Overcoming Limitations of Secret Key Generation in Block Fading Channels Under Active Attacks

Arsenia Chorti

Overcoming Limitations of Secret Key Generation in Block Fading Channels Under Active Attacks

Arsenia Chorti
School of Computer Science and Electronic Engineering, University of Essex
Wivenhoe Park, Colchester, CO4 3SQ, UK
Email: achorti@essex.ac.uk

***Abstract*—The topic of physical layer key agreement in Gaussian block fading channels in the presence of active adversaries is investigated in the present contribution. Frequency hopping versus frequency spreading are studied as potential defence strategies against denial of service (DoS) attacks in the form of jamming. We begin by investigating the optimal power allocation policy for the jammer – in the case of frequency spreading – when side information is available. Through numerical evaluations it is shown that effect of the availability of side information on the jammer's impact is minimal. Next, the competitive interaction between the legitimate nodes and the jammer is formulated as a one-shot zero-sum game; it is found that under short term power constraints, the legitimate nodes should optimally employ frequency hopping while the jammer should employ frequency spreading. Comparing the achievable secret key generation rates in systems with and without frequency hopping demonstrates that increasing the available bandwidth can diminish the limitations of secret key generation in the presence of active adversaries.**

***Index Terms*—Physical layer security, secret key generation, frequency hopping, denial of service attacks, active attack**

I. Introduction

One of the most mature topics in physical layer security is the generation of secret keys via public discussion, based on either the so-called source model or the so-called channel model [1]–[5]; in [6] a joint source-channel model was investigated. However, such schemes are known to be vulnerable to denial of service attacks (DoS) in the form of jamming from an active adversary or interference from benign network users. As an example, in [7] and [8] the effect of pilot contamination was investigated for received signal strength (RSS) schemes. More importantly, in [9] the effect of jamming was demonstrated to substantially decrease the achievable SKG rates; with increasing jamming power the SKG rates were shown to asymptotically diminish.

In this work anti-jamming approaches for SKG systems in Gaussian block fading channels are investigated by focusing on the possible use of frequency hopping versus frequency spreading. We begin our investigation by deriving the optimal power allocation policies for the pair of legitimate nodes and the jammer under short-term power constraints. Subsequently, the competitive interaction between the legitimate nodes and the active adversary is formulated as a one-shot zero-sum game. The pure strategy "Hop, Spread" is shown to be the Nash equilibrium of this game, i.e, under jamming attacks the legitimate nodes should employ frequency hopping while the jammer should spread the available jamming power equally across the whole band. Through simulation results it is demonstrated that frequency hopping can alleviate the impact of Gaussian jamming and that the achievable SKG rates increase with increasing bandwidth resources.

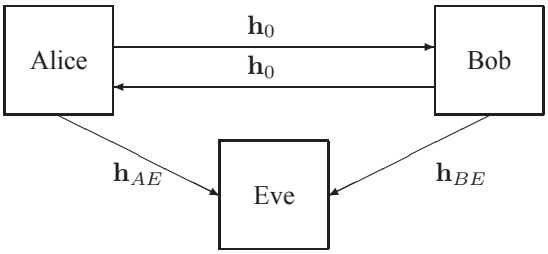

Fig. 1. System model.

The rest of the paper is organized as follows. The system model is described in Section II. Furthermore, in Section III the optimal power allocation strategies for the pair of legitimate nodes and the jammer are derived. The game theoretic study of frequency hopping versus frequency spreading under jamming attacks is discussed in Section IV. Finally, the paper conclusions are drawn in Section V.

II. System Model

The system model is shown in Fig.1 with Alice and Bob denoting legitimate nodes and Eve a jammer transmitting Gaussian noise like signals. A parallel flat fading channel model is considered in which a transmission frame encompasses $M \geq 2$ parallel subchannels [10]. The fading channel coefficients are modeled to be i.i.d. random variables, i.e., they remain constant over each transmission block of N channel uses and change independently from one block to the next. Commonly in literature N is assumed sufficiently large ($N \to \infty$) and each codeword spans $M \times N$ channel uses. The case of $M = 1$ corresponds to systems without frequency hopping. Finally, the channel between Alice and Bob is assumed to be reciprocal and stationary during each transmission cycle and to change independently from one transmission cycle to the next.

