commonly, the received signal strength (RSS) has been used as the CSI parameter for generating the shared key [15], while in [9, 16] the CSI phase has been used.

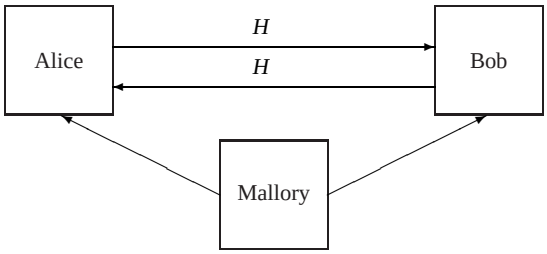

Fig. 1 System model of the SKG process. Alice and Bob denote the legitimate nodes and Mallory an active adversary.

2) Information reconciliation: Discrepancies in the quantizer local outputs due to imperfect channel estimation are reconciled through public discussion using Slepian Wolf decoders. Numerous practical information reconciliation approaches using standard forward error correction (FEC) codes such as low density parity check codes have been proposed [17], [18], while in [9] the possibility of employing short Bose, Chaudhuri, Hocquenghem (BCH) FEC codes has also been explored.
3) Privacy amplification: Applying universal hash functions to the reconciled information ensures that the generated keys are uniformly distributed and completely unpredictable by an adversary [19]. Privacy amplification ensures that the generated keys have maximum entropy (i.e., are uniformly distributed). More importantly, it ensures that even if an adversary has access to (even a large) part of the decoder output, the final secret key can be unpredictable [20].

The baseline SKG system model in the presence of an active adversary is depicted in Fig. 1. Following standard nomenclature of information security, the legitimate nodes are referred to as Alice and Bob while the malicious active adversary as Mallory. The SKG process exploiting rich multipath wireless channels includes two distinct cycles over which the channel coefficients between Alice and Bob are assumed to be reciprocal and stationary and then to change independently [20, 21], i.e., both cycles take place within the channel's coherence time[1]. The main channel fading coefficient is denoted by H and is modeled as a complex zero-mean Gaussian circularly symmetric random variable $H \sim \mathscr{CN}(0, \sigma_H^2)$.

Typically, in modern communication systems, tampering attacks are averted by the employment of public key encryption (PKE) schemes when no pre-shared secret (i.e., a pre-established key at both Alice and Bob) is available. To be deemed adequately robust, current PKE schemes rely on trapdoor functions such as the Rivest-Shamir-Adleman (RSA) protocol or Diffie-Hellman (DH) variants with key lengths of at least 2048 bits. However, the computational resources required to generate symmetric keys using RSA or DH are substantial. Even more importantly, increasing computing power and especially the potential of quantum computing, threatens

[1] This assumption does not affect the nature of the conclusions reached. For more realistic channel models that account for correlation of the fading coefficients see [22] and related works.

these schemes. As a result, the key generation phase in the PKE protocol can be a limiting factor in the performance of resource constrained systems such as sensor networks, and, physical layer security alternatives would be worth exploring [23].

To develop robust algorithms that can withstand tampering attacks, standard symmetric key block ciphers and message authentication (MAC) protocols can be used in conjunction with SKG [6–9,15]. Reviewing such a possible scheme, let us assume that Alice wishes to transmit over a wireless multipath channel a secret message `m` to Bob. The following algorithms are employed: the SKG scheme, a symmetric encryption algorithm denoted by `Es` with corresponding decryption `Ds` and a MAC denoted by `Sign` with a corresponding verification algorithm `Ver` .

The SKG procedure is launched between Alice and Bob; at the output of her Slepian Wolf decoder Alice obtains a secret key `K` and a corresponding coset. She breaks her key in two parts `K={Ke, Ki}` and uses the first part of the key to encrypt the message as the ciphertext `cipher=Es(Ke, m)`. Subsequently, using the second part of the key she signs the ciphertext using the signing algorithm `t=Sign(Ki, cipher)` and transmits to Bob the extended ciphertext $\mathtt{C} = [\mathtt{coset}||\mathtt{cipher}||\mathtt{t}]$.

