EFFICIENT INFORMATION LEAKAGE NEUTRALIZATION ON A RELAY-ASSISTED MULTI-CARRIER INTERFERENCE CHANNEL

Zuleita Ho†, Eduard Jorswieck† and Sabrina Gerbracht**

TU Dresden
Faculty of Electrical and Computer Engineering,
Communications Laboratory, Dresden, Germany
{zuleita.ho, eduard.jorswieck, sabrina.gerbracht}@tu-dresden.de

ABSTRACT

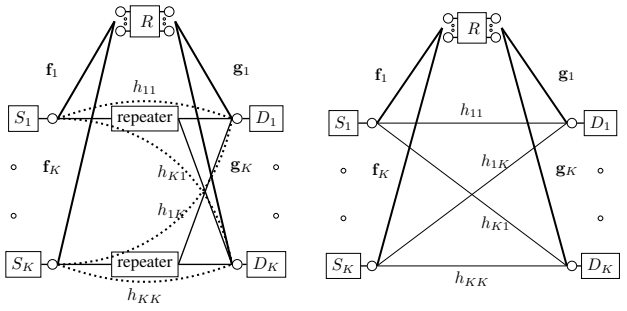
In heterogeneous dense networks where spectrum is shared, users privacy remains one of the major challenges. When the receivers are not only interested in their own signals but also in eavesdropping other users' signals, the cross talk becomes information leakage. We propose a novel and efficient secrecy rate enhancing relay strategy EFFIN for *information leakage neutralization*. The relay matrix is chosen such that the effective *leakage* channel (spectral and spatial) is zero. Thus, it ensures secrecy regardless of receive processing employed at eavesdroppers and does not rely on wiretaps codes to ensure secrecy, unlike other physical layer security techniques such as artificial noise. EFFIN achieves a higher sum secrecy rate over several state-of-the-art baseline methods.

***Index Terms*—** Interference relay channel; Interference neutralization; Amplify-and-forward relay; worst-case secrecy rate; multi-antenna systems

I. INTRODUCTION

The trend of future wireless network systems is towards spectrum sharing over different wireless infrastructures. With isolated wireless infrastructures, such as multiple non-cooperating LTE cells, ensuring data security remains a major technical challenge. Physical layer security techniques provide an alternative approach when the front-ends are of limited computation capability and are not able to carry out standard cryptography methods such as symmetric key and asymmetric key encryption. Physical layer security techniques [1]–[3] provide an additional protection to the conventional secure transmission methods using cryptography. Due to space limitation, we are not able to list all physical layer security results, interested readers are referred to recent tutorial papers [4], [5].

†This work has been performed in the framework of the European research project DIWINE, which is partly funded by the European Union under its FP7 ICT Objective 1.1 - The Network of the Future.*This work is supported by the German Research Foundation (DFG) in the Collaborative Research Center 912 "Highly Adaptive Energy-Efficient Computing".



(a) a relay-assisted network (b) instantaneous relay network

Fig. 1. The wireless relay-assisted network with layer one repeaters and one smart relay is shown in subfigure (a). The dotted lines demonstrate the equivalent links between a source and a destination taking into account the presence of the repeaters. All paths from source to destination nodes take two time slots (through either the smart relay or repeaters). The equivalent channel is established in subfigure (b) by replacing the relay as an instantaneous relay. Information going through the instantaneous relay arrives at the destinations at the same time as over the direct links.

In relay-assisted multi-user systems, a potential malicious user in the system can lead to compromised confidentiality. Many novel strategies have been proposed to improve the secrecy in relay systems, including cooperative jamming [6], [7], noise-forwarding [8], signal-forwarding strategies [9], [10] and multi-carrier relay systems with external eavesdropper(s) [11], [12]. Yet, a joint optimization of secrecy rates over the frequency-spatial resources in a relay-assisted multi-user interference channel (with internal eavesdroppers) remains an open problem. This is the goal of our paper.

