Fundamental Rate Limits of Physical Layer Spoofing

Jie Xu, *Member, IEEE*, Lingjie Duan, *Member, IEEE*, and Rui Zhang, *Fellow, IEEE*

***Abstract*—This letter studies an emerging wireless communication intervention problem at the physical layer, where a legitimate spoofer aims to spoof a malicious link from Alice to Bob, by replacing Alice's transmitted source message with its target message at Bob side. From an information-theoretic perspective, we are interested in characterizing the maximum achievable spoofing rate of this new spoofing channel, which is equivalent to the maximum achievable rate of the target message at Bob, under the condition that Bob cannot decode the source message from Alice. We propose a novel combined spoofing approach, where the spoofer sends its own target message, combined with a processed version of the source message to cancel the source message at Bob. For both cases when Bob treats interference as noise (TIN) or applies successive interference cancelation (SIC), we obtain the maximum achievable spoofing rates by optimizing the power allocation between the target and source messages at the spoofer.**

***Index Terms*—Wireless communication intervention, physical layer spoofing, achievable spoofing rate, power allocation.**

I. Introduction

The emergence of infrastructure-free wireless communications (e.g., mobile ad hoc networks and unmanned aerial vehicle (UAV) communications) imposes new challenges on the public security, since they may be misused by malicious users to commit crimes or even terror attacks. To overcome this issue, authorized parties can launch legitimate information eavesdropping (see, e.g., [1]–[4]) and jamming (see, e.g., [5]–[8]) on suspicious and malicious wireless communication links, so as to monitor and intervene in them for the purpose of detecting and preventing security attacks.

We focus on the emerging wireless communication intervention at the physical layer. Different from the jamming intervention that can only disrupt or disable target links, we propose a new intervention via physical layer spoofing to change the communicated information over malicious links while keeping their operation. Such a physical layer spoofing has been first investigated in our previous work [9] by considering a three-node spoofing channel (see Fig. 1), where a legitimate spoofer aims to spoof an ongoing malicious link from Alice to Bob, by replacing Alice's transmitted source message with its target message at Bob side. We have proposed a symbol-level spoofing approach in [9] for the spoofer to minimize the spoofing-symbol-error-rate of the target message at Bob under practical phase-shift keying modulations. Nevertheless, the fundamental information-theoretic limits of such a new spoofing channel remain unaddressed, thus motivating our study in this work.

Manuscript received October 20, 2016; revised December 7, 2016; accepted December 23, 2016. The associate editor coordinating the review of this paper and approving it for publication was S. Zhang.

J. Xu is with the School of Information Engineering, Guangdong University of Technology (e-mail: jiexu.ustc@gmail.com). He is also with the Engineering Systems and Design Pillar, Singapore University of Technology and Design.

L. Duan is with the Engineering Systems and Design Pillar, Singapore University of Technology and Design (e-mail: lingjie_duan@sutd.edu.sg).

R. Zhang is with the Department of Electrical and Computer Engineering, National University of Singapore (e-mail: elezhang@nus.edu.sg). He is also with the Institute for Infocomm Research, A*STAR, Singapore.

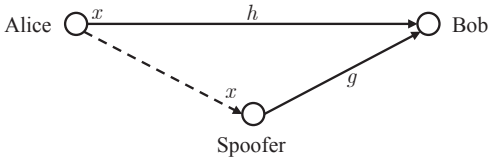

Fig. 1. A three-node spoofing channel, where a legitimate spoofer aims to change the communicated information from Alice to Bob.

In this letter, we are interested in characterizing the maximum achievable spoofing rate of the spoofing channel in Fig. 1, which is equivalent to the maximum achievable rate of the target message at Bob, while ensuring that Bob cannot decode the source message. We propose a new combined spoofing approach, where the spoofer sends its own target message, combined with a processed version of the source message to cancel it at Bob. In particular, we assume Alice transmits with a constant rate, and consider two cases when Bob treats interference as noise (TIN) and applies successive interference cancelation (SIC), respectively. To successfully spoof in the former case, the spoofer should make the received target message at Bob be stronger than the source message; and in the latter case, the spoofer should make the maximum achievable rate of the source message (under different decoding orders) be strictly smaller than Alice's communication rate. In both cases, we obtain the maximum achievable spoofing rates by optimizing the power allocation between the target and source messages at the spoofer. Numerical results show that our proposed combined spoofing approach with optimized power allocation outperforms other benchmark spoofing schemes.

