Opportunistic Secure Transmission for Wireless Relay Networks with Modify-and-Forward Protocol

Quoc-Tuan Vien[†], Tuan Anh Le[†], Trung Q. Duong[‡]
[†]Middlesex University, London, UK. Email: {q.vien, t.le}@mdx.ac.uk.
[‡]Queen's University Belfast, Northern Ireland, UK. Email: trung.q.duong@qub.ac.uk.

Abstract—**This paper investigates the security at the physical layer in cooperative wireless networks (CWNs) where the data transmission between nodes can be realised via either direct transmission (DT) or relaying transmission (RT) schemes. Inspired by the concept of physical-layer network coding (PNC), a secure PNC-based modify-and-forward (SPMF) is developed to cope with the imperfect shared knowledge of the message modification between relay and destination in the conventional modify-and-forward (MF). In this paper, we first derive the secrecy outage probability (SOP) of the SPMF scheme, which is shown to be a general expression for deriving the SOP of any MF schemes. By comparing the SOPs of various schemes, the usage of the relay is shown to be not always necessary and even causes a poorer performance depending on target secrecy rate and quality of channel links. To this extent, we then propose an opportunistic secure transmission protocol to minimise the SOP of the CWNs. In particular, an optimisation problem is developed in which secrecy rate thresholds (SRTs) are determined to find an optimal scheme among various DT and RT schemes for achieving the lowest SOP. Furthermore, the conditions for the existence of SRTs are derived with respect to various channel conditions to determine if the relay could be relied on in practice.**

I. Introduction

Security at the physical layer has attracted the interest of broader communications societies [1]–[3], especially in cooperative wireless networks (CWNs). In CWNs, the data transmission from a source node to a destination node can be realised with the assistance of a single or multiple relay nodes. Therefore, in order to protect data from vulnerable attacks in CWNs, the security of both direct and relaying links need to be considered.

Various secure relaying transmission (RT) strategies were investigated in [4]–[7]. Specifically, secure amplify-and-forward and decode-and-forward cooperation schemes were analysed in [4], [5]. Modify-and-forward (MF) cooperation scheme was proposed in [6], [7] where the relay first modifies the message received from the source and then forwards the modified message to the destination. With MF scheme, it is shown that an improved secrecy outage probability is achieved in comparison with the counterparts using other relaying techniques.

In [6], the modification operation at the relay is assumed to be inherently shared between legitimate users and thus only the interested destination can recover the original message. However, over the wireless media in practice, the channel dedicated for sharing knowledge between the relay and destination also suffers from fading and background noise, which may cause performance degradation. Inspired by the concept of physical-layer network coding (PNC), a secure PNC-based MF (SPMF) was then proposed in [7] to cope with the practical security issue of the imperfect shared knowledge of the message modification between the relay and the destination in the conventional MF scheme. With SPMF scheme, such assumption of perfect shared information is relaxed, while only channel statistics are assumed to be known at the destination. However, the performance of the SPMF scheme as well as its effectiveness compared to other schemes were only validated through the simulation results.

In this paper, we first derive the secrecy outage probability (SOP) of the SPMF scheme. A detailed analysis is provided to verify the effectiveness of the SPMF in comparison with the direct transmission (DT) [8] and MF [6]. The derived SOP of the SPMF is shown to be a general expression which can be used to derive the SOP of the MF scheme in [6] as a special case. Additionally, the SPMF scheme is shown to achieve a lower SOP for higher security compared to the MF scheme in the scenario of imperfect shared knowledge of message modification between the relay and destination, while the DT scheme achieves a better performance than both RT schemes, i.e. MF and SPMF, at a high target secrecy rate. This means the usage of relay node is not always beneficial, especially when the link between the source and the relay and/or the link between the relay and the destination suffer(s) from severe fading and noise. This accordingly motivates us to investigate the conditions of the link quality when the relay should be used in the RT schemes to provide a higher secure communication.

As a second contribution of this paper, we propose an opportunistic secure transmission protocol for CWNs. The proposed protocol aims at finding an optimal scheme among DT and RT schemes that achieves the lowest SOP. It is shown that there exist secrecy rate thresholds (SRTs) which are the crossing points between the SOPs of various schemes. The optimisation problem is thus turned into finding the SRTs with respect to various channel conditions. Particularly, in order to verify the existence of the SRTs, we derive the conditions of the channel quality which not only facilitate the finding of the optimal scheme for a secure CWN, but also help in determining if the relay could be relied on in practical CWNs.

II. System Model

Figure 1 illustrates the system model of a CWN under investigation consisting of a source node $\mathcal{S}$, a destination node

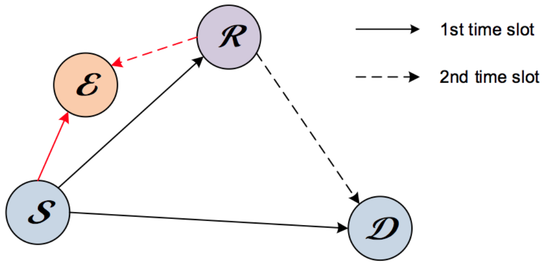

Fig. 1: System model of a CWN in the presence of an eavesdropper.

$\mathcal{D}$ and a relay node $\mathcal{R}$ in the presence of an eavesdropper node $\mathcal{E}$. A half-duplex single-antenna system is considered where each node is equipped with a single antenna and can either transmit or receive data, but not simultaneously. It is assumed that there exists a direct link $\mathcal{S} \to \mathcal{D}$ and thus $\mathcal{S}$ may transmit a data packet to $\mathcal{D}$ either with or without the assistance of $\mathcal{R}$. In Fig. 1, $\mathcal{E}$ is assumed to be located between $\mathcal{S}$ and $\mathcal{D}$ and in the vicinity of $\mathcal{R}$. Therefore, there exists two wiretap links from both $\mathcal{S}$ and $\mathcal{R}$ to $\mathcal{E}$.