We assume that the relay employs an amplify-and-forward (AF) strategy which provides flexibility in implementation as the relay is transparent to the modulation and coding schemes and induces negligible signal processing delays [13]. The novel notion of *relay-without-delays*, also known as instantaneous relays if the relays are memoryless [14]–

[16], refers to relays that forward signals consisting of both current symbol and symbols in the past, instead of only the past symbols as in conventional relays. As shown in Figure 1, the instantaneous relay model provides a matching model of layer-1 repeaters connected networks (such as LTE networks) and helps us analyze the system performance of nowadays repeaters connected networks[1].

In order to provide secure transmission over relay-assisted multi-carrier networks, we propose a relay strategy termed as *information leakage neutralization* which algebraically neutralizes information leakage from each transmitter in the network to each eavesdropper on each frequency subcarrier. This method is adopted from a technique on relay networks, termed as interference neutralization (IN). IN has been applied to eliminate interference in various systems [13], [18], [19] including instantaneous relay channels [20]. Our prior work shows that IN is effective in improving secrecy rates in a two-hop wiretap channel [21]. The proposed method in this paper differs from previous works above as the neutralization over multi-carrier systems is of high complexity. Another important difference is that here the relays have multiple antennas. In this paper, the eavesdroppers are also the users of the system and the corresponding channel state information is assumed to be accurate and available at the relay.

II. SYSTEM MODEL

For simplicity of presentation, the relay is assumed to have $N = 2$ antennas and the transmitters and receivers are equipped with one antenna and share $M = 2$ frequency subcarriers. Note that the proposed algorithm applies to arbitrary number of antennas N and frequency subcarriers M. Transmitter i, $i = 1, 2$, transmits symbols $\mathbf{x}_i \in \mathbb{C}^{2\times 1}$ which are spread over 2 frequency subcarriers by precoding matrix $\mathbf{P}_i$. For the ease of notation, we assume that precoding matrix $\mathbf{P}_i$ is a square matrix. When user i transmits $S_i \leq 2$ symbols, then zeros are padded in $\mathbf{x}_i$ so that its dimension is always 2×1 and correspondingly zero columns are padded in $\mathbf{P}_i$. If user i transmits one symbol on subcarrier 1 but nothing on subcarrier 2, then $\mathbf{P}_i = [a, 0; 0, 0]$ for some complex scalar a. If $\mathbf{P}_i$ is diagonal, then each symbol is only sent on one frequency. Denote the m-th transmit symbol of user i as $\mathbf{x}_i(m)$ which is randomly generated, mutually independent and with covariance matrix $\mathbf{I}_2$. The precoding matrix $\mathbf{P}_i$ satisfies the transmit power constraint of user i: $\mathrm{tr}\left(\mathbf{P}_i \mathbf{P}_i^{\mathrm{H}}\right) \leq P_i^{max}$. Denote the channel gain from transmitter (TX) i to receiver (RX) j on frequency m as $h_{ji}(m)$. The received signal of user i through the direct paths of the interference channel is given by,

$$\mathbf{y}_i = \sum_{j=1}^{2} \begin{bmatrix} h_{ij}(1) & 0 \\ 0 & h_{ij}(2) \end{bmatrix} \mathbf{P}_j \begin{bmatrix} x_j(1) \\ x_j(2) \end{bmatrix} + \begin{bmatrix} n_i(1) \\ n_i(2) \end{bmatrix}.$$