Bob checks the integrity of the received ciphertext as follows: from `C` he extracts `coset, cipher` and `t`. From `coset` and his own observation he evaluates `K={Ke, Ki}`. Subsequently, Bob evaluates `v=Ver(Ki, cipher, t)`; `v` is either equal to $\perp$ if the integrity test failed or `cipher` if the integrity test was successful. The integrity test will fail if any part of `C` was modified; for example, if `coset` was modified during the transmission then Bob would have evaluated a wrong key `K` and the integrity test would have failed. If the integrity test was successful then Bob decrypts `m=Ds(Ke, cipher)`.

It is clear form the above that building semantically secure A.E. protocols using the SKG procedure is straightforward as long as the channel channel probing phase of the scheme is robust against active attacks. Therefore it is of particular interest to study man in the middle (MiM) and denial of service attacks during the channel excitation phase of the SKG protocol. In the following Sections two such active attacks during the channel probing are discussed. Firstly, MiM attacks referred to as ”injection” attacks are investigated in Section 3; an active adversary – Mallory – tries to control part of the generated secret key `K` by spoofing the channel estimation phase of the SKG scheme. Subsequently, in Section 4, DoS in the form of jamming are studied. In either case Mallory’s optimal strategy is discussed and respective countermeasures are proposed.

3 MiM in SKG Systems: Injection Attacks

We begin our discussion of injection attacks by investigating optimal signalling schemes for SKG systems.

3.1 Optimal Signalling

Let us assume that Alice and Bob exchange a probe signal X and that their respective observations Z_A and Z_B, can be expressed as

$$Z_A = XH + N_A, \tag{1}$$
$$Z_B = XH + N_B, \tag{2}$$

where X denotes the channel input and N_A and N_B denote zero mean Gaussian random variables that model the impact of additive white Gaussian noise with $(N_A, N_B) \sim \mathscr{CN}(0, \mathrm{diag}(\sigma_A^2, \sigma_B^2))$. An upper bound on the SKG rate is given by $\min[I(Z_A;Z_B), I(Z_A;Z_B|Z_M)]$, where Z_M denotes the adversarial observation [1], [2]. In Rayleigh fading channels in particular, the above bound can be made tight and the SKG capacity can be expressed as $C = I(Z_A;Z_B)$ if Z_M is uncorrelated with Z_A and Z_B due to the decorrelation properties of the fading coefficients over short distances (of the order of a wavelength) [24], [18]. In the following we assume that the decorrelation property holds.

For the above system model with an average power constraint $\mathbb{E}[|X|^2] \leq P$ and assuming the adversary's observation is independent from Z_A, Z_B, the input distribution of X maximizing the secret key capacity $C = I(Z_A;Z_B)$ is discrete with a finite number of mass points, similarly to the optimal input distribution of Rayleigh fading channels without CSI at the transmitter and the receiver [25]. To verify the validity of this statement we begin by formulating the signalling optimization problem as

$$\max_{p(x)} I(Z_A;Z_B) \tag{3}$$
$$\text{s.t. } \mathbb{E}[|X|^2] \leq P.$$

where $p(x)$ is the pdf of X. (1), (2) correspond to the two-look channel [26, pp. 290] with input variable XH and power constraint $\mathbb{E}[|XH|^2] = \mathbb{E}[|X|^2]\mathbb{E}[|H|^2] = \mathbb{E}[|X|^2]\sigma_H^2 \leq P\sigma_H^2$. The input distribution that maximizes $I(Z_A;Z_B)$ is Gaussian [26] while the convexity of the mutual information dictates transmitting with maximum power.

Remark 1: Since $H \sim \mathscr{CN}\left(0, \sigma_H^2\right)$, scalar signalling $X = \sqrt{P}$ preserves the Gaussianity of the input and is therefore optimal. This is the standard signalling method employed in SKG systems, e.g., [18]. However, it is worth noting that the Gaussianity of the product XH is also preserved when X is a zero-mean symmetric Bernoulli random variable with support $k = \{-\sqrt{P}, \sqrt{P}\}$ and probability mass function $p_X(-\sqrt{P}) = p_X(\sqrt{P}) = 0.5$. Next, it is demonstrated that using the latter signalling as opposed to the former can be employed as a simple defense mechanism, reducing injection type of attacks to jamming attacks.