In the DT scheme, $\mathcal{S}$ transmits data directly to $\mathcal{D}$, while in the RT scheme, the cooperative data transmission from $\mathcal{S}$ to $\mathcal{D}$ is realised via two time slots as follows: *i) Time slot 1*: $\mathcal{S}$ transmits the data packet to both $\mathcal{R}$ and $\mathcal{D}$ and *ii) Time slot 2*: $\mathcal{R}$ processes the data packet received from $\mathcal{S}$ prior to forwarding the processed data to $\mathcal{D}$.

The communication channel between $\mathcal{A}$ and $\mathcal{B}$, $\{\mathcal{A}, \mathcal{B}\} \in \{\mathcal{S}, \mathcal{R}, \mathcal{E}, \mathcal{D}\}$, $\mathcal{A} \neq \mathcal{B}$, is assumed to experience identical and independently distributed (i.i.d.) quasi-static Rayleigh flat fading $h_{\mathcal{AB}}$ which is time-invariant over the whole transmission of a data packet and vary independently in the next data packet. The instantaneous and average signal-to-noise ratio (SNR) of the link $\mathcal{A} \to \mathcal{B}$ are denoted by $\gamma_{\mathcal{AB}}$ and $\bar{\gamma}_{\mathcal{AB}}$, respectively. The probability density function (pdf) and cumulative density function (cdf) of a random variable X are denoted by $f_X(\cdot)$ and $F_X(\cdot)$, respectively.

III. SPMF Scheme

In this section, we introduce the data transmission, decoding and encryption process in a general MF scheme, i.e. SPMF scheme, for enhancing the security of a two-hop CWN.

In the first time slot, $\mathcal{S}$ transmits a data packet $\mathbf{x}$ to both $\mathcal{R}$ and $\mathcal{D}$. Over the eavesdropper channel, $\mathcal{E}$ also receives the data packet from $\mathcal{S}$. The received signal at node $\mathcal{X}$, $\mathcal{X} \in \{\mathcal{R}, \mathcal{D}, \mathcal{E}\}$, is given by

$$\mathbf{r}_{\mathcal{X}}^{(1)} = \sqrt{\Lambda_{\mathcal{S}}} h_{\mathcal{SX}} \mathbf{x} + \mathbf{n}_{\mathcal{X}}^{(1)}, \tag{1}$$

where $\Lambda_{\mathcal{S}}$ is the power of the source $\mathcal{S}$ and $\mathbf{n}_{\mathcal{X}}^{(1)}$ is an independent circularly symmetric complex Gaussian (CSCG) noise vector at node $\mathcal{X}$ with each entry having zero mean and variance of σ_0^2. Then, $\mathcal{X}$ decodes the data from $\mathcal{S}$, which is denoted by $\bar{\mathbf{x}}_{\mathcal{X}}^{(1)}$.

In the second time slot, after decoding the data packet received from $\mathcal{S}$, the relay node $\mathcal{R}$ linearly combines the decoded data, i.e. $\bar{\mathbf{x}}_{\mathcal{R}}^{(1)}$, with the encrypted key (denoted by $\mathbf{k}$) using the PNC approach as follows:

$$\mathbf{x}_{\mathcal{R}}^{(2)} = \alpha \bar{\mathbf{x}}_{\mathcal{R}}^{(1)} + \beta \mathbf{k}, \tag{2}$$

where α and β are random PNC coefficients satisfying $\alpha^2 + \beta^2 = 1$.

Through the second hop, $\mathcal{D}$ is expected to receive the data from $\mathcal{R}$; however, $\mathcal{E}$ could overhear the same information. The received signal at node $\mathcal{Y}$, $\mathcal{Y} \in \{\mathcal{D}, \mathcal{E}\}$, is given by

$$\mathbf{r}_{\mathcal{Y}}^{(2)} = \sqrt{\Lambda_{\mathcal{R}}} h_{\mathcal{RY}} \mathbf{x}_{\mathcal{R}}^{(2)} + \mathbf{n}_{\mathcal{Y}}^{(2)}, \tag{3}$$

where $\Lambda_{\mathcal{R}}$ is the power of the relay $\mathcal{R}$ and $\mathbf{n}_{\mathcal{Y}}^{(2)}$ is a CSCG noise vector at node $\mathcal{Y}$ with each entry having zero mean and variance of σ_0^2. Substituting (2) into (3), we obtain

$$\mathbf{r}_{\mathcal{Y}}^{(2)} = \sqrt{\Lambda_{\mathcal{R}}} h_{\mathcal{RY}} \alpha \bar{\mathbf{x}}_{\mathcal{R}}^{(1)} + \sqrt{\Lambda_{\mathcal{R}}} h_{\mathcal{RY}} \beta \mathbf{k} + \mathbf{n}_{\mathcal{Y}}^{(2)}. \tag{4}$$

As the PNC coefficients and encrypted key are unknown to the eavesdropper, it is assumed that $\mathcal{E}$ does not attempt to decode the data overheard in the second time slot, but only decodes the data in the first time slot as $\bar{\mathbf{x}}_{\mathcal{E}}^{(1)}$. Meanwhile, $\mathcal{D}$ is able to decode the data in both time slots as $\bar{\mathbf{x}}_{\mathcal{D}}^{(1)}$ and $\bar{\mathbf{x}}_{\mathcal{D}}^{(2)}$ if the information of α, β and $\mathbf{k}$ is perfectly shared between $\mathcal{R}$ and $\mathcal{D}$. In the case of imperfectly shared information at $\mathcal{D}$, maximum likelihood detection can be used given the known channel statistics of the link $\mathcal{R} \to \mathcal{D}$.