II. System Model

As shown in Fig. 1, we consider a three-node spoofing channel, where two malicious users Alice and Bob communicate to plan or commit crimes, and a legitimate spoofer aims to change the communicated data from Alice to Bob to defend against them. Practically, the malicious users can be identified *a priori* via, e.g., legitimate information eavesdropping [1]–[4]. We define h and g as the complex channel coefficients of the malicious link from Alice to Bob and the spoofing link from the spoofer to Bob, respectively.

First, we consider the case without spoofing. Let s denote the source message transmitted by Alice with unit power. The received signal by Bob is given by

$$y = h\sqrt{P}s + n, \tag{1}$$

where P denotes the constant transmit power of Alice, and n denotes the receiver noise at Bob being a circularly symmetric

complex Gaussian (CSCG) random variable with zero mean and unit variance. The capacity of the malicious link is given as $C \triangleq \log_2(1+|h|^2P)$, which is achieved when Alice employs Gaussian signaling (i.e., setting s as a CSCG random variable with zero mean and unit variance). Suppose that Alice communicates with Bob with a constant communication rate R no greater than the channel capacity C, i.e., $R \leq C$, where R is chosen based on the quality of service (QoS) requirement.

Next, we consider the case with spoofing. The spoofer aims to change Bob's decoded message from Alice's source message s to its desired target message. It is assumed that the spoofer has the perfect information of the source message s and the channel coefficients h and g. This assumption is made to help derive the spoofing rate upper bound, similar to that in the prior works in the information-theoretic literature (see, e.g., the correlated jamming in [7] and the cognitive radio channel in [10]).[1] In this case, the spoofer can use the same codebook of s for sending the target message, such that Bob will decode the target message without awareness of being spoofed. Let x denote the target message with unit power, which is in general independent of s. We consider a combined spoofing approach, where the spoofer designs its spoofing signal z to be a combined version of both the source message s and the target message x with proper processing. Particularly, we have $z = \alpha s + \beta x$, where α and β denote the complex transmit coefficients for the messages s and x, respectively. In this case, the received signal y at Bob can be expressed as

$$y = h\sqrt{P}s + gz + n = \left(h\sqrt{P} + g\alpha\right)s + g\beta x + n. \quad (2)$$

By denoting Q as the maximum spoofing power at the spoofer, then we have

$$|\alpha|^2 + |\beta|^2 \leq Q. \quad (3)$$

In order to successfully spoof the malicious communication, the spoofer should design the spoofing signal (i.e., the transmit coefficients α and β) such that Bob is only able to successfully decode the target message x but fails to decode the source message s. In this case, the successful spoofing critically depends on the decoding method employed by Bob. We consider two typical Bob receivers as follows, including the practical TIN receiver and the information-theoretically optimal SIC receiver. It is assumed that the spoofer is aware of which receiver being employed by Bob.

1) TIN receiver at Bob: Bob does not know the coexistence of the two messages s and x, and thus considers the stronger one between them to be its desired signal, and treats the other one (the co-channel interference) to be noise. In this case, the received message x at Bob should have a stronger power than s such that the spoofing is successful.

2) SIC receiver at Bob: Bob is able to detect the coexistence of s and x, and accordingly attempts to use SIC to decode both of them. From the successfully decoded ones (if any), Bob will decide which the desired message is. In particular, Bob first decodes one message (x or s) by treating the other as noise, and then cancels it from the received message y to decode the other one. Generally speaking, Bob can use two different decoding orders (first x and then s, or first s and then x).

Under both receiver cases, we aim to characterize the maximum achievable spoofing rates of the target message x, provided that Bob cannot decode the source message s.[2]

III. Spoofing TIN Receiver at Bob

A. Problem Formulation for TIN Receiver

When Bob employs the TIN receiver, the spoofer can successfully spoof the malicious communication link only when the received power of the target message x is greater than that of the source message s. Mathematically, it must hold that $|g\beta|^2 > |h\sqrt{P}+g\alpha|^2$. Note that this strict inequality constraint may make the associated optimization problem ill-posed: an optimizer on the boundary of the feasible region may not be attainable. To address this issue, we revise it to be a non-strict inequality constraint as

$$|g\beta|^2 \geq |h\sqrt{P} + g\alpha|^2 + \delta_1, \quad (4)$$

where $\delta_1 > 0$ is a sufficiently small positive constant.