Each cycle includes the transmission of two consecutive probe signals, from Alice to Bob and from Bob to Alice. Alice and Bob broadcast probe signals with power

$\mathbf{p} = \left[p^{(1)}, \ldots, p^{(M)}\right]$ over the corresponding subchannels while Eve transmits jamming signals with power $\gamma = \left[\gamma^{(1)}, \ldots, \gamma^{(M)}\right]$. Denoting by $\mathbf{h}_0 = \left[h_0^{(1)}, \ldots, h_0^{(M)}\right]$ the vector of the fading coefficients in the link between Alice and Bob over the M subchannels, by $\mathbf{h}_{EA} = \left[h_{EA}^{(1)}, \ldots, h_{EA}^{(M)}\right]$ the vector of the fading coefficients in the link between Eve and Alice and by $\mathbf{h}_{EB} = \left[h_{EB}^{(1)}, \ldots, h_{EB}^{(M)}\right]$ the vector of the fading coefficients in the link between Eve and Bob, Alice's and Bob's observations on the i-th subchannel – denoted by $z_A^{(i)}$ and $z_B^{(i)}$ respectively – can be expressed as,

$$z_A^{(i)} = \sqrt{p^{(i)}} h_0^{(i)} + \sqrt{\gamma^{(i)}} h_{EA}^{(i)} + n_A^{(i)} = h_0^{(i)} + n_1^{(i)}, \quad (1)$$

$$z_B^{(i)} = \sqrt{p^{(i)}} h_0^{(i)} + \sqrt{\gamma^{(i)}} h_{EB}^{(i)} + n_B^{(i)} = h_0^{(i)} + n_2^{(i)}, \quad (2)$$

for $i = 1, \ldots, M$. $n_A^{(i)}$ and $n_B^{(i)}$ denote independent and identically distributed (i.i.d.) zero-mean unit variance Gaussian random variables modeling the effect of white noise on the system and $n_1^{(i)} = \sqrt{\gamma^{(i)}} h_{EA}^{(i)} + n_A^{(i)}$, $n_2^{(i)} = \sqrt{\gamma^{(i)}} h_{EB}^{(i)} + n_B^{(i)}$.

III. Optimal Power Allocation over Block Fading Channels

In the following, we assume the following short-term power constraints are in place:

$$\frac{1}{M} \sum_{i=1}^{M} p^{(i)} \leq P, \; p^{(i)} \geq 0, \; i = 1, \ldots, M, \quad (3)$$

$$\frac{1}{M} \sum_{i=1}^{M} \gamma^{(i)} \leq P_j, \; \gamma^{(i)} \geq 0, \; i = 1, \ldots, M, \quad (4)$$

where P denotes the short-term average power constraint for the legitimate users and P_j the corresponding short-term average power constraint for the jammer.

Starting from the results in [11] and extending them to block fading channels, the SKG capacity C_k can be expressed as

$$C_k(\mathbf{p}, \gamma) = \frac{1}{M} \sum_{i=1}^{M} \log_2 \left(1 + \frac{P^{(i)}}{N_1^{(i)} + N_2^{(i)} + \frac{N_1^{(i)} N_2^{(i)}}{P^{(i)}}} \right), \quad (5)$$

where

$$P^{(i)} = {\sigma_0^2}^{(i)} p^{(i)}, \quad (6)$$

$$N_1^{(i)} = 1 + {\sigma_{EA}^2}^{(i)} \gamma^{(i)}, \quad (7)$$

$$N_2^{(i)} = 1 + {\sigma_{EB}^2}^{(i)} \gamma^{(i)}, \quad (8)$$

and ${\sigma_0^2}^{(i)} = \mathbb{E}\left[|h_0^{(i)}|^2\right]$, ${\sigma_{EA}^2}^{(i)} = \mathbb{E}\left[|h_{EA}^{(i)}|^2\right]$ and ${\sigma_{EB}^2}^{(i)} = \mathbb{E}\left[|h_{EB}^{(i)}|^2\right]$.

