ACTIVE EAVESDROPPING VIA SPOOFING RELAY ATTACK

Yong Zeng and Rui Zhang

Department of Electrical and Computer Engineering, National University of Singapore
{elezeng, elezhang}@nus.edu.sg

ABSTRACT

This paper studies a new active eavesdropping technique via the so-called *spoofing relay attack*, which could be launched by the eavesdropper to significantly enhance the *information leakage rate* from the source over conventional passive eavesdropping. With this attack, the eavesdropper acts as a relay to spoof the source to vary transmission rate in favor of its eavesdropping performance by either enhancing or degrading the effective channel of the legitimate link. The maximum information leakage rate achievable by the eavesdropper and the corresponding optimal operation at the spoofing relay are obtained. It is shown that such a spoofing relay attack could impose new challenges from a physical-layer security perspective since it leads to significantly higher information leakage rate than conventional passive eavesdropping.

***Index Terms*—** Physical-layer security, active eavesdropping, spoofing relay attack.

1. INTRODUCTION

Wireless communications are vulnerable to eavesdropping by unintended recipients due to the broadcast nature of wireless channels. The conventional cryptographic mechanism [1], though provides an effective approach for secure communications, is facing with unprecedented challenges due to the fast growing computation power of the eavesdroppers, the increased complexity in key generation and management, etc. Recently, there has been a significant research interest in achieving secure wireless communications by exploiting the inherent wireless channel characteristics of the legitimate and adversary users, which is known as *physical-layer security* [2]. Under the classic wiretap channel framework [3], numerous efforts have been devoted to characterizing the *secrecy capacity* [4–6], or the maximum transmission rate at which the message can be reliably decoded at the legitimate receiver without leaking any useful information to the eavesdropper.

Most of the existing works on physical-layer security have assumed the theoretical setup with passive eavesdroppers only. In practice, the eavesdropper could launch proactive attacks to enhance their eavesdropping performance, a technique known as *active eavesdropping* [7]. For instance, in multi-antenna time-division duplexing (TDD) systems with reverse-link channel training, the eavesdropper may attack the channel training phase by sending identical pilots as the legitimate receiver, so that the estimated channel at the source transmitter, based on which precoding is designed for the data transmission phase, is a linear combination of those of the legitimate and eavesdropping links. Such an active attack is known as *pilot contamination attack* [8], by which the eavesdropper can enhance its effective channel from the source transmitter, and hence boost its eavesdropping capacity, while simultaneously degrading the channel of the legitimate link. Various schemes have been proposed to detect such a pilot contamination attack [9–13].

In this paper, we study a new active attack termed *spoofing relay attack*, which could be launched by the eavesdropper to significantly enhance the effective *information leakage rate* eavesdropped from the source over the conventional passive eavesdropping. With this attack, the eavesdropper acts as a relay to spoof the source to vary transmission rate in favor of its eavesdropping performance, assuming that adaptive rate transmission is adopted at the source based on the effective channel to the legitimate receiver. Specifically, if the eavesdropper has a better channel than that of the legitimate receiver, it will enhance the effective channel of the legitimate link by forwarding a constructive signal to the receiver, which leads to higher transmission rate by the source, and hence higher information leakage rate; otherwise, it will degrade the effective channel of the legitimate link via forwarding a destructive signal to the receiver, so as to spoof the source to reduce transmission rate to make it decodable by the eavesdropper. The maximum information leakage rate achievable by such a spoofing relay attack is derived, which is shown to be significantly higher than that attainable by conventional passive eavesdropping.

Compared to other active eavesdropping techniques such as the pilot contamination attack, the spoofing relay attack could lead to more severe security risks, since it has a broader applicability, regardless of single- or multi-antenna, TDD or frequency-division duplexing (FDD) systems. Furthermore, it is also more difficult to be detected, since the legitimate user may attribute the change in its effective channel to the environmental variations, e.g., the presence of a new signal path. Devising effective detection schemes and countermeasures against the new spoofing relay attack is an interesting problem, which is left for our future work.

