KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 6 (2020) 104–108

www.elsevier.com/locate/icte

Secure transmission in an unfriendly environment

Lukman A. Olawoyin[a,*], Nasir Faruk[a], Abdulkarim A. Oloyede[a], Segun I. Popoola[b,c], Temitayo C. Adeniran[a], Nazmat T. Surajudeen-Bakinde[d], Abubakar Abdulkarim[e]

[a] *Department of Telecommunication Science, University of Ilorin, Nigeria*
[b] *Department of Engineering, Manchester Metropolitan University, M1 5GD, Manchester, UK*
[c] *Department of Electrical and Information Engineering, Covenant University, Ota, Nigeria*
[d] *Department of Electrical and Electronics Engineering, University of Ilorin, Nigeria*
[e] *Department of Electrical Engineering, ABU, Zaria, Nigeria*

Received 17 May 2019; accepted 8 September 2019
Available online 1 October 2019

Abstract

This work investigates and show the performance of destination assisted node in ensuring secure communication in a dual-hop broadcast system. The information transmission occurs between the transmitters which are assumed to be equipped with single antenna through a number of intermediate untrusted relays to the receiver in the presence of multiple passive eavesdroppers. This work assumes that there is no direct link between the transmitter and the receiver and hence, the relay node, receives either the information or noise signal at every transmission processes. Since the transmission occurs in a two-phase, the legitimate receiver is contributing a degrading noise to both the eavesdropper and relay node channels during the first phase while it receives information from the transmitter through the relay during the second phase. Simulation results are used to illustrate the performance of the proposed scheme.
© 2020 The Korean Institute of Communications and Information Sciences (KICS). Publishing services by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Keywords: Artificial noise; Full-duplex; Secure transmission; Average secrecy capacity; Secure outage probability

1. Introduction

Wireless communication has become the common means of transmitting information signal from the transmitter to the receiver(s) in recent times due to its ubiquitous, openness in nature and constant availability. Leveraging on this property, it is very easy for unintended receiver to have access to transmitted signal(s) in terms of eavesdropping or interception which leads to compromise the security, integrity and privacy of the transmitted signal(s). Security in wireless system had been traditionally achieved by cryptographic approaches which are usually implemented at the upper layer of open system interconnect (OSI) [1]. However, various research efforts had shown that the use of cryptographic method leverages on the computational power of the eavesdropper which usually proved not effective if the eavesdropper has high computational power which can give it the ability to obtain channel information about the transmitted signal, and hence information secrecy is compromised. Due to fading nature of wireless channel, signals transmitted over the wireless medium undergo severe signal degradations during the transmission from the source to the respective receiver. Leveraging on this property, the use of physical layer approaches helps achieve a secure communication in wireless broadcast channel.

The author in [2] introduced the concept of wire-tap channel where it was shown that secret communication in wireless broadcast system is attainable if the channel capacity of the main receiver is higher than the channel capacity of the eavesdropper. This study relies on information-theoretic approach where coding and signal processing technique are used to achieve system secrecy [3,4] (and references therein) to achieve information security in wireless system. The various approaches of using Artificial Noise (AN) as jamming signal to secure information transmission in broadcast wireless system by degrading the eavesdropper channel had been discussed by [5,6]. The use of cooperative communication which involves the use of relay node that helps to retransmit information between the source and the legitimate receiver had

* Corresponding author.
E-mail address: olawoyin.la@unilorin.edu.ng (L.A. Olawoyin).
Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2019.09.001
2405-9595/© 2020 The Korean Institute of Communications and Information Sciences (KICS). Publishing services by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

been discussed by several authors and it was shown that the secrecy increases with the relay node but there is problem of increase in system complexity and power consumption. Shuiyin et al. [5] and many authors had studied the physical-layer security in the presence of external eavesdroppers that are different from the relay which tried to intercept the communication between the source and the receiver. The concept of untrusted node was considered in the case of defense system, financial application, and government intelligence networks, where some privilege information has be shared among few nodes in the entire system. This can also be found in ad hoc network where communication is only expected between certain nodes in the network. In this case, the relaying node, being from different network, may be considered untrusted [7]. Kalamkar et al. [8] had equally shown that communication via an untrusted relay can be beneficial for the relay channel with orthogonal components while it was shown that the positive secrecy rate is achievable with the destination assisted jamming, where the destination sends jamming signals during the source–relay communication. Untrusted relay scheme was discussed by [5] where the relay node acts as both the helper and eavesdropper while the authors in [6] proposed the use of beamforming technique and AN to achieve secure communication in two-hop systems. The AN is used to impair the Eve's channel while the receiver is not affected by the noise since there is orthogonal projection between the transmitter to the legitimate receiver's channel. All the proposed schemes have a major challenge since the CSI of the receiver must be known to the transmitter which leads to additional bandwidth and power consumption since there is need for a feedback information from the receiver to the transmitter so as to estimate its channel. Also, in case of imperfect channel estimation, AN signal may leak to the receiver's channel which will lead to reduction in its SNR