3.2 Injection Attacks

MiM in the form of injection type of attacks constitute one of the most serious limitations in SKG systems extracting secret keys from RSS measurements [5, 11, 12] (it is yet unknown whether this attack can be launched to systems using CSI or the phase of the received signal [13]). Various possible approaches have so far surfaced on how to launch injection attacks; in [5] the attack consisted in controlling the movement of intermediate objects in the wireless medium, thus generating predictable changes in the received RSS (e.g., by obstructing or not a LOS), while in [11] whenever similar channel envelope measurements were received from Alice and Bob, Mallory spoofed the SKG process by injecting a MiM signal W.

Irrespective of the practical approach used to launch the attack, Alice's and Bob's observations respectively under injection type of attacks can be expressed as:

$$Z_A = XH + W + N_A, \tag{4}$$
$$Z_B = XH + W + N_B. \tag{5}$$

where W denotes the spoofing signal.

Assuming a power constraint $\mathbb{E}[|W|^2] \leq \Gamma$, an upper bound of the secret key rate controlled Mallory is given by

$$L \leq I(Z_A, Z_B; W). \tag{6}$$

The optimal injection signal corresponds to capacity maximizing two-look Gaussian channel and can be shown to be Gaussian [26]. Assuming that $W \sim \mathscr{CN}(0, \Gamma)$ we have that

$$\begin{aligned} I(Z_A, Z_B; W) &= h(Z_A, Z_B) - h(XH + N_A, XH + N_B) \\ &= \log(2\pi e)^2 |K| - \log(2\pi e)^2 |Q| \\ &= \log\left(1 + \frac{\Gamma}{P\sigma_H^2 + \frac{\sigma_A^2 \sigma_B^2}{\sigma_A^2 + \sigma_B^2}}\right), \end{aligned} \tag{7}$$

where $(Z_A, Z_B) \sim \mathscr{CN}(\mathbf{0}, K)$ with

$$K = \begin{pmatrix} P\sigma_H^2 + \Gamma + \sigma_A^2 & P\sigma_H^2 + \Gamma \\ P\sigma_H^2 + \Gamma & P\sigma_H^2 + \Gamma + \sigma_B^2 \end{pmatrix}$$

and $(XH + N_A, XH + N_B) \sim \mathscr{CN}(\mathbf{0}, Q)$ with

$$Q = \begin{pmatrix} P\sigma_H^2 + \sigma_A^2 & P\sigma_H^2 \\ P\sigma_H^2 & P\sigma_H^2 + \sigma_B^2 \end{pmatrix}. \tag{8}$$

In the following two possible countermeasures are discussed based on the availability of side information regarding the injection signal W.

3.3 Defense against MiM with Side Information

Injection type of attacks can be averted at the privacy amplification stage [12]. However, it is necessary for Alice and Bob to be able to estimate the necessary compression rate to suppress information leakage to Mallory. This task is not trivial as Alice and Bob would need to be able to measure L, which is only possible when side information regarding the power Γ of W is available at Alice and Bob.

For the system model described in (4) and (5) the achievable rate $I(Z_A;Z_B)$ at the output of the Slepian Wolf decoders can be evaluated as:

$$\begin{aligned} I(Z_A;Z_B) &= h(Z_A)+h(Z_B)-h(Z_A,Z_B) \\ &= \log\left(1+\frac{P\sigma_H^2+\Gamma}{\sigma_A^2+\sigma_B^2+\frac{\sigma_A^2\sigma_B^2}{P\sigma_H^2+\Gamma}}\right). \end{aligned} \tag{9}$$

Assuming that Mallory does not have any side information regarding H, the secret key rate is upper bounded by [1]

$$\begin{aligned} C &\le \min[I(Z_A;Z_A|W),I(Z_A;Z_B)] \\ &= I(Z_A;Z_B|W) \\ &= h(Z_A,Z_B|W)-h(N_A,N_B) \\ &= \log\left(1+\frac{P\sigma_H^2}{\sigma_A^2+\sigma_B^2+\frac{\sigma_A^2\sigma_B^2}{P\sigma_H^2}}\right). \end{aligned} \tag{10}$$

