A Secure Network Coding based Modify-and-Forward Scheme for Cooperative Wireless Relay Networks

Quoc-Tuan Vien[†], Tuan Anh Le[†], Huan X. Nguyen[†], Hoc Phan[‡]
[†]School of Science and Technology, Middlesex University, The Burroughs, London NW4 4BT, UK.
Email: {q.vien, t.le, h.nguyen}@mdx.ac.uk.
[‡]School of Systems Engineering, University of Reading, Whiteknights, Reading, Berkshire RG6 6AY, UK.
Email: h.phan@reading.ac.uk.

***Abstract*—This paper investigates the security at the physical layer of cooperative relay communications. Inspired by the principle of physical-layer network coding (PNC), we propose a new secure relaying scheme, namely secure PNC-based modify-and-forward (SPMF). In the proposed scheme, the relay node linearly combines the decoded data from the source node with an encrypted key before conveying the mixed data to the destination node. As both the linear PNC operation and encrypted key at the relay are unknown to the eavesdropper, the SPMF scheme provides a double security level in the system. Particularly, taking into account the practical scenario of the imperfect knowledge shared between the relay and destination, the secrecy outage probability (SOP) of the proposed SPMF scheme is analysed and evaluated in comparison with modify-and-forward, cooperative jamming, decode-and-forward and direct transmission schemes. The proposed scheme is shown to achieve a performance improvement of up to 3 dB when compared to the conventional schemes under imperfect knowledge of shared information between the nodes.**

I. Introduction

Security at the physical layer has recently attracted increasing interests of broader communications societies, especially in the context of cooperative communications [1]. On the other hand, user cooperation has been identified as an innovative change enabling multi-hop communications to not only extend the coverage region but also provide higher spatial diversity gain [2]. The connection between a subscriber and a legitimate transmitter can be realised with the assistance of multiple intermediate nodes (or relay nodes) employing either amplify-and-forward (AF) or decode-and-forward (DF) protocols [3]. Therefore, in order to protect data from vulnerable attacks in wireless communication systems, the security of both the direct and relaying links needs to be considered.

From the physical-layer perspective, an information theoretic approach has been shown to be able to provide secure communications between legitimate users by using jamming signals and appropriate channel coding [1]. A basic approach was originally proposed in [4] for noiseless channel where the data is encrypted by simply XORing with shared secret key. The noisy channel was then investigated in [5] where Wyner first introduced the concept of wiretap channels. It is shown that the innate irregularity and diversity of the message could harm the eavesdropper, and thus strengthen the legitimate communications. Specifically, independent transmitters can help in transmitting jamming signals to improve the secrecy rate of the legitimate users [6], [7]. However, such cooperative jamming (CJ) can cause interferences that reduce the decoding rate at the legitimate receivers [8].

Motivated by the concept of network coding (NC) for improving the throughput of lossless networks [9], [10], secure NC has been proposed in [11], [12] to improve the security of wiretap channels. A vast number of works have investigated the performance of physical-layer NC (PNC) in wireless relay networks (WRNs) (e.g. in [13]–[15]). The principle of the PNC is that the relays perform algebraic linear/logic operations on received packets from multiple transmission source nodes and then forward the combined packets to the destination nodes in the subsequent transmissions.

Considering relaying strategies for secure communications in WRNs, AF-based and DF-based cooperation were investigated in [16], [17]. Recently, a new cooperation scheme, namely modify-and-forward (MF), has been proposed in [18] where the relay first modifies the message received from the source and then forwards the modified message to the destination. As it is assumed that the modification operation at the relay is inherently shared between legitimate users, only the interested destination can recover the original message and thus an improved secrecy outage probability is achieved in comparison with the counterparts using different relaying techniques. However, over the practical wireless medium, the channel dedicated for sharing knowledge between the relay and destination also suffers from fading and background noise, which may cause performance degradation of the MF scheme. To the best of the authors' knowledge, this work is the first attempt to address this practical security issue of the imperfect shared knowledge between the relay and the destination.