A. Power Allocation in Frequency Spreading Systems

It is reasonable to assume that Alice and Bob do not have any information on the channel CSI; as a result their optimal power allocation policy in frequency spreading is the solution of the following optimization problem

$$\arg\max_{\mathbf{p}} C_k(\mathbf{p}, \gamma) \text{ s.t. } (3). \quad (9)$$

Due to the fact that (5) is non-decreasing in $\mathbf{p}$, the optimal power allocation policy – denoted by $\mathbf{p}^*$ – is the equidistribution of the power resources, i.e.,

$$\mathbf{p}^* = [P, \ldots, P]. \quad (10)$$

This is a general result for the maximization of monotonic cost functions in blind scenarios; for details on a proof using dynamic programming see the blind scenario in Appendix B of [12].

Furthermore, with respect to Eve we investigate two possible scenarios. First, if jamming is injected without knowledge of the variance of the channel fading coefficients in the links to Alice and Bob (blind scenario), in analogy to the blind scenario for Alice and Bob the optimal power allocation policy for Eve is to evenly distribute the available power, i.e.,

$$\gamma^* = [P_j, \ldots, P_j]. \quad (11)$$

On the other hand – accounting for the worst case scenario – if we assume that Eve has knowledge of ${\sigma_0^2}^{(i)}, {\sigma_{EA}^2}^{(i)}, {\sigma_{EB}^2}^{(i)}, i = 1, \ldots, M$ and of the power allocation policy (10), γ^* can be evaluated as the solution of the optimization problem

$$\arg\min_{\gamma} C_k(\mathbf{p}^*, \gamma) \text{ s.t. } (4). \quad (12)$$

Since nonnegative weighted summation preserves convexity, it is easy to check that $C_k(\mathbf{p}^*, \gamma)$ is convex in γ. The Karush-Kuhn-Tucker (KKT) necessary conditions for solving (12) provide us with a system of M quartic equations along the linear constraint. Although quartic equations can be solved analytically, obtaining a closed form solution for the Lagrange multiplier and γ as a function of M, P, P_j is overly complex.

Alternatively, a simple heuristic (suboptimal) policy can be obtained by maximizing the sum of the denominators of the ratios in (12), thereby evaluating γ by

$$\arg\max_{\gamma} \sum_{i=1}^{M} N_1^{(i)} + N_2^{(i)} + \frac{N_1^{(i)} N_2^{(i)}}{P^{(i)}}, \text{ s.t. } (4), \quad (13)$$

which gives,

$$\gamma^{(i)} = \frac{\lambda P - {\sigma_{EA}^2}^{(i)} P - {\sigma_{EB}^2}^{(i)} P - {\sigma_{EA}^2}^{(i)} - {\sigma_{EB}^2}^{(i)}}{2 {\sigma_{EA}^2}^{(i)} {\sigma_{EB}^2}^{(i)}}, \quad (14)$$

while λ can be evaluated by replacing (14) into (4).

In Fig. 2 numerical evaluations of the SKG rates versus the number of blocks M for P $= \{5, 10, 15\}$ dB and $P_j = 10$ dB are presented for Rayleigh block fading channels assuming that the legitimate nodes employ the optimal blind policy $\mathbf{p}^*$. In all cases ${\sigma_0^2}^{(i)}, {\sigma_{EA}^2}^{(i)}, {\sigma_{EB}^2}^{(i)}$ are drawn from uniform distributions in $(0, 1)$ and each point on the curves is computed as the average of 10^4 runs. The simulation results demonstrate that the secret key capacity is fairly constant with M. Interestingly, the jammer's gain in adopting the optimal policy as opposed to the heuristic or the blind is small.

Furthermore, in Fig. 3 the impact of the average jamming power on the SKG rates is investigated for $M = 10$ and P$= 10$

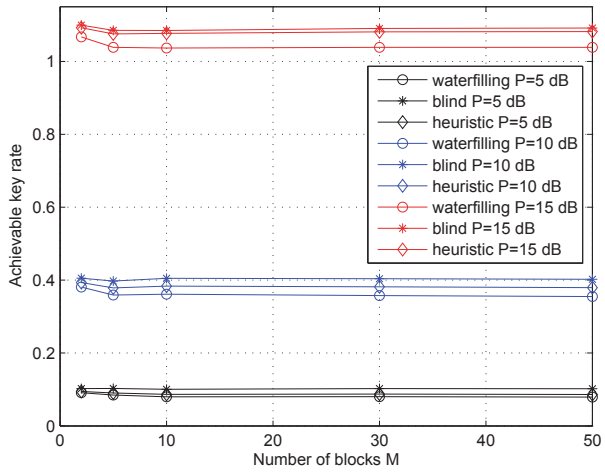

Fig. 2. SKG rate in the presence of jamming for $P = \{5, 10, 15\}$ dB and $P_j = 10$ dB vs the number of blocks M for Rayleigh block fading channels.