Therefore, the necessary compression rate D at the privacy amplification stage is lower bounded by

$$\begin{aligned} D &\ge I(Z_A;Z_B)-I(Z_A;Z_B|W) \\ &= \log\left(1+\frac{(P\sigma_H^2+\Gamma)^2}{(P\sigma_H^2+\Gamma)(\sigma_A^2+\sigma_B^2)+\sigma_A^2\sigma_B^2}\right) \\ &\quad -\log\left(1+\frac{(P\sigma_H^2)^2}{P\sigma_H^2(\sigma_A^2+\sigma_B^2)+\sigma_A^2\sigma_B^2}\right). \end{aligned} \tag{11}$$

As long as Mallory does not have a practically noiseless channel, rate compression of the (maximum achievable) rate $I(Z_A;Z_B)$ at the outputs of the Slepian Wolf decoders by at least D ensures that Alice and Bob can establish a secret key without leakage to Mallory.

3.4 Defense against MiM without Side Information

An alternative countermeasure against MiM attacks was proposed in [12], denoted by user introduced randomness (UIR). The central idea behind the proposed approach was the post-multiplication of Alice's and Bob's observation by local zero-mean independent random variables to eliminate any correlation between the injected signals observed by Alice and Bob. Following this approach it is possible to reduce injection attacks to jamming attacks. Motivated by the UIR approach and taking into consideration *Remark 1*, we propose the following modification of the standard SKG protocol with constant signalling $X=\sqrt{P}$, detailed in the following.

Alice and Bob observe local sources of randomness denoted by ω_A and ω_B respectively. According to the output of ω_A Alice transmits a random probe signal X following a zero-mean symmetric Bernoulli distribution with support $k=\{-\sqrt{P},\sqrt{P}\}$ and success probability $p=0.5$, $X\sim\mathscr{B}(p,k)$. Likewise, Bob observes ω_B and generates a random probe signal $Y\sim\mathscr{B}(p,k)$. Finally Alice and Bob use X,Y to post-multiply their observations so that the secret key is to be generated from the new observations

$$\tilde{Z}_A = XYH + XW + XN_A, \tag{12}$$

$$\tilde{Z}_B = XYH + YW + YN_B. \tag{13}$$

Due to the fact that X,Y are independent and zero-mean, it is straightforward to show that XW and YW are uncorrelated while the Gaussianity of $\tilde{Z}_A,\tilde{Z}_B$ is preserved. Alice and Bob extract the common key from the new common randomness XYH instead of H. On the other hand, since XH,YH,XN_A,Y_NB are independent zero-mean Gaussian random variables, the proposed scheme renders injection attacks to uncorrelated jamming attacks.

Assuming that Mallory does not have any information on XYH, the secret key capacity is upper bounded by [1]

$$\begin{aligned}\tilde{C} &\leq \min[I(\tilde{Z}_A;\tilde{Z}_A|W),I(\tilde{Z}_A;\tilde{Z}_B)]\\ &= I(\tilde{Z}_A;\tilde{Z}_B)\\ &= \log\left(1+\frac{P\sigma_H^2}{\sigma_A^2+\sigma_B^2+2\Gamma+\frac{(\sigma_A^2+\Gamma)(\sigma_B^2+\Gamma)}{P\sigma_H^2}}\right).\end{aligned} \tag{14}$$

4 Jamming Attacks

There have been numerous analyses of proactive and reactive jamming attacks in wireless systems [27], the main difference between the two being whether the malicious node injects jamming signals constantly or during certain parts of the communication cycle. It has been found that standard methods for identifying and pro-

tecting against reactive jamming attacks can fail because of the low energy required to launch the attack compared to proactive jamming. It can be deduced that with respect to (w.r.t.) SKG systems it is necessary for Mallory to disrupt only one of the two communication cycles in order to inflict an efficient attack.

Based on this observation, the set up for the study of jamming attacks is detailed in the following: During the first cycle, Alice broadcasts probe signals X while Mallory observes the channel and obtains an estimate $\hat{H}$ of the main channel CSI that satisfies [28], [29]

$$H = \sqrt{1-\alpha^2}\hat{H} + \alpha\tilde{H}, \tag{15}$$

where $\tilde{H} \sim \mathscr{CN}(0,\sigma_H)$ denotes the estimation error and $\alpha \in [0,1]$. For $\alpha = 0$ Mallory has a perfect estimate of the main channel CSI while for $\alpha = 1$ Mallory has no main channel CSI. In analogy to the first cycle, during the second cycle Bob broadcasts Y.