In particular, we propose a new secure relaying scheme, namely secure PNC-based MF (SPMF), for a two-hop WRN consisting of a source node, a relay node and a destination node. In the proposed scheme, the relay node first decodes the data received from the source node and then linearly combines the decoded data with the encrypted key following

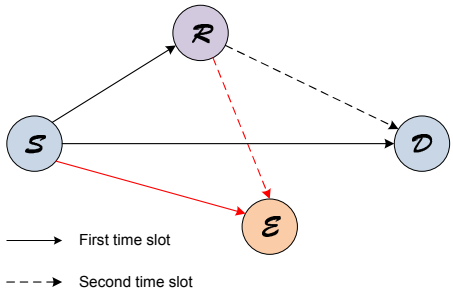

Fig. 1: System model of a two-hop WRN.

the PNC approach before forwarding to the destination node. The novelty of the proposed SPMF scheme lies in the fact that the assumption of perfectly shared information of PNC parameters and encrypted key is relaxed, while only channel statistics are assumed to be known at the destination.

Furthermore, the secrecy outage probability (SOP) is derived to analyse the effectiveness of the proposed SPMF scheme in relation to other conventional schemes, such as direct transmission (DT) [19], DF [16], CJ [6] and MF [18]. It is observed that in the context of imperfect channels for sharing knowledge between the relay and destination nodes, the proposed SPMF achieves an improved SOP for higher security compared to all other schemes.

II. System Model

The system model of a two-hop WRN under investigation is illustrated in Fig. 1. A source node ($\mathcal{S}$) wants to transmit a data packet to a destination node ($\mathcal{D}$) with the assistance of a relay node ($\mathcal{R}$). A half-duplex system is considered where all nodes can either transmit or receive data, but not simultaneously. The data transmission from $\mathcal{S}$ to $\mathcal{D}$ in the two-hop WRN basically consists of two time slots as follows: *i) Time slot 1*: $\mathcal{S}$ transmits data packet to both $\mathcal{R}$ and $\mathcal{D}$ and *ii) Time slot 2*: $\mathcal{R}$ processes the data packet received from $\mathcal{S}$ and then forwards the processed data to $\mathcal{D}$.

Investigating the security issue of the WRN, shown in Fig. 1, we assume that there exists an eavesdropper ($\mathcal{E}$) which is located between $\mathcal{S}$ and $\mathcal{D}$ and in the vicinity of $\mathcal{R}$. Nodes $\mathcal{S}$ and $\mathcal{R}$ transmit data with power Λ_S and Λ_R, respectively. 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.) Rayleigh flat fading $h_{\mathcal{AB}}$ having $E[|h_{\mathcal{AB}}|^2] = 1/d^{\nu}_{\mathcal{AB}}$, where $E[\cdot]$ denotes the statistical expectation function, $d_{\mathcal{AB}}$ denotes the distance between $\mathcal{A}$ and $\mathcal{B}$, and ν denotes the path loss exponent between a pair of transceiver nodes. A block-fading model is considered where all the channel gains are time-invariant over the whole transmission of a data packet and vary independently from data packet to 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.

III. Proposed SPMF Scheme

In this section, we introduce the data transmission, decoding and encryption process in our proposed SPMF scheme for enhancing the security of a two-hop WRN.

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

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

where $\Lambda_{\mathcal{S}}$ is the power of the source $\mathcal{S}$ and $\mathbf{n}^{(1)}_{\mathcal{X}}$ 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 $\bar{\mathbf{x}}^{(1)}_{\mathcal{X}}$.

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. $\bar{\mathbf{x}}^{(1)}_{\mathcal{R}}$) with the encrypted key (denoted by $\mathbf{k}$) using the PNC approach [10]. The signal forwarded from $\mathcal{R}$ is therefore expressed as

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

where α and β are PNC parameters 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 $\mathcal{Y}$, $\mathcal{Y} \in \{\mathcal{D},\mathcal{E}\}$, in the second time slot is given by

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

where $\Lambda_{\mathcal{R}}$ is the power of the relay $\mathcal{R}$ and $\mathbf{n}^{(2)}_{\mathcal{Y}}$ 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

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

As the PNC parameters and encrypted key are assumed to be unknown to the eavesdropper, $\mathcal{E}$ only decodes the data in the first time slot as $\bar{\mathbf{x}}^{(1)}_{\mathcal{E}}$. Meanwhile, $\mathcal{D}$ is able to decode the data in both time slots as $\bar{\mathbf{x}}^{(1)}_{\mathcal{D}}$ and $\bar{\mathbf{x}}^{(2)}_{\mathcal{D}}$ if the information of α, β and $\mathbf{k}$ is perfectly shared between $\mathcal{R}$ and $\mathcal{D}$. In case of imperfectly shared information at $\mathcal{D}$, maximum likelihood detection can be used given the known channel statistics of the link $\mathcal{R} \to \mathcal{D}$.