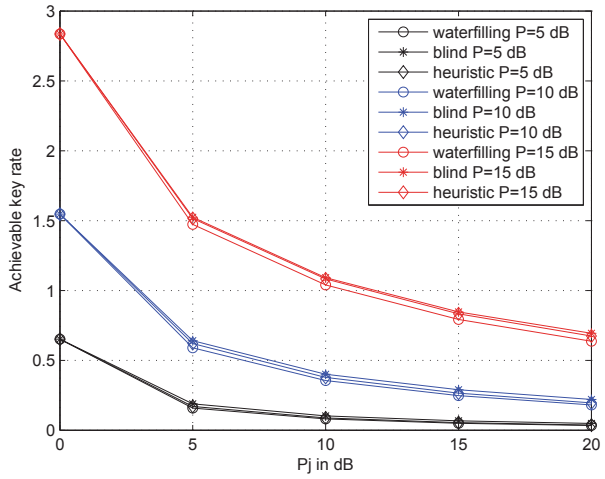

Fig. 3. SKG rate in the presence of jamming for $M = 10$ and $P = \{5, 10, 15\}$ dB vs P_j.

dB. As expected increasing the jamming power decreases the secret key rates. Similarly to the results in Fig. 2 it is shown that the gap between the optimal, the heuristic and the blind jamming policies is negligible.

An important conclusion that can be drawn from the previous analysis is that a jammer adopting a blind power allocation policy is almost as effective as one that adopts the optimal power allocation policy. In light of this result in the remainder of this study we assume that both the legitimate users and the jammer adopt blind power allocation policies in frequency spreading scenarios. In particular, we assume that in the case of frequency spreading the available power is equally distributed across the block of M subchannels.

TABLE I
TWO PLAYER ZERO-SUM DESCRIPTION OF THE JAMMING GAME

	J(H)	J(S)
L(H)	$u_{h,h}$	$u_{h,s}$
L(S)	$u_{s,h}$	$u_{s,s}$

B. Power Allocation in Frequency Hopping Systems

Frequency hopping systems are equivalent to $M = 1$. Due to the monotonicity of the logarithmic function it is straightforward to show that both the legitimate nodes and the jammer should use all available power to transmit on the randomly chosen subchannel when frequency hopping is adopted.

IV. FREQUENCY HOPPING VERSUS FREQUENCY SPREADING

In this section we investigate the jamming and counter-jamming strategies for the legitimate nodes – denoted henceforth as player L – and the jammer – denoted as player J – under short term power constraints in the form of (3) and (4), respectively. We employ the system SKG capacity C_k as the metric of interest and model the competitive interaction between L and J as the following zero-sum game:

$$\mathcal{G}(P, P_j) = \{\mathcal{A}_L, \mathcal{A}_J, u\}, \tag{15}$$

where $u = C_k$ is the utility function for the two players. The sets $\mathcal{A}_L, \mathcal{A}_J$ contain the actions available to L and J respectively:

$$\mathcal{A}_L = \{H(P), S(P)\}, \tag{16}$$
$$\mathcal{A}_J = \{H(P_j), S(P_j)\}, \tag{17}$$

where $H(\cdot)$ represents random hopping over M parallel subchannels with equal probability and $S(\cdot)$ represents spreading equally the power over the entire frequency band available. Based on the above, the two-player zero-sum game can be described in matrix form in Table I. We discuss in further detail the possible strategies below.