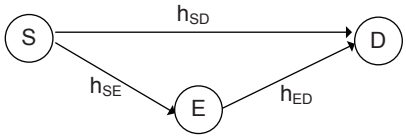


Fig. 1: A point-to-point link with an active eavesdropper.

2. SYSTEM MODEL AND PROBLEM FORMULATION

As shown in Fig. 1, we consider a point-to-point wireless communication system where the source $\mathbf{S}$ sends information to the destination $\mathbf{D}$ in the presence of an eavesdropper $\mathbf{E}$. We assume that *adaptive rate transmission* is adopted at $\mathbf{S}$ based on the channel condition perceived at $\mathbf{D}$. However, both $\mathbf{S}$ and $\mathbf{D}$ are unaware of the presence of $\mathbf{E}$, so that no dedicated coding as in conventional physical-layer security (see e.g. [2]-[6]) is applied to prevent the eavesdropping by $\mathbf{E}$. On the other hand, the eavesdropper $\mathbf{E}$ can conduct either passive or active eavesdropping, as discussed below.

2.1. Passive Eavesdropping

With passive eavesdropping, $\mathbf{E}$ remains silence throughout the communication between $\mathbf{S}$ and $\mathbf{D}$, but tries to decode the information from $\mathbf{S}$. In this case, the channel capacity of the legitimate link from $\mathbf{S}$ to $\mathbf{D}$, which is also assumed to be the transmission rate by $\mathbf{S}$, is $R_D = \log_2\left(1 + P_S|h_{SD}|^2/\sigma^2\right)$ in bits/second/Hz (bps/Hz), where h_{SD} is the complex-valued channel gain from $\mathbf{S}$ to $\mathbf{D}$, P_S is the transmission power at $\mathbf{S}$, and σ^2 is the power of the additive white Gaussian noise (AWGN) at $\mathbf{D}$. Similarly, the channel capacity between $\mathbf{S}$ and $\mathbf{E}$ is $R_E = \log_2\left(1 + P_S|h_{SE}|^2/\sigma^2\right)$ in bps/Hz, with h_{SE} denoting the channel from $\mathbf{S}$ to $\mathbf{E}$. If $R_E \geq R_D$ or equivalently $|h_{SE}|^2 \geq |h_{SD}|^2$, i.e., the eavesdropper has a better channel than the legitimate receiver, $\mathbf{E}$ can reliably decode the information sent by $\mathbf{S}$ with arbitrarily small error. As a result, the effective *information leakage rate* is given by $R_{\text{leak}} = R_D$. On the other hand, if $R_E < R_D$, or the eavesdropper has a weaker channel than the legitimate receiver, then it is impossible for $\mathbf{E}$ to decode the information from $\mathbf{S}$ with arbitrarily small error. In this case, we define the effective information leakage rate as $R_{\text{leak}} = 0$.[1] Therefore, the information leakage rate can be expressed as

$$R_{\text{leak}} = \begin{cases} R_D, & \text{if } R_E \geq R_D \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

2.2. Active Eavesdropping via Spoofing Relay Attack

In this subsection, we consider an active eavesdropper that launches the spoofing relay attack to enhance the information leakage rate. With such an attack, the eavesdropper $\mathbf{E}$ operates in a full-duplex mode with simultaneous information reception and relaying [14]. We assume the simple amplify-and-forward (AF) relaying by $\mathbf{E}$ since it incurs the minimal processing delay. By assuming an ideal full-duplex operation with perfect self-interference cancellation [14], the signal received by $\mathbf{E}$ prior to processing noise addition is $y_E = h_{SE}\sqrt{P_S}d_S$, where $d_S \sim \mathcal{CN}(0,1)$ denotes the circularly-symmetric complex Gaussian (CSCG) distributed information-bearing symbol sent by $\mathbf{S}$. As shown in Fig. 2, the received signal y_E is split into two parts at $\mathbf{E}$, one for information relaying aiming to alter the effective channel of the legitimate link from $\mathbf{S}$ to $\mathbf{D}$, and the other for information decoding so as to eavesdrop the message sent by $\mathbf{S}$. Denote by $0 \leq \rho \leq 1$ the power splitting ratio for the signal part split for information relaying. The transmitted signal x_E by $\mathbf{E}$ can then be expressed as