IV. Secrecy Outage Probability Analysis

In this section, we derive the SOP of the SPMF scheme for CWN.[1] The SOP of the DT scheme and the MF scheme are also provided for comparison. The SOP is defined as the probability that the wireless system fails to achieve a target secrecy rate [4], i.e.

$$P_{out} \triangleq \Pr\{C_s < R_s\}, \tag{5}$$

where $R_s > 0$ is the target secrecy rate and C_s is the instantaneous secrecy capacity. Here, C_s can be computed by

$$C_s = \max\{C_d - C_e, 0\}, \tag{6}$$

where C_d and C_e are the instantaneous channel capacity of the data links to $\mathcal{D}$ and the eavesdropping links to $\mathcal{E}$, respectively.

A. SPMF Scheme

Following the same approach as in [7], the maximum rate for reliable communications of relaying link $\mathcal{S} \to \mathcal{R} \to \mathcal{D}$ can be expressed by

$$C_d = \min\left\{\frac{1}{2}\log_2(1+\gamma_{\mathcal{SR}}), \frac{1}{2}\log_2(1+\gamma_{\mathcal{SD}} + \gamma'_{\mathcal{RD}})\right\}, \tag{7}$$

where $\gamma_{\mathcal{SR}}$ and $\gamma_{\mathcal{SD}}$ denote the instantaneous SNR of the link $\mathcal{S} \to \mathcal{R}$ and $\mathcal{S} \to \mathcal{D}$, respectively, in the first time slot, and $\gamma'_{\mathcal{RD}}$ denotes the instantaneous signal-to-interference-plus-noise ratio (SINR) of the link $\mathcal{R} \to \mathcal{D}$ in the second time slot. Here, the instantaneous SNR $\gamma_{\mathcal{SR}}$ and $\gamma_{\mathcal{SD}}$ can be computed from (1) as

$$\gamma_{\mathcal{SR}} = \frac{\Lambda_{\mathcal{S}} |h_{\mathcal{SR}}|^2}{\sigma_0^2}, \tag{8}$$

[1] It is noted that only simulation results were shown in [7] due to page constraint, while in this paper, detailed analysis is provided to verify the effectiveness of the SPMF scheme as well as motivating us to propose an opportunistic relaying protocol in Section V.

$$\gamma_{\mathcal{SD}} = \frac{\Lambda_{\mathcal{S}}|h_{\mathcal{SD}}|^2}{\sigma_0^2}. \tag{9}$$

In the second time slot, $\mathcal{D}$ receives the combined data from $\mathcal{R}$ consisting of both the interested information and encrypted key. From (4), $\gamma'_{\mathcal{RD}}$ can be determined by

$$\gamma'_{\mathcal{RD}} = \frac{\Lambda_{\mathcal{R}}|h_{\mathcal{RD}}|^2\alpha^2}{\Lambda_{\mathcal{R}}|h_{\mathcal{RD}}|^2\beta^2 + \sigma_0^2}. \tag{10}$$

Over the eavesdropper channel, the maximum rate for reliable eavesdropping at $\mathcal{E}$ is given by

$$C_e = \frac{1}{2}\log_2(1+\gamma_{\mathcal{SE}}), \tag{11}$$

where $\gamma_{\mathcal{SE}}$ is given by

$$\gamma_{\mathcal{SE}} = \frac{\Lambda_{\mathcal{S}}|h_{\mathcal{SE}}|^2}{\sigma_0^2}. \tag{12}$$

Substituting (7) and (11) into (6) and (5), we have

$$\begin{aligned} P_{out}^{(SPMF)} = &\Pr\{\max\{\log_2(1+\min\{\gamma_{\mathcal{SR}},\gamma_{\mathcal{SD}}+\gamma'_{\mathcal{RD}}\}) \\ &-\log_2(1+\gamma_{\mathcal{SE}}),0\} < 2R_s\}. \end{aligned} \tag{13}$$

In order to derive (13), let us firstly find the pdf of $\gamma_{\mathcal{SR}}$, $\gamma_{\mathcal{SD}}$, $\gamma'_{\mathcal{RD}}$ and $\gamma_{\mathcal{SE}}$ (see (8), (9), (10) and (12)). Since the links between nodes are assumed to be experienced Rayleigh flat fading, the pdf of the SNR $\gamma_{\mathcal{AB}}$, $\mathcal{AB} \in \{\mathcal{SR},\mathcal{SD},\mathcal{SE}\}$ is given by [9]

$$f_{\gamma_{\mathcal{AB}}}(\gamma_{\mathcal{AB}}) = \frac{1}{\bar{\gamma}_{\mathcal{AB}}}\exp\left(-\frac{\gamma_{\mathcal{AB}}}{\bar{\gamma}_{\mathcal{AB}}}\right), \tag{14}$$

while the pdf of the SINR $\gamma'_{\mathcal{RD}}$ can be obtained using the following Lemma 1.

Lemma 1. *If $X = c|Z|^2$, where c is a positive constant, Z is a zero-mean complex Gaussian random variable with variance of 1, and $Y = \frac{a^2X}{b^2X+1}$, where $a^2+b^2=1$ and $a \geqslant b \geqslant 0$, then the pdf of Y is given by*

$$f_Y(y) = \frac{a^2}{c(a^2-b^2y)^2}\exp\left[-\frac{y}{c(a^2-b^2y)}\right]. \tag{15}$$

Proof. See Appendix A. □

From Lemma 1, the pdf of $\gamma'_{\mathcal{RD}}$ can be expressed by

$$f_{\gamma'_{\mathcal{RD}}}(\gamma_{\mathcal{RD}}) = \frac{\alpha^2}{\bar{\gamma}_{\mathcal{RD}}(\alpha^2-\beta^2\gamma_{\mathcal{RD}})^2}\exp\left[\frac{-\gamma_{\mathcal{RD}}}{\bar{\gamma}_{\mathcal{RD}}(\alpha^2-\beta^2\gamma_{\mathcal{RD}})}\right]. \tag{16}$$

Remark 1 (*General pdf function of SINR $\gamma'_{\mathcal{RD}}$*)**.** It can be observed that, when $\alpha=1$ and $\beta=0$, (16) is simplified to be the pdf of the SNR of Rayleigh fading channel with no interference (see (14)), i.e.

$$f_{\gamma_{\mathcal{RD}}}(\gamma_{\mathcal{RD}}) = \frac{1}{\bar{\gamma}_{\mathcal{RD}}}\exp\left(-\frac{\gamma_{\mathcal{RD}}}{\bar{\gamma}_{\mathcal{RD}}}\right). \tag{17}$$

This accordingly reflects the novelty of our work in the SOP analysis with respect to the conventional MF scheme in [6], which is a special case of our proposed SPMF.