1) **Payoff $u_{h,h}$: L hopping versus J hopping**
When both players play "Hop" over M subchannels, each of them chooses with probability $\frac{1}{M}$ a subchannel to transmit with full power – either MP or MP_j, respectively – a probe signal or a jamming signal, correspondingly. The probability that L and J choose different subchannels is given by $\frac{1}{M}\left(1 - \frac{1}{M}\right)$ while the probability that the same subchannel is chosen is $\frac{1}{M^2}$. As a result, the utility function when both players randomly hop over M subchannels, denoted by $u_{h,h}$ in the following, can be expressed as in (18) at the bottom of the next page.

2) **Payoff $u_{h,s}$: L hopping versus J spreading**
In this scenario L transmits probe signals with full power on a randomly selected subchannel out of M available. On the other hand J spreads the jamming power to the entire band. The value of the utility function in this case, denoted by $u_{h,s}$, is given in (19) at the bottom of the next page.

3) **Payoff $u_{s,h}$: L spreading versus J hopping**
In this scenario L transmits probe signals over the entire block of M subchannels while J randomly jams one of them. In this case the value of the utility function, denoted by $u_{s,h}$, is given in (20) at the bottom of this page.

4) **Payoff $u_{s,s}$: L spreading versus J spreading**
Both players utilize the entire block of M subchannels and as a result the value of the utility function, denoted by $u_{s,s}$, is given in (21) at the bottom of this page.

To identify the players' optimal strategies, we need to investigate the ordering of the payoffs, given in the following lemma:

Lemma 1: For $M \in \mathbb{N}^+, M \geq 2$ the following hold:

$$u_{h,h} > u_{s,h}, \tag{22}$$
$$u_{h,s} > u_{s,s}, \tag{23}$$
$$u_{h,h} > u_{h,s}, \tag{24}$$
$$u_{s,h} > u_{s,s}. \tag{25}$$

Proof: See the Appendix. ■

Based on Lemma 1, the following Theorem characterizes the optimal pure strategy of the players:

Theorem 1: The pure strategy profile $(H(P), S(P_j)) \in \mathcal{A}_L \times \mathcal{A}_J$ is a Nash equilibrium of the game $\mathcal{G}(P, P_j)$.

Proof: Using the minimax criterion and Lemma 1, the game's saddle point is $(H(P), S(P_j))$. ■

Interestingly, the previous analysis reveals that from the standpoint of legitimate users frequency hopping should be adopted in SKG systems under jamming attacks. On the other hand, an active adversary can increase its effectiveness in compromising the SKG rates by equally distributing the available jamming power across the entire frequency band. In Fig. 4 the effect of the number of available subchannels M on the SKG rates is investigated when the optimal strategy "Hop, Spread" is adopted by the pair of legitimate users and the adversary for $P = 10$ dB and $P_j = \{5, 10, 15\}$ dB, averaged over 10^4 runs. In contrast to Fig. 2 that showed that the SKG rates did not increase with M in systems without frequency hopping (equivalently, using the "Spread, Spread" strategy), it is demonstrated that in frequency hopping systems the impact of an active adversary can be limited by increasing M. As a result, at the expense of increasing the necessary system bandwidth, SKG systems can counteract on active DoS attacks in the form of jamming.

V. Conclusions

The performance of block fading SKG systems under jamming attacks has been investigated using game theoretic tools. Assuming short term power constraints for the legitimate users and the jammer, a potential jammer has been demonstrated to maximize its impact by spreading the available power across the entire frequency band. On the other hand, the employment of frequency hopping by the legitimate nodes has been shown to alleviate the impact of jamming. As a result, at the expense of increased bandwidth resources it is shown that PL-SKG systems are not limited by jamming attacks when frequency hopping can be employed.

Appendix

In the following we set:

$$a_i = P\sigma_0^{2^{(i)}},$$

$$u_{h,h} = \sum_{i=1}^{M} \frac{1}{M}\left(1-\frac{1}{M}\right)\log_2\left(1+\frac{MP\sigma_0^{2^{(i)}}}{2+\frac{1}{MP\sigma_0^{2^{(i)}}}}\right) + \frac{1}{M^2}\log_2\left(1+\frac{MP\sigma_0^{2^{(i)}}}{2+MP_j\left(\sigma_{EA}^{2}{}^{(i)}+\sigma_{EB}^{2}{}^{(i)}\right)+\frac{\left(1+MP_j\sigma_{EA}^{2}{}^{(i)}\right)\left(1+MP_j\sigma_{EB}^{2}{}^{(i)}\right)}{MP\sigma_0^{2^{(i)}}}}\right) \tag{18}$$