The circular Gaussian noise with unit variance received on the m-th subcarrier at RX i is denoted as $n_i(m)$. We denote the received signal at the relay as a stacked vector of the received signal at each frequency m, with $\mathbf{y}_r(m) \in \mathbb{C}^{2\times 1}$ representing the received signal on frequency m and the a-th element in $\mathbf{y}_r(m)$ representing the signal at the a-th antenna. The received signal at the relay is given by,

$$\mathbf{y}_r = \sum_{j=1}^{2} \begin{bmatrix} \mathbf{f}_j(1) & \mathbf{0}_{2\times 1} \\ \mathbf{0}_{2\times 1} & \mathbf{f}_j(2) \end{bmatrix} \mathbf{P}_j \begin{bmatrix} x_j(1) \\ x_j(2) \end{bmatrix} + \begin{bmatrix} \mathbf{n}_r(1) \\ \mathbf{n}_r(2) \end{bmatrix},$$

where $\mathbf{n}_r(m) \in \mathbb{C}^{2\times 1}$ is a circular Gaussian noise vector received at frequency m with identity covariance matrix and $\mathbf{f}_j(m)$ is the complex vector channel from user j to the relay on frequency m. The relay processes the received signal $\mathbf{y}_r$ by a multiplication of matrix $\mathbf{R} \in \mathbb{C}^{4\times 4}$ and forwards the signal to the RXs. Denote the channel from relay to RX i on frequency m by $\mathbf{g}_i(m) \in \mathbb{C}^{2\times 1}$. With the assumption of instantaneous interference relay channel, the signals through the direct path (through a layer-1 relay embedded in the system) and through the intelligent relay arrive at the RXs at the same time. The received signal at RX i is thus given by

$$\mathbf{y}_i = \sum_{j=1}^{2} \left(\mathbf{H}_{ij} + \mathbf{G}_i^{\mathrm{H}} \mathbf{R} \mathbf{F}_j\right) \mathbf{P}_j \mathbf{x}_j + \mathbf{G}_i^{\mathrm{H}} \mathbf{R} \mathbf{n}_r + \mathbf{n}_i .$$

where $\mathbf{H}_{ij} = \mathrm{diag}\left(h_{ij}(1), h_{ij}(2)\right)$, $\mathbf{G}_i = \mathrm{diag}\left(\mathbf{g}_i(1), \mathbf{g}_i(2)\right)$, $\mathbf{F}_i = \mathrm{diag}\left(\mathbf{f}_j(1), \mathbf{f}_j(2)\right)$ and the equivalent channel from TX j to RX i as $\bar{\mathbf{H}}_{ij} = \mathbf{H}_{ij} + \mathbf{G}_i^{\mathrm{H}} \mathbf{R} \mathbf{F}_j$. An achievable rate of user 1 is

$$r_1(\mathbf{R}) = \mathcal{C}\left(\mathbf{I}_2 + \bar{\mathbf{H}}_{11} \mathbf{P}_1 \mathbf{P}_1^{\mathrm{H}} \bar{\mathbf{H}}_{11}^{\mathrm{H}} \cdot \left(\bar{\mathbf{H}}_{12} \mathbf{P}_2 \mathbf{P}_2^{\mathrm{H}} \bar{\mathbf{H}}_{12}^{\mathrm{H}} + \mathbf{G}_1^{\mathrm{H}} \mathbf{R} \mathbf{R}^{\mathrm{H}} \mathbf{G}_1 + \mathbf{I}_2\right)^{-1} \right)$$

where $\mathcal{C}(\mathbf{X}) = \log_2 \det(\mathbf{X})$. Consider that RX 2 is a potential eavesdropper. We compute the worst-case scenario in which RX 2 decodes all other symbols perfectly before decoding the messages from TX 1 and RX 2 sees a MIMO channel and decodes messages $\mathbf{x}_1$ utilizing both frequencies (with a MMSE receive filter for example). An achievable rate is then

$$r_{2\leftarrow 1}(\mathbf{R}) = \mathcal{C}\left(\mathbf{I}_2 + \bar{\mathbf{H}}_{21} \mathbf{P}_1 \mathbf{P}_1^{\mathrm{H}} \bar{\mathbf{H}}_{21}^{\mathrm{H}} \left(\mathbf{G}_2^{\mathrm{H}} \mathbf{R} \mathbf{R}^{\mathrm{H}} \mathbf{G}_2 + \mathbf{I}_2\right)^{-1} \right).$$

An achievable secrecy rate of user 1 is then the achievable rate of user 1 $r_1(\mathbf{R})$ minus the leakage rate to user 2

[1] In modern networks such as LTE, wireless links are often connected using boosters or layer-1 repeaters (simple amplifiers) [17]. If the time consumed for the signals to travel from a source to a repeater or from a repeater to a destination is counted as one unit, then the total time for the signal to travel from a source to a destination is two units - the same amount of time for the signal to travel from a source through a smart AF relay to a destination.