In this case, the received signal-to-interference-plus-noise-ratio (SINR) for the target message x at Bob is $\gamma(\alpha,\beta) = \frac{|g\beta|^2}{|h\sqrt{P}+g\alpha|^2+1}$. Accordingly, the achievable spoofing rate (in bps/Hz) is expressed as follows by assuming x is CSCG and s is also CSCG as the "worst-case" noise.

$$r(\alpha,\beta) = \log_2\left(1 + \frac{|g\beta|^2}{|h\sqrt{P}+g\alpha|^2+1}\right). \quad (5)$$

As a result, the achievable spoofing rate maximization problem is formulated as

$$\text{(P1)}: \max_{\alpha,\beta}\ r(\alpha,\beta)$$
$$\text{s.t. (3) and (4)}.$$

B. Optimal Spoofing Solution to Problem (P1)

First, we reformulate (P1) as an equivalent problem with a single real decision variable. It is evident that the optimality of (P1) is attained when the processed source message s from the spoofer is destructively combined at Bob with that from Alice, and the sum-power constraint in (3) is tight. In other words, we have

$$\alpha = -\frac{hg^*}{|h||g|}\tilde{\alpha}, \quad (6)$$

$$\beta = \sqrt{Q - |\tilde{\alpha}|^2}, \quad (7)$$

where the superscript $*$ denotes the conjugate operation, and $\tilde{\alpha} \geq 0$ denotes the magnitude of α. Here, since both the objective function and constraints of (P1) are irrespective of the phase of β, in (7) we decide β to be a real variable without loss of optimality. Therefore, (P1) is equivalently reformulated as follows to optimize an SINR function $\tilde{\gamma}(\tilde{\alpha})$ with only a real decision variable $\tilde{\alpha}$.

$$\text{(P1.1)}: \max_{\tilde{\alpha}\geq 0}\ \tilde{\gamma}(\tilde{\alpha}) \triangleq \frac{|g|^2(Q-\tilde{\alpha}^2)}{(|h|\sqrt{P}-|g|\tilde{\alpha})^2+1}$$
$$\text{s.t. } 2|g|^2\tilde{\alpha}^2 - 2|h||g|\sqrt{P}\tilde{\alpha} + |h|^2P - |g|^2Q + \delta_1 \leq 0. \quad (8)$$

[1] Though beyond the scope of this letter, please refer to [9] for a detailed example for the spoofer to practically obtain s, h and g, and synchronize with Alice and Bob, where the spoofer can act as a fake relay to join the malicious network in obtaining such information. Also, the spoofer can work in a full-duplex mode (e.g., amplify and forward) to obtain s via eavesdropping from Alice and at the same time spoof Bob.

[2] In practice, the spoofer can choose any rate (for x) no larger than the maximum achievable spoofing rate, provided with successful spoofing.

Next, we check the feasibility of problem (P1.1) (and thus (P1)).

Lemma 3.1: Problem (P1.1) (and thus (P1)) is feasible if and only if $Q \geq \frac{|h|^2P+2\delta_1}{2|g|^2}$.

Proof: Note that the constraint in (8) can be rewritten as $2|g|^2\left(\tilde{\alpha}-\frac{|h|\sqrt{P}}{2|g|}\right)^2+\frac{|h|^2P}{2}-|g|^2Q+\delta_1\leq 0$, which specifies a nonempty feasible set if and only if $\frac{|h|^2P}{2}-|g|^2Q+\delta_1\leq 0$. Equivalently, problem (P1.1) is feasible if and only if $Q\geq\frac{|h|^2P+2\delta_1}{2|g|^2}$. This proposition thus follows. ∎

Finally, we obtain the optimal solutions to (P1.1) and (P1) when they are feasible. In this case, the constraint in (8) is equivalently expressed as

$$\underline{\omega}\leq\tilde{\alpha}\leq\overline{\omega}, \tag{9}$$

where $\underline{\omega}=\frac{|h|\sqrt{P}-\sqrt{2|g|^2Q-|h|^2P-2\delta_1}}{2|g|}$ and $\overline{\omega}=\frac{|h|\sqrt{P}+\sqrt{2|g|^2Q-|h|^2P-2\delta_1}}{2|g|}$ denote the minimum and maximum values of $\tilde{\alpha}$ for the TIN spoofing to be successful, respectively. Furthermore, by checking its first-order derivative, we can show that there exist one local maximum point $\tilde{\alpha}_1$ and one local minimum point $\tilde{\alpha}_2$ for the SINR function $\tilde{\gamma}(\tilde{\alpha})$, which are given by