$$u_{h,s} = \sum_{i=1}^{M} \frac{1}{M}\log_2\left(1+\frac{MP\sigma_0^{2^{(i)}}}{2+P_j\left(\sigma_{EA}^{2}{}^{(i)}+\sigma_{EB}^{2}{}^{(i)}\right)+\frac{\left(1+P_j\sigma_{EA}^{2}{}^{(i)}\right)\left(1+MP_j\sigma_{EB}^{2}{}^{(i)}\right)}{MP\sigma_0^{2^{(i)}}}}\right) \tag{19}$$

$$u_{s,h} = \sum_{i=1}^{M} \frac{1}{M}\left(1-\frac{1}{M}\right)\log_2\left(1+\frac{P\sigma_0^{2^{(i)}}}{2+\frac{1}{P\sigma_0^{2^{(i)}}}}\right) + \frac{1}{M^2}\log_2\left(1+\frac{P\sigma_0^{2^{(i)}}}{2+MP_j\left(\sigma_{EA}^{2}{}^{(i)}+\sigma_{EB}^{2}{}^{(i)}\right)+\frac{\left(1+MP_j\sigma_{EA}^{2}{}^{(i)}\right)\left(1+MP_j\sigma_{EB}^{2}{}^{(i)}\right)}{P\sigma_0^{2^{(i)}}}}\right) \tag{20}$$

$$u_{s,s} = \sum_{i=1}^{M} \frac{1}{M}\log_2\left(1+\frac{P\sigma_0^{2^{(i)}}}{2+P_j\left(\sigma_{EA}^{2}{}^{(i)}+\sigma_{EB}^{2}{}^{(i)}\right)+\frac{\left(1+P_j\sigma_{EA}^{2}{}^{(i)}\right)\left(1+P_j\sigma_{EB}^{2}{}^{(i)}\right)}{P\sigma_0^{2^{(i)}}}}\right) \tag{21}$$

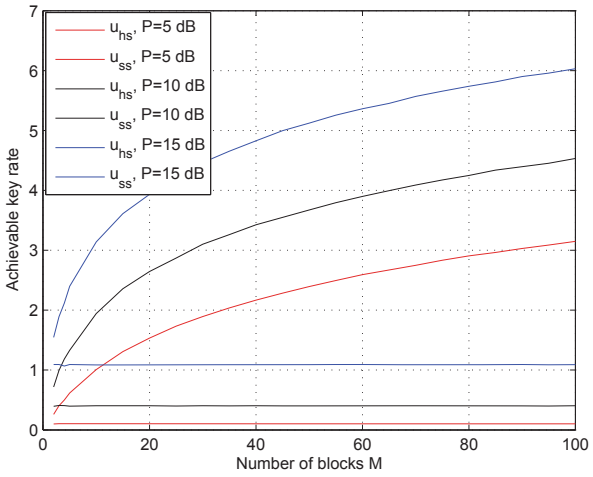

Fig. 4. SKG when the "Hop, Spread" and the "Spread, Spread" strategies are employed vs M for $P = 10$ dB.

$$
\begin{aligned}
b_i &= P_j\left(\sigma_{EA}^{2\ (i)} + \sigma_{EB}^{2\ (i)}\right), \\
c_i &= P_j\sigma_{EA}^{2\ (i)}, \\
d_i &= P_j\sigma_{EB}^{2\ (i)}, \\
y_i &= 1 + \frac{a_i x}{2 + \frac{1}{a_i x}}, \\
z_i &= 1 + \frac{a_i x}{2 + b_i + \frac{(1+c_i)(1+d_i)}{a_i x}} \\
w_i &= 1 + \frac{a_i x}{2 + b_i x + \frac{(1+c_i x)(1+d_i x)}{a_i x}} \\
, f_1^{(i)}(x) &= \log_2\left(y_i\right) \\
f_2^{(i)}(x) &= \log_2\left(z_i\right), \\
f_3^{(i)}(x) &= \log_2\left(w_i\right).
\end{aligned}
$$