In standard SKG systems $\alpha = 1$, however in the present investigation we allow for the possibility of a very powerful adversary using ray tracing techniques as proposed in [13]. The motivation behind investigating scenarios with $\alpha < 1$ lies the numerous practical systems implementing basic versions of the SKG approach using the RSS as the source of shared randomness due to ease of implementation and not accounting for phase information in the CSI; in these types of systems, particularly in Rician environments it is possible to retrieve a noisy version of the shared randomness variable. Furthermore, we assume that Mallory is able to obtain a perfect estimate of its CSI to Alice and Bob.

In this work we assume that Mallory attempts to obtain an estimate of the main channel CSI over the first cycle and transmit a jamming signal J over the second with power Γ. Based on the above, Alice's and Bob's observations, denoted by Z_A and Z_B, respectively, can be expressed as

$$Z_A = H_0 X + N_A, \tag{16}$$

$$Z_B = H_0 X + GJ + N_B, \tag{17}$$

where $G \sim \mathscr{CN}(0,\sigma_G^2)$ models the Bob-Mallory link CSI, $(N_A, N_B) \sim \mathscr{CN}(\mathbf{0}, \mathbf{I}_2)$ denote i.i.d. circularly symmetric complex Gaussian random variables modeling the effect of white noise on the system and $\mathbf{I}_n$ the identity matrix of dimension n. For the establishment of the secret key Alice needs to transmit reconciliation data to Bob at a minimum rate $h(Z_2|Z_1)$ [1], [2], [24]. Using this model, in [10] the metric employed to evaluate the impact of a jammer on the SKG process was defined by

$$R = \frac{h(Z_2|Z_1)}{C}, \tag{18}$$

where C denotes the SKG capacity. In this study, for simplicity the derivation of optimal jamming schemes and of the power allocation policies for the jammer employs as objective function the raw rate of reconciliation data $h(Z_2|Z_1)$.

4.1 Full Main Channel CSI at Mallory: Correlated Jamming

For simplicity, in the following, we assume that the legitimate users employ constant signalling $X = Y = \sqrt{P}$. In the case of perfect CSI availability at the jammer, it has been shown that correlated jamming is optimal in point-to-point as well as multi-user and multiple input multiple output systems [30, 31]. We will demonstrate that the same is true in the case of SKG systems when $\alpha = 0$. When the jammer has a perfect estimate of the main channel CSI H the SKG capacity is $C = 0$ and it can be argued that jamming is not necessary; however, the following analysis will serve as the basis in deriving the jamming strategy in the realistic scenario $\alpha > 0$.

In this context, following the methodology introduced in [10] we assume that Mallory's objective is the disruption of the SKG process (instead of eavesdropping), by increasing the cost of the reconciliation phase, i.e., by maximizing $h(Z_B|Z_A)$. Employing this criterion the following proposition formalizes the jammer's optimal jamming strategy.

Proposition 1 When full CSI is available at the jammer, the optimal jamming signal J that maximizes the minimum required rate of reconciliation data $h(Z_B|Z_A)$ is linear to H.

Proof: The jammer wishes to maximize

$$h(Z_B|Z_A) = h(Z_A, Z_B|H) + h(H) - h(Z_A). \tag{19}$$

The maximization is achieved by maximizing the term $h(Z_A, Z_B|H)$ that is controlled by the jammer; $h(H)$ and $h(Z_A)$ are independent of the jammer's actions. We show that a linear jamming signal achieves this goal.

We have that

$$\begin{aligned} & h(Z_A, Z_B|H) \\ & = h(Z_A, Z_B - \lambda H|H) \\ & \leq h(Z_A, Z_B - \lambda H) \qquad (20) \\ & \leq \log\left((2\pi e)^2|\Lambda|\right), \qquad (21) \end{aligned}$$

where (20) holds because conditioning reduces entropy and Λ is the covariance matrix of $(Z_A, Z_B - \lambda H)$. Regarding (21), we note that for a given autocorrelation matrix the entropy is maximized by a Gaussian distribution [26]. (20) and (21) hold for arbitrary λ; here we choose $\lambda = \frac{\mathbb{E}[Z_B H^*]}{\sigma_H^2}$.