In cooperative jamming, the performance of the system is highly dependent on the jamming strategy as well as the power allocation level at the different nodes. For instance, in a low state jamming power the amount of noise reaching an eavesdropper will be too low to have a degrading effect which will make secure communication venerable to attack. Also, if the transmit power of the relay node is very high, the possibility of AN leakage to the destination node is very high [9]. Also, authors in [10,11] proposed an approach where both the relay and jammer are powered by source transmission. In the work, the authors observed that as the jammer gets closer to the information source, the average secrecy rate first increases and then decreases, this shows that the jammer can cause a stronger interference but with the adequate power allocation from the relay will ensure adequate security. The authors in [12–14] introduced the use of power splitting relay (PSR) and time switching relay (TSR) technique to achieve more secure and robust communication. It was observed that PSR achieves greater secrecy capacity more than TSR when the channel condition is unfavorable to the eavesdropper for wiretapping.

In this work, a confidential message to be exchanged between the transmitter and legitimate receiver through multiple relay nodes is considered assuming that no link existed between the transmitter and the receiver. In order to address this problem, a dual-hop transmission between the transmitter and the receiver is used where during the first-hop transmission, the receiver node generates an AN from its terminal node and broadcast which can be received by all the relay nodes and the eavesdropper but transmitter (no direct transmission) since all the relay nodes are considered as potential eavesdropper while during the second-hop transmission, the transmitter transmits information signal which is conveyed to the receivers through the intermediate relay nodes. More so, we consider the optimal power allocation at each of the relay node to maximize the end-to-end achievable rate. Our focus is to optimize the channel between the relay and the destination node. The benefit is to achieve a more secure transmission in such a way that the potential eavesdropper will be experiencing a corrupted signal at every transmission processes. Considering the foregoing information, we can observe from this work that it has some advantages over the conventional uses of AN which includes (a) the CSI of the eavesdropper is not required at the transmitter since there is no direct link between transmitter and receiver, (b) single antenna is enough at the transmitter since the degrading noise is generated by the receiver (c) the AN cannot be completely removed by Eve even if eavesdropper is close to transmitter.

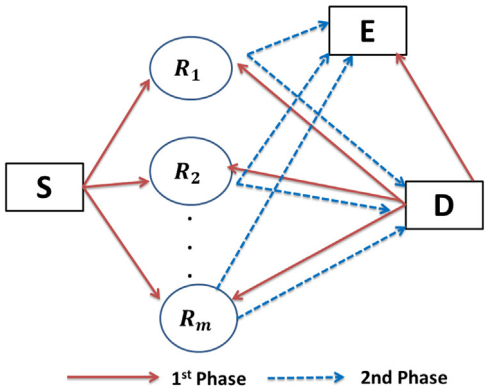


Fig. 1. The system model for two-hop untrusted relay network.

The rest of this paper is organized as follows. Section 2 introduces the system model and performance analysis is introduced in Section 3. Section 4 presents the numerical results and the paper is concluded in Section 5.

2. System model

In a simple dual-hop cellular system that comprises of broadcast and medium access control (MAC) as shown in Fig. 1, where the information source (S) is communicating a confidential message with a destination node (D) through the number of M untrusted intermediary relay nodes i.e. $M = \{R_1, R_2, \ldots, R_M\}$ in the presence of a passive eavesdropper (E) whose intention is to intercept the transmitted signal between S and D. It is assumed that all the nodes involved in the system model are equipped with single antenna and they assumed to be operating in half duplex mode i.e. the relay