Remark 1 (*Improved Security with SPMF*)**.** As shown in (4), in order to encrypt the data packet forwarded from the relay node $\mathcal{R}$, two layers of security are integrated into the proposed SPMF scheme including the PNC parameters (i.e. α and β) and the encrypted key (i.e. $\mathbf{k}$). Also, it can be observed that the encrypted key can be treated as interference (or jamming). Therefore, a higher security can be achieved by appropriately controlling these parameters to cope with the imperfect knowledge of the sharing information.

IV. Secrecy Outage Probability Analysis

In this section, we derive the SOP of the proposed SPMF scheme for a WRN. For comparison and completeness of the analysis, we also provide the SOPs of various schemes

for secure communications including DT, DF, CJ and MF schemes. The SOP is defined as the probability that the wireless system fails to achieve a target secrecy rate [16], 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.

We now proceed to derive C_d and C_e of the proposed SPMF scheme.

A. Proposed SPMF Scheme

Following the same approach as in [3] for DF protocol, the maximum rate for reliable communications of relaying link $\mathcal{S} \to \mathcal{R} \to \mathcal{D}$ can be expressed by

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

The instantaneous SNR $\gamma_{\mathcal{SR}}$ and $\gamma_{\mathcal{SD}}$ in the first time slot can be computed, respectively, from (1) as

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

and

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

In the second time slot, $\mathcal{D}$ receives the combined data from $\mathcal{R}$ consisting of both the interested information and encrypted key. In this paper, as the encrypted key and PNC parameters are assumed to be not perfectly known at $\mathcal{D}$, the instantaneous SNR of the link $\mathcal{R} \to \mathcal{D}$ has to be replaced by instantaneous signal-to-interference-plus-noise ratio (SINR). 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, $\mathcal{E}$ can only eavesdrop the data in the first time slot. Therefore, 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), the SOP of the proposed SPMF scheme is obtained as

$$P_{out}^{(SPMF)} = \Pr\left\{\max\left\{\log_2(1+\min\{\gamma_{\mathcal{SR}}, \gamma_{\mathcal{SD}}+\gamma_{\mathcal{RD}}\} - \log_2\{1+\gamma_{\mathcal{SE}}\}, 0\right\} < 2R_s\right\}. \tag{13}$$

It is noted that the derivation of the closed-form expression for the SOP in (13) is challenging when considering the instantaneous SINR term $\gamma_{\mathcal{RD}}$ (see (10)). Due to the page constraint, in this paper, we verify the effectiveness of the proposed SPMF through the numerical results in Section V. The analysis is deferred as an extension to the future work.

Remark 2 (*Relax of Perfect Knowledge Assumption*)**.** From (10), it can be observed that imperfect knowledge of shared information (i.e. encrypted key and PNC parameters) is taken into account in the derivation of $\gamma_{\mathcal{RD}}$ in the proposed SPMF scheme. In the conventional MF scheme [18] with perfectly shared knowledge between $\mathcal{R}$ and $\mathcal{D}$, $\gamma_{\mathcal{RD}}$ is expressed by

$$\gamma_{\mathcal{RD}}^{(MF)} = \frac{\Lambda_{\mathcal{R}}|h_{\mathcal{RD}}|^2}{\sigma_0^2}.$$

Therefore, the MF scheme can be regarded as a special case of the SPMF when $\alpha = 1$ and $\beta = 0$.