$$x_E = v\left(\sqrt{\rho}h_{SE}\sqrt{P_S}d_S + n_E^{(R)}\right), \tag{2}$$

where v is the complex-valued amplification coefficient at $\mathbf{E}$, and $n_E^{(R)} \sim \mathcal{CN}(0,\sigma^2)$ denotes the AWGN introduced during the relaying operation at $\mathbf{E}$. By assuming that the processing delay due to the AF relaying at $\mathbf{E}$ is negligible, the signal received at $\mathbf{D}$ can be expressed as

$$y_D = h_{SD}\sqrt{P_S}d_S + h_{ED}x_E + n_D, \tag{3}$$

$$= \left(h_{SD} + v\sqrt{\rho}h_{SE}h_{ED}\right)\sqrt{P_S}d_S + vh_{ED}n_E^{(R)} + n_D, \tag{4}$$

where h_{ED} denotes the channel from $\mathbf{E}$ to $\mathbf{D}$, and $n_D \sim \mathcal{CN}(0,\sigma^2)$ is the AWGN at $\mathbf{D}$. It is observed from (4) that by adjusting the power splitting ratio ρ and the amplification coefficient v, the eavesdropper $\mathbf{E}$ is able to alter the effective channel from $\mathbf{S}$ to $\mathbf{D}$. The effective capacity of the legitimate link can then be expressed as $\tilde{R}_D = \log_2(1+\tilde{\gamma}_D)$, where $\tilde{\gamma}_D$ is the effective signal-to-noise ratio (SNR) at $\mathbf{D}$, which can be obtained from (4) as a function of ρ and v, given by

$$\tilde{\gamma}_D(\rho, v) = \frac{\left|h_{SD} + v\sqrt{\rho}h_{SE}h_{ED}\right|^2 P_S}{(1+|v|^2|h_{ED}|^2)\sigma^2}. \tag{5}$$

On the other hand, at the information decoder of $\mathbf{E}$, the signal based on which the message from $\mathbf{S}$ is decoded can be expressed as

$$\tilde{y}_E = \sqrt{1-\rho}h_{SE}\sqrt{P_S}d_S + n_E^{(D)}, \tag{6}$$

where $n_E^{(D)} \sim \mathcal{CN}(0,\sigma^2)$ denotes the AWGN at the information decoder of $\mathbf{E}$. Thus, the information rate achievable by $\mathbf{E}$ is $\tilde{R}_E = \log_2(1+\tilde{\gamma}_E)$, where $\tilde{\gamma}_E$ is the SNR as a function of ρ given by

$$\tilde{\gamma}_E(\rho) = \frac{(1-\rho)|h_{SE}|^2 P_S}{\sigma^2}. \tag{7}$$

To study the worst-case scenario under the spoofing relay attack, we assume that perfect channel state information (CSI)

[1] Note that in this case $\mathbf{E}$ may still extract useful information from its received signal; while in this paper we consider a more stringent setup where the message from $\mathbf{S}$ needs to be decoded at $\mathbf{E}$ with arbitrarily small error.

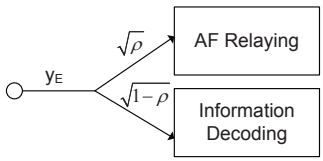


Fig. 2: The architecture of a spoofing relay.

of all links is available at $\mathbf{E}$. The investigation on the spoofing relay attack with imperfect or limited CSI at $\mathbf{E}$ is left for our future work. The objective of $\mathbf{E}$ is to optimize the power splitting ratio ρ and the amplification coefficient v so that the information leakage rate is maximized. Based on the definition in (1), the problem can be formulated as

$$(\mathrm{P1}): \begin{cases} \max\limits_{v,\rho} & \tilde{R}_D \\ \text{s.t.} & \tilde{R}_E \geq \tilde{R}_D \\ & 0 \leq \rho \leq 1, \\ & |v|^2 \left(\rho |h_{SE}|^2 P_S + \sigma^2\right) \leq P_E, \end{cases} \tag{8}$$

where P_E denotes the maximum transmission power at $\mathbf{E}$.