Further derivation of (13) leads to the following finding:

Theorem 1. *The SOP of the proposed SPMF scheme is obtained by* (18) *(see the top of next page), where*

$$f_X(x) = \frac{1}{\bar{\gamma}_{\mathcal{SR}}}\exp\left(-\frac{x}{\bar{\gamma}_{\mathcal{SR}}}\right), \tag{19}$$

$$f_Y(y) = \frac{1}{\bar{\gamma}_{\mathcal{SD}}}\exp\left(-\frac{y}{\bar{\gamma}_{\mathcal{SD}}}\right), \tag{20}$$

$$f_Z(z) = \frac{\alpha^2}{\bar{\gamma}_{\mathcal{RD}}(\alpha^2-\beta^2z)^2}\exp\left(-\frac{z}{\bar{\gamma}_{\mathcal{RD}}(\alpha^2-\beta^2z)}\right), \tag{21}$$

$$f_W(w) = \frac{1}{\bar{\gamma}_{\mathcal{SE}}}\exp\left(-\frac{w}{\bar{\gamma}_{\mathcal{SE}}}\right). \tag{22}$$

Proof. See Appendix B. □

B. DT Scheme

In DT scheme, the relay is assumed to be unavailable and thus, for fair comparison, $\mathcal{S}$ sends the encoded data to $\mathcal{D}$ using the power of $2\Lambda_{\mathcal{S}}$. The SOP of the DT is given by [8]

$$P_{out}^{(DT)} = 1 - \frac{\bar{\gamma}_{\mathcal{SD}}}{\bar{\gamma}_{\mathcal{SD}} + 2^{R_s}\bar{\gamma}_{\mathcal{SE}}}\exp\left(\frac{1-2^{R_s}}{2\bar{\gamma}_{\mathcal{SD}}}\right). \tag{23}$$

C. MF Scheme

In MF scheme, $\mathcal{R}$ decodes the source message and then forwards the modified message to $\mathcal{D}$ [6]. As the message difference is assumed to be perfectly shared between $\mathcal{R}$ and $\mathcal{D}$, $\mathcal{D}$ can decode the message while $\mathcal{E}$ cannot. The MF scheme is a special case of the SPMF scheme when $\alpha=1$ and $\beta=0$, and thus the SOP of the MF scheme, i.e. $P_{out}^{(MF-perfect)}$, can be computed by (24) as in the following Lemma 2.

Lemma 2. *For the special case $\alpha=1$ and $\beta=0$, the SOP of the SPMF scheme is given by*

$$P_{out}^{(SPMF)} = P_{out}^{(MF-perfect)} = 1 - \frac{\Phi(\bar{\gamma}_{\mathcal{RD}}) - \Phi(\bar{\gamma}_{\mathcal{SD}})}{\bar{\gamma}_{\mathcal{RD}} - \bar{\gamma}_{\mathcal{SD}}}, \tag{24}$$

where

$$\begin{aligned} \Phi(x) \triangleq &\left(1+\frac{x}{\bar{\gamma}_{\mathcal{SR}}}\right)e^{(1-2^{2R_s})(\bar{\gamma}_{\mathcal{SR}}^{-1}+x^{-1})} \\ &\times\left(\frac{1}{\bar{\gamma}_{\mathcal{SR}}^{-1}+x^{-1}} - \frac{1}{2^{-2R_s}\bar{\gamma}_{\mathcal{SE}}^{-1}+\bar{\gamma}_{\mathcal{SR}}^{-1}+x^{-1}}\right). \end{aligned} \tag{25}$$

Proof. The proof can be obtained from (18) where the pdf of $\gamma_{\mathcal{RD}}$ in (21) is replaced by (17). □

Remark 2 (*SOP of MF Scheme with Imperfect Knowledge of Shared Information*)**.** In the MF-imperfect scheme,[2] the PNC-based modification process at $\mathcal{R}$, i.e. α and β, are not known at $\mathcal{D}$. In this case, $\mathcal{D}$ simply supposes that $\alpha=\beta=1/\sqrt{2}$. The SOP of the MF-imperfect scheme is therefore given by

$$\begin{aligned} P_{out}^{(MF-imperfect)} = &\Pr\{\max\{\min\{\frac{1}{2}\log_2(1+\gamma_{\mathcal{SR}}), \\ &\frac{1}{2}\log_2(1+\gamma_{\mathcal{SD}}+\gamma''_{\mathcal{RD}})\} - \frac{1}{2}\log_2(1+\gamma_{\mathcal{SE}}),0\} < R_s\}, \end{aligned} \tag{26}$$

where $\gamma''_{\mathcal{RD}}$ is determined by (10) when $\alpha=\beta=1/\sqrt{2}$, i.e.

$$\gamma''_{\mathcal{RD}} = \frac{\Lambda_{\mathcal{R}}|h_{\mathcal{RD}}|^2/2}{\Lambda_{\mathcal{R}}|h_{\mathcal{RD}}|^2/2+\sigma_0^2}. \tag{27}$$

Accordingly, $P_{out}^{(MF-imperfect)}$ can be obtained as in Theorem 1 using (18) with $\alpha=\beta=1/\sqrt{2}$.