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 scheme is derived as in [19], i.e.

$$P_{out}^{(DT)} = 1 - \frac{\bar{\gamma}_{\mathcal{SD}}}{\bar{\gamma}_{\mathcal{SD}} + 2^{R_s}\bar{\gamma}_{\mathcal{SE}}}\exp\left(\frac{1-2^{R_s}}{2\bar{\gamma}_{\mathcal{SD}}}\right). \tag{14}$$

C. DF Scheme

In this scheme, $\mathcal{R}$ follows the conventional DF relaying scheme [3]. That is, $\mathcal{R}$ decodes the data from $\mathcal{S}$, re-encodes the decoded data and then forwards the encoded data to $\mathcal{D}$. According to [16], the SOP of the DF scheme is given by

$$P_{out}^{(DF)} = \frac{2^{-2R_s}\bar{\gamma}_{\mathcal{SR}}\left[\Theta(\bar{\gamma}_{\mathcal{SE}})\Delta(\bar{\gamma}_{\mathcal{SE}}) - \Theta(\bar{\gamma}_{\mathcal{RE}})\Delta(\bar{\gamma}_{\mathcal{RE}})\right]}{(\bar{\gamma}_{\mathcal{RE}} - \bar{\gamma}_{\mathcal{SE}})(\bar{\gamma}_{\mathcal{RD}} - \bar{\gamma}_{\mathcal{SD}})} + \frac{\Theta(\bar{\gamma}_{\mathcal{RE}}) - \Theta(\bar{\gamma}_{\mathcal{SE}})}{\bar{\gamma}_{\mathcal{RE}} - \bar{\gamma}_{\mathcal{SE}}}, \tag{15}$$

where

$$\Theta(x) \triangleq \frac{x^2}{2^{-2R_s}\bar{\gamma}_{\mathcal{SR}} + x}\exp\left(\frac{1-2^{-2R_s}}{x}\right), \tag{16}$$

$$\Delta(x) \triangleq \frac{\bar{\gamma}_{\mathcal{SR}}}{x(1+\bar{\gamma}_{\mathcal{SR}}/\bar{\gamma}_{\mathcal{SD}}) + 2^{-2R_s}\bar{\gamma}_{\mathcal{SR}}} - \frac{\bar{\gamma}_{\mathcal{SR}}}{x(1+\bar{\gamma}_{\mathcal{SR}}/\bar{\gamma}_{\mathcal{RD}}) + 2^{-2R_s}\bar{\gamma}_{\mathcal{SR}}}. \tag{17}$$

D. CJ Scheme

In [6], various CJ schemes were investigated. The principle of the CJ is that different transmitters transmit jamming signals with the aim of harming the illegitimate receiver. In the context of the considered WRN, $\mathcal{R}$ transmits jamming signals while $\mathcal{S}$ transmits the data to $\mathcal{D}$. Due to the autonomous property of the jamming signals, they may confuse $\mathcal{E}$ to eavesdrop the data from $\mathcal{S}$. However, such jamming signals in terms of Gaussian noise could harm both $\mathcal{D}$ and $\mathcal{E}$. Following [6], the SOP of the CJ scheme is computed by

$$P_{out}^{(CJ)} = 1 - \frac{2^{-\delta}}{\bar{\gamma}_{\mathcal{RD}}\zeta} + \frac{2^{-\delta}}{\bar{\gamma}_{\mathcal{RD}}\bar{\gamma}_{\mathcal{RE}}\zeta^2}\left[\frac{2^{2R_s}\bar{\gamma}_{\mathcal{SE}}(\zeta+1)}{\bar{\gamma}_{\mathcal{SD}}} \times \Xi\left(\frac{1+\theta}{\bar{\gamma}_{\mathcal{RE}}}\right) + (\zeta-\theta)\Xi\left(\frac{1+\theta}{\theta}(\delta+\bar{\gamma}_{\mathcal{RD}}^{-1})\right)\right], \tag{18}$$

where $\delta \triangleq (2^{2R_s}-1)\bar{\gamma}_{\mathcal{SD}}^{-1}$, $\theta \triangleq 2^{2R_s}\bar{\gamma}_{\mathcal{SE}}\bar{\gamma}_{\mathcal{SD}}^{-1}$, $\zeta \triangleq \delta + \bar{\gamma}_{\mathcal{RD}}^{-1} - \theta\bar{\gamma}_{\mathcal{RE}}^{-1}$ and $\Xi(x) \triangleq e^x E_1(x)$. Here, $E_1(x) \triangleq \int_x^\infty e^{-t}t^{-1}dt$ is the exponential integral [20].

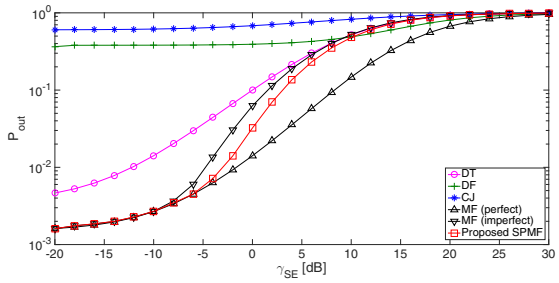

Fig. 2: SOP versus SNR of the link $\mathcal{S} \to \mathcal{E}$.

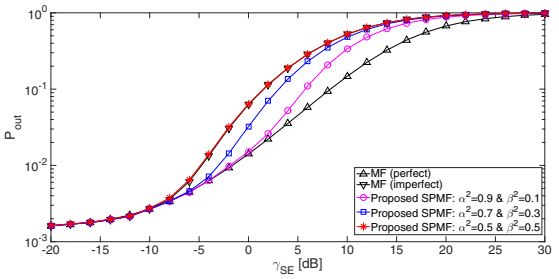

Fig. 3: SOP versus SNR of the link $\mathcal{S} \to \mathcal{E}$ with various PNC parameters.

E. MF Scheme

In MF scheme, $\mathcal{R}$ decodes the source message and then forwards the modified message to $\mathcal{D}$ [18]. 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. As derived in [18], the SOP of the MF scheme is

$$P_{out}^{(MF)} = 1 - \frac{\Phi(\bar{\gamma}_{\mathcal{RD}}) - \Phi(\bar{\gamma}_{\mathcal{SD}})}{\bar{\gamma}_{\mathcal{RD}} - \bar{\gamma}_{\mathcal{SD}}}, \tag{19}$$

where

$$\Phi(x) \triangleq \left(1 + \frac{x}{\bar{\gamma}_{\mathcal{SR}}}\right) e^{(1-2^{2R_s})(\bar{\gamma}_{\mathcal{SR}}^{-1} + x^{-1})} \times \left(\frac{1}{\bar{\gamma}_{\mathcal{SR}}^{-1} + x^{-1}} - \frac{1}{2^{-2R_s}\bar{\gamma}_{\mathcal{SE}}^{-1} + \bar{\gamma}_{\mathcal{SR}}^{-1} + x^{-1}}\right). \tag{20}$$

V. Numerical Results

This section shows the numerical results of the SOP achieved with the proposed SPMF in WRNs. In order to verify the effectiveness of the proposed scheme, the performance of DT [19], DF [16], CJ [6] and MF [18] with either perfect or imperfect knowledge of shared information between the relay and destination are provided for comparison. The results are obtained with MATLAB under different scenarios of the wireless channel quality, PNC parameters and the target secrecy rate.

A. Impacts of Source-Eavesdropper Link

Figure 2 plots the SOP of various schemes for secure WRNs as a function of the average SNR of the link $\mathcal{S} \to \mathcal{E}$ (i.e. $\bar{\gamma}_{\mathcal{SE}}$). The range of $\bar{\gamma}_{\mathcal{SE}}$ is selected to cover -20 to 30 dB to characterise the performance over a wide band of channel quality conditions. The other channel SNRs are arbitrarily set as $\bar{\gamma}_{\mathcal{SR}} = 20$ dB, $\bar{\gamma}_{\mathcal{SD}} = 10$ dB, $\bar{\gamma}_{\mathcal{RD}} = 20$ dB and $\bar{\gamma}_{\mathcal{RE}} = 15$ dB. It is also assumed that the target secrecy rate is $R_s = 0.1$ b/s/Hz and the PNC parameters are $\{\alpha^2 = 0.7, \beta^2 = 0.3\}$. As shown in Fig. 2, a higher $\bar{\gamma}_{\mathcal{SE}}$ causes a higher SOP as the eavesdropper can more reliably decode the source message. It can be observed that the proposed SPMF scheme achieves a lower SOP compared to the DT, DF, CJ and MF (imperfect) schemes at most of the range of $\bar{\gamma}_{\mathcal{SE}}$, while the MF (perfect) scheme can be regarded as a performance benchmark for the scenario of perfectly shared knowledge between $\mathcal{R}$ and $\mathcal{D}$. This accordingly verifies our observation in Remark 1 regarding the improved security with the proposed SPMF scheme.

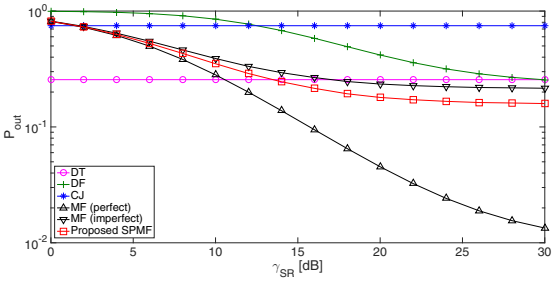

Fig. 4: SOP versus SNR of the link $\mathcal{S} \to \mathcal{R}$.

B. Impacts of PNC Parameters

Investigating the impacts of PNC parameters on the performance of the proposed SPMF, Fig. 3 shows the comparison of SOP between the SPMF and MF schemes against $\bar{\gamma}_{\mathcal{SE}}$ with respect to various $\{\alpha, \beta\}$. The SNRs of the other links and the target secrecy rate are set similar to those in Fig. 2. It can be seen that the proposed SPMF scheme achieves the same performance as the MF (imperfect) scheme when $\alpha^2 = \beta^2 = 0.5$. As α increases, an improved SOP of up to 3 dB is achieved approaching the MF (perfect) scheme. This reflects the generality of the SPMF scheme and also confirms the statement in Remark 2 showing that the MF (perfect) scheme is regarded as a special case with $\{\alpha = 1, \beta = 0\}$.

C. Impacts of Source-Relay Link

In WRNs, the link $\mathcal{S} \to \mathcal{R}$ needs to be considered for reliable relaying. Fig. 4 plots SOP versus $\bar{\gamma}_{\mathcal{SR}}$ with various schemes including DT, DF, CJ, MF (imperfect), MF (perfect) and the proposed SPMF schemes. The SNRs of other channels are set as $\bar{\gamma}_{\mathcal{SD}} = 10$ dB, $\bar{\gamma}_{\mathcal{RD}} = 20$ dB, $\bar{\gamma}_{\mathcal{RE}} = 15$ dB and $\bar{\gamma}_{\mathcal{SE}} = 5$ dB. The target secrecy rate is also set as $R_s = 0.1$ b/s/Hz and the PNC parameters are $\{\alpha^2 = 0.7, \beta^2 = 0.3\}$. It can be observed in Fig. 4 that, a lower SOP is achieved with DF, MF and SPMF schemes at high $\bar{\gamma}_{\mathcal{SR}}$. In fact, the high-quality link $\mathcal{S} \to \mathcal{R}$ provides a reliable relaying, and thus $\mathcal{R}$ can help to enhance the security in WRNs. At low $\bar{\gamma}_{\mathcal{SR}}$ (e.g. $\bar{\gamma}_{\mathcal{SR}} < 10$ dB), $\mathcal{R}$ may not be able to reliably decode the data message from $\mathcal{S}$ and thus the DT scheme is beneficial. Additionally, in Fig. 4, the performance of the DT and CJ schemes is shown to be independent of $\bar{\gamma}_{\mathcal{SR}}$ as there is no relay involved in the DT scheme and the jamming process at

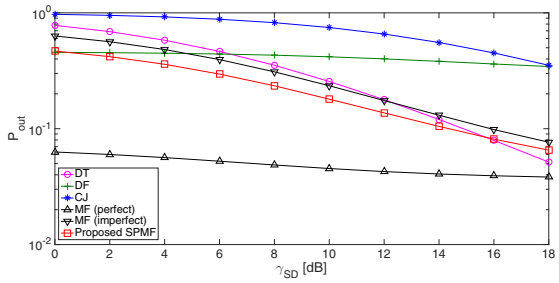

Fig. 5: SOP versus SNR of the link $\mathcal{S} \to \mathcal{D}$.

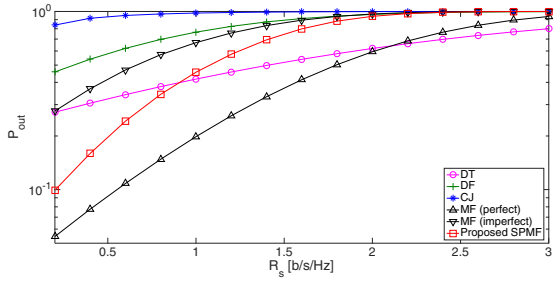

Fig. 6: SOP versus target secrecy rate.

$\mathcal{R}$ in the CJ scheme does not rely on the reliability of the link $\mathcal{S} \to \mathcal{R}$.

D. Impacts of Source-Destination Link

Taking into account the direct link $\mathcal{S} \to \mathcal{D}$ in WRNs, Fig. 5 plots the SOP of various schemes as a function of $\bar{\gamma}_{\mathcal{SD}}$. The SNRs of other links are $\bar{\gamma}_{\mathcal{SR}} = 20$ dB, $\bar{\gamma}_{\mathcal{RD}} = 20$ dB, $\bar{\gamma}_{\mathcal{RE}} = 15$ dB and $\bar{\gamma}_{\mathcal{SE}} = 5$ dB. Similarly, the target secrecy rate and the PNC parameters are $R_s = 0.1$ b/s/Hz and $\{\alpha^2 = 0.7, \beta^2 = 0.3\}$. It can be observed in Fig. 5 that the proposed SPMF scheme achieves a lower SOP than the DF, CJ and MF (imperfect) schemes. The SPMF is shown to be better than DT scheme at low $\bar{\gamma}_{\mathcal{SD}}$ (e.g. $\bar{\gamma}_{\mathcal{SD}} < 16$ dB). However, at high $\bar{\gamma}_{\mathcal{SD}}$, the DT scheme is shown to be the best scheme as the usage of $\mathcal{R}$ is not necessary in this case even may cause performance loss.

E. Impacts of Target Secrecy Rate

Figure 6 shows the SOP of various schemes versus the target secrecy rate (i.e. R_s). 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. It can be seen in Fig. 6 that the SOP increases over R_s. The SPMF scheme is shown to achieve an improved SOP performance than DF, CJ and MF (imperfect) schemes, while the DT scheme achieves a better performance at high R_s (i.e. when $R_s > 0.9$ b/s/Hz). In fact, the relaying schemes rely on the quality of both $\mathcal{S} \to \mathcal{R}$ and $\mathcal{R} \to \mathcal{D}$ links, and thus can only provide an improved security at low R_s.

VI. Conclusions

In this paper, an efficient SPMF scheme has been proposed for secure WRNs to cope with the imperfectly shared knowledge between the relay and destination in the conventional MF scheme. By employing PNC at the relay with encrypted key, the proposed scheme has been shown to provide a higher security compared to the conventional DT, DF, CJ and MF (imperfect) schemes with respect to various channel conditions and target secrecy rates. Although the DT scheme should be more favourable without the need of the relay node when either the SNR of the link $\mathcal{S} \to \mathcal{R}$ is low or that of the link $\mathcal{S} \to \mathcal{D}$ is high, the proposed SPMF has been shown to be more beneficial over various relaying protocols. Specifically, when compared to the conventional MF scheme, the proposed scheme has been shown to achieve an improved SOP performance of up to 3 dB in the practical WRN with imperfect knowledge of shared information between the nodes.

References

[1] 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.

[2] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity - Part I. System description," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927–1938, Nov. 2003.

[3] J. Laneman, D. Tse, and G. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[4] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[5] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[6] J. Vilela, M. Bloch, J. Barros, and S. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

[7] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[8] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[9] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[10] R. Koetter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[11] T. Cui, T. Ho, and J. Kliewer, "On secure network coding with nonuniform or restricted wiretap sets," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 166–176, Jan. 2013.

[12] N. Cai and R. Yeung, "Secure network coding on a wiretap network," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424–435, Jan. 2011.

[13] S. Zhang, S. C. Liew, and P. P. Lam, "Hot topic: Physical-layer network coding," in *Proc. ACM MobiCom'06*, Los Angeles, CA, USA, Sep. 2006, pp. 358–365.

[14] Q.-T. Vien, B. G. Stewart, H. Tianfield, and H. X. Nguyen, "Cooperative retransmission for wireless regenerative multirelay networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 2, pp. 735–747, Feb. 2013.

[15] Q.-T. Vien, H. X. Nguyen, P. Shah, E. Ever, and D. To, "Relay selection for efficient HARQ-IR protocols in relay-assisted multisource multicast networks," in *Proc. IEEE VTC 2014-Spring*, Seoul, Korea, May 2014, pp. 1–5.

[16] 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.

[17] 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.

[18] 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.

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

[20] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Academic Press, 2007.