3. OPTIMAL SOLUTION

To find the optimal solution to (P1), notice that $\tilde{R}_D$ and $\tilde{R}_E$ in (P1) can be respectively replaced by $\tilde{\gamma}_D(v,\rho)$ and $\tilde{\gamma}_E(\rho)$ due to their monotonic relations. Furthermore, for any fixed power splitting ratio $0 \leq \rho \leq 1$, we first obtain the maximum achievable SNR at $\mathbf{D}$, denoted as $\tilde{\gamma}_D^{\max}(\rho)$, by optimizing the amplification coefficient v as

$$\tilde{\gamma}_D^{\max}(\rho) \triangleq \begin{cases} \max\limits_{v} & \tilde{\gamma}_D(\rho, v) \\ \text{s.t.} & |v|^2 \leq \frac{P_E}{\rho |h_{SE}|^2 P_S + \sigma^2}. \end{cases} \tag{9}$$

It follows from (5) that at the optimal solution to (9), the phase of v should be chosen such that the two signal paths from $\mathbf{S}$ to $\mathbf{D}$ add constructively, i.e., $\angle v = \angle h_{SD} - \angle h_{SE} - \angle h_{ED}$, where $\angle z$ denotes the phase of a complex number z. We term such a strategy of the spoofing relay as *constructive information forwarding*, since it helps enhance the effective channel of the legitimate link from $\mathbf{S}$ to $\mathbf{D}$. In addition, the magnitude of the optimal v to (9) can be obtained by examining its first-order derivative, and the resulted maximum SNR can be expressed as

$$\tilde{\gamma}_D^{\max}(\rho) = \begin{cases} \left(1 + \frac{\rho |h_{SE}|^2}{|h_{SD}|^2}\right) \tilde{P}_S |h_{SD}|^2, & 0 \leq \rho \leq \rho_1 \\ \frac{\left(\sqrt{1+\rho |h_{SE}|^2 \tilde{P}_S} + \frac{|h_{SE}||h_{ED}|}{|h_{SD}|}\sqrt{\rho \tilde{P}_E}\right)^2 \tilde{P}_S |h_{SD}|^2}{1+\rho |h_{SE}|^2 \tilde{P}_S + |h_{ED}|^2 \tilde{P}_E}, & \\ & \rho_1 < \rho \leq 1, \end{cases}$$

where $\rho_1 \triangleq \min\left\{1, \frac{-1+\sqrt{1+4\tilde{P}_S \tilde{P}_E |h_{SD}|^2 |h_{ED}|^2}}{2|h_{SE}|^2 \tilde{P}_S}\right\}$, with $\tilde{P}_S \triangleq P_S/\sigma^2$ and $\tilde{P}_E \triangleq P_E/\sigma^2$. It can be verified that $\tilde{\gamma}_D^{\max}(\rho)$ is a monotonically increasing function of $0 \leq \rho \leq 1$.

In particular, if $\rho = 0$, i.e., no information forwarding is applied at $\mathbf{E}$, we have $v = 0$ and $\tilde{\gamma}_D^{\max}(0) = \tilde{P}_S |h_{SD}|^2$. This corresponds to the special case of passive eavesdropping previously discussed in Section 2.1.

On the other hand, for fixed $0 \leq \rho \leq 1$, the minimum achievable SNR at $\mathbf{D}$, denoted as $\tilde{\gamma}_D^{\min}(\rho)$, can be obtained by solving

$$\tilde{\gamma}_D^{\min}(\rho) \triangleq \begin{cases} \min\limits_{v} & \tilde{\gamma}_D(\rho, v) \\ \text{s.t.} & |v|^2 \leq \frac{P_E}{\rho |h_{SE}|^2 P_S + \sigma^2}. \end{cases} \tag{10}$$