$r_{2\leftarrow 1}(\mathbf{R})$ [22]:

$$r_1^s(\mathbf{R}) = \left(r_1(\mathbf{R}) - r_{2\leftarrow 1}(\mathbf{R})\right)^+. \quad (1)$$

Our goal is to choose $\mathbf{R}$ such that the secrecy leakage is zero: $\bar{\mathbf{H}}_{ij}\,\mathbf{P}_j = \mathbf{0}$ for $i \neq j$. Consequently, the leakage rate $r_{i\leftarrow j}(\mathbf{R}) = 0$ and the secrecy rate in (1) is $r_i^s(\mathbf{R}) = r_i(\mathbf{R})$[2]. For the feasibility and limitations of information leakage neutralization, please refer to [23]. The optimization of the sum secrecy rates is formulated in the following.

$$\begin{aligned}
\max_{\mathbf{R},\{\mathbf{P}_i\}} \sum_{i=1}^{2} \mathcal{C}\left(\mathbf{I}_M + \bar{\mathbf{H}}_{ii}\,\mathbf{P}_i\,\mathbf{P}_i^{\mathrm{H}}\,\bar{\mathbf{H}}_{ii}^{\mathrm{H}}\left(\mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{R}^{\mathrm{H}}\,\mathbf{G}_i + \mathbf{I}_M\right)^{-1}\right) \\
\left(\mathbf{H}_{ij} + \mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}_j\right)\mathbf{P}_j = \mathbf{0}, \quad i,j = 1,2, i \neq j, \\
\mathrm{tr}\left(\mathbf{P}_i\,\mathbf{P}_i^{\mathrm{H}}\right) \leq P_i^{max}, \\
\mathrm{tr}\left(\mathbf{R}\left(\sum_{i=1}^{K}\mathbf{F}_i\,\mathbf{P}_i\,\mathbf{P}_i^{\mathrm{H}}\,\mathbf{F}_i^{\mathrm{H}}\right)\mathbf{R}^{\mathrm{H}}\right) \leq P_r^{max}.
\end{aligned}$$

III. INFORMATION LEAKAGE NEUTRALIZATION

Recall that the information leakage neutralization criteria $\left(\mathbf{H}_{ij} + \mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}_j\right)\mathbf{P}_i = \mathbf{0}$, when $\mathbf{P}_i$ is invertible, is equivalent to

$$\mathbf{H}_{ij} + \mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}_j = \mathbf{0}.$$

Due to the block diagonal structure of $\mathbf{H}_{ij}$, $\mathbf{G}_i$ and $\mathbf{F}_j$, one feasible solution of the above equation is a block diagonal $\mathbf{R}$. The information leakage neutralization constraint breaks down to the optimization over the diagonal blocks $\mathbf{R}_{mm}$ in $\mathbf{R}$:

$$\begin{cases} h_{12}(m) + \mathbf{g}_1^{\mathrm{H}}(m)\,\mathbf{R}_{mm}\,\mathbf{f}_2(m) = 0, \\ h_{21}(m) + \mathbf{g}_2^{\mathrm{H}}(m)\,\mathbf{R}_{mm}\,\mathbf{f}_1(m) = 0 \end{cases}. \quad (2)$$