receives during the first-phase and transmits during the second-phase. In order to ascertain the effect of relay node, we assume that there is no direct link between the information source, destination node and eavesdropper. The channel between node a and node b where $a, b \in \{S, D, E, R_1\}$ is denoted by $h_{a,b}$ and is modeled as complex Gaussian variable with zero mean and variance σ^2 i.e. $(0, \sigma^2)$. All $\{h_{ab}\}$ are mutually independent and remain constant within one frame and vary independently from one frame to another frame. The channels are assumed to be symmetrical and reciprocal, i.e. $h_{ab} = h_{ba}$. The additive noise at each receiver is modeled as independent and identically distributed (i.i.d.) complex Gaussian variables distributed as $\mathcal{CN}\left(0, \sigma^2\right)$. The instantaneous CSI of each channel is locally known to the receiver and is also known to the transmitter by the channel reciprocity technique. However, the instantaneous channel state information (CSI) about the eavesdropper channel. $h_{\{E,R_i\}}, h_{\{D,R_i\}}$ is unknown to source, relay and destination nodes since the passive eavesdropper never transmits any signal so as not to remain anonymous. The local CSI known to each node is not shared with other nodes except that each relay node should report scaling factors β defined latter in the text to D. Since there is no interface between relay nodes to share signals and local CSIs, and the CSI of the eavesdropper link is unavailable, the multiple relay nodes cannot cooperate in unveiling the transmitted source message, precoding the signal so as to maximize the secrecy capacity, or jointly transmitting AN has no impact on destination node. In this approach, we also assumed that there is no common jamming signals or seeds of random noise generator that are known both for source and destination.

In this dual-hop scheme, to achieve a secure transmission, S first broadcasts information signal x with zero mean and power P_s which is denoted as $x \sim \mathcal{CN}(0, P_S)$ to all relay nodes, where $P_S = \mathbb{E}\left[|x|^2\right]$ is the transmit power at the transmitter. At the same time, D broadcasts an artificial noise $w \sim \mathcal{CN}(0, P_D)$ simultaneously. We assume that w is independent with x.

3. Performance analysis

In this, to achieve a secure transmission, S first broadcasts information signal x with zero mean and power P_s which is denoted as $x \sim CN(0, P_S)$ to all relay nodes, where $P_S = \mathbb{E}\left[|x|^2\right]$ is the transmit power at the transmitter. Also, D broadcasts an AN $w \sim CN(0, P_D)$ simultaneously. We assume that is independent with s. The signals received by the relay node and eavesdropper during this transmission phase can be written, respectively, as

$$y_i = h_{S,R_i} x + h_{D,R_i} w + n_{R_i}. \quad i = 1, 2, \ldots, M \tag{1}$$

$$y_E^1 = h_{DE}^T w + n_E^1 \tag{2}$$

where $n_{R_i}, n_E^{(1)} \sim CN(0, \sigma^2)$ are the additive noises. $h_{S,R}$, $h_{D,R}$ and $h_{D,E}$ are the channel coefficient between source and relay, destination node and relay, and destination node and eavesdropper. On the other hand, in the second transmission phase, when the relay node employs AF protocol to retransmit the signal to $h_{D,E}$ and E, each of the relays $R_i, i = 1, 2, \ldots, M$ transmit $x_i = \beta_i y_i + z_i$ where

$$\beta_i = e^{-j\left(\varphi_{S,R_i} + \varphi_{D,R_i}\right)} \times \sqrt{P_R - P_i} \Big/ \sqrt{P_S \left|h_{S,R_i}\right|^2 + P_D \left|h_{D,R_i}\right|^2 + \sigma^2} \tag{3}$$

Where $\varphi_{S,R_i} = \angle h_{S,R_i}$ are the phases between source and relay, and destination and relay, respectively. $P_S = \mathbb{E}\left[|z_i|^2\right]$ is the power of the artificial noise z_i, P_R is the individual power constraint of each relay nodes. Assume that R_i will broadcast β_i to D. It was assumed that $\varphi_{S,R_i}, \varphi_{D,R_i}$ are i.i.d variables uniformly distributed over $(0, 2\pi)$, and that is the Box–Muller transform of $(\varphi_{S,R_i}, \varphi_{D,R_i})$, then $z_i \sim CN(0, P_i)$. The power of z_i is determined by

$$P_i = P_z \cdot \min\left(1, |h_{D,R_i}|^{-2}\right) \tag{4}$$

where P_z is the maximum power allocated to Z_i. When the link quality $R_i \to D$ is relatively better, more power will be used for forwarding y_i. Similarly, in this transmission phase, the signal received by D is expressed as

$$y_D = \sum_{i=1}^{M} h_{D,R_i} \left(\beta_i y_i + z_i\right) + n_D \tag{5}$$

$$y_D = \alpha_x^D x + \alpha_w^D w + \sum_{i=1}^{M} h_{D,R_i} z_i + \sum_{i=1}^{M} \beta_i h_{D,R_i} n_{R_i} + n_D \tag{6}$$

where $n_D \sim CN(0, \sigma^2)$ is the additive noise, $\alpha_x^D = \sum_i \beta_i h_{S,R_i} h_{D,R_i}$, and $\alpha_w^D = \sum_i \beta_i h_{D,R_i}^2$ are known to D. In addition, D can retrieve φ_{S,R_i} from β_i and hence it can reconstruct Z_i. Therefore, the AN $\alpha_w^D w$, $\sum_{i=1}^{M} h_{D,R_i} z_i$ can be removed by interference cancellation.