It follows from (5) that at the optimal solution to (10), the two signal paths from $\mathbf{S}$ to $\mathbf{D}$ should add destructively, i.e., $\angle v = \pi + \angle h_{SD} - \angle h_{SE} - \angle h_{ED}$. Such a strategy at $\mathbf{E}$ is termed as *destructive information forwarding*, which essentially degrades the effective channel of the legitimate link from $\mathbf{S}$ to $\mathbf{D}$. Furthermore, by taking the first order derivative with respect to the magnitude of v, the corresponding optimal value of (10) can be expressed as

$$\tilde{\gamma}_D^{\min}(\rho) = \begin{cases} \frac{\left(\sqrt{1+\rho |h_{SE}|^2 \tilde{P}_S} - \frac{|h_{SE}||h_{ED}|}{|h_{SD}|}\sqrt{\rho \tilde{P}_E}\right)^2 \tilde{P}_S |h_{SD}|^2}{1+\rho |h_{SE}|^2 \tilde{P}_S + |h_{ED}|^2 \tilde{P}_E}, & \\ & 0 \leq \rho \leq \rho_2 \\ 0, & \rho_2 < \rho \leq 1, \end{cases}$$

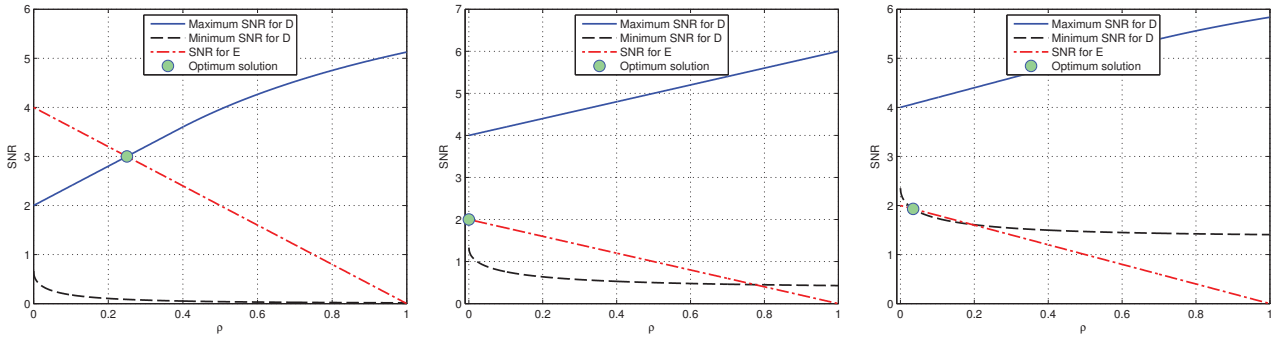
where $\rho_2 = C$ if $0 \leq C \leq 1$, and $\rho_2 = 1$ otherwise, with $C \triangleq \frac{|h_{SD}|^2}{|h_{SE}|^2\left(|h_{ED}|^2 \tilde{P}_E - |h_{SD}|^2 \tilde{P}_S\right)}$. In particular, if $\rho = 0$, i.e., no information forwarding by $\mathbf{E}$, we have $\tilde{\gamma}_D^{\min}(0) = \frac{\tilde{P}_S |h_{SD}|^2}{1+|h_{ED}|^2 \tilde{P}_E}$. This corresponds to degrading the SNR at $\mathbf{D}$ via *jamming*, i.e., by amplifying the noise with full power at $\mathbf{E}$. For $\rho > 0$, both destructive information forwarding and jamming (i.e., noise amplification) contribute to the SNR degradation at $\mathbf{D}$, as can be seen from the expression of $\tilde{\gamma}_D^{\min}(\rho)$.

Since $\tilde{\gamma}_D(\rho, v)$ is a continuous function of v, for any fixed $0 \leq \rho \leq 1$, the set of achievable SNRs at $\mathbf{D}$ is given by the interval $\left[\tilde{\gamma}_D^{\min}(\rho), \tilde{\gamma}_D^{\max}(\rho)\right]$. Consequently, (P1) reduces to finding the optimal power splitting ratio ρ via solving

$$(\mathrm{P2}): \begin{cases} \max\limits_{0 \leq \rho \leq 1, \tilde{\gamma}_D} & \tilde{\gamma}_D \\ \text{s.t.} & \tilde{\gamma}_D^{\min}(\rho) \leq \tilde{\gamma}_D \leq \tilde{\gamma}_D^{\max}(\rho) \\ & \tilde{\gamma}_D \leq \tilde{\gamma}_E(\rho), \end{cases} \tag{11}$$

which can be solved by considering the following three cases.