[2] For brevity, the MF schemes with perfect and imperfect knowledge of shared information are denoted as MF-perfect and MF-imperfect, respectively.

$$
\begin{aligned}
P_{out}^{(SPMF)} = & \int_0^{2^{2R_s}-1} f_X(x) \int_0^x f_Y(y) \int_{x-y}^{\infty} f_Z(z) dz dy dx \\
& + \int_{2^{2R_s}-1}^{\infty} f_X(x) \int_{2^{-2R_s}(1+x)-1}^{x} f_W(w) \int_0^x f_Y(y) \int_{x-y}^{\infty} f_Z(z) dzdydwdx \\
& + \int_0^{2^{2R_s}-1} f_Y(y) \int_0^{2^{2R_s}-1-y} f_Z(z) \int_{y+z}^{\infty} f_X(x) dxdzdy \\
& + \int_0^{2^{2R_s}-1} f_Y(y) \int_{2^{2R_s}-1-y}^{\infty} f_Z(z) \int_{2^{-2R_s}(1+y+z)-1}^{\infty} f_W(w) \int_{y+z}^{\infty} f_X(x) dxdwdzdy \qquad (18)
\end{aligned}
$$

V. Opportunistic Secure MF Protocol for CWNs

Intuitively, the usage of relay may be unnecessary unless the link between source and relay and the link between relay and destination do not suffer from severe fading and noise. This accordingly raises a research problem to find out when the relay should be used to provide a higher secure communication over the DT scheme. Inspired by that fact, we introduce the following optimisation problem

$$\min_{X \in \{DT, MF, SPMF\}} P_{out}^{(X)}. \qquad (28)$$

The optimisation problem in (28) aims at finding an optimal scheme among DT, MF and SPMF schemes that achieves the lowest SOP.

As shown later in the numerical results, there exists a crossing point between the SOP of DT scheme and that of RT scheme. Therefore, in order to solve (28), it is necessary to find the conditions of the crossing point between SOP curves of the DT and RT schemes. Let us first introduce the following proposition:

Proposition 1. *Given two non-negative increasing functions $f(x)$ and $g(x)$ with $\frac{df(x)}{dx} > \frac{dg(x)}{dx} > 0$, then $\exists! x' > 0 : f(x') = g(x')$ iff $f(0) < g(0)$.*

Proof. See Appendix C. □

Proposition 1 is helpful in determining the existence of the crossing points between various SOP curves as in the following Theorem 2. For simplicity in the analysis, let us consider DT and MF-perfect scheme.

Theorem 2. *On the subject of target secrecy rate, i.e. R_s, if $\bar{\gamma}_{\mathcal{SD}}\bar{\gamma}_{\mathcal{SE}} < \bar{\gamma}_{\mathcal{SR}}^2$, $\bar{\gamma}_{\mathcal{SD}} < \sqrt{\bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{SE}}/2}$ and $\bar{\gamma}_{\mathcal{SD}} < \sqrt{\bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{RD}}/2}$, then there exists a single crossing point of two SOP curves for the DT and RT schemes. That is $\exists! R_s' > 0 : P_{out}^{(DT)}(R_s') = P_{out}^{(RT)}(R_s')$*

Proof. See Appendix D. □

For convenience, let Ω_{cross} denote the set of conditions for the crossover of DT and RT schemes in Theorem 2, i.e.

$$
\begin{aligned}
\Omega_{cross} = \{ & \bar{\gamma}_{\mathcal{SD}}\bar{\gamma}_{\mathcal{SE}} < \bar{\gamma}_{\mathcal{SR}}^2 \wedge \bar{\gamma}_{\mathcal{SD}} < \sqrt{\bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{SE}}/2} \\
& \wedge \bar{\gamma}_{\mathcal{SD}} < \sqrt{\bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{RD}}/2} \}.
\end{aligned} \qquad (29)
$$

We have the following observation:

Remark 3 (*Existence of a Secrecy Rate Threshold (SRT) for Opportunistic Secure RT Protocol*)**.** From Theorem 2, if the channel quality satisfies the condition set Ω_{cross} in (29), then there exists a SRT, i.e. R_{th}, which is the crossing point between the SOPs of DT and RT schemes. Specifically, it can be deduced that

$$
\begin{cases}
P_{out}^{(DT)}(R_s) > P_{out}^{(RT)}(R_s) & \text{if } R_s < R_{th} \\
P_{out}^{(DT)}(R_s) \leq P_{out}^{(RT)}(R_s) & \text{if } R_s \geq R_{th}
\end{cases} \qquad (30)
$$

This accordingly means that we should select the RT scheme for a lower SOP if the target secrecy rate is smaller than the SRT, while the DT scheme is preferable to achieve a higher target secrecy rate. Also, notice that if the SRT does not exist, i.e. the condition set Ω_{cross} is not satisfied, then the DT scheme should be selected as $P_{out}^{(DT)}(R_s) < P_{out}^{(RT)}(R_s)$.

Therefore, given Ω_{cross}, solving the optimisation problem (28) is turned into finding SRT between DT and RT schemes, i.e.

$$R_{th} = R_s | P_{out}^{(DT)}(R_s) = P_{out}^{(RT)}(R_s). \qquad (31)$$

Using the derived SOPs of various schemes in Section IV, R_{th} can be found via a simple numerical method and the optimal scheme can be opportunistically determined as in Remark 3.

VI. Numerical Results

In this section, we first show the SOP achieved with various schemes in CWN to verify the analytical findings in Section IV. We then present the findings of SRTs for determining the opportunistic secure communication protocol under different scenarios of wireless channel link quality. The results are obtained with MATLAB under different scenarios of the wireless channel quality and the target secrecy rate.