Now let's assume that the jammer employs linear jamming so that the jamming signal can be expressed as

$$J = \frac{\kappa}{G} H + \sqrt{v}, \tag{22}$$

where $\kappa \in \mathbb{R}$ and $v \in \mathbb{R}^+$. Substituting (22) into (16)-(17), the observations at Alice and Bob can then be rewritten as

$$Z_A = \sqrt{P}H + N_A, \tag{23}$$

$$Z_B = \left(\sqrt{P} + \kappa\right)H + \sqrt{v}G + N_B. \tag{24}$$

Next, suppose that optimal $\tilde{J}$ is found so that $h(Z_A, Z_B|H)$ is maximized, or, equivalently, (21) is satisfied with equality. We define R such that

$$R = \tilde{J} - \frac{\mathbb{E}\left[\tilde{J}H^*\right]}{\sigma_H^2}H, \tag{25}$$

so that R is uncorrelated with H. Exploiting this fact, the power of the optimal jamming signal is found to be

$$\mathbb{E}\left[|\tilde{J}|^2\right] = \frac{\mathbb{E}\left[\left|\tilde{J}H^*\right|^2\right]}{\sigma_H^2} + \mathbb{E}\left[|R|^2\right],$$

and must satisfy the power constraint so that the optimal jamming signal is feasible.

We observe that setting

$$\kappa = \frac{\mathbb{E}\left[\tilde{J}GH^*\right]}{\sigma_H^2}, \tag{26}$$

$$v = \mathbb{E}\left[|R|^2\right], \tag{27}$$

results in J having the same power as $\tilde{J}$. Furthermore, the autocorrelation matrix Λ is the same for both J and $\tilde{J}$. Since uncorrelated Gaussian signals are also independent, $\tilde{J}$ achieves (20) and (21) with equality, and therefore so does J. In conclusion, J has power equal to that of the optimal jamming signal and satisfies the same constraints as the optimal jamming signal; as a result, J is optimal. □

Remark: If Mallory has enough available power then the optimal jamming signal can designed so that $\kappa = -\sqrt{P}$, i.e., Bob's transmission during the second cycle can be completely canceled off.

4.2 Imperfect Main Channel CSI at Mallory: Linear Jamming

Now let us assume that Mallory has imperfect main channel CSI s.t. $H = \sqrt{1-\alpha^2}\hat{H} + \alpha\tilde{H}$ for some $\alpha \in (0,1)$ and perfect channel CSI for the link Mallory-Alice. Based on the analysis in 4.1 Mallory can simply inject linear jamming in the form

$$J = \frac{\kappa}{G}\sqrt{1-\alpha^2}\hat{H}, \tag{28}$$

so that Bob's observation can be expressed as:

$$Z_B = (\sqrt{P} + \kappa)H + \tilde{N}_B, \tag{29}$$

with $\tilde{N}_B = N_B - \alpha\kappa\tilde{H}$. Similarly to the case of perfect main channel CSI, $h(Z_B|Z_A)$ is maximized for $\kappa = -\sqrt{P}$ if the jammer has sufficient power resources. When imperfect main channel CSI $\hat{H}$ is at Mallory's disposal, the jamming signal that maximizes the rate of reconciliation data $h(Z_B|Z_A)$ is linear to $\hat{H}$.

4.3 Absence of Main Channel CSI at Mallory: Uncorrelated Jamming

Next, the optimal jamming is characterized in absence of main channel CSI, i.e., $\alpha = 1$ in the following proposition.

Proposition 2: For $\alpha = 1$ when no main channel CSI is available at the jammer the optimal jamming signal J is the constant signal $J = \sqrt{\Gamma}$.