Case 1: $\tilde{\gamma}_D^{\max}(0) < \tilde{\gamma}_E(0)$, or $|h_{SD}|^2 < |h_{SE}|^2$, as illustrated in Fig. 3(a). In this case, $\mathbf{E}$ has a better channel than the legitimate receiver $\mathbf{D}$. Intuitively, $\mathbf{E}$ should perform constructive information forwarding to enhance the effective channel of $\mathbf{D}$ so as to increase the information leakage rate. It follows from Fig. 3(a) that the optimal solution to (P2) is given by the intersection point of the two curves $\tilde{\gamma}_D^{\max}(\rho)$ and $\tilde{\gamma}_E(\rho)$. As $\tilde{\gamma}_D^{\max}(\rho)$ and $\tilde{\gamma}_E(\rho)$ are monotonically increasing and decreasing functions over $0 \leq \rho \leq 1$, respectively, and



(a) Case 1: $|h_{SD}|^2 < |h_{SE}|^2$ (b) Case 2: $\frac{|h_{SD}|^2}{1+|h_{ED}|^2\tilde{P}_E} \leq |h_{SE}|^2 \leq |h_{SD}|^2$ (c) Case 3: $|h_{SE}|^2 < \frac{|h_{SD}|^2}{1+|h_{ED}|^2\tilde{P}_E}$

Fig. 3: Three cases for the optimal power splitting solution.

$\tilde{\gamma}_D^{\max}(1) > \tilde{\gamma}_E(1) = 0$, the equation $\tilde{\gamma}_D^{\max}(\rho) = \tilde{\gamma}_E(\rho)$ has one unique solution $\rho^\star$, which can be obtained numerically.

Case 2: $\tilde{\gamma}_D^{\min}(0) \leq \tilde{\gamma}_E(0) \leq \tilde{\gamma}_D^{\max}(0)$, or $\frac{|h_{SD}|^2}{1+|h_{ED}|^2\tilde{P}_E} \leq |h_{SE}|^2 \leq |h_{SD}|^2$, as illustrated in Fig. 3(b). In this case, the eavesdropping link is worse than the legitimate link, but it becomes better if jamming with full power is applied at $\mathbf{E}$ to degrade the legitimate link. It follows from Fig. 3(b) that the optimal solution to (P2) is $\rho^\star = 0$, i.e., no information forwarding and only jamming is applied by $\mathbf{E}$ with normalized jamming power $\tilde{P}_E^\star = \frac{1}{|h_{ED}|^2}\left(\frac{|h_{SD}|^2}{|h_{SE}|^2} - 1\right)$ to degrade the legitimate link SNR to the same level as that at $\mathbf{E}$.

Case 3: $\tilde{\gamma}_E(0) < \tilde{\gamma}_D^{\min}(0)$, or $|h_{SE}|^2 < \frac{|h_{SD}|^2}{1+|h_{ED}|^2\tilde{P}_E}$, as illustrated in Fig. 3(c). In this case, the eavesdropping link is worse than the legitimate link even after jamming with full power by $\mathbf{E}$. Therefore, destructive information forwarding and jamming should be both applied at $\mathbf{E}$ to further degrade the legitimate link. It follows from Fig. 3(c) that the optimal solution $\rho^\star$ to (P2) is obtained by solving $\tilde{\gamma}_D^{\min}(\rho) = \tilde{\gamma}_E(\rho)$ in the interval $0 \leq \rho \leq 1$, which can be reduced to a quartic equation and hence solved efficiently. Note that if more than one solutions exist, the one with the smallest magnitude is the optimal solution. On the other hand, if no such a solution exists, it implies that problem (P2), and hence (P1), is infeasible, i.e., the spoofing relay attack is not sufficient to degrade the source transmission rate to a level achievable by the eavesdropper with its given power constraint.