$$\tilde{\alpha}_1=\frac{|h|^2P+|g|^2Q+1}{2|h||g|\sqrt{P}}-\frac{\sqrt{(|h|^2P+|g|^2Q+1)^2-4|h|^2|g|^2PQ}}{2|h||g|\sqrt{P}} \tag{10}$$

and $\tilde{\alpha}_2=\frac{|h|^2P+|g|^2Q+1}{2|h||g|\sqrt{P}}+\frac{\sqrt{(|h|^2P+|g|^2Q+1)^2-4|h|^2|g|^2PQ}}{2|h||g|\sqrt{P}}$, respectively. In particular, $\tilde{\gamma}(\tilde{\alpha})$ is first increasing over $\tilde{\alpha}\in[0,\tilde{\alpha}_1]$, then decreasing over $\tilde{\alpha}\in(\tilde{\alpha}_1,\tilde{\alpha}_2)$, and finally increasing over $\bar{\alpha}\in[\tilde{\alpha}_2,+\infty)$. Since $\lim_{\tilde{\alpha}\to\infty}\tilde{\gamma}(\tilde{\alpha})=-1$ but $\tilde{\gamma}(\tilde{\alpha})>0,\forall\tilde{\alpha}\in[0,\tilde{\alpha}_1]$, it is evident that $\tilde{\alpha}_1$ is the globally optimal point to maximize $\tilde{\gamma}(\tilde{\alpha})$ without any constraints. Then we have the following proposition.

Proposition 3.1: The optimal solution to (P1.1) is given by

$$\tilde{\alpha}^\star=\max\left(\underline{\omega},\tilde{\alpha}_1\right), \tag{11}$$

and thus the optimal solution to (P1) is $\alpha^\star=-\frac{hg^*}{|h||g|}\tilde{\alpha}^\star$ and $\beta^\star=\sqrt{Q-|\alpha^\star|^2}$.

Proof: The optimal solution to (P1.1) can be easily verified based on the monotonic property of $\tilde{\gamma}(\tilde{\alpha})$ together with the fact that $\tilde{\alpha}_1\leq\overline{\omega}$ and $\tilde{\alpha}_1\leq\sqrt{Q}$. Then, by substituting $\tilde{\alpha}^\star$ in (11) into (6) and (7), the optimal solution to (P1) is derived. Therefore, this proposition is proved. ∎

IV. Spoofing SIC Receiver at Bob

A. Problem Formulation for SIC Receiver

When Bob employs the SIC receiver, the spoofer needs to design its spoofing signal such that Bob is able to decode the target message x but fails to decode the source message s for the purpose of successful spoofing. In general, the spoofer should consider the following two cases, depending on the decoding orders employed by Bob. Here, Bob can be viewed as a receiver of a two-user multiple-access channel (MAC) by considering Alice and the spoofer as the two transmitters.

In the first case, Bob first decodes s by treating x as noise, and then subtracts s from the received signal y to decode x. Accordingly, the maximum achievable rates of s and x at the receiver of Bob (under given α and β) are given as follows by assuming both s and x are CSCG.

$$r_s^{(\mathrm{I})}=\log_2\left(1+\frac{|h\sqrt{P}+g\alpha|^2}{|g\beta|^2+1}\right), \tag{12}$$

$$r_x^{(\mathrm{I})}=\log_2\left(1+|g\beta|^2\right). \tag{13}$$

In order to prevent Bob from successfully decoding s, the spoofer should ensure that its maximum achievable rate is smaller than Alice's communication rate, i.e.,

$$r_s^{(\mathrm{I})}<R. \tag{14}$$

Since Bob fails to decode s, the decoding of x should suffer from the interference of s, and therefore the achievable spoofing rate is given as $r(\alpha,\beta)$ in (5).

In the second case, Bob first decodes x by treating s as noise, and then cancels x from y to decode s. Accordingly, the maximum achievable rates of s and x (under given α and β) at the receiver of Bob are respectively given by

$$r_s^{(\mathrm{II})}=\log_2\left(1+|h\sqrt{P}+g\alpha|^2\right), \tag{15}$$

$$r_x^{(\mathrm{II})}=\log_2\left(1+\frac{|g\beta|^2}{|h\sqrt{P}+g\alpha|^2+1}\right). \tag{16}$$

To prevent Bob from decoding s, the spoofer should ensure that

$$r_s^{(\mathrm{II})}<R. \tag{17}$$

In this case, the rate $r_x^{(\mathrm{II})}$ in (16), which equals $r(\alpha,\beta)$ in (5), is the achievable spoofing rate.