Proof: The case of absence of main channel CSI can be treated as a subcase of the full CSI availability case examined in 4.1. Based on this observation, as shown in the proof of Proposition 4.1, the optimal jamming signal can be expressed as $J = \frac{\mathbb{E}[JGH^*]}{\sigma_H^2 G}H + \sqrt{v}$. In absence of knowledge of H, the term JG is *necessarily* uncorrelated with H so that $J = \frac{\mathbb{E}[JG]\mathbb{E}[H^*]}{\sigma_H^2 G}H + \sqrt{v} = \sqrt{v}$. Finally, due to the convexity of the entropy, maximization is achieved when the power constraint is satisfied with equality, i.e., $J = \sqrt{v} = \sqrt{\Gamma}$. □

5 Conclusions

In this study optimal signalling schemes were derived for SKG systems. Furthermore, a detailed analysis of injection type of attacks has revealed that it is possible to reduce them to jamming attacks by suitable signalling. Finally, the impact of correlated and uncorrelated jamming has been studied.

References

1. R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. part I: secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.
2. U. Maurer, "Secret key agreement by public discussion based on common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 5, pp. 733–742, May 1993.
3. L. Lai, Y. Liang, and H. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 480–490, Apr. 2012.
4. I. Csiszár and P. Narayan, "Secrecy capacities for mulitple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.
5. S. Jana, S. P. Nandha, 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 *Proc. 15th Annual Int. Conf. Mobile Comput. Netw.* ACM, 2009, pp. 321–332.

6. U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-part I: definitions and a completeness result," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 822–831, Apr. 2003.
7. ——, "Secret-key agreement over unauthenticated public channels-part II: the simulatability condition," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 832–838, Apr. 2003.
8. ——, "Secret-key agreement over unauthenticated public channels-part III: privacy amplification," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 839–851, Apr. 2003.
9. C. Saiki and A. Chorti, "A novel physical layer authenticated encryption protocol exploiting shared randomness," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Florence, Italy, Sep. 2015, pp. 113–118.
10. M. Zafer, D. Agrawal, and M. Srivatsa, "Limitations of generating a secret key using wireless fading under active adversary," *IEEE/ACM Trans. Netw.*, vol. 20, no. 5, pp. 1440–1451, Oct. 2012.
11. S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," in *Proc. 17th Europ. Symp. Research Comput. Security – Comput. Security (ESORICS)*, S. Foresti, M. Yung, and F. Martinelli, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 235–252.
12. J. Rong and Z. Kai, "Physical layer key agreement under signal injection attacks," in *IEEE Conf. Commun. Netw. Security (CNS)*, 2015, pp. 254–262.
13. W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.
14. Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE Int. Conf. Computer Commun. (INFOCOM)*, 2011, pp. 1422–1430.
15. S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.* ACM, 2008, pp. 128–139.
16. A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE Int. Conf. Acoustics, Speech Signal Process. (ICASSP)*, Las Vegas, NV, Mar. 30 Apr. 4 2008, pp. 3013–3016.
17. C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. Int. Symp. Inform. Theory (ISIT)*, Seatle, US, Jul. 2006, pp. 2593–2597.
18. C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–154, Jun. 2010.
19. U. Maurer, R. Renner, and S. Wolf, *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*. Springer London, 2007, ch. Unbreakable Keys from Random Noise, pp. 21–44.
20. M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, UK: Cambridge University Press, 2011.
21. A. Mukherjee, S.A.A., Fakoorian, H. Jing, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Comm. Surveys Tuts*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart. 2014.
22. C. Chen and M. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb. 2011.
23. A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.
24. R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in UWB channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.
25. I. C. Abou-Faycal, M. D. Trott, and S. Shamai, "The capacity of discrete-time memoryless rayleigh-fading channels," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1290–1301, May 2001.
26. T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ: John Wiley and Sons, Inc., 2006.

27. S. Fang, Y. Liu, and P. Ning, "Wireless communications under broadband reactive jamming attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 3, pp. 394–408, Mar. 2016.
28. A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
29. G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, Jun. 2014.
30. M. Médard, "Capacity of correlated jamming channels," in *Proc. 35th Annu. Allerton Conf. Commun., Control Comp.*, Monticello, IL, Sep.-Oct. 1997.
31. S. Shafiee and S. Ulukus, "Mutual information games in multiuser channels with correlated jamming," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4598–4607, Oct. 2009.