Similarly, the signal received by the eavesdropper during the 2nd phase can be expressed as

$$y_E^{(2)} = \alpha_x^E x + \alpha_w^E w + \sum_{i=1}^{M} h_{E,R_i}^T z_i + \sum_{i=1}^{M} \beta_i h_{E,R_i}^T n_{R_i} + n_E^{(2)} \tag{7}$$

where $n_E^{(2)} \sim CN(0, \sigma^2)$ is the additive noise. Also, $\alpha_x^E = \sum_i \beta_i h_{S,R_i} h_{E,R_i}$, and $\alpha_w^E = \sum_i \beta_i h_{D,R_i} h_{E,R_i}$. It is worth noting that the eavesdropper can obtain an estimation of w from the signal it has received during the first phase, i.e. y_E^1 in (2). Taking this estimated w as pilot signal, eavesdropper can also blindly estimate α_w^E. Therefore, we may reasonably assume that the eavesdropper can partially cancel the interference term α_w^E.

Considering worst-case scenario, we also assume that this term has been canceled completely. The effective received signal at the eavesdropper is defined as

$$\tilde{y}_E^{(2)} = \alpha_x^E x + \sum_{i=1}^{M} h_{E,R_i} (z_i + \beta_i n_{R_i}) + n_E^{(2)}. \tag{8}$$

From the foregoing, power can be optimally allocated P_S, P_D, P_R and P_Z in order to achieve best secrecy performance, but for the reason of simplicity, we assume equal power allocation among all the nodes and set $P_s = P_D = P_R = P$, $P_Z = P/2$.

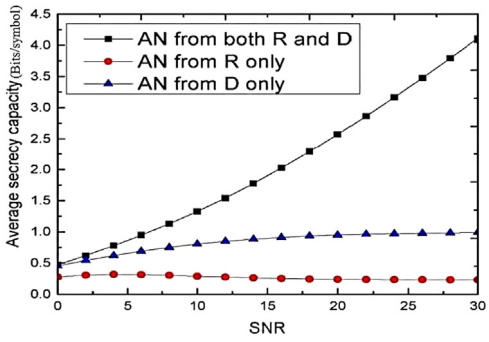


Fig. 2. The average secrecy capacity.

From (5), (7) and (1), the instantaneous SNR at D, E and R_i can be written as

$$\gamma_D = \bar{\gamma} \cdot \left|\alpha_x^D\right|^2 \Big/ \sum_{i=1}^{M} |\beta_i h_{D,R_i}|^2 + 1 \tag{9}$$

$$\gamma_E = \bar{\gamma} \cdot \left|\alpha_x^E\right|^2 \Big/ \sum_{i=1}^{M} \left(\frac{P_i}{\sigma^2} + |\beta_i|^2\right) |h_{E,R_i}|^2 + 1 \tag{10}$$

$$\gamma_i = \bar{\gamma} \cdot |h_{S,R_i}|^2 \big/ \bar{\gamma} |h_{D,R_i}|^2 + 1. \quad i = 1, 2, \ldots, M \tag{11}$$

where $\bar{\gamma} = P/\sigma^2$. The secrecy capacity and the secrecy outage probability can be written as

$$C_s = \frac{1}{2}(\log(1 + \gamma_D/1 + \gamma))^+, \tag{12}$$

$$P_{out} = \Pr\{C_s < R_s\} = \Pr\{(1 + \gamma_D/1 + \gamma) < \gamma_{th}\} \tag{13}$$

where $\gamma = \max\{\gamma_E, \gamma_1, \gamma_2, \ldots, \gamma_M\}$, $(a)^+ = \max(a, 0)$, $\gamma_{th} = 2^{2R_s}$ is the threshold SNR