A. SOP of DT & RT Schemes

Figure 2 plots the SOP of various schemes as a function of the target secrecy rate, i.e. R_s. Four schemes are considered for comparison, including DT [8], MF-perfect [6], MF-imperfect and our proposed SPMF. The SNRs of all links are set as $\bar{\gamma}_{\mathcal{SR}} = 20$ dB, $\bar{\gamma}_{\mathcal{RD}} = 20$ dB, $\bar{\gamma}_{\mathcal{SD}} = 10$ dB, $\bar{\gamma}_{\mathcal{RE}} = 15$ dB and $\bar{\gamma}_{\mathcal{SE}} = 5$ dB. The PNC coefficients are arbitrarily set as $\alpha = 3\beta$. In Fig. 2, as noticed in the proof of Theorem 2, it can be seen that the SOP increases with R_s and the gradient of the SOP of the RT schemes is higher than that of the DT scheme. The SPMF scheme is shown to achieve an

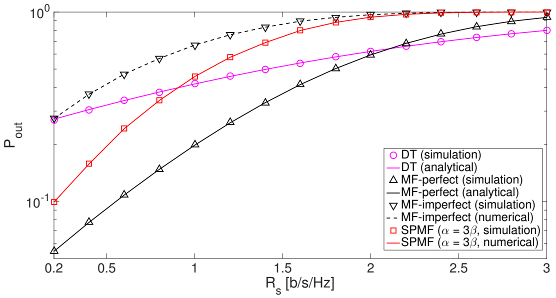

Fig. 2: SOP versus target secrecy rate.

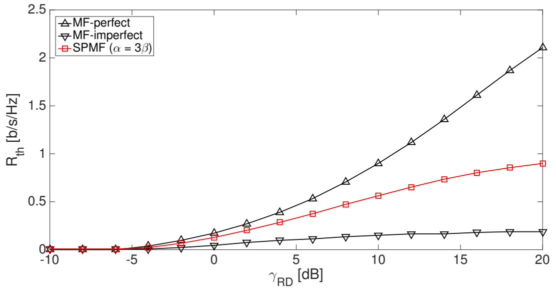

Fig. 4: SRT of various RT schemes versus $\bar{\gamma}_{\mathcal{RD}}$.

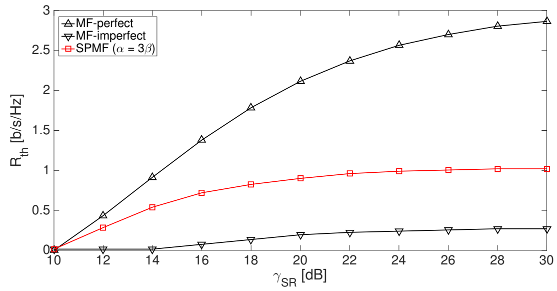

Fig. 3: SRT of various RT schemes versus $\bar{\gamma}_{\mathcal{SR}}$.

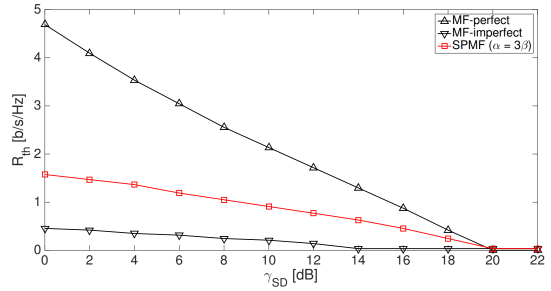

Fig. 5: SRT of various RT schemes versus $\bar{\gamma}_{\mathcal{SD}}$.

improved SOP performance than the MF-imperfect scheme, while the DT scheme achieves a better performance at high R_s, i.e. when $R_s > 0.9$ b/s/Hz. This accordingly verifies the statement in Remark 3 regarding the existence of the SRTs. Additionally, the numerical and analytical results in Section IV are shown to be consistent with the simulation results.

B. Impacts of Source-Relay Link on SRT

Considering the impact of the link $\mathcal{S} \to \mathcal{R}$ on determining SRT for opportunistic secure communication protocol, Fig. 3 plots the SRT, i.e. R_{th}, of three RT schemes, including MF-perfect, MF-imperfect and SPMF, as a function of the average SNR of the link $\mathcal{S} \to \mathcal{R}$, i.e. $\bar{\gamma}_{\mathcal{SR}}$. The range of $\bar{\gamma}_{\mathcal{SR}}$ is assumed to be from 10 to 30 dB. The SNRs of other channel links are set as $\bar{\gamma}_{\mathcal{SD}} = 10$ dB, $\bar{\gamma}_{\mathcal{RD}} = 20$ dB, $\bar{\gamma}_{\mathcal{SE}} = 5$ dB and $\bar{\gamma}_{\mathcal{RE}} = 15$ dB. It can be observed in Fig. 3 that $R_{th} = 0$ when $\bar{\gamma}_{\mathcal{SR}} \leq 10$ dB. In fact, when $\bar{\gamma}_{\mathcal{SR}}$ is too low, the condition set in Theorem 2, i.e. Ω_{cross} in (29), is not satisfied, and thus there do not exist any crossing points between the SOP curves of the DT scheme and other schemes. This accordingly means that the DT scheme is optimal in the low-SNR regime of the link $\mathcal{S} \to \mathcal{R}$ (see Remark 3). It can also be observed in Fig. 3 that R_{th} increases as $\bar{\gamma}_{\mathcal{SR}}$ increases.