By combining the two cases, the successful spoofing only requires (17) to hold, since if it holds, (14) will hold automatically. Note that in the above two cases, Bob cannot decode s regardless of the decoding orders used with SIC; as a result, it can only treat the decoded target message x as its desired message. Also note that (17) is a strict inequality constraint. To address this issue, we revise (17) as follows similarly as in (4).

$$\log_2(1+|h\sqrt{P}+g\alpha|^2)+\delta_2\leq R, \tag{18}$$

where δ_2 is a sufficiently small positive constant. The achievable spoofing rate maximization problem is formulated as

$$(\mathrm{P2}):\ \max_{\alpha,\beta}\ r(\alpha,\beta)$$
$$\text{s.t. (3) and (18).}$$

B. Optimal Spoofing Solution to Problem (P2)

Similar to (P1), it can be shown that the optimality of (P2) is attained when (6) and (7) hold. In this case, (P2) is equivalently reformulated as

$$(\mathrm{P2.1}):\ \max_{0\leq\tilde{\alpha}\leq\sqrt{Q}}\ \tilde{\gamma}(\tilde{\alpha})$$
$$\text{s.t. } \underline{\chi}\leq\tilde{\alpha}\leq\overline{\chi}, \tag{19}$$

where $\underline{\chi}=\frac{|h|\sqrt{P}-\sqrt{2^{R-\delta_2}-1}}{|g|}$ and $\overline{\chi}=\frac{|h|\sqrt{P}+\sqrt{2^{R-\delta_2}-1}}{|g|}$ denote the minimum and maximum values of $\tilde{\alpha}$ for the SIC spoofing to be successful, respectively.

Next, we check the feasibility of problem (P2.1) (and thus (P2)).

Lemma 4.1: Problem (P2.1) (and thus (P2)) is feasible if and only if $Q\geq\underline{\chi}^2$.

Proof: The feasible condition of problem (P2.1) can be obtained by noting that $\tilde{\alpha}\leq\sqrt{Q}$ and $\underline{\chi}\leq\tilde{\alpha}$ should be satisfied

at the same time. ■

Finally, when problems (P2.1) and (P2) are feasible, their optimal solutions are obtained in the following proposition.

Proposition 4.1: The optimal solution to (P2.1) is given by

$$\bar{\alpha}^{\star\star} = \max\left(\underline{\chi}, \tilde{\alpha}_1\right), \tag{20}$$

where $\tilde{\alpha}_1$ is the globally optimal point to maximize $\tilde{\gamma}(\tilde{\alpha})$, as given in (10). Then, the optimal solution to (P2) is given by $\alpha^{\star\star} = -\frac{hg^*}{|h||g|}\bar{\alpha}^{\star\star}$ and $\beta^{\star\star} = \sqrt{Q - |\alpha^{\star\star}|^2}$.

Proof: Similar to Proposition 3.1 and based on the monotonic property of $\tilde{\gamma}(\tilde{\alpha})$, the optimal solution to (P2.1) is obtained as $\bar{\alpha}^{\star\star}$ in (20). Substituting it into (6) and (7), the optimal solution to (P2) is derived. Therefore, this proposition is proved. ■

It is interesting to compare the optimally designed spoofing signals for TIN and SIC receivers at Bob, respectively. First, it is observed from Lemmas 3.1 and 4.1 that the minimally required spoofing power for the TIN receiver is irrespective of the communication rate R by Alice, while that for the SIC receiver is monotonically decreasing with respect to R. As a result, when R is large (particularly when $2^R - 1 > (1 - \frac{1}{\sqrt{2}})^2|h|^2P$ by neglecting the sufficiently small δ_1 and δ_2), the minimally required spoofing power for the SIC receiver is smaller than that for the TIN receiver, and thus the SIC Bob receiver is easier to be spoofed than the TIN one in this case. Next, it is observed from Propositions 3.1 and 4.1 that if $\tilde{\alpha}_1 \geq \underline{\omega}$ and $\tilde{\alpha}_1 \geq \underline{\chi}$ both hold, then the designed spoofing signals become identical for both receivers. This happens when the spoofing power budget Q becomes sufficiently large.