The block matrix $\mathbf{R}_{mm}$ must satisfy

$$\underbrace{\begin{bmatrix} \left(\mathbf{f}_1^{\mathrm{T}}(m) \otimes \mathbf{g}_2^{\mathrm{H}}(m)\right) \\ \left(\mathbf{f}_2^{\mathrm{T}}(m) \otimes \mathbf{g}_1^{\mathrm{H}}(m)\right) \end{bmatrix}}_{\mathbf{A}(m)} \mathrm{vec}(\mathbf{R}_{mm}) = \underbrace{\begin{bmatrix} -h_{12}(m) \\ -h_{21}(m) \end{bmatrix}}_{\mathbf{b}(m)} + \mathbf{z}.$$

The vector $\mathbf{z}$ is any vector in the null space of $\mathbf{A}(m)$. Multiplying both sides with the pseudo-inverse of $\mathbf{A}(m)$, we have $\mathrm{vec}\left(\mathbf{R}_{mm}\right) = \left(\mathbf{A}(m)\right)^{\dagger}\left(\mathbf{b}(m) + \mathbf{z}\right)$. Substitute this into the relay transmit power constraint, we see that any non-zero $\mathbf{z}$ contributes to an increase of relay transmit power. With a limited power budget at relay, we propose to implement information leakage neutralization with the least relay transmit power and set $\mathbf{z} = \mathbf{0}$. Thus, the relay matrix has the m-th diagonal block equal to

$$\mathbf{R}_{mm} = \mathrm{vec}^{-1}\left(\left(\mathbf{A}(m)\right)^{\dagger}\mathbf{b}(m)\right) \quad (3)$$

[2]Note that IN is different from conventional zero-forcing techniques because IN neutralizes the equivalent leakage channel to zero and thus the eavesdroppers are not able to overhear the secrete message regardless of receive processing employed. Also, IN does not rely on wiretap codes to ensure secrecy, unlike other methods such as artificial noise.

where $\mathrm{vec}(.)^{-1}$ is to reverse the vectorization of a vector columnwise to a matrix and † denotes a pseudo inverse. From (3), we obtain the relay design $\mathbf{R} = \mathrm{diag}\left(\mathbf{R}_{11}, \ldots, \mathbf{R}_{MM}\right)$, the optimal precoding matrices $\{\mathbf{P}_i\}$ are computed by solving $\mathcal{Q}_1$.

$$\begin{aligned}
\mathcal{Q}_1: \max_{\{\mathbf{Q}_i\},\mathbf{Q}_i \succeq 0} \quad & \sum_{i=1}^{K} \mathcal{C}\left(\mathbf{I}_M + \mathbf{Q}_i\,\mathbf{W}_i\right) \\
\text{such that} \quad & \mathrm{tr}\left(\mathbf{Q}_i\right) \leq P_i^{max}, \quad i = 1, \ldots, K, \\
& \sum_{i=1}^{K} \mathrm{tr}\left(\mathbf{Q}_i\,\mathbf{X}_i\right) \leq \bar{P}_r^{max}.
\end{aligned}$$

where we replace $\mathbf{P}_i\,\mathbf{P}_i^{\mathrm{H}}$ by positive semi-definite variable $\mathbf{Q}_i$ and denote the following matrices $\mathbf{W}_i = \bar{\mathbf{H}}_{ii}^{\mathrm{H}}\left(\mathbf{G}_i^{\mathrm{H}}\,\mathbf{R}\,\mathbf{R}^{\mathrm{H}}\,\mathbf{G}_i + \mathbf{I}_M\right)^{-1}\bar{\mathbf{H}}_{ii}$ and $\mathbf{X}_i = \mathbf{F}_i^{\mathrm{H}}\,\mathbf{R}^{\mathrm{H}}\,\mathbf{R}\,\mathbf{F}_i$ and $\bar{P}_r^{max} = P_r^{max} - \mathrm{tr}\left(\mathbf{R}\,\mathbf{R}^{\mathrm{H}}\right)$. The objective in $\mathcal{Q}_1$ is concave in $\mathbf{Q}_i$ as $\mathbf{W}_i$ is positive semi-definite and the constraints are linear in $\mathbf{Q}_i$. Thus, $\mathcal{Q}_1$ is a semi-definite program and can be solved readily using convex optimization solvers, e.g. CVX[3]. The optimal $\mathbf{P}_i$ is obtained by performing eigenvalue decomposition on $\mathbf{Q}_i = \mathbf{U}_i\,\mathbf{D}_i\,\mathbf{U}_i^{\mathrm{H}}$ and $\mathbf{P}_i = \mathbf{U}_i\,\mathbf{D}_i^{1/2}$. The pseudo-code of the EFFIN is given in Algorithm 1.