C. Impact of Relay-Destination Link on SRT

The impact of the link $\mathcal{R} \to \mathcal{D}$ on SRT is shown in Fig. 4 where R_{th} of three RT schemes, including MF-perfect, MF-imperfect and SPMF, is plotted versus $\bar{\gamma}_{\mathcal{RD}}$. The range of $\bar{\gamma}_{\mathcal{RD}}$ is assumed to be from 10 to 20 dB, while the SNRs of other channel links are set as $\bar{\gamma}_{\mathcal{SR}} = 20$ dB, $\bar{\gamma}_{\mathcal{SD}} = 10$ dB, $\bar{\gamma}_{\mathcal{SE}} = 5$ dB and $\bar{\gamma}_{\mathcal{RE}} = 15$ dB. It can be observed in Fig. 4 that $R_{th} = 0$ as $\bar{\gamma}_{\mathcal{RD}} \leq -6$ dB and R_{th} increases with $\bar{\gamma}_{\mathcal{RD}}$. Similar to Fig. 3, this confirms the existence of SRTs at certain range of the SNR of the link $\mathcal{R} \to \mathcal{D}$ satisfying the condition set Ω_{cross} (see (29)) as noted in Theorem 2 and Remark 3, while the DT scheme is beneficial in the low-SNR regime of relaying links.

D. Impact of Source-Destination Link on SRT

Taking into account the direct link $\mathcal{S} \to \mathcal{D}$, Fig. 5 plots R_{th} of various RT schemes as a function of $\bar{\gamma}_{\mathcal{SD}}$. The range of $\bar{\gamma}_{\mathcal{SD}}$ is assumed to vary from 0 to 22 dB to represent various scenarios of the direct link. The SNRs of other channel links are set as $\bar{\gamma}_{\mathcal{SR}} = 20$ dB, $\bar{\gamma}_{\mathcal{RD}} = 20$ dB, $\bar{\gamma}_{\mathcal{SE}} = 5$ dB and $\bar{\gamma}_{\mathcal{RE}} = 15$ dB. Different from Figs. 3 and 4, it can be observed in Fig. 5 that the increase of $\bar{\gamma}_{\mathcal{SD}}$ results in a lower R_{th} and such decrease approaches 0 as $\bar{\gamma}_{\mathcal{SD}} \geq 20$ dB. In fact, it can be intuitively seen that, if the direct link is of high quality, then the DT scheme is more beneficial than the RT schemes with a lower SOP. This accordingly results in the decrease of R_{th}. Especially, when $\bar{\gamma}_{\mathcal{SD}} \geq 20$ dB, the condition set Ω_{cross} is not satisfied, and hence, as noticed in Remark 3, the DT scheme is optimal in the high-SNR regime of the direct link.

VII. Conclusions

In this paper, we have derived the SOP of SPMF scheme in CWN. The derived expression is a general form of both the SPMF and the conventional MF scheme either with or without knowledge of shared information between relay and destination. The SPMF scheme is shown to provide higher security compared to the MF scheme with imperfect knowledge of shared information, while a better performance is achieved with the DT scheme at high target secrecy rate. Furthermore, we have proposed an opportunistic secure MF protocol by finding the SRTs for determining the optimal scheme with or without the assistance of the relay. Depending on the quality of channel links, the conditions for the existence of the SRTs have been derived. It is shown that the SRTs increase as the

SNR of either source-relay or relay-destination link increases, while the increase of the SNR of source-destination link results in lower SRTs.

Appendix A
Proof of Lemma 1

Given $a^2 + b^2 = 1$ and $a \geqslant b \geqslant 0$, the cdf of Y can be computed by

$$F_Y(y) = \Pr\{Y \leqslant y\} = \Pr\left\{X \leqslant \frac{y}{a^2 - b^2 y}\right\} \tag{32}$$

Note that the cdf of X is given by

$$F_X(x) = 1 - \exp\left(-\frac{x}{c}\right), \tag{33}$$

From (32) and (33), we have

$$F_Y(y) = F_X\left(\frac{y}{a^2 - b^2 y}\right) = 1 - \exp\left(-\frac{y}{c(a^2 - b^2 y)}\right) \tag{34}$$

Taking differentiation of (34) w.r.t y, we can obtain (15).

Appendix B
Proof of Theorem 1

For brevity, let $X = \gamma_{\mathcal{SR}}$, $Y = \gamma_{\mathcal{SD}}$, $Z = \gamma_{\mathcal{RD}}$ and $W = \gamma_{\mathcal{SE}}$. We can rewrite (13) as

$$\begin{aligned} P_{out}^{(SPMF)} = \Pr\{\max\{&\log_2(1 + \min\{X, Y + Z\}) \\ &- \log_2(1 + W), 0\} < 2R_s\}. \end{aligned} \tag{35}$$

It can be seen that $P_{out}^{(SPMF)} = 1$ if $W \geqslant \min\{X, Y + Z\}$. However, such scenario is counter-intuitive in our considered system model aiming at providing secured communications. Therefore, let us analyse $P_{out}^{(SPMF)}$ for the scenario $W \leqslant \min\{X, Y + Z\}$. From (35), we have

$$P_{out}^{(SPMF)} = P_1 + P_2, \tag{36}$$

where

$$P_1 \triangleq \Pr\{2^{-2R_s}(1 + X) - 1 < W\} \Pr\{X \leqslant Y + Z\}, \tag{37}$$

$$P_2 \triangleq \Pr\{2^{-2R_s}(1 + Y + Z) - 1 < W\} \Pr\{X > Y + Z\}. \tag{38}$$

It can be observed that, if $X \leqslant \min\{Y, 2^{2R_s} - 1\}$, then $\Pr\{2^{-2R_s}(1 + X) - 1 < W\} = 1$ and $\Pr\{X \leqslant Y + Z\} = 1$ since $W \geqslant 0$ and $Z \geqslant 0$. Also, if $Y + Z \leqslant \min\{X, 2^{2R_s} - 1\}$, then $\Pr\{2^{-2R_s}(1 + Y + Z) - 1 < W\} = 1$ and $\Pr\{X > Y + Z\} = 1$ since $W \geqslant 0$. Deriving P_1 and P_2, we can obtain (18). The Theorem is proved.