4. Numerical results

For simplicity, we assume that all links have the same average channel gain, i.e. $h_{ab} = 1, \forall a, b \in \{S, D, E, R_i\}$. The average secrecy capacity and secrecy outage probability are used to evaluate the performance of two-hop scheme. In Fig. 2, we assume that 10 numbers of intermediate relay nodes were used while the transmission rate is assumed to be 0.2 bits/s/Hz, it was found that the overall system secrecy performance improves considerably. Furthermore, it can be seen that when only the relay node transmits AN to E node the secrecy performance achieved is relatively lower as compared to when D only transmits. This can be explained as E closes to D more than relay terminal while at the same time D did not contribute any additional noise to degrade the eavesdropper channel. The performance increases considerably when relay node and D are in jointly contribute AN transmission. This shows that even with untrusted relay terminal, information secrecy is obtained when D terminal contributes additional noise. Fig. 3 is the secrecy outage probability (SOP) curve, the curve shows the degree of impossibility for E to intercept the hidden transmitted codewords as the number of noise sources increases.

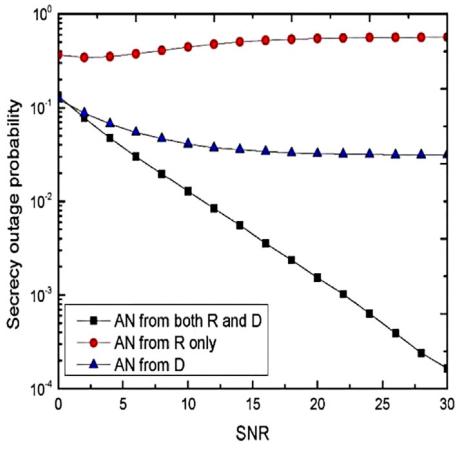


Fig. 3. The secrecy outage probability.

5. Conclusion

In this work, we examined the performance of using destination assisted node to achieve secure communication in broadcast system with untrusted relay node. The numerical results obtained show that secure communication is possible in such situation when the destination node contribute noise signal to degrade the signal quality of the relay node and equally has the capacity to remove its own self-interference signal.

Declaration of competing interest

The authors declare that there is no conflict of interest in this paper.

References

[1] F. Lisheng, Y. Nan, D. Trung, E. Maged, K. George, Exploiting direct links for physical layer security in multiuser multirelay networks, IEEE Trans. Wirel. Commun. 15 (6) (2016) 3856–3867.
[2] B. Mandal S. Chandra, S. Alam, S. Patra, comparative and analytical study on symmetric key cryptography, Intern. Conf. Electro. Comm. and Comput. Eng. (ICECCE), Hosur, (2014) 131-136.
[3] A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 31, (4) 1355-1387.
[4] C. Xiaoming, Z. Caijun, Y. Chau, C. Hsiao-Hwa, Multi-antenna relay aided wireless physical layer security, IEEE Commun. Mag. 58 (2015) 40–46.
[5] L. Shuiyin, H. Yi, E. Viterbo, Practical secrecy using artificial noise, IEEE Commun. Lett. 17 (7) (2007) 1483–1486.
[6] Y. Liu, L. Wang, T. Duy, M. Elkashlan, Q. Duong, Relay selection for security enhancement in cognitive relay networks, IEEE Wirel. Commun. Lett. 4 (1) (2015) 46–49.
[7] X. Chen, J. Chen, T. Liu, Secure transmission in wireless powered massive MIMO relaying systems: Performance analysis and optimization, IEEE Trans. Veh. Commun. 65 (10) (2016) 8025–8035.
[8] S. Kalamkar, A. Banerjee, Secure Communication via a Wireless Energy Harvesting Untrusted Relay, IEEE Trans. Veh. Tech. 66, (3) 2199-2213.
[9] Z. Ahmed, Y. Aylin, The two-hop interference untrusted-relay channel with confidential messages, IEEE Infor. Theo. Worksh, Jeju, 2015 1-6.
[10] X. He, A. Yener, Two-Hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming, IEEE Global Telecommunication Conference. New Orleans, 2008, 1-5.

[11] X. Gong, L. Hong, Y. Hao, D. Feihong, R. Baoquan, Robust amplify-and-forward relay beamforming for security with mean square error constraint, IET Commun. 9 (5) (2015) 1081–1087.

[12] L. Jiang, C. Qin, X. Zhang, H. Tian, Secure beamforming design for SWIPT in cooperative D2D communications, Chin. Commun. 14 (1) (2017) 20–33.

[13] D. Wang, P. Ren, J. Cheng, Cooperative secure communication in