Algorithm 1 The pseudo-code for Efficient Information Leakage Neutralization (EFFIN)

1: **for** $m = 1 \rightarrow M$ **do** ▷ Compute block diagonal relay processing matrix
2: Compute $\mathbf{R}_{mm} = \mathrm{vec}^{-1}\left(\left(\mathbf{A}(m)\right)^{\dagger}\mathbf{b}(m)\right)$ with
$\mathbf{A}(m) = \begin{bmatrix} \left(\mathbf{f}_1^{\mathrm{T}}(m) \otimes \mathbf{g}_2^{\mathrm{H}}(m)\right) \\ \left(\mathbf{f}_2^{\mathrm{T}}(m) \otimes \mathbf{g}_1^{\mathrm{H}}(m)\right) \end{bmatrix}, \mathbf{b}(m) = \begin{bmatrix} -\mathbf{h}_{12}(m) \\ -\mathbf{h}_{21}(m) \end{bmatrix}.$
3: **end for**
4: The relay processing matrix is $\mathbf{R} = \mathrm{diag}\left(\mathbf{R}_{11}, \ldots, \mathbf{R}_{MM}\right)$.
5: Solve $\mathcal{Q}_1$ using convex optimization solvers and obtain optimal $\{\mathbf{Q}_i\}$.
6: **for** $i = 1 \rightarrow 2$ **do** ▷ Compute precoding matrices
7: Perform eigen-value decomposition, $\mathbf{Q}_i = \mathbf{U}_i\,\mathbf{D}_i\,\mathbf{U}_i^{\mathrm{H}}$. Set $\mathbf{P}_i = \mathbf{U}_i\,\mathbf{D}_i^{1/2}$.
8: **end for**

IV. SIMULATION RESULTS

To illustrate the effectiveness of the proposed algorithms, we provide in this section numerical simulations for different

[3]Given block diagonal $\mathbf{R}$ in (3), the equivalent channel $\mathbf{W}_i$ and matrix $\mathbf{X}_i$ are also block diagonal. It is possible to solve $\mathcal{Q}_1$ using water-filling with $K+1$ Lagrange multipliers. For large problem size, it may be more computational efficient using a tailor made water-filling method. For medium size problems and illustrative purposes, we propose here to solve by semi-definite programming.

system settings. As an example, we simulate the secrecy rates of a relay assisted network with $K = 2$ users, $M = 8$ frequency subcarriers and $N = 2$ antennas at the relay. We compare EFFIN to the following algorithms. Baseline 1 (Repeater): the relay is a layer 1 relay and is only able to forward signals without additional signal processing. This corresponds to setting $\mathbf{R} = \mathbf{I}_{MN}\sqrt{\frac{P_r^{max}}{MN}}$. Baseline 2 (IC): the relay shuts down, i.e. $\mathbf{R} = \mathbf{0}_{MN}$, and we obtain an interference channel where users eavesdrop each other. For each baseline algorithm, we assume full spectrum sharing-users are allowed to use the entire spectrum. Each TX measures the channel qualities of the direct channel and the channel from itself to the other RX. Based on the measured channel qualities, each TX excludes frequency subcarriers with zero secrecy rates and transmits on the channels with non-zero secrecy rates. For subcarriers at which more than one user would like to transmit, we assume that the TXs coordinate so that the TX with a high secrecy rate would transmit on that subcarrier. Despite such coordination, each user eavesdrops other users on each subcarrier.