Appendix C
Proof of Proposition 1

From $\frac{df(x)}{dx} > \frac{dg(x)}{dx} > 0$, there exist $x_1 > 0$ and $x_2 > 0$:

$$\frac{f(x_1) - f(0)}{x_1} > \frac{g(x_2) - g(0)}{x_2}. \tag{39}$$

If $f(0) < g(0)$, then there exists a crossing point $x' = x_1 = x_2 > 0$ such that $f(x') = g(x')$ and thus $(f(x') - f(0))/x' > (g(x') - g(0))/x'$ satisfying (39). Conversely, if there exists a crossing point $x' = x_1 = x_2 > 0$ satisfying (39), then we can easily deduce that $f(0) < g(0)$.

Proof of uniqueness: Let us assume that there exists $0 < x'' \neq x'$ satisfying $f(x'') = g(x'')$ and $f(x') = g(x')$. We can easily see that it contradicts the fact that $\dfrac{df(x)}{dx} > \dfrac{dg(x)}{dx}$. Therefore, $\exists! x' > 0 : f(x') = g(x')$ if and only if $f(0) < g(0)$.

Appendix D
Proof of Theorem 2

As $R_s \to 0$, from (23) we have

$$P_{out}^{(DT)} \to \frac{\bar{\gamma}_{\mathcal{SE}}}{\bar{\gamma}_{\mathcal{SD}} + \bar{\gamma}_{\mathcal{SE}}} \triangleq P_0^{(DT)}. \tag{40}$$

In the RT protocol, as $R_s \to 0$, $\Phi(x)$ in (25) approaches

$$\Phi(x) \to \frac{x^2 \bar{\gamma}_{\mathcal{SR}}}{x\bar{\gamma}_{\mathcal{SR}} + x\bar{\gamma}_{\mathcal{SE}} + \bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{SE}}}. \tag{41}$$

Substituting (41) into (24), we can easily obtain $P_0^{(RT)}$ as $R_s \to 0$. Denote $\Delta = P_0^{(RT)} - P_0^{(DT)}$. Solving $\Delta < 0$, after some mathematical manipulations, we have

$$\begin{aligned} &\Delta < 0 \Leftrightarrow \bar{\gamma}_{\mathcal{SR}}[\bar{\gamma}_{\mathcal{RD}}(\bar{\gamma}_{\mathcal{SD}}^2 - \bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{SE}}/2) + \bar{\gamma}_{\mathcal{SE}} \\ &\times(\bar{\gamma}_{\mathcal{SD}}^2 - \bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{RD}}/2)] + \bar{\gamma}_{\mathcal{SD}}\bar{\gamma}_{\mathcal{RD}}(\bar{\gamma}_{\mathcal{SD}}\bar{\gamma}_{\mathcal{SE}} - \bar{\gamma}_{\mathcal{SR}}^2) < 0. \end{aligned} \tag{42}$$

It can be seen that, if $\bar{\gamma}_{\mathcal{SD}}\bar{\gamma}_{\mathcal{SE}} < \bar{\gamma}_{\mathcal{SR}}^2$, $\bar{\gamma}_{\mathcal{SD}} < \sqrt{\bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{SE}}/2}$ and $\bar{\gamma}_{\mathcal{SD}} < \sqrt{\bar{\gamma}_{\mathcal{SR}}\bar{\gamma}_{\mathcal{RD}}/2}$, then $\Delta < 0$, i.e. $P_0^{(RT)} < P_0^{(DT)}$. Additionally, as in the conventional relaying scheme, the gradient of the SOP performance of the RT scheme is higher than that of the DT scheme and the SOP of both schemes increases as a function of the target secrecy rate, i.e. $\dfrac{dP_{out}^{(RT)}}{dR_s} > \dfrac{dP_{out}^{(DT)}}{dR_s} > 0$. Therefore, from Proposition 1, we can conclude that $\exists! R_s' > 0 : P_{out}^{(DT)}(R_s') = P_{out}^{(RT)}(R_s')$.

Acknowledgement

This work was supported in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22, by the Newton Institutional Link under Grant ID 172719890, by U.K. Engineering and Physical Sciences Research Council under Grant EP/P019374/1, and by Royal Society Research Grant under Grant ID RG160302.

References

[1] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: state of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[2] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[3] T. A. Le, H. X. Nguyen, Q.-T. Vien, and M. Karamanoglu, "Secure information transmission in the presence of energy-harvesting eavesdroppers in multi-cell networks," in *Proc. IEEE GLOBECOM 2015*, Sandiego, CA, USA, Dec. 2015, pp. 1–6.

[4] F. Gabry, R. Thobaben, and M. Skoglund, "Outage performances for amplify-and-forward, decode-and-forward and cooperative jamming strategies for the wiretap channel," in *Proc. IEEE WCNC'11*, Cancun, Mexico, Mar. 2011, pp. 1328–1333.

[5] R. Bassily and S. Ulukus, "Secure communication in multiple relay networks through decode-and-forward strategies," *J. Commun and Netw.*, vol. 14, no. 4, pp. 352–363, Aug. 2012.

[6] S. W. Kim, "Modify-and-forward for securing cooperative relay communications," in *International Zurich Seminar on Communications (IZS)*, Zurich, Switzerland, Feb. 2014, pp. 136–139.

[7] Q.-T. Vien, T. A. Le, H. X. Nguyen, and H. Phan, "A secure network coding based modify-and-forward scheme for cooperative wireless relay networks," in *Proc. IEEE VTC 2016-Spring*, Nanjing, China, May 2016, pp. 1–5.

[8] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT'06*, Seattle, WA, USA, Jul. 2006, pp. 356–360.

[9] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*, 2nd ed. John Wiley & Sons, 2005.