A. Proof of $u_{h,h} > u_{s,h}$

Treating a_i, b_i, c_i, d_i as non-negative parameters, we note that the family of functions $f_1^{(i)}$ and $f_3^{(i)}$ are continuous, differentiable and monotonically increasing for x in $\mathbb{R}^+$, we have that $\frac{df_1^{(i)}(x)}{dx} > 0, \frac{df_3^{(i)}(x)}{dx} > 0$. As a result, for $M > 2$, $f_1^{(i)}(M) > f_1^{(i)}(1)$ and $f_3^{(i)}(M) > f_3^{(i)}(1)$. Consequently,

$$f_1^{(i)}(M) + f_3^{(i)}(M) > f_1^{(i)}(1) + f_3^{(i)}(1) \Rightarrow u_{h,h} > u_{s,h}.$$

B. Proof of $u_{h,s} > u_{s,s}$

Following a similar argument to the one presented above, $f_2^{(i)}$ is a family of continuous, differentiable and monotonically increasing functions of x in $\mathbb{R}^+$ since $\frac{df_2^{(i)}(x)}{dx} > 0$. Therefore, for $M \geq 2$ we have that

$$f_2^{(i)}(M) > f_2^{(i)}(1) \Rightarrow u_{h,s} > u_{s,s}. \tag{26}$$

C. Proof of $u_{h,h} > u_{h,s}$

For $M \geq 2$ we have that

$$
\begin{aligned}
u_{h,h} - u_{h,s} &= \sum_{i=1}^{M} \frac{1}{M}\log_2\left(\frac{y_i}{z_i}\right) + \frac{1}{M^2}\log_2\left(\frac{w_i}{y_i}\right) \\
&\geq \sum_{i=1}^{M} \frac{1}{M}\log_2\left(\frac{y_i}{z_i}\right) + \frac{1}{2M}\log_2\left(\frac{w_i}{y_i}\right) \\
&= \sum_{i=1}^{M} \frac{1}{2M}\log_2\left(\frac{y_i w_i}{z_i^2}\right) > 0.
\end{aligned} \tag{27}
$$

The last inequality is due to the fact that the family of functions $F(x) = y_i w_i - z_i^2$ are continuous, differentiable and monotonically increasing with $F(1) > 0$, and, as a result $\log_2\left(\frac{y_i w_i}{z_i^2}\right) > 0, i = 1, \ldots, M \Rightarrow \sum_{i=1}^{M} \frac{1}{2M}\log_2\left(\frac{y_i w_i}{z_i^2}\right) > 0$.

D. Proof of $u_{s,h} > u_{s,s}$

Following a similar line of reasoning as above, for $M \geq 2$ we have that

$$
\begin{aligned}
u_{s,h} - u_{s,s} &= \sum_{i=1}^{M} \frac{1}{M}\log_2\left(\frac{y_i x}{z_i x}\right) + \frac{1}{M^2}\log_2\left(\frac{w_i x}{y_i x}\right) \\
&\geq \sum_{i=1}^{M} \frac{1}{2M}\log_2\left(\frac{y_i w_i}{z_i^2}\right) > 0.
\end{aligned} \tag{28}
$$

REFERENCES

[1] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, 1973.

[2] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. Part I: secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, 1993.

[3] 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.

[4] 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.

[5] T.-H. Chou, S. Draper, and A. M. Sayeed, "Key generation using external source excitation: Capacity, reliability and secrecy exponent," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2455–2474, Apr. 2012.

[6] 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.

[7] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," in *Computer Security - ESORICS 2012*, ser. Lecture Notes in Computer Science, S. Foresti, M. Yung, and F. Martinelli, Eds., 2012, vol. 7459, pp. 235–252.

[8] X. Zhou, B. Maham, and A. Hjørungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

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

[10] G. Caire, G. Taricco, and E. Biglieri, "Optimum power control over fading channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1468–1489, Jul. 1999.

[11] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. Int. Symp. Inf. Theory, ISIT06*, Seatle, US, Jul. 2006, pp. 2593–2597.

[12] A. Chorti, K. Papadaki, and H. Poor, "Optimal power allocation in block fading channels with confidential messages," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 4708–4719, Sep. 2015.