In Figure 2, we show achievable sum secrecy rates over varying the transmit power constraint at the relay from 0 to 30 dB while keeping the transmit power constraint at the TXs at 10 dB. As the IC does not utilize the relay, the achievable sum secrecy rates are constant as the relay power constraint increases. The achievable sum secrecy rates achieved by a repeater decreases with relay transmit power. This is due to the increased amplification noise in AF relaying. However, utilizing an intelligent relay and choosing the relaying scheme, one can improve the achievable secrecy rate significantly, about 550% over a simple repeater and about 200% over IC.

In Figure 3, we simulate the achievable sum secrecy rate by the transmit power constraint at TXs from 0 to 30 dB while keeping the transmit power at relay constraint at $23, 27, 30$ dB. As the transmit power at TX increases, the sum secrecy rates saturate in both baseline algorithms. With the proposed information leakage neutralization, we see that the sum secrecy rates grow unbounded with the TX power as each user enjoys a leakage free frequency channel. Note that the sum secrecy rates achieved by relay with power constraint at $23, 27, 30$ dB are plotted in dotted, dashed and solid lines respectively.

V. CONCLUSION

We propose an efficient relay and transmit precoders design for information leakage neutralization on the relay-assisted interference relay channel with internal eavesdroppers. With the proposed design, the system is broken down to parallel information leakage free frequency channels. The proposed designs show tremendous improvement in secrecy rates compared to baseline methods and grow unbounded with transmit power from transmitters.

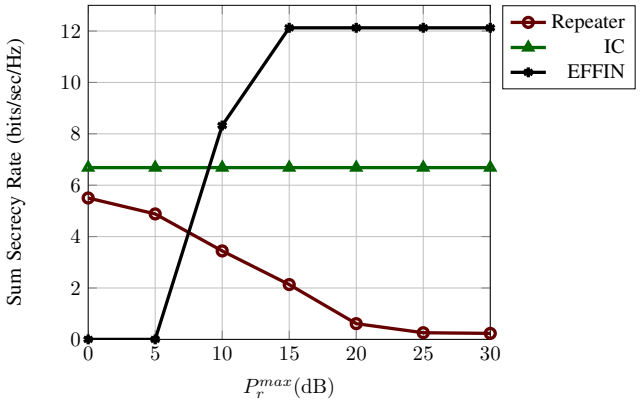


Fig. 2. The achievable secrecy rates of a two-user IRC with 8 frequency subcarriers is shown with varying relay power constraint. The TX power constraints are 10 dB and there are two antennas at the relay. The proposed scheme EFFIN outperforms baseline algorithms Repeater and IC by 550% and 200% respectively.

VI. REFERENCES

[1] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*, Now Publishers Inc., 2009.

[2] R.-H. Liu and W. Trappe, Eds., *Securing Wireless Communications at the Physical Layer*, Springer, 2009.

[3] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[4] Y.-S. Shiu, S.-Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-W. Chen, "Physical Layer Security in Wireless Networks: A Tutorial," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[5] H. V. Poor, "Information and Inference in the Wireless Physical Layer," *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 40–47, Feb. 2012.

[6] G. Zheng, L. C. Choo, and K. K. Wong, "Optimal Cooperative Jamming To Enhance Physical Layer Security Using Relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[7] J. Huang and A. L. Swindlehurst, "Cooperative Jamming for Secure Communications in MIMO Relay Networks," *IEEE Transaction on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[8] L. Lai and H. El Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sept. 2008.