4. NUMERICAL RESULTS

We assume that the source $\mathbf{S}$ and the legitimate receiver $\mathbf{D}$ are separated by a fixed distance $d_{SD} = 1000$ meters, and the eavesdropper $\mathbf{E}$ moves along the line from $\mathbf{S}$ to $\mathbf{D}$ with the distance d_{SE} varying from 50 to 3000 meters. We assume line-of-sight (LoS) channels with free-space path loss model, and the operating frequency is assumed to be 1.8 GHz. The source transmission power P_S is set to a value such that the received SNR at $\mathbf{D}$ (without eavesdropper's attack) is 10 dB. By assuming $P_E = P_S$, Fig. 4 plots the information leakage rate R_{leak} versus d_{SE} by passive eavesdropping versus the studied active eavesdropping, with R_{leak} given by

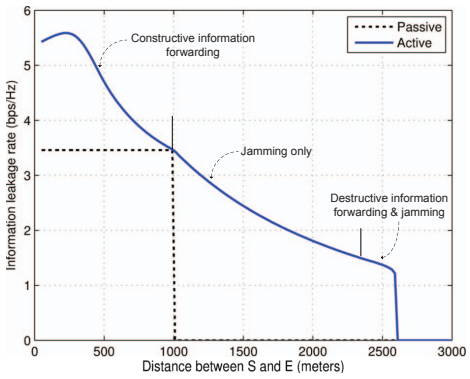


Fig. 4: The information leakage rate with passive versus active eavesdropping.

(1). Fig. 4 shows that with passive eavesdropping, a constant R_{leak}, whose value is determined by the legitimate link, is achieved when $\mathbf{E}$ has a better channel than $\mathbf{D}$, i.e., $d_{SE} \leq d_{SD}$; whereas if $d_{SE} > d_{SD}$, R_{leak} drops to zero since $\mathbf{E}$ cannot reliably decode the information from $\mathbf{S}$. In contrast, with the active spoofing relay attack, $\mathbf{E}$ is able to achieve much higher information leakage rate. Fig. 4 also shows the three different strategies of the spoofing relay attack by the eavesdropper, namely constructive information forwarding, jamming, and both destructive information forwarding and jamming, which correspond to the three cases for determining the optimal power splitting ratio studied in Section 3.

5. CONCLUSION

This paper studies a new active eavesdropping technique via the spoofing relay attack. Depending on the channel conditions, the eavesdropper constructively or destructively forwards the information signal to the destination, so as to spoof the source to increase or decrease the transmission rate to maximize the information leakage rate. It is shown that with this new attack, the eavesdropper can significantly enhance the information leakage rate over the conventional passive eavesdropping. This paper opens a new avenue for investigating the physical-layer security with more intelligent eavesdroppers than conventional passive listeners.

6. REFERENCES

[1] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May 1988.

[2] Y. Liang, H. V. Poor, and S. Shamai, *Information theoretic security*, Foundations and Trends in Communications and Information Theory, 2009.

[3] A. D. Wyner, "The wire-tap channel," *Bell Sys. Techn. Journ.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[4] A. Khisti and G. Wornell, "Secure transmission with multiple antennas –II: the MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[6] Y. W. P. Hong, P. C. Lan, and C. C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Aug. 2013.

[7] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: an overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, June 2015.

[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] D. Kapetanovic, G. Zheng, K.-K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO," in *Proc. PIMRC*, Sept. 2013, pp. 13–18.

[10] A. A. Kapetanovic, D. Nahari, A. Stojanovic, and F. Rusek, "Detection of active eavesdroppers in massive MIMO," in *Proc. PIMRC*, Sept. 2014, pp. 585–589.

[11] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.

[12] J.-M. Kang, C. In, and H.-M. Kim, "Detection of pilot contamination attack for multi-antenna based secrecy systems," in *IEEE VTC Spring*, May 2015, pp. 1–5.

[13] J. K. Tugnait, "Self-contamination for detection of pilot contamination attack in multiple antenna systems," *IEEE Wireless Commun. Lett.*, vol. PP, no. 99, July 2015.

[14] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sept. 2014.