V. Numerical Results

In this section, we provide numerical results to show the achievable spoofing rates of our proposed combined spoofing approach with optimal spoofing signals design. We compare our results with two benchmark schemes in the following.

- *Heuristic combined spoofing with perfect source message cancelation*: The spoofer tries to cancel all the source message by setting $\alpha = -\frac{hg^*\sqrt{P}}{|g|^2}$, and accordingly β is given in (7). This scheme only works when $Q > \frac{|h|^2P}{|g|^2}$ for both TIN and SIC Bob receivers, where the minimally required spoofing power $\frac{|h|^2P}{|g|^2}$ is twice of that in Lemma 3.1 for our proposed optimal combined spoofing.
- *Naive spoofing*: The spoofer uses all its transmit power to send the target message s, which corresponds to the case with $\alpha = 0$ and $\beta = \sqrt{Q}$. This scheme only applies to the case with the TIN receiver at Bob when $Q > \frac{|h|^2P}{|g|^2}$.

In the simulation, we normalize the channel coefficients to be $h = 1$ and $g = 1$ for the purpose of illustration, while our results can be easily extended to the other values of h and g. We set $P = 10$ dB, and $R = 2$ bps/Hz. Fig. 2 shows the maximum achievable spoofing rate versus the spoofing power Q at the spoofer. It is observed that the two benchmark schemes achieve positive spoofing rates (or successfully spoof) only when $Q > 10$ dB, while the optimal combined spoofing does so when $Q > 5$ dB for the TIN receiver at Bob and when Q is larger than 3 dB for the SIC receiver. It is also observed that when Q is larger than 7 dB, the optimal combined spoofing achieves the same maximum achievable

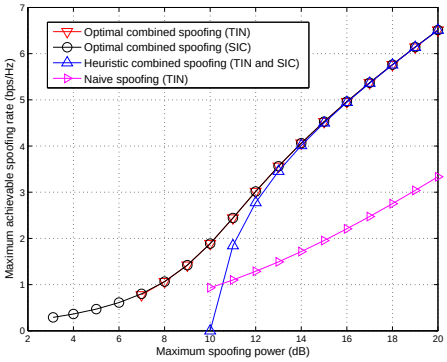

Fig. 2. The maximum achievable spoofing rate versus the spoofing power Q at the spoofer.

spoofing rate for both TIN and SIC receivers, and outperforms both benchmarks schemes. The heuristic combined spoofing is observed to achieve the same performance as the optimal one when $Q > 16$ dB. This shows that in this case, it is optimal for the spoofer to perfectly cancel the source message and then allocate the remaining power for the target message.

VI. Conclusion

This letter studied the achievable spoofing rates of the new wireless communication intervention via physical layer spoofing, where a legitimate spoofer sends a combined version of both the source and target messages to confuse a malicious link from Alice to Bob. We proposed optimal spoofing signal designs when Bob employs the TIN and SIC receivers, respectively. It is our hope that this work can provide new insights on the fundamental information-theoretic limits of the physical layer spoofing. How to extend the results to general multi-antenna and multiuser scenarios is an interesting research direction worth pursuing in the future work.

References

[1] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Wireless Commun. Letters*, vol. 5, no. 1, pp. 80-83, Feb. 2016.

[2] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," in *Proc. IEEE ICC*, 2016.

[3] Y. Zeng and R. Zhang, "Active eavesdropping via spoofing relay attack," in *Proc. IEEE ICASSP*, 2016.

[4] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1449-1461, Dec. 2016.

[5] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727-1765, Sep. 2016.

[6] M. Medard, "Capacity of correlated jamming channels," in *Proc. 35th Allerton Conf.*, Monticello, IL, Oct. 1997, pp. 1043-1052.

[7] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2119-2123, Sep. 2004.

[8] Q. Liu, M. Li, X. Kong, and N. Zhao, "Disrupting MIMO communications with optimal jamming signal design," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5313-5325, Oct. 2015.

[9] J. Xu, L. Duan, and R. Zhang, "Transmit optimization for symbol-level spoofing," submitted to *IEEE Trans. Wireless Commun.*. [Online] Available: https://arxiv.org/abs/1608.00722

[10] N. Devroye, P. Mitran, and V. Tarokh, "Achievable rates in cognitive radio channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 1813-1827, May 2006.