[9] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

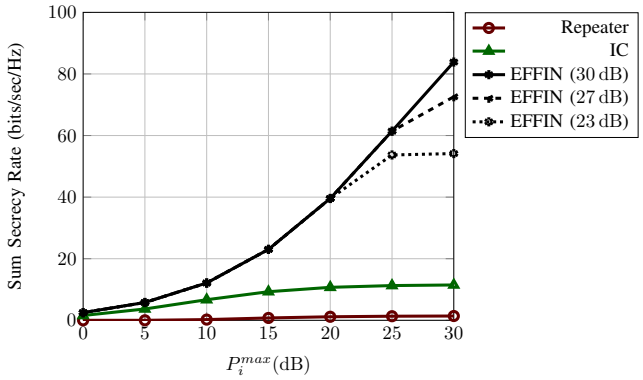


Fig. 3. The achievable secrecy rates of a two-user IRC with 8 frequency subcarriers is shown with varying transmitter power constraints. The relay power constraint is 30 dB and there are two antennas at the relay. The secrecy rates achieved by EFFIN grows unbounded with the transmit power at TX whereas the secrecy rates achieved by baseline algorithms saturate in high SNR regime.

[10] R. Bassily and S. Ulukus, "Secure Communication in Multiple Relay Networks Through Decode-and-Forward Strategies," *Journal of Communications and Networks*, vol. 14, no. 4, pp. 352–363, Aug. 2012.

[11] C. Jeong and I.-M. Kim, "Optimal Power Allocation for Secure Multicarrier Relay Systems," *IEEE Transactions on Signal Processing*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.

[12] D. W.-K. Ng, E. S. Lo, and R. Schober, "Secure Resource Allocation and Scheduling for OFDMA Decode-and-Forward Relay Networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.

[13] S. Berger, M. Kuhn, and A. Wittneben, "Recent Advances in Amplify-and-Forward Two-Hop Relaying," *IEEE Communications Magazine*, vol. 47, no. 7, pp. 50–56, July 2009.

[14] A. El Gamal, N. Hassanpour, and J. Mammen, "Relay Networks With Delays," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3413–3431, Oct. 2007.

[15] V. R. Cadambe and S. A. Jafar, "Degrees of Freedom of Wireless Networks with Relays, Feedback, Cooperation and Full Duplex Operation," *IEEE Transactions on Information Theory*, vol. 55, no. 5, pp. 2334–2344, May 2009.

[16] N. Lee and S. A. Jafar, "Aligned Interference Neutralization and the Degrees of Freedom of the 2 User Interference Channel with Instantaneous Relay," *submitted to IEEE Transactions on Information Theory, available at http://arxiv.org/abs/1102.3833*, pp. 1–17, 2011.

[17] E. Seidel, "Initial Thoughts on LTE Advanced for 3GPP Release 10," in *LTE World Summit, Berlin*, 2009.

[18] S. Mohajer, S. N. Diggavi, and D. N. C. Tse, "Approximate Capacity of a Class of Gaussian Relay-Interference Networks," in *2009 IEEE International Symposium on Information Theory*, June 2009, vol. 57, pp. 31–35.

[19] B. Rankov and A. Wittneben, "Spectral Efficient Protocols for Half-duplex Fading Relay Channels," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 2, pp. 379–389, Feb. 2007.

[20] Z. K.-M. Ho and E. Jorswieck, "Instantaneous Relaying: Optimal Strategies and Interference Neutralization," *IEEE Transactions on Signal Processing*, vol. 60, no. 12, pp. 6655 – 6668, Dec. 2012.

[21] S. Gerbracht, E. A. Jorswieck, G. Zheng, and B. Ottersten, "Non-regenerative Two-Hop Wiretap Channels using Interference Neutralization," in *Proceedings of IEEE International Workshop on Information Forensics and Security (WIFS)*, 2012.

[22] A. Khisti and G. Wornell, "Secure Transmission with Multiple Antennas - Part II: The MIMOME Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515 – 5532, Nov. 2010.

[23] Z. K.-M. Ho, E. Jorswieck, and S. Gerbracht, "Information Leakage Neutralization for the Relay-Assisted Multi-Carrier Interference Channel," *will appear in Journal on Selected Areas of Communications, available at http://tnt.wcms-file2.tu-dresden.de/BibtexDbMng/upload/ZG12.pdf*, 2012.