Razfar *et al. EURASIP Journal on Wireless Communications and Networking* (2017) 2017:6
DOI 10.1186/s13638-016-0788-9

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

On robustness of physical layer network coding to pollution attack

Mojtaba Razfar*, Joel Castro and Ali Abedi

Abstract

Link layer network coding (LLNC) promises to provide high throughput in relay networks through combining packets at the relays and trading communication for computation. The emerging area of physical layer network coding (PLNC) exploits the electromagnetic nature of signals and eliminates the need for addition at the packet level, while making signal design and coding schemes adaptable to the channel conditions. Although network coding has been extensively studied recently, physical layer network coding has not received the attention it deserves. Several recent works introduced the pollution attack at the network layer; however, the network performance at the physical layer with pollution attacks has not been evaluated before. The main challenge with the pollution attack involves propagation of the corrupted packets in an epidemic manner, which degrades performance of the network. As PLNC schemes boost up the network throughput, a thorough study evaluating this superiority to the LLNC scheme in presence of an intruder is necessary. The robustness of both schemes towards an attack have been studied in this article.

Keywords: Physical layer network coding (PLNC), Link layer network coding (LLNC), Pollution attack, Wireless networks, Relay networks

1 Introduction

The main difference between a wireless and a wired network is the fact that the signals can be broadcasted to multiple users simultaneously. In order to improve the four-stage traditional routing [1, 2], network coding has been introduced to attain the maximum possible information flow and to increase the network throughput [3–7]. Inspired by traditional network coding, physical layer network coding (PLNC) has been proposed to improve network throughput, reduce network congestion, and improve network robustness [8, 9]. In wireless networks with limited bandwidth and power resources, PLNC has potential for significant performance improvements. This is done by taking advantage of the inherent additive nature of electromagnetic waves, demonstrating a better performance with respect to the throughput of the network. However, the additive nature of PLNC makes the network susceptible to pollution attacks. Network coding (LLNC) also allows corrupted packets to propagate widely and significantly affect the data recovery procedure. Previous works in network coding security emphasized on the protection of data propagation procedures and the detection of pollution attacks [10–15]. Although these schemes are elegant from the theoretical point of view, they are not efficient with respect to cost and network throughput when used in practice. When detection and elimination methods are used at the network layer, the added complexity and overhead make these higher layer methods inefficient [16]. This calls for a robust coding method that can tolerate intruder attacks without adding too much control overhead to the network. In this paper, the overall network performance from a physical layer perspective has been evaluated for the first time. The goal of this work is to show that the PLNC schemes outperform the LLNC schemes when it comes to an attack. Two cases where the attack power remains low or high are studied.

The pollution attack concept at the network layer has been introduced in [11]. With the advent of the PLNC schemes, pollution attacks may be managed at lower layers. It has been shown that the injected packets can be detected at the physical layer using maximum

*Correspondence: mojtaba.razfar@maine.edu
WiSe-Net Laboratory, Department of Electrical and Computer Engineering, University of Maine, Orono, ME, USA

likelihood (ML) detection [16]. Whenever a relay becomes an intruder with a probability of P, the packet can be restored by removing the faulty information using the method presented in [16, 17]. However, this work has been done at the packet level, while PLNC deals with the data at the physical layer. PLNC is used in [18] to localize the Sybil nodes in wireless networks. Nonetheless, the full effect of the intruder on the network has yet to be investigated. Network coding based on DeNoise-and-Forward (DNF) was introduced in [9] to enhance the conventional wireless network design and to bring real gains in a communication-theoretic sense. Based on this scheme, optimized constellation for a two-way relaying channel has been proposed in which a higher throughput compared to LLNC scheme is promised [19]. Similar results have been reported in [20, 21], where the authors confirm the results of [19], analytically. This method is referred to as Adaptive-DeNoise-and-Forward (ADNF hereafter). For comparison purposes, the Amplify-and-Forward (AF) and ADNF PLNC schemes with a lower and higher complexity at the relay node are selected. More sophisticated schemes such as Compute-and-Forward [22, 23] are not considered in this paper. However, the material introduced in this paper can help the researchers study these schemes as well. To the best of the authors' knowledge, a comprehensive study investigating the effect of the pollution attack on the PLNC scheme has not been carried out before. The goal of this paper is to investigate the effects of the pollution attack on the PLNC schemes (ADNF and AF), compared to the LLNC scheme, and present a fair comparison among them. What motivates the authors is to find out which of the ADNF, AF, or LLNC schemes performs better in the presence of an intruder. This work focuses on the case where the intruder's presence is not known to the network. The comparison is carried out for different attack scenarios. In this work, a detailed analysis of the error probability for the PLNC schemes with an intruder is provided. The three schemes are being thoroughly analyzed and compared. The closed-form error probability approximation of the AF and LLNC schemes with and without an intruder for the case where the users experience a Rician fading and the intruder experiences a Rayleigh fading is derived. This is based on the assumption that the users operate in line of sight, while the intruder attempts to hide and only relies on scattered and non-line-of-sight operation. Note that the derivations for this type of network (Rician-Rayleigh attack) are novel and have not been evaluated before. The channel realization impact has also been studied. That is, the simulation results for the case where the users experience a Rayleigh fading (where there is no LOS present) have been illustrated. To understand the channel realization impact, simulation results for the two cases where the users experience a Rayleigh fading or a Rician fading with high Rician K-factor is presented as well. A lower bound for the ADNF scheme with an intruder is also presented.

The organization of the rest of the paper is as follows. The network model for the LLNC, AF, and ADNF schemes with pollution attack scenario is presented in Section 2. Performance of these three schemes is analyzed in Section 3. Section 4 provides the numerical and simulation results demonstrating the robustness of the PLNC scheme in the presence of pollution attacks. Section 5 presents the discussions and conclusions.

2 Network model

Throughout the paper, certain assumptions and notations are applied. The users transmit their data using a general M-PSK ($\mathrm{M} = 2^k$) modulation with gray mapping regardless of the scheme. It is assumed that the M-PSK constellation has unity energy. $\mathcal{M}$ denotes the constellation mapper, and for QPSK, it is denoted as $\mathcal{M}_{\mathrm{QPSK}}(S_k) = \left\{\frac{1+j}{\sqrt{2}}, \frac{-1+j}{\sqrt{2}}, \frac{1-j}{\sqrt{2}}, \frac{-1-j}{\sqrt{2}}\right\}$. Noise is assumed to be circularly symmetric complex Gaussian random with zero mean and variance of σ^2. S_1, S_2, S_I, and S are the digital source data per symbol from users 1, 2, intruder, and relay, respectively. That is, k-bit binary tuples ($M = 2^k$) in $\mathbb{Z}_M = \{0, 1, \ldots, M-1\}$. $\mathcal{C}$ is the denoising mapper. A quasi-static slow fading with a certain Rician K-factor for users, and Rayleigh fading for the intruder, is assumed. The symbol I resembles the intruder. The transmission power of the users and the relay is assumed to be the same and is denoted as P_S. An identical noise variance at the users and the relay is also assumed, i.e., $\sigma_1^2 = \sigma_2^2 = \sigma_R^2 = \sigma^2$. In the proposed model, the users communicate with the relay with LOS similar to [19], while the intruder is assumed to communicate without LOS. The most appropriate wireless channel model for these two cases are therefore Rician and Rayleigh fading. This is justified noting the fact that intruders often try to keep their locations and channel state information (CSI) hidden to avoid being detected by legitimate network users. Moreover, investigation of this scenario is important, since it is highly probable that we face heterogeneous networks. For simplicity, a reciprocal channel for both stages is assumed.

In a two-way relay channel (TWRC) [24] with physical layer network coding, the throughput of the system is increased dramatically when compared to the traditional network coding method. However, when a third unexpected user (intruder) enters the network, one may wonder how the network is going to handle the situation if corrupted packets are injected into the network. In this work, a TWRC network model with an intruder inside the network is analyzed. The intruder may attack the relay and/or the users. It should be emphasized that the "intruder" effect here differs from the conventional interference effect in wireless networks. The difference is

that the intruder attacks the network in such a way that its locations and channel status is unknown to the relay [25]. Hence, the performance analysis should be treated differently from the networks with conventional interference. In general, one or multiple intruders may enter the network. They inject data into the network to degrade the performance. For simplicity, we evaluate the case with one intruder. There are three main scenarios for an attack by the intruder.

The first scenario is an attack on the relay only. Attacks can occur when the relay is receiving the signals from the two users. The relay is a natural target since corrupting its packets can affect both users' received signals. Another scenario involves an attack on the users. These two nodes would only be affected during the receiving of a signal from the relay, and thus, the intruder has no interaction with the relay. The last scenario consists of a combination of attacks on both sending nodes and the relay. In this combination, the attacks occur both when the relay is receiving the users' signals and when the users are receiving the signal from the relay. Although the attack on both the users and the relay is practical, the intruder has to attack at both time slots which will exhaust its power. Figure 1 shows the network model for a single intruder attack on both LLNC and PLNC schemes. For the PLNC scheme, the assumption is that the relay receives the signals at the same time from the two users. This allows us to ignore the symbol-level synchronization effect. Nonetheless, symbol and phase synchronization among the nodes for a TWRC model with no intruder have been studied in [8, 26] and more thoroughly in [27]. In [8] and [27], the authors have shown that although the lack of carrier-phase, carrier-frequency, and time-based synchronizations does effect the network, the effect is generally acceptable in wireless environment. For the LLNC scheme, it is assumed that the attack happens during the first time slot. Since the relay is the most susceptible node inside the network (due to multiple access interference), the focus of this work is on a network with an attack on the relay only. The intruder attacks the network at the first time slot. This gives us a fair comparison where the intruder is present only in one time slot for all schemes. An example for networks with an intruder can be a wireless network with static wireless nodes, quasi-free-space channel properties such as the ones observed in wireless sensor networks deployed in large areas [28]. Another common scenario can be described with an example in a wireless network for TWRC model where two users (cell phones) try to communicate via a base station (relay). A third example is satellite communication, wherein two end nodes on the earth can only communicate with each other via a satellite relay [8]. IEEE 802.11 packet exchange can also be a good example for practical implementations of this scheme [29]. This gives us an insight for the performance in a real-time scenario.

The attack model is simple. It is assumed that the intruder uses the same type of device as the users [30]. This allows the intruder to avoid being detected. The attack can occur with different attack-to-signal ratios (ASRs) defined as the ratio of the average received attack signal power to the user signal power. Note that the ASR may vary randomly in a wireless transmission scenario. To keep the comparison fair, this scenario is not illustrated. The intruder modifies the received messages and thus influences the demodulation/denoising of the received data. Digital wireless attacks for signals such as Bluetooth and Wi-Fi are possible with very low power. For the transmission power of the intruder (P_I), the example of reactive (or responsive) attacker can be used where the intruder looks for ongoing transmissions in order to compose their

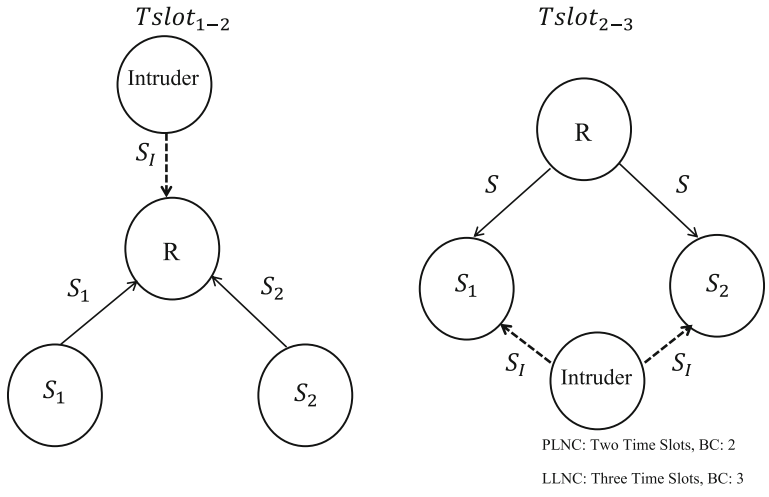

Fig. 1 PLNC and LLNC network model with an intruder performing pollution attack

attack signal (the intruder applies power management to identify the appropriate direction of transmission, power, and timing for its attack) [28]. Through the transmission of a high power signal on the same frequency of a user, the intruder can create a competing signal that collides with and, in effect, cancels out the users' signal. Cell phones (users), which are designed to increase power in the case of low levels of interference, react to this interference. Consequently, the intruder must be aware of any increases in power by the users and match that power level accordingly. A type of reactive intruder called intelligent intruder uses this knowledge to disrupt the communications. In fact, intelligent intruders could be considered as a type of reactive intruders. By using intelligent attack techniques, the attacker decreases its probability of detection and consumption of energy than basic reactive one.

The details of LLNC, AF, and ADNF schemes are discussed next. Section 2.1 discusses the LLNC network model, Section 2.2 discusses the AF network model, and Section 2.2 describes the ADNF network model.

2.1 LLNC System Model

For the TWRC network model, the data transmission process for LLNC and PLNC schemes is shown in Fig. 2. The last two slots of a four-stage transmission are shortened into one slot in LLNC scheme by allowing the relay to add (XOR denoted by $\oplus$) the received symbols S_1, and S_2.

$$S = S_1 \oplus S_2 \tag{1}$$

The last time slot is where the relay broadcasts S back to the users. The users will then be able to recover the information from the other user by adding their own symbol to the symbol received from the relay.

$$\begin{aligned} S_2 &= S \oplus S_1, \\ S_1 &= S \oplus S_2 \end{aligned} \tag{2}$$

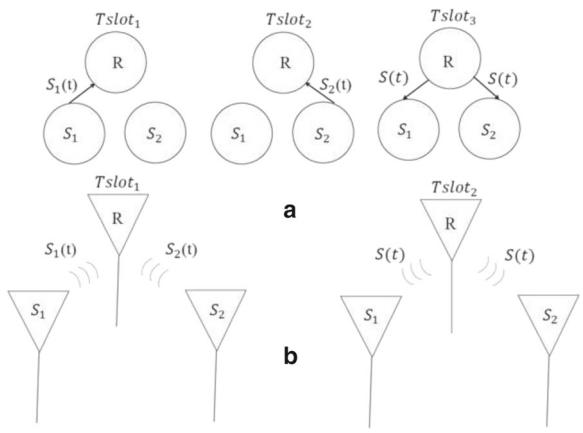

Fig. 2 a LLNC. **b** PLNC

Let X_1 and X_2 be the modulated transmitted symbols of the two transmitting nodes. From Fig. 1, at two consecutive time slots, node $k \in \{1, 2\}$ transmits its data to the relay. The two received signals at the relay for the first time slot, where the intruder is present, and for the second time slot where there is no intruder presence, are written as

$$Y_{R_1|S_I} = \sqrt{P_S} H_1 X_1 + \sqrt{P_I} H_I X_I + N_R \tag{3}$$

$$Y_{R2} = \sqrt{P_S} H_2 X_2 + N_R \tag{4}$$

where $S_I \in \{\mathbb{Z}_M\}$ is the intruder's signal, $\mathcal{M}(S_I) = X_I$ is the modulated signal, P_I is the transmission power, H_I is the channel coefficient with Rayleigh distribution, all for intruder, and N_R is the noise at the relay. The relay detects the symbols in a similar manner as shown in [31]:

$$\hat{S}_{1|S_I} = \mathbb{Q}\left(\frac{H_1 Y_{R1}}{|H_1|^2}\right) \tag{5}$$

$$\hat{S}_2 = \mathbb{Q}\left(\frac{H_2 Y_{Rk}}{|H_2|^2}\right) \tag{6}$$

where $\mathbb{Q}(.)$ denotes hard decision. The relay broadcasts the XOR version $S = \hat{S}_1 \oplus \hat{S}_2$ for the case with no intruder attack and $S = \hat{S}_{1|S_I} \oplus \hat{S}_2$ for the case with the intruder attack of the demodulated symbols back to the user nodes. For simplicity, reciprocal channel conditions are assumed here as well. The received signal at the users can be written as

$$Y_{Bk} = \sqrt{P_S} H_k X + N_k \tag{7}$$

where $X = \mathcal{M}(S)$. The two nodes detect the relay's transmitted data Y_{Bk} from the relay as

$$\hat{S}_{Rk} = \mathbb{Q}\left(\frac{H_k Y_{Bk}}{|H_k|^2}\right) \tag{8}$$

The two users demodulate their detected symbols and then extract the information from the other user as follows

$$\bar{S}_2 = \hat{S}_{R1} \oplus S_1 \tag{9}$$

$$\bar{S}_1 = \hat{S}_{R2} \oplus S_2 \tag{10}$$

PLNC, on the other hand, makes the process even faster by combining the first two stages of the process. The users are allowed to send the symbols during the same time slot. At the second time slot, after processing, the relay broadcasts the processed data back to the users. The two PLNC network models are described next.

2.2 AF system model

The AF model has two stages of operation. The first stage is referred to as the *MA stage*, where the two users transmit their data to the relay, simultaneously. The second

stage is the *relaying stage*, where the relay performs a combining operation on the received data (this can be as simple as XOR in LLNC or more complicated as discussed later) and broadcasts the signal back to the users. The main difference between the AF scheme and the ADNF scheme is that during the MA stage, the relay only amplifies the signal and broadcasts it back to the users. Unlike the ADNF scheme, the AF scheme does not take a more realistic wireless channel model (i.e., fading) into account. As it can be seen later, due to this reason, the AF idea falls behind the ADNF scheme in terms of performance. However, when it comes to an attack, it is unknown whether ADNF outperforms the AF scheme or not. Hence, this work analyzes the performance of the AF scheme in presence of an intruder as well.

The received signal at the relay at MA stage can be written as

$$R_{\mathrm{AF}|S_I} = \sqrt{P_S}H_1X_1 + \sqrt{P_S}H_2X_2 + \mathrm{att} + N_R \tag{11}$$

where $\mathrm{att} = \sqrt{P_I}H_IX_I$. In a similar manner to [32], the relay amplifies the received signal with an amplification factor as

$$\beta = \sqrt{\frac{P_S}{P_S|H_1|^2 + P_S|H_2|^2 + \sigma^2}} \tag{12}$$

It should be noted that the intruder term is not present in the amplification factor. This is because the relay is not aware of the CSI of the intruder's channel. The relay broadcasts the amplified signal $X_B = \beta R_{\mathrm{AF}}$ to the two users. Perfect channel estimation at the users is assumed here. The users receive the signal as follows

$$\begin{aligned} A_1 &= \sqrt{P_S}\left(\beta {H_1}^2X_1 + \beta H_1H_2X_2\right) + Z_1 + \beta H_1\mathrm{att} \\ A_2 &= \sqrt{P_S}\left(\beta {H_2}^2X_2 + \beta H_2H_1X_1\right) + Z_2 + \beta H_2\mathrm{att} \end{aligned} \tag{13}$$

where $Z_i = \beta H_iN_R + N_i$ and $i \in \{1, 2\}$. After self-interference cancelation [32], the signals at the two users can be written as

$$\begin{aligned} \hat{A}_1 &= \sqrt{P_S}\beta H_1H_2X_2 + Z_1 + \beta H_1\mathrm{att} \\ \hat{A}_2 &= \sqrt{P_S}\beta H_2H_1X_1 + Z_2 + \beta H_2\mathrm{att} \end{aligned} \tag{14}$$

The signal-to-attack-and-noise Ratio (SANR) at user 1 and user 2 for the AF scheme is written as

$$\begin{aligned} \gamma_1 &= \frac{P_S\beta^2|H_1|^2|H_2|^2}{\left(\beta^2|H_1|^2 + 1\right)\sigma^2 + P_I\beta^2|H_1|^2|H_I|^2} \\ \gamma_2 &= \frac{P_S\beta^2|H_2|^2|H_1|^2}{\left(\beta^2|H_2|^2 + 1\right)\sigma^2 + P_I\beta^2|H_2|^2|H_I|^2} \end{aligned} \tag{15}$$

For the case with no intruder attack, the term $P_I\beta^2|H_i|^2|H_I|^2, i \in 1, 2$, will not be present.

2.3 ADNF system model

The DNF was originally introduced in [9]. The goal of DNF is to increase the throughput of the system when compared to AF [29, 33] and Decode-and-Forwarding (DF) [24, 34]. In the DF relaying, the relay combines the data using XOR operation as shown in (1), while the AF relaying allows the addition of the data provided by the multiple access (MA) channel. In the AF method, for high signal-to-noise ratios (SNR), the throughput is twice as much as the traditional four-stage routing. The problem with this method appears at low SNRs. This results in erroneous received data and degrading network throughput. DNF addresses this problem by not decoding the data from the two users. Nonetheless, it can make an estimate of the sum of the two signals coming from the two users with the help of a decision process that decreases the noise impact. This improvement makes the DNF stand out among the two other methods. The modulation schemes optimized for the two-way relay channel for ADNF has been investigated in [19]. Similar to AF scheme, this scheme also has a two stage process. The two stages are briefly explained next.

2.3.1 MA stage

During the MA stage, the users transmit their data using QPSK modulation. The users send their data as $X_1 = \mathcal{M}(S_1)$ and $X_2 = \mathcal{M}(S_2)$. A quasi-static and a perfect CSI at the relay is assumed here. In other words, the channel is constant for a block of transmission and varies independently from one block to another. Each of the channels is assumed to be slow fading. Imperfect channel estimation (channel estimation error) has been studied in [35, 36], where it has been shown that there exists a statistical lower bound on the variance of estimation error that allows operation with no network coding error. For simplicity, however, this effect is not investigated in this paper since the main goal of this work is to study the effect of the pollution attack on the network. Extension of these results to the case where the channels are not estimated perfectly is straight forward. As shown in Fig. 1, during the first time slot, the intruder attacks the network. The relay may receive false information from the users due to the attack. The received signal at the relay is written as

$$R_{\mathrm{ADNF}|S_\mathrm{I}} = \sqrt{P_S}H_1X_1 + \sqrt{P_S}H_2X_2 + \mathrm{att} + N_R \tag{16}$$

2.3.2 Relaying stage

The ML detection as shown in (17) is used at the relay to get the estimates of the two users' information based on the received complex number R_{ADNF}.

$$(\hat{S}_1, \hat{S}_2) = \underset{(S_1,S_2)\in\mathbb{Z}_M\times\mathbb{Z}_M}{\operatorname{argmin}} \left|R_{\mathrm{ADNF}} - (H_1M(S_1) + H_2M(S_2))\right|^2 \tag{17}$$

The relay maps the received signal R_{ADNF}, using a denoising function, into a quantized signal, X_R. Note that here, the relay is not aware of the third-party intruder and only assumes that there are two users sending out their data. Therefore, for the case where the users transmit QPSK modulation, it uses the same code-maps and table used in Fig. 4 and Table I of [19]. Moreover, the relay performs the ML based on the information from the two users and not the intruder. As mentioned in [19], for higher order modulation schemes, a simplified code-map is proposed that reduces the number of network codes and limits or eliminates the usage of irregular modulations at the BC stage. However, there are still many singular fade states that can degrade the performance. The authors in [37, 38] have shown that by utilizing convolutional or LDPC codes, the performance of the network can be improved.

The users receive the broadcasted signal code from the relay under the quasi-static slow fading channel. This code can have a cardinality greater than or equal to M (for QPSK, $M = 4$), depending on the selected code-map, where either $M-$ PSK or $(M+N)-$ QAM, $(N \geq 1)$ will be broadcasted. For simplicity, a reciprocal channel for both stages is assumed. Note that the denoising maps are designed by minimizing the pairwise error probability between the codewords at the MA stage and to maximize the minimum square distance between the constellation points. In other words, the best denoising maps are designed in favor of increasing the minimum Euclidean distance. The squared Euclidean distance between the data transmitted from the senders and its candidates, i.e., $(S_1, S_2) \rightarrow (\hat{S}_1, \hat{S}_2)$, is as shown in [19]

$$d^2_{(S_1,S_2)-(\hat{S}_1,\hat{S}_2)} = |H_1|^2 \left| (\Delta(S_1, \hat{S}_1) + \gamma e^{j\theta} \Delta(S_2, \hat{S}_2) \right|^2 \tag{18}$$

where $\Delta(s, \hat{s}) = \mathcal{M}(s) - \mathcal{M}(\hat{s})$. If the data pair is erroneous, that is, $\mathcal{C}(\hat{S}_1, \hat{S}_2) \neq \mathcal{C}(S_1, S_2)$, the pairwise error probability (PEP) is calculated as

$$\begin{aligned} P_e(S_1, S_2) \rightarrow (\hat{S}_1, \hat{S}_2) &= Q\left(\frac{d_{(S_1,S_2)-(\hat{S}_1,\hat{S}_2)}}{\sigma\sqrt{2}} \right) \\ &\leq e^{-\frac{d^2_{\min}}{4\sigma^2}} \end{aligned} \tag{19}$$

where the last term comes from the Chernoff bound [39], Q is the complementary Gaussian cumulative distribution function defined in [39], and $d^2_{\min}$ is the minimum squared distance of the numerator of (18). That is,

$$d^2_{\min} = \min_{\mathcal{C}(\hat{S}_1,\hat{S}_2) \neq \mathcal{C}(S_1,S_2)} d^2_{(S_1,S_2)-(\hat{S}_1,\hat{S}_2)} \tag{20}$$

For a channel realization H (H_1 and H_2), the overall error probability at the relay is a weighted sum of all the possible erroneous data pairs $\mathcal{C}(\hat{S}_1, \hat{S}_2) \neq \mathcal{C}(S_1, S_2)$ where the most dominant factor in calculating the overall error is the minimum Euclidean distance between the data transmitted from the users and its candidates [19]. This is shown in (21). It should be noted that since the closed-form expression for the decision regions are too complex to derive, the exact error probability calculation is a complicated task. Hence, the PEP, which is a tight bound for exact error probability is being used [39].

$$\begin{aligned} P^R_{e|H}|S_I = \frac{1}{M^2} \sum_{(S_1,S_2)\in\mathbb{Z}^2_M} \sum_{(S'_1,S'_2)\neq(S_1,S_2)\in\mathbb{Z}^2_M} \\ P_{e|S_I}\left((\hat{S}_1, \hat{S}_2) = (S'_1, S'_2), \mathcal{C}(S'_1, S'_2) \neq (\hat{S}_1, \hat{S}_2) \right) \end{aligned} \tag{21}$$

3 Performance analysis

Performance of LLNC, AF, and ADNF schemes are studied and compared in this section. Since the relay dominates the network and is the most susceptible node in the network [19], for the analysis purposes, the performance of the network with an intruder attack on the relay is illustrated. The attack on the nodes (broadcast stage attack) can be derived and illustrated in a similar manner and is left as a future work.

3.1 LLNC performance evaluation

As previously shown in Fig. 2a and Eq. (1), the linear network coding scheme is a three-stage relaying process that boosts the throughput when compared to the traditional four-stage relaying. The performance of the network with and without the intruder is investigated.

3.1.1 Performance with no intruder

First case is when the probability of attack of the intruder is zero ($P_a = 0$). The symbol error probability (SER) at the relay $P_{s\rightarrow r}$, at the users $P_{r\rightarrow s}$, and at the end-to-end error probability P_{ete} is derived next.

In the first and second time slots, the SER at the relay is calculated as [39]

$$P_{s_j\rightarrow r} = P(\hat{S}_j \neq S_j) \tag{22}$$

where $P(\hat{S}_j \neq S_j) = Q\left(\frac{d_j|h_j|}{\sqrt{2\sigma^2}}\right)$, $j \in \{1, 2\}$, and d_j is the Euclidean distance between two M-PSK signal points. Here, $Q(u)$ is denoted as

$$Q(u) = \frac{1}{\sqrt{2\pi}} \int_u^\infty e^{-\frac{t^2}{2}} dt \tag{23}$$

In calculating (22), the minimum Euclidean distance is used. To calculate the average error probability, the integral in ([40] equation 5.1) needs to be evaluated and is given by,

$$\bar{P} = \int_0^{\infty} \underbrace{aQ(\sqrt{b\gamma})}_{\text{(i)}} f_{\gamma}(\gamma) d\gamma \tag{24}$$

where $(a, b) > 0$ are modulation-specific constants. For example, for high SNRs, and for QPSK modulation over AWGN, (i) can be approximated as $2Q\left(\sqrt{\gamma}\right)$. The probability density function (PDF) of the Rician fading is written as

$$f_{\bar{\gamma}}(\gamma) = \frac{(1+K)e^{-K}}{\bar{\gamma}} e^{-\frac{(1+K)\gamma}{\bar{\gamma}}} I_0\left(2\sqrt{\frac{K(1+K)\gamma}{\bar{\gamma}}}\right) \tag{25}$$

where $(\gamma \geq 0)$, $\bar{\gamma}$ is the average SNR, γ is defined as the instantaneous SNR per symbol, i.e., $\gamma = H^2 \frac{P_S}{\sigma^2}$, and $I_0(.)$ is the zero-order modified Bessel function of the first kind [40]. K is the Rician K-factor defined as the ratio of the powers of the LOS component to the scattered components. Substituting (25) into (24), and using the alternative version of the Q function $Q_{\text{alt}}(u) = \frac{1}{\pi} \times \int_0^{\frac{\pi}{2}} e^{-\frac{u^2}{2\sin^2\theta}} d\theta$ [40], (24) can be simplified as

$$\bar{P}_{s_j \to r} \frac{a}{\pi} \int_0^{\frac{\pi}{2}} M_{\gamma}\left(-\frac{b^2}{2\sin^2\theta}\right) d\theta \tag{26}$$

where $M_{\gamma}(s) \triangleq \int_0^{\infty} e^{s\gamma} p_{\gamma}(\gamma) d\gamma$ is the moment-generating function (MGF) [40]. Next, using Eq. (5.11) in [40], with some algebraic manipulation, the average SER for QPSK modulation scheme at high SNRs can be written as

$$\bar{P}_{s_j \to r} \approx \frac{2(1+K)}{\pi} \int_0^{\frac{\pi}{2}} \frac{e^{-\frac{K\bar{\gamma}\sin^2\theta}{1+K+\frac{1}{2}\bar{\gamma}\sin^2\theta}}}{1+K+\frac{1}{2}\bar{\gamma}\sin^2\theta} d\theta \tag{27}$$

In a similar way, the $P_{r \to s_j}$ and $\bar{P}_{r \to s_j}$ can be calculated. The end-to-end error probability is directly affected by the relay and the bit-wise XOR operation. Let $P_{\text{xor}} = P(S_1 \oplus S_2 \neq \hat{S}_1 \oplus \hat{S}_2)$, where $S_1 \neq \hat{S}_1$ and $S_2 \neq \hat{S}_2$, denote the probability of error in decoding XOR-ed data at the relay, given that both estimates of the two transmitted signals are in error. For a general M-PSK modulation, there are $M \times M$ possible pair combinations. Excluding the correct pair, the XOR-ed error probability at the relay can be calculated. For example, for a QPSK modulation, without loss of generality, if the two users transmit the pair (0,1), the possible erroneous decoded pairs at the relay that will result in correct XOR operation are {(1,0), (3,2), (2,3)}. The possible erroneous decoded pairs at the relay that will result in wrong XOR operation are {(2,2), (3,3), (1,2), (1,3), (3,0), (2,0)}. Furthermore, as mentioned in (22), the error probability of decoding each individual pair with one symbol per time slot depends on the Euclidean distance between the two QPSK signal points. Hence, $P_{\text{xor}} = 1 - \frac{3}{9} = \frac{2}{3}$. For the transmitted pair (0, 1), Table 1 shows all the possible nine pair combinations with their associated probabilities.

The average error probability at the relay is

$$\begin{aligned} \bar{P}_{\text{relay}} = &\left(\bar{P}_{s_1 \to r}\right)\left(1 - \bar{P}_{s_2 \to r}\right) \\ &+ \left(1 - \bar{P}_{s_1 \to r}\right)\left(\bar{P}_{s_2 \to r}\right) \\ &+ \left(\bar{P}_{s_1 \to r}\right)\left(\bar{P}_{s_2 \to r}\right)(P_{\text{xor}}) \end{aligned} \tag{28}$$

Assuming $\bar{P}_{s_1 \to r} \approx \bar{P}_{s_2 \to r} = \bar{P}_{s \to r}$, $\bar{P}_{\text{relay}}$ can be written as

$$P_{\text{relay}} \approx \bar{P}_{s \to r}(2 + \bar{P}_{s \to r}(P_{\text{xor}} - 2)) \tag{29}$$

The average end-to-end error probability from user 1 to user 2 is written as

$$\begin{aligned} \bar{P}_{\text{ete}1 \to 2} &\approx (P_{\text{relay}})(1 - \bar{P}_{r \to s_2}) \\ &\quad + (1 - P_{\text{relay}})(\bar{P}_{r \to s_2}) \\ &\quad + (P_{\text{relay}})(\bar{P}_{r \to s_2}) \\ &= P_{\text{relay}} + \bar{P}_{r \to s_2}(1 - P_{\text{relay}}) \end{aligned} \tag{30}$$

Table 1 Probability of error for transmitted symbol pair (0,1) with the wrong estimated symbol pairs ($\sigma^2 = 1$)

Type	$(\hat{S}_1, \hat{S}_2)$	$P_1 = Q(2/\sqrt{2})$	$P_2 = Q(\sqrt{2/2})$	P_e	Correct/erroneous XOR Decoding
Desired incorrect pairs	(1, 0)	0.0786	0.1587	$P_2 \times P_2 = 0.0252$	Correct
	(2, 3)	0.0786	0.1587	$P_2 \times P_2 = 0.0252$	Correct
	(3, 2)	0.0786	0.1587	$P_1 \times P_1 = 0.0062$	Correct
Undesired incorrect Pairs	(2, 2)	0.0786	0.1587	$P_2 \times P_1 = 0.0125$	Erroneous
	(3, 3)	0.0786	0.1587	$P_1 \times P_2 = 0.0125$	Erroneous
	(1, 2)	0.0786	0.1587	$P_2 \times P_1 = 0.0125$	Erroneous
	(1, 3)	0.0786	0.1587	$P_2 \times P_2 = 0.0252$	Erroneous
	(3, 0)	0.0786	0.1587	$P_1 \times P_2 = 0.0125$	Erroneous
	(2, 0)	0.0786	0.1587	$P_2 \times P_2 = 0.0252$	Erroneous

3.1.2 Performance with an intruder

The performance of the network with the intruder ($P_{\mathrm{a}} = 1$) is discussed here ("a" denotes attack). At the first time slot, along with the transmission of the first node, the intruder attacks the network. Same assumption has been made in [41], where the eavesdropper starts overhearing from the beginning of the time slot. The scenario is considered as the worst case scenario. It is assumed that the relay is not aware of the attack inside the network. Assuming that the intruder attack during the first time slot, the error probability of the incorrectly estimated symbols at the relay can be written as [39]

$$\begin{aligned} P_{s_1\to r|S_I} &= P(\hat{S}_1 \neq S_1|P_{\mathrm{a}} = 1) = Q\left(\sqrt{\frac{d_{1I}}{2\sigma^2}}\right) \\ P_{s_2\to r} &= P(\hat{S}_2 \neq S_2) = Q\left(\frac{d_2|H_2|}{\sqrt{2\sigma^2}}\right) \end{aligned} \tag{31}$$

where d_{1I} is the squared Euclidean distance between the two M-PSK signal points [39] and is expressed as

$$d_{1I} = |H_1|^2|M(S_1) - M(\check{S}_1)|^2 \tag{32}$$

where $\check{S}_1$ is the estimate of the transmitted signal S_1 based on (4). The receiver, which is not aware of the intruder, assumes a 4-point signal constellation for detection and demodulation. However, if the intruder is somehow detected by the receiver, the constellation map goes beyond 4 points (16 points). Obviously the error probability would be improved and would be calculated in a different manner. The average error probability at the relay is

$$\bar{P}_{\mathrm{relay}|S_I} \approx \bar{P}_{s_1\to r|S_I} + \bar{P}_{s_2\to r} + \bar{P}_{s_1\to r|S_I}\bar{P}_{s_2\to r}(P_{\mathrm{xor}} - 2) \tag{33}$$

The only term in (33) that is needed to be calculated is $\bar{P}_{s_1\to r|S_I}$. To do so, we use the cumulative distribution function -based approach that is widely used [42]. Let $X = \frac{P_S|H_1|^2}{\sigma^2}$, and $Z = \frac{P_I|H_I|^2}{\sigma^2}$. The SANR for user 1 to the relay link can be written as $\gamma_1 = \frac{X}{Z+1}$. Similar to the method described in [42], in order to calculate the average error probability, the outage probability needs to be evaluated. The outage probability is known to be the probability that γ_1 falls below an acceptable SNR threshold γ_{th} and can be written as

$$P_{\mathrm{out}} = F_{\gamma_1}(\gamma_{\mathrm{th}}) = P_r(\gamma_1 \leq \gamma_{\mathrm{th}}) \tag{34}$$

where $P_r(.)$ denotes the probability. Recall that the users' channels are subject to a Rician fading. In order to derive the outage probability of γ_1 conditioned on Z, the complementary CDF of X is used. Now, (34) can be written as

$$\begin{aligned} P_{\mathrm{out}} &= \int_0^\infty P_r(X < \gamma_{\mathrm{th}}(z+1))f_Z(z)dz \\ &= 1 - \int_0^\infty C_X(\gamma_{\mathrm{th}}(z+1))f_Z(z)dz \end{aligned} \tag{35}$$

where $C_X(.) = 1 - F_X(.)$. Substituting the PDFs of the intruder's channel, which is Rayleigh distributed, as well as the users channel into (35), and by using the infinite-series representation of $I_0(.)$ in [43], Eq. (8.447.1), and with the help of Eq. (3.351.2) in [43], the integral can be simplified to

$$P_{\mathrm{out}} \approx 1 - \Delta_1 e^{-K}\sum_{i=0}^{\infty}\frac{(K\Delta_1)^i}{(i!)^2} \times \int_0^\infty\int_{\gamma_{\mathrm{th}}(z+1)}^\infty e^{-\Delta_1 x}x^i dx f_Z(z)dz \tag{36}$$

$$= 1 - \Delta_1 e^{-K}\sum_{i=0}^{\infty}\sum_{k=0}^{i}\frac{(K\Delta_1)^i}{(i!)(k!)(\Delta_1)^{i-k+1}} \tag{37}$$

$$\times \int_0^\infty e^{-\gamma_{\mathrm{th}}(z+1)\Delta_1}(\gamma_{\mathrm{th}}(z+1))^k f_Z(z)dz \tag{38}$$

$$= 1 - \Delta_1 e^{-K}\sum_{i=0}^{\infty}\sum_{k=0}^{i}\frac{(K\Delta_1)^i(\gamma_{th})^k e^{\frac{-\gamma_{\mathrm{th}}\Delta_1\bar{\gamma}_z}{\bar{\gamma}_z}}}{(i!)(k!)(\Delta_1)^{i-k+1}\bar{\gamma}_z} \tag{39}$$

$$\times \int_0^\infty e^{-z\left(\frac{\gamma_{\mathrm{th}}\bar{\gamma}_z\Delta_1+1}{\bar{\gamma}_z}\right)}(z+1)^k dz \tag{40}$$

where $\Delta_1 = \left(\frac{1+K}{\bar{\gamma}_x}\right)$, $\Delta_2 = \frac{\gamma_{\mathrm{th}}\bar{\gamma}_z\Delta_1+1}{\bar{\gamma}_z}$, and $\bar{\gamma}_x$, $\bar{\gamma}_y$, and $\bar{\gamma}_z$ are the average received SNRs of user 1, user 2, and the intruder, respectively. Noting Eq. (3.382.4) in [43], and some algebraic manipulations, the outage probability is written as

$$P_{\mathrm{out}} \approx 1 - \Delta_1 e^{-K} \times \sum_{i=0}^{\infty}\sum_{k=0}^{i}\frac{e^{\frac{1}{\bar{\gamma}_z}}\gamma_{\mathrm{th}}{}^k\Delta_2^{-1-k}(K\Delta_1)^i\Gamma(k+1,\Delta_2)}{i!\,k!\,\Delta_1{}^{i-k+1}\bar{\gamma}_z} \tag{41}$$

where $\Gamma(.,.)$ is the complementary incomplete gamma function defined in [43], Eq. (8.350.2). The approximation comes from using the infinite series representation of the gamma function. The average SER can be calculated using the widely used CDF-based approach [32]. For

a general modulation type, the average error probability can be written as

$$\bar{P}_e = E\left[aQ(\sqrt{2b\gamma_{\text{th}}})\right] = \frac{a}{2}\sqrt{\frac{b}{\pi}}\int_0^\infty \frac{e^{-b\gamma_{\text{th}}}}{\sqrt{\gamma_{\text{th}}}}F(\gamma_{\text{th}})d\gamma_{\text{th}} \tag{42}$$

Using Eqs. (8.352.2) in [43] and (42), (41) further is simplified to

$$\bar{P}_{s_1\to r|S_I} \approx \frac{a}{2} - \sqrt{\frac{a^2b}{4\pi}}\Delta_1 e^{-K} \times \sum_{i=0}^{\infty}\sum_{k=0}^{i}\sum_{l=0}^{k}\frac{(K\Delta_1)^i\,\bar{\gamma}_z^{k-l}}{i!\,l!\,{\Delta_1}^{i-k+1}} \tag{43}$$

$$\times \int_0^\infty {\gamma_{th}}^{k-\frac{1}{2}} e^{\left(-\gamma_{\text{th}}\left(\frac{D+b\bar{\gamma}_z}{\bar{\gamma}_z}\right)\right)}(D\gamma_{\text{th}}+1)^{l-k-1}d\gamma_{\text{th}} \tag{44}$$

Noting Eq. (3.383.5) in [43], the average error probability is calculated and written as

$$\bar{P}_{s_1\to r|S_I} \approx \frac{a}{2} - \frac{\sqrt{a^2b}\Delta_1 e^{-K}}{\sqrt{4\pi}} \times \sum_{i=0}^{\infty}\sum_{k=0}^{i}\sum_{l=0}^{k}\frac{\bar{\gamma}_z^{k-l}D^{-k-\frac{1}{2}}\,(K\Delta_1)^i}{i!\,l!\,{\Delta_1}^{i-k+1}} \times \Gamma\left(k+\frac{1}{2}\right)\psi\left(k+\frac{1}{2}, l+\frac{1}{2}, \frac{b+\Delta_1}{D}\right) \tag{45}$$

where $\psi(.,.,.)$ is the Tricomi confluent hypergeometric function as defined in [43], Eq. (9.211.4), and $D = \bar{\gamma}_z\Delta_1$. The closed-form expression does converge and can easily be plotted in Matlab or other simulation software. For different values of $\bar{\gamma}_z$, it can be seen that the SER varies. The average end-to-end error probability from node 1 to node 2 is

$$\bar{P}_{\text{ete1}\to 2|S_I} \approx P_{\text{relay}|S_I} + \bar{P}_{r\to s_2}(1 - P_{\text{relay}|S_I}) \tag{46}$$

3.2 AF performance evaluation

The performance without an intruder with $P_{\text{a}} = 0$ is evaluated next.

3.2.1 Performance with no intruder

In order to evaluate the error probability, the outage probability needs to be calculated. The method described in [32] is used here. Let $X = \frac{P_S|H_1|^2}{\sigma^2}$, $Y = \frac{P_S|H_2|^2}{\sigma^2}$. By substituting (12) into (15) without the intruder term and applying algebraic manipulation, it can be shown that the effective SNRs at the two users are given by

$$\gamma_1 = \frac{XY}{2X+Y+1}, \quad \gamma_2 = \frac{XY}{2Y+X+1} \tag{47}$$

It has been shown in [44] that $\gamma_1 > \gamma_2$ if $Y > X$ and $\gamma_2 > \gamma_1$ if $X > Y$. Therefore, the outage probability is expressed as

$$\begin{aligned} P_{\text{out}} &= P(\min\{\gamma_1,\gamma_2\} < \gamma_{\text{th}}) \\ &= 1 - P(\gamma_1 > \gamma_{\text{th}}, \gamma_2 > \gamma_{\text{th}}) \\ &= 1 - P(\gamma_1 > \gamma_{\text{th}}|X > Y) - P(\gamma_2 > \gamma_{\text{th}}|Y > X) \\ &= 1 - (P_1 + P_2) \end{aligned} \tag{48}$$

Next, using [32] and [44], and after some simple algebraic manipulations, P_1 can be written as

$$P_1 = P\left\{X > \max\left[Y, \frac{\gamma_{\text{th}}(1+Y)}{Y-2\gamma_{\text{th}}}\right], Y > (2\gamma_{\text{th}})\right\} \tag{49}$$

$$= \int_{2\gamma_{\text{th}}}^\infty \int_{\max\left(y, \frac{\gamma_{\text{th}}(1+y)}{y-2\gamma_{\text{th}}}\right)}^\infty f_X(x)dx f_Y(y)dy \tag{50}$$

where $f_X(x)$ and $f_Y(y)$ are the PDFs of the Rician-distributed random variables (RV) X and Y, respectively. P_2 can be calculated in a similar manner. The limits on the integral comes from the conditions in (47). Since evaluating (50) is a cumbersome task, for high SNRs, the integration region of the variable x can be reduced to (y, ∞). It can be shown that the average SER of the network can be expressed as (51). Here, $\Delta_1 = \left(\frac{1+K}{\bar{\gamma}_x}\right)$; $\Delta_2 = \left(\frac{1+K}{\bar{\gamma}_y}\right)$; $\Delta_3 = \Delta_1 + \Delta_2$; γ_x, $\bar{\gamma}_y$ and $\bar{\gamma}_z$ are the average SNRs for user 1, user 2, and intruder, respectively; and $n!!$ is expressed as

$$n!! = \begin{cases} \prod_{i=1}^{n/2} 2i, & n \text{ even} \\ \prod_{i=1}^{n+1/2} 2i-1, & n \text{ odd} \\ -1!! = 0!! = 1 \end{cases}$$

$$\bar{P}_{eAF|P_a=0} \approx \frac{a}{2} - \left(\frac{\sqrt{a^2b}\Delta_1\Delta_2 e^{-2K}}{\sqrt{\pi}}\sum_{i=0}^{\infty}\sum_{j=0}^{\infty}\sum_{k=0}^{i}\sum_{l=0}^{j+k} \frac{(2l-1)!!\,(K\Delta_1)^i\,(K\Delta_2)^j\,(j+k)!\,(2\Delta 3+b)^{-l-\frac{1}{2}}}{i!\,(j!)^2k!\,{\Delta_1}^{i-k+1}\Delta_3^{j+k-l+1}}\right) \tag{51}$$

3.2.2 Performance with an intruder

Performance of the network with an intruder is studied next. For all the schemes, the intruder attacks during the first time slot (MA stage). In order to evaluate the error probability, the outage probability needs to be calculated. The method described in [32] is being used here. Let $X = \frac{P_S|H_1|^2}{\sigma^2}$, $Y = \frac{P_S|H_2|^2}{\sigma^2}$, and $Z = \frac{P_I|H_I|^2}{\sigma^2}$. Now, by substituting (12) into (15) and applying algebraic manipulation, it can be shown that the effective SANRs at the two users are given by

$$\begin{aligned}\gamma_1 &= \frac{XY}{2X+Y+XZ+1}\\ \gamma_2 &= \frac{XY}{2Y+X+YZ+1}\end{aligned} \tag{52}$$

Following the same method used in the case with no intruder attack and with some simple algebraic manipulations, P_1 can be written as

$$\begin{aligned}P_1 =& P\{X > \max[Y, V_1], Y > V_2\}\\ =& E_Z\left(\int_{2\gamma_{\text{th}}+z\gamma_{\text{th}}}^{\infty}\int_{\max(y,v_1)}^{\infty} f_X(x)f_Y(y)dxdy\right)\end{aligned} \tag{53}$$

where $f_X(x)$ and $f_Y(y)$ are the PDFs of the Rician-distributed RV X and Y, respectively, $V_1 = \frac{\gamma_{\text{th}}(1+Y)}{Y-2\gamma_{\text{th}}-Z\gamma_{\text{th}}}$, $V_2 = 2\gamma_{\text{th}} + Z\gamma_{\text{th}}$, PSY $= \psi\left(l+\frac{1}{2}, m+\frac{1}{2}, \frac{b+2\Delta_3)}{N}\right)$, and E_Z is the expected value over complex value, Z. The limits on the integral comes from the conditions in (52). The expected value is to evaluate the effect of the intruder on the network. Since evaluating the integral above is a cumbersome task, for high SNRs, the integral region of the variable x can be reduced to (y, ∞). Similar assumption has been applied in [32, 44]. Appendix proves that for high SNRs, the average SER of the network can be expressed as (54). The closed-form expression in (54) shows the impact of the intruder on the network. It can be seen that as the power of the intruder increases, the SER decreases. This equation does converge and can numerically evaluated for different values of $\bar{\gamma}_z$.

$$\begin{aligned}\bar{P}_{eAF|P_a=1} \approx\\ \frac{a}{2} - \left(\frac{\sqrt{a^2b}\Delta_1\Delta_2 e^{-2K}}{\sqrt{\pi}}\sum_{i=0}^{\infty}\sum_{j=0}^{\infty}\sum_{k=0}^{i}\sum_{l=0}^{j+k}\sum_{m=0}^{l}\right.\\ \left.\frac{\bar{\gamma}_z^{l-m}2^m(K\Delta_1)^i(K\Delta_2)^j(j+k)!N^{-l-\frac{1}{2}}\Gamma\left(l+\frac{1}{2}\right)\text{PSY}}{i!(j!)^2k!m!\,{\Delta_1}^{i-k+1}\Delta_3^{j+k-l+1}}\right)\end{aligned} \tag{54}$$

3.3 ADNF performance evaluation

For the ADNF scheme, the performance of the network is studied next. Similar to the previous sections, for a network with an intruder, the focus of this paper is on the MA stage as it dominates the overall system performance.

3.3.1 Performance with no intruder

The first case occurs when the probability of an attack by an intruder is zero ($P_a = 0$). The average error probability at the relay is due to three kinds of errors: first, the average probability that user 2 has its data decoded correctly at the relay and user 1 has not; second, the average error probability that user 1 has its data decoded correctly by the relay and user 2 has not; and third, the average cluster error probability ($\bar{P}_{\text{CEP}}$) that the relay incorrectly decodes to $(\hat{S}_1, \hat{S}_2)$ ([21] equation 11). The average SER at the relay is upper bounded as shown in [21]

$$\bar{P}_{\text{relay}} \leq 2\bar{P}_{s_j\to r} + \bar{P}_{\text{CEP}} \tag{55}$$

The error probability at the users, $P_{r\to s}$, is a function of the modulation scheme and transmitted code. For the method where the irregular modulation schemes is deployed to enhance the overall network performance, a special case for the QPSK modulation scheme is presented. If no irregular modulation scheme is used, the performance analysis becomes straightforward. In the BC stage, following the channel conditions [19], either QPSK or 5QAM is selected. Let $\mathcal{C}(S_2, S_1) = \mathbb{C}$ and $\mathcal{C}(\hat{S}_2, \hat{S}_1) = \hat{\mathbb{C}}$. The error probability at the users can be written as

$$P_{r\to s} = \alpha P_{\text{QPSK}}(\hat{\mathbb{C}} \neq \mathbb{C}) + (1-\alpha)P_{5\text{QAM}}(\hat{\mathbb{C}} \neq \mathbb{C}) \tag{56}$$

where $0 \leq \alpha \leq 1$ is the QPSK occurrence factor, $P_{\text{qpsk}}(\hat{\mathbb{C}} \neq \mathbb{C}) = Q\left(\frac{d_j|h_j|}{\sqrt{2\sigma^2}}\right)$, $j \in \{1, 2\}$, which can be calculated using (58), and, d_j is the Euclidean distance of two QPSK signal points based on $\mathbb{C}$ and $\hat{\mathbb{C}}$ of the corresponding node. Our simulation results show that both the cardinalities (4 and 5) are equally likely to be used; hence, $\alpha = \frac{1}{2}$ is used hereafter. The error probability of 5QAM can be found using Fig. 3. Since the exact error probability is difficult to obtain due to asymmetrical shape of the 5QAM, we approximated the error probability in the following manner. The asymptomatic optimized 5QAM has been designed using sphere packing approach in [19]. To obtain a unity average power per symbol, the radius R has been calculated. Since the minimum Euclidean distance between all the constellation points are the same ($d_{\min} = 2 * R = 1.2456$), the error probability of 5QAM

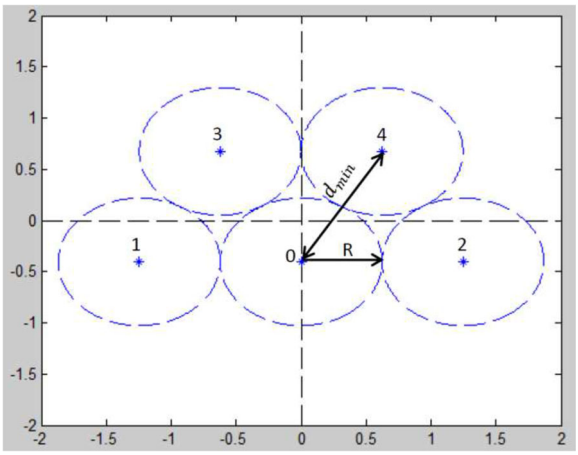

Fig. 3 5QAM constellation showing the minimum distance $d_{\min} = 1.2456$ and the radius $R = 0.6228$ [19]

can be calculated following [39]. Let $Q\left(\frac{d_{\min}}{\sqrt{2\sigma^2}}\right) = Q(Z)$ denote the probability of decoding a wrong symbol from a different region. The total SER of 5QAM is calculated as

$$\begin{aligned} P_{5\text{QAM}} &= \sum_{i=0}^{4} P(\hat{S}_i \neq S_i), i \in \{0,1,2,3,4\} \\ &\approx \frac{4}{5}Q(Z) + 2 \times \frac{2}{5}Q(Z) + 2 \times \frac{3}{5}Q(Z) \\ &= \frac{14}{5}Q(Z) \end{aligned} \tag{57}$$

Note that (57) has not been derived in [19]. As also mentioned in [19], the 5QAM shows a 1.1-dB loss when compared to QPSK. However, 5-ary denoising can avoid the distance shortening that does happen in the MA access due to the interference of the signals. Our analysis confirms the statement mentioned in [19]. The average error probability of 5QAM over Rician fading channel can be obtained by plugging in the average SER of 5QAM over AWGN in high SNR regime: $Q\left(\sqrt{\frac{(1.2456)^2}{2}\gamma}\right)$ into (24) with the similar steps followed as the SER for QPSK. Simplifying the expression results in the average error probability as follows

$$\bar{P}_{s_j \to r} \approx \frac{14(1+K)}{5\pi} \int_0^{\frac{\pi}{2}} \frac{e^{\left(-\frac{0.385K\bar{\gamma}\sin^2\theta}{1+K+0.385\bar{\gamma}\sin^2\theta}\right)}}{1+K+0.385\bar{\gamma}\sin^2\theta} d\theta \tag{58}$$

The average end-to-end error probability can be written as

$$\bar{P}_{\text{ete}} \leq P_{\text{relay}} + \bar{P}_{r \to s}(1 - P_{\text{relay}}) \tag{59}$$

The above equation shows that the overall error probability is directly proportional to the error happening at both the MA and BC stages, where the MA stage is the dominant factor due to the addition of the two signals (MA interference).

3.3.2 Performance with an intruder

The effect of the intruder on the network is studied next ($P_a = 1$). Note that the estimates of the transmitted signals are based on (11). The relay, without any knowledge of the intruder, considers a 16-point constellation point at the receiver. If the relay was aware of the intruder and its channel state information, other steps could be applied to avoid the high error probability that is being caused by the attack. In this case, the constellation map at the receiver becomes 64 points rather than 16. Therefore, the code-maps in Fig. 4 of [19] have to be changed and applied accordingly.

Using (55), the average error probability can be written as

$$\bar{P}_{\text{relay}|S_I} \leq 2\bar{P}_{s_j \to r|S_I} + \bar{P}_{\text{CEP}|S_I} \tag{60}$$

where $\bar{P}_{s_j \to r|S_I}$ is the probability of the point-to-point fading channels given an intruder is present inside the network, which is calculated using (45) in the previous section. The average cluster error probability given the intruder is present inside the network is defined as follows

$$\bar{P}_{\text{CEP}|S_I} = P\{(S_1, S_2) \to (S_1', S_2')\}|S_I \tag{61}$$

In other words, P_{CEP} is the probability that the relay incorrectly decodes to (S_1', S_2'), with the two pairs, $\{(S_1', S_2'), (S_1, S_2)\}$, not being present in the same cluster. This probability is written at the top of the next page.

$$P\{\{(S_1,S_2) \to (S_1',S_2')\}|S_I\} = P\{\{(\hat{S}_1,\hat{S}_2) = (S_1',S_2'), \mathcal{C}(S_1',S_2') \neq \mathcal{C}(S_1,S_2)\}|S_I\} \tag{62}$$

$$\bar{P}_{\text{CEP}|S_I} \leq \frac{(K+1)^2 e^{\left(-2K + \frac{K(K+1)\left|1-\frac{\Delta_{S_1}}{\Delta_{S_2}}\right|^2}{\left(K+1+SANR\frac{|\Delta_{S_2}|^2}{4}\right)\delta_s^2 + (K+1)\left(1+\frac{|\Delta_{S_1}|^2}{|\Delta_{S_2}|^2}\right)}\right)}}{2\left(K+1+SANR\frac{|\Delta_{S_2}|^2}{4}\right)\left(\left(K+1+SANR\frac{|\Delta_{S_2}|^2}{4}\right)\delta_s^2 + (K+1)\left(1+\frac{|\Delta_{S_1}|^2}{|\Delta_{S_2}|^2}\right)\right)} \tag{63}$$

With the help of the line of proof in [21] that did not consider an intruder, for a network with an intruder, the average CEP can be written as (62). Substituting SANR into ([21] equation 11), the average CEP can be written as (63). The following definitions from [21] are necessary to understand (63). $\Delta_{S_i} = S_i - S_i', i \in \{1, 2\}$, and δ_s represents the largest radius of the enclosed circle in the region associated with a specified singular fade state in which it can be removed by the clustering. For the ADNF scheme, SANR is defined as signal power to attack and noise power ratio and is written as $\text{SANR} = \frac{P_S}{P_I + \sigma^2}$. Note that the relay does not factor in the intruder in its estimates [21]. As we see later, the results shown in (63) explains the severity of intruder effect on this scheme.

4 Numerical and simulation results

4.1 Network coding-SER analysis

The SER comparison among four schemes is shown in Fig. 4. It illustrates the theoretical and simulation plot of average end-to-end SER vs. SNR with no intruder. For comparison purposes, the Non-Adaptive-Denoise-and-Forward scheme (fixed network coding) [21] denoted as NADNF has also been shown in this figure. It is assumed that the intruder uses QPSK modulation with gray mapping. The attack can occur with different ASRs. The threshold SNR is chosen as $\gamma_{\text{th}} = 2$-dB. Table 2 describes the simulation setup.

It is observed that the LLNC scheme outperforms the other three schemes. This superiority is small when compared to the ADNF scheme but is noticeable when compared to the AF scheme. The inferiority is due to the effect of MA interference, where users send their signal at the same time during the MA stage. This effect is the highest for the AF scheme, where the amplification of noise degrades the performance. For the ADNF scheme, at high SNRs, the CEP can be removed by removing the singular points, which results in a better performance than the NADNF scheme. Note that the two singular points 0 and ∞ are inevitable. This explains the effect of fading on the MA schemes. For the AWGN channel, however, PLNC outperforms the LLNC scheme [8]. Having said that, the time efficiency of the two time slot schemes makes the two PLNC schemes superior to the LLNC scheme in terms of end-to-end throughput.

Table 2 Simulation parameters

Attribute	Value
Number of symbols	1536×10^4
Attack to signal ratio (ASR)	$0.1 - 1$
Modulation scheme (users)	QPSK
Modulation scheme (intruder)	QPSK
Modulation scheme (relay)	QPSK/5QAM
γ_{th}	2 dB

Next, the results for the case when the intruder is inside the network is illustrated. The users experience a Rician fading (with a Rician Factor $K = 1$) and the intruder experiences a Rayleigh fading ($K = 0$). The performance comparison of the three schemes LLNC, ADNF, and AF with an intruder is illustrated in Fig. 5. The ASR varies between 0.1 and 1. The intruder attacks the relay in the first time slot for all the schemes. It can be seen that ASR directly affects the performance. Noting the fact that MA stage dominates the network performance, it can be seen that the relay is the most susceptible node inside the network. It can also be seen that as ASR increases, the performance of AF and LLNC schemes get closer towards each other. The ADNF scheme has the worst performance

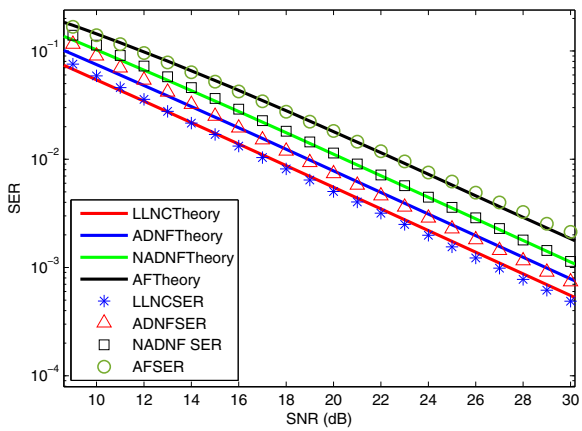

Fig. 4 SER comparison of the four schemes over Rician fading channel ($K = 1$)

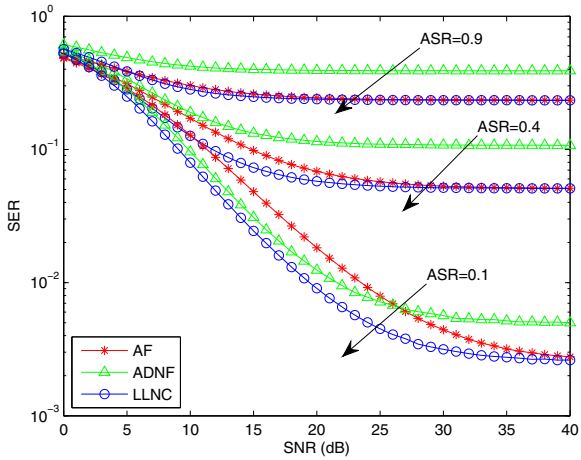

Fig. 5 SER comparison of the three schemes with an intruder with different ASRs

amongst all the other schemes. The reason behind this is the fact that the ADNF scheme uses denoising maps that are used for a network with two users and one relay. Since the relay is not aware of the intruder, it makes the estimates only based on the two users. Hence, the effect of intruder becomes much more visible. This is less severe for the AF and LLNC schemes, where the complexity of relay's operation is much less resulting in a less destructive attack. It can be inferred from the figure that for lower ASRs (ASRs < 0.1), the situation becomes different where the ADNF scheme performs better than AF. This is because the intruder becomes less destructive (lower power) and its effect on MA stage will be negligible. It should be noted that for a network with fading channels (mainly for wireless applications), regardless of an attack, the LLNC scheme performs better than all other schemes in terms of end-to-end SER.

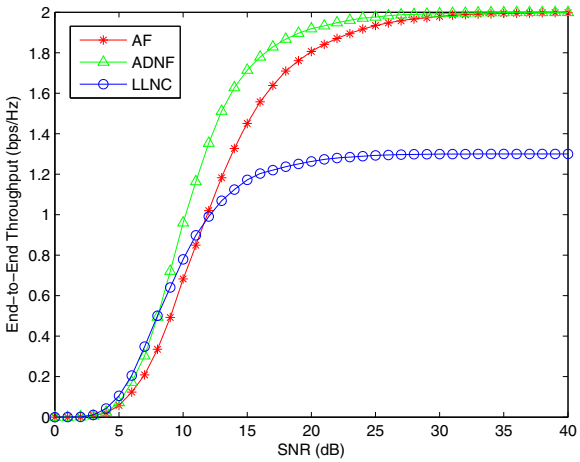

Fig. 6 End-to-end throughput of the three schemes with ASR = 0 (no attack)

4.2 Network coding-throughput analysis

Since the end-to-end throughput is an important parameter in evaluating the performance of the network, the results are demonstrated based on this factor as well. Throughput factors time into the account, which makes PLNC schemes more efficient than the LLNC. The data to be transmitted is encapsulated in a packet with the length of 256 symbols. A quasi-static slow-fading channel is assumed. The packet erasure model is being used, where the probability of successful transmission (or the probability that a packet is received successfully at the receiver) is defined as

$$P_{\text{success}} = P(\text{SNR} \geq \Theta), P_a = 0 \tag{64}$$

$$P_{\text{success}} = P(\text{SANR} \geq \Theta), P_a = 1 \tag{65}$$

where Θ is chosen to be 2 dB and SANR is defined as the average received signal to attack plus noise ratio as

$$\text{SANR} = \frac{P_s H_i^2}{P_I H_I^2 + \sigma^2}, i \in \{1, 2\} \tag{66}$$

As mentioned earlier, the intruder attacks the network in the first time slot. The three figures, Figs. 6, 7 and 8, show the end-to-end throughput for the three schemes with an intruder attacking the relay with different ASRs. It can be seen that ASR directly affects the performance. Another observation is the fact that when the ASR is below a certain threshold, the performance stays within a reasonable range and the throughput does not drop significantly. However, this would not be the case for the BC stage attack since the intruder only affects one of the nodes. These results do make sense due to the fact that all nodes are unaware of the presence of the intruder and the relay assumes that there are only two nodes present in the network. For ASRs $\geq$ 0.1, it can be seen that the AF scheme outperforms ADNF and LLNC schemes at high SNRs. The ADNF scheme also outperforms the LLNC scheme at high SNRs, if the ASRs are kept below a certain threshold. Note that the ADNF scheme uses the code-maps illustrated in Fig. 4 and Table I in [19], which are not the best code-maps for the situation, where a third user/intruder is present. In order to improve the performance of this scheme, either the code-maps need to be changed or the relay may use detection schemes to estimate the CSI to eliminate the intruder. In both cases, the relay does need to be aware of the intruder inside the network. One way to ensure this is to have the intruder attack with a high power. In practical cases, the intruder attacks with a low ASR (ASRs < 0.1) to remain undetectable. Therefore, the ADNF scheme will always outperform the AF and LLNC scheme at high SNRs for practical scenarios.

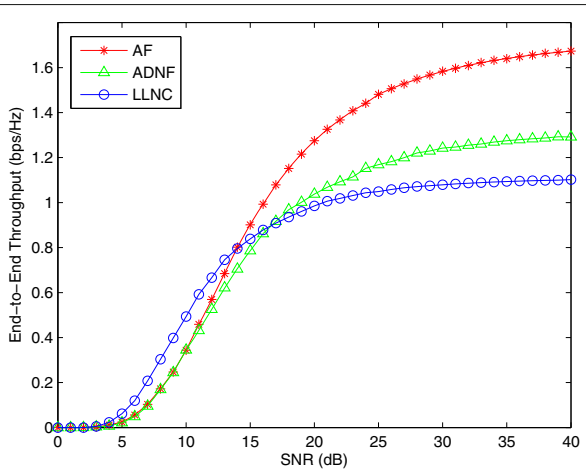

Fig. 7 End-to-end throughput of the three schemes with ASR = 0.5

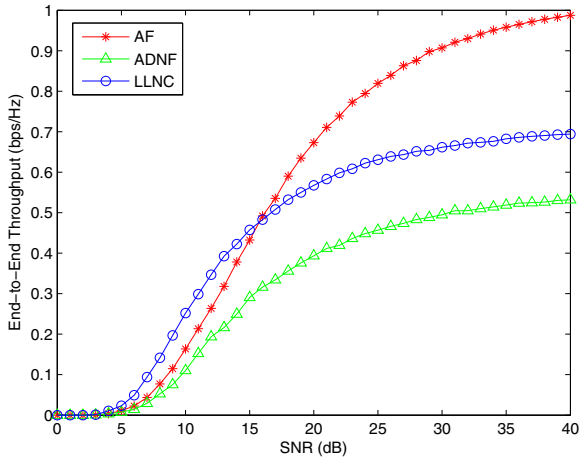

Fig. 8 End-to-end throughput of the three schemes with ASR = 1

4.3 Channel realization impact

So far, it is assumed that there is a direct LOS between the users and the relay node while the intruder's channel is subjected to Rayleigh fading. However, it is a common scenario, where the users can be a in dense environment, where there is no direct LOS between the users and the relay ($K = 0$). As it can be seen from Fig. 9, the overall throughput of the network degrades for the ADNF, AF, and LLNC schemes when compared to the case where the users experience a Rician fading. This performance degradation is more visible for the ADNF scheme. This is due to the fact that the performance improvement by 5-ary denoising becomes minimal at a low or zero Rician K-factor. That is, the optimized constellation mapping loses its efficiency in choosing the best network map to increase the minimum distance profile as K decreases. As the Rician K-factor increases ($K = 10$), the performance of the ADNF scheme improves significantly with a higher Rician K-factor (where there is a LOS) when compared to the AF scheme as explained in [19]. This can be observed in Fig. 10. However, due to the destructive nature of the attack and the design of the relay node, in the ADNF scheme, the performance falls below the AF scheme at high SNRs. In summary, the performance of the network does get impacted by the channel model and does degrade if the LOS disappears. However, the attack power is the dominant factor in the performance degradation.

5 Conclusions

In this work, the effects of pollution attack on the performance of the three schemes ADNF, AF, and LLNC at the physical layer are investigated. The analytical approximation results for the SER performance of the three schemes with and without an intruder have been illustrated as well. From an end-to-end SER perspective, it has been shown that LLNC scheme outperforms the ADNF and AF schemes regardless of the presence of the intruder. With the end-to-end throughput perspective, it has been shown that with an intruder in the network, and with reasonably high ASRs, the AF outperforms ADNF and LLNC schemes at high SNRs. It has also been observed that ADNF scheme does outperform the other schemes if the ASRs are kept low (for a realistic wireless environment). In order for the ADNF scheme to perform better, complexity of the system has to be increased, where the denoising maps need to be redesigned for a larger network. A future direction is to evaluate the network performance with a channel that experiences large-scale fading, where the distance between nodes (or the intruder) becomes an important factor in network behavior. One can evaluate other types of attacks. For instance, the intruder may use

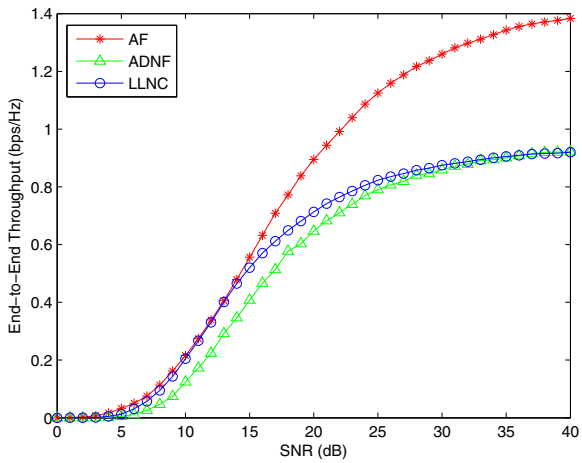

Fig. 9 End-to-end throughput of the three schemes with ASR = 0.5 under Rayleigh-Rayleigh fading

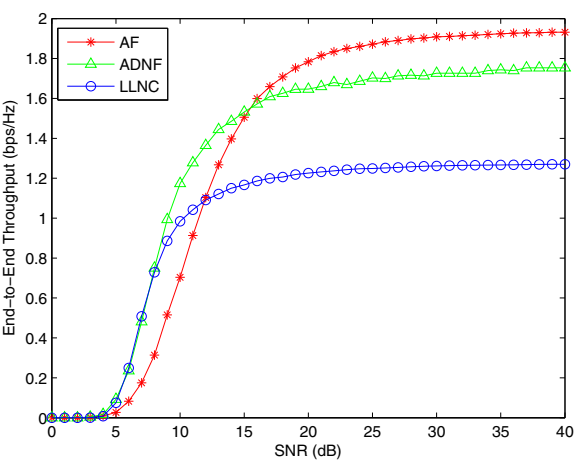

Fig. 10 End-to-end throughput of the three schemes with ASR = 0.5 under Rician-Rayleigh fading ($K = 10$)

other modulation schemes to attack the network. Appropriate counterattack schemes for this model are also left as a future work. One important future work that can lead us to an unsolved problem is when the relay is aware of the presence of an intruder. So far, the relay has only assumed that there are only two users in the network; therefore, the code-maps are designed accordingly. Although the intruder can not be considered a valid node, it gives us a good way of dealing with multiple nodes in the network and scaling up PLNC to multiple nodes.

Appendix

By inserting the PDFs of the two users in (53), (67) is derived, where $\bar{\gamma}_x$ and $\bar{\gamma}_y$ are the average received SNRs, and $I_0(.)$ is the zero-order modified Bessel function of the first kind [40].

$$P_1 \approx E_Z\left(\int_{2\gamma_{\text{th}}+z\gamma_{\text{th}}}^{\infty}\int_{y}^{\infty}\frac{(1+K)^2}{\bar{\gamma}_x\bar{\gamma}_y}e^{\left(-2K-\frac{(1+K)x}{\bar{\gamma}_x}-\frac{(1+K)y}{\bar{\gamma}_y}\right)} I_0\left(2\sqrt{\frac{K(1+K)x}{\bar{\gamma}_x}}\right)I_0\left(2\sqrt{\frac{K(1+K)y}{\bar{\gamma}_y}}\right)dxdy\right) \tag{67}$$

$$= E_Z\left(\frac{(1+K)^2e^{-2K}}{\bar{\gamma}_x\bar{\gamma}_y}\sum_{i=0}^{\infty}\sum_{j=0}^{\infty}\frac{(K\Delta_1)^i(K\Delta_2)^j}{(i!)^2(j!)^2}\int_{2\gamma_{\text{th}}+z\gamma_{\text{th}}}^{\infty}\int_{y}^{\infty}e^{-\Delta_1 x}e^{-\Delta_2 y}x^i y^j dxdy\right) \tag{68}$$

$$= E_Z\left(\frac{(1+K)^2e^{-2K}e^{-\gamma_{\text{th}}(z+2)(\Delta_1+\Delta_2)}}{\bar{\gamma}_x\bar{\gamma}_y}\sum_{i=0}^{\infty}\sum_{j=0}^{\infty}\sum_{k=0}^{i}\sum_{l=0}^{j+k}\frac{(K\Delta_1)^i(K\Delta_2)^j i!\,(j+k)!\,(\gamma_{\text{th}}(z+2))^l}{(i!)^2(j!)^2k!\,{\Delta_1}^{i-k+1}l!\,(\Delta_1+\Delta_2)^{j+k-l+1}}\right) \tag{69}$$

$$= \left(\frac{(1+K)^2e^{-2K}e^{-2\gamma_{\text{th}}(\Delta_1+\Delta_2)}}{\bar{\gamma}_x\bar{\gamma}_y\bar{\gamma}_z}\sum_{i=0}^{\infty}\sum_{j=0}^{\infty}\sum_{k=0}^{i}\sum_{l=0}^{j+k}\frac{{\gamma_{\text{th}}}^l(K\Delta_1)^i(K\Delta_2)^j(j+k)!}{(i!)(j!)^2k!\,{\Delta_1}^{i-k+1}l!\,(\Delta_1+\Delta_2)^{j+k-l+1}}\right) \times\int_0^{\infty}e^{\left(\frac{\gamma_{\text{th}}\bar{\gamma}_z(\Delta_1+\Delta_2)+1}{\bar{\gamma}_z}\right)}(z+2)^l dz \tag{70}$$

$$= \Delta_1\Delta_2e^{-2K}\sum_{i=0}^{\infty}\sum_{j=0}^{\infty}\sum_{k=0}^{i}\sum_{l=0}^{j+k}\frac{e^{\frac{2}{\bar{\gamma}_z}}{\gamma_{\text{th}}}^l\Delta_4^{-1-l}(K\Delta_1)^i(K\Delta_2)^j(j+k)!\,\Gamma(l+1,2\Delta_4)}{\bar{\gamma}_z i!\,(j!)^2k!\,l!\,{\Delta_1}^{i-k+1}\,(\Delta_3)^{j+k-l+1}} \tag{71}$$

$$P_{out} \approx 1-\left(2\Delta_1\Delta_2e^{-2K}\sum_{i=0}^{\infty}\sum_{j=0}^{\infty}\sum_{k=0}^{i}\sum_{l=0}^{j+k}\frac{e^{\frac{2}{\bar{\gamma}_z}}{\gamma_{\text{th}}}^l\Delta_4^{-1-l}(K\Delta_1)^i(K\Delta_2)^j(j+k)!\,\Gamma(l+1,2\Delta_4)}{\bar{\gamma}_z i!\,(j!)^2k!\,l!\,{\Delta_1}^{i-k+1}\Delta_3^{j+k-l+1}}\right) \tag{72}$$

$$\bar{P}_{eAF} \approx \frac{a}{2}-\left(\frac{\sqrt{a^2b}\Delta_1\Delta_2e^{-2K}}{\sqrt{\pi}}\right)\times\sum_{i=0}^{\infty}\sum_{j=0}^{\infty}\sum_{k=0}^{i}\sum_{l=0}^{j+k}\sum_{m=0}^{l}\frac{\bar{\gamma}_z^{l-m}2^m(K\Delta_1)^i(K\Delta_2)^j(j+k)!\,N^{-l-\frac{1}{2}}\Gamma(l+\frac{1}{2})\psi\left(l+\frac{1}{2},m+\frac{1}{2},\frac{b+2\Delta_3)}{N}\right)}{i!\,(j!)^2k!\,m!\,{\Delta_1}^{i-k+1}\Delta_3^{j+k-l+1}} \tag{73}$$

The exact closed form of (67) is unknown. However, by using the infinite-series representation of $I_0(.)$ in [43], Eq. (8.447.1), (67) can be further simplified. By letting $\Delta_1 = \left(\frac{1+K}{\bar{\gamma}_x}\right)$ and $\Delta_2 = \left(\frac{1+K}{\bar{\gamma}_y}\right)$, and after some algebraic manipulations, this integral is shown in (68). Using Eq. (3.351.2) in [43], (68) is further simplified to (69). Recall that $Z = \frac{P_I|H_I|^2}{\sigma^2}$, and the intruder experienced a Rayleigh fading, which is exponentially distributed [39] and is expressed as

$$f_Z(z) = \frac{1}{\bar{\gamma}_z}e^{-\frac{z}{\bar{\gamma}_z}} \tag{74}$$

After inserting (74) into (69), and using Eq. (3.382.4) in [43], and after some algebraic manipulations, the integration with respect to z results in (71), where $\Delta_3 = \Delta_1+\Delta_2$, $\Delta_4 = \frac{\gamma_{\text{th}}\bar{\gamma}_z\Delta_3+1}{\bar{\gamma}_z}$, and $\Gamma(.,.)$ is the complementary incomplete gamma function defined in [43], Eq. (8.350.2). The outage probability can be written as (71). By inserting (72) into (42), applying Eq. (3.383.5) in [43], and applying rigorous algebraic manipulation, the average SER of the network can be expressed as (73). Here, $\psi(.,.,.)$ is the Tricomi confluent hypergeometric function as defined in [43], Eq. (9.211.4), and $N = \bar{\gamma}_z\Delta_3$. This completes the proof.

Competing interests
The authors declare that they have no competing interests.

Received: 6 December 2015 Accepted: 7 December 2016
Published online: 03 January 2017

References

1. MO Hasna, M-S Alouini, End-to-end performance of transmission systems with relays over rayleigh-fading channels. IEEE Trans. Wirel. Commun. **2**(6), 1126–1131 (2003)
2. GK Karagiannidis, TA Tsiftsis, RK Mallik, Bounds for multihop relayed communications in Nakagami-m fading. IEEE Trans. Commun. **54**(1), 18–22 (2006)
3. R Ahlswede, N Cai, S Li, R Yeung, Network information flow. IEEE Trans. Inf. Theory. **46**(4), 1204–1216 (2000)
4. S-YR Li, RW Yeung, N Cai, Linear network coding. IEEE Trans. Inf. Theory. **49**(2), 1204–1216 (2003)

5. A Khreishah, IM Khalil, P Ostovari, J Wu, Flow-based XOR network coding for lossy wireless networks. IEEE Trans. Wirel. Commun. **11**(6), 2321–2329 (2012)
6. MH Amerimehr, F Ashtiani, Delay and throughput analysis of a two-way opportunistic network coding-based relay network. IEEE Trans. Wirel. Commun. **13**(5), 2863–2873 (2014)
7. S Katti, H Rahul, W Hu, D Katabi, M Medard, J Crowcroft, XORs in the air: practical wireless network coding. IEEE/ACM Trans. Netw. **16**(3), 497–510 (2008)
8. S Zhang, S-C Liew, P Lam, Physical-layer network coding. ACM MobiCom, 358–365 (2006)
9. P Popovski, H Yomo, in *2006 IEEE International Conference on Communications (ICC)*. The anti-packets can increase the achievable throughput of a wireless multi-hop network (IEEE, 2008), pp. 3885–3890. doi:10.1109/ICC.2006.255688
10. J Dong, R Curtmola, R Sethi, C Nita-Rotaru, in *2008 Workshop on Secure Network Protocols 2008 (NPSecE)*. Toward secure network coding in wireless networks: Threats and challenges (IEEE, 2008), pp. 33–38. doi:10.1109/NPSEC.2008.4664878
11. J Dong, R Curtmola, C Nita-Rotaru, in *2009 Proceedings of the Second ACM Conference on Wireless Network Security*. Practical defenses against pollution attacks in intra-flow network coding for wireless mesh networks (ACM, 2009), pp. 111–122. doi:10.1145/1952982.1952989
12. M Krohn, M Freedman, D Mazieres, in *2004 IEEE Security and Privacy*. On-the-fly verification of rateless erasure codes for efficient content distribution (IEEE, 2004), pp. 226–240. doi:10.1109/SECPRI.2004.1301326
13. D Charles, K Jain, K Lauter, in *40th Annual Conference on Information Sciences and Systems*. Signatures for network coding (IEEE, 2006), pp. 857–863. doi:10.1109/CISS.2006.286587
14. Z Yu, Y Wei, B Ramkumar, Y Guanr, in *Proceedings of INFOCOM 08*. An efficient signature-based scheme for securing network coding against pollution attacks (IEEE, 2008), pp. 1409–1417. doi:10.1109/INFOCOM.2008.199
15. F Zhao, T Kalker, M Medard, K Han, in *Proc. of ISIT*. Signatures for content distribution with network coding (IEEE, 2007), pp. 556–560. doi:10.1109/ISIT.2007.4557283
16. SW Kim, in *Communcation Society Conference of Sensor, Mesh and Ad Hoc Communications and Networks. IEEE*. Integrated detection and mitigation of pollution attack in wireless network coding: physical layer approach (IEEE, 2012), pp. 97–99. doi:10.1109/SECON.2012.6276359
17. S Kim, SW Kim, Recycling polluted packet at the physical layer in wireless network coding. IEEE Commun. Lett. **17**(5), 856–859 (2013)
18. Z Li, D Pu, W Wang, A Wyglinski, in *2010 IEEE GLOBECOM*. Node localization in wireless networks through physical layer network coding (IEEE, 2010), pp. 1–5. doi:10.1109/GLOCOM.2010.5684085
19. T Koike-Akino, P Popovski, V Tarokh, Optimized constellations for two-way wireless relaying with physical network coding. IEEE J. Sel. Areas. Commun. **27**(5), 773–787 (2009)
20. V Namboodiri, VT Muralidharan, BS Rajan, in *Proc. IEEE WCNC*. Wireless bidirectional relaying and latin squares (IEEE, 2012), pp. 1404–1409. doi:10.1109/WCNC.2012.6214000
21. VT Muralidharan, BS Rajan, Performance analysis of adaptive physical layer network coding for wireless two-way relaying. IEEE Trans Wirel Commun. **12**(3), 1328–1339 (2013)
22. B Nazer, M Gastpar, Compute-and-forward: harnessing interference through structured codes. IEEE Trans Inf Theory. **57**(10), 6463–6486 (2011)
23. W Nam, SY Chung, YH Lee, Capacity of the Gaussian two-way relay channel to within 1/2 bit. IEEE Trans Inf Theory. **56**(11), 5488–5494 (2010)
24. B Rankov, A Wittneben, in *2006 Proc Int Symp Inf Theory*. Achievable rate regions for the two-way relay channel. (IEEE), pp. 1668–1672. doi:10.1109/ISIT.2006.261638
25. M Ghogho, A Swami, in *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. Characterizing physical-layer secrecy with unknown eavesdropper locations and channels (IEEE, 2011), pp. 3432–3435. doi:10.1109/ICASSP.2011.5947123
26. MC Valenti, D Torrieri, T Ferrett, Noncoherent physical-layer network coding with FSK modulation: Relay receiver design issues. IEEE Trans. Commun. **59**(9), 2595–2604 (2011)
27. L Lu, S-C Liew, Asynchronous physical-layer network coding. IEEE Trans. Wirel. Commun. **11**(2), 819–831 (2012)
28. C Popper, NO Tippenhauer, B Danev, S Capkun, in *2011 16th European Symposium on Research in Computer Security (ESORICS)*. Investigation of signal and message manipulations on the wireless channel (Springer ESORICS, 2011), pp. 40–59. doi:10.1007/978-3-642-23822-2_3
29. S Katti, S Gollakota, D Katabi, in *2007 Proc. ACM SIGCOMM*. Embracing wireless interference: analog network coding (ACM SIGCOMM, 2007), pp. 397–408. doi:10.1145/1282427.1282425
30. W Xu, in *2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking Services (MobiQuitous)*. On adjusting power to defend wireless networks from jamming (IEEE, 2007), pp. 1–6. doi:10.1109/MOBIQ.2007.4451072
31. RM Legnain, RHM Hafez, ID Marsland, BER analysis of three-phase XOR-and-forward relaying using Alamouti STBC. IEEE Commun. Letters. **16**(9), 1458–1461 (2012)
32. L Yang, K Qaraqe, E Serpedin, M-S Alouini, Performance analysis of amplify-and-forward two-way relaying with co-channel interference and channel estimation error. IEEE Trans. Commun. **61**(6), 2221–2231 (2013)
33. P Popovski, H Yomo, in *2006 IEEE 63rd Vehicular Technology Conference*. Bi-directional amplification of throughput in a wireless multi-hop network (IEEE, 2006), pp. 588–593. doi:10.1109/VETECS.2006.1682892
34. P Popovski, H Yomo, in *2007 IEEE International Conference on Communications*. Physical network coding in two-way wireless relay channels (IEEE, 2007), pp. 707–712. doi:10.1109/ICC.2007.121
35. K Yasami, A Razi, A Abedi, Analysis of channel estimation error in physical layer network coding. IEEE Commun. Let. **15**(10), 1029–1031 (2011)
36. K Yasami, A Abedi, in *2011 Proc. IEEE CCNC*. Effect of channel estimation error on performance of physical layer network coding. (IEEE), pp. 751–752. doi:10.1109/CCNC.2011.5766656
37. T Koike-Akino, P Popovski, V Tarokh, in *2009 IEEE International Conference on Communications (ICC)*. Denoising strategy for convolutionally-coded bidirectional relaying (IEEE, 2009), pp. 1–5. doi:10.1109/ICC.2009.5198893
38. J Liu, M Tao, Y Xu, Pairwise check decoding for LDPC coded two-way relay block fading channels. IEEE Trans. Commun. **60**(8), 2065–2076 (2012)
39. JG Proakis, *Digital Communication*. (McGraw-Hill, NewYork, 2001). Fourth Edition
40. MK Simon, M-S Alouini, *Digital Communication over Fading Channels*. (Wiley, New Jersey, 2004). Second Edition
41. K Lu, S Fu, Y Qian, T Zhang, in *IEEE International Conference on Communications, 2009. ICC'09*. On the security performance of physical-layer network coding (IEEE, 2009), pp. 1–5. doi:10.1109/ICC.2009.5199266
42. HA Suraweera, HK Garg, A Nallanathan, Performance analysis of two hop amplify-and-forward systems with interference at the relay. IEEE Commun. Let. **14**(8), 692–694 (2010)
43. IS Gradshteyn, IM Ryzhik, *Table of Integrals, Series, and Products*. (Academics, San Diego, 2000). Sixth edition
44. X Xu, Y Cai, C Cai, W Yang, in *2011 Proc. IEEE WCSP*. Overall outage probability of two-way amplify-and-forward relaying in Nakagami-m fading channels (IEEE, 2011), pp. 1–4. doi:10.1109/WCSP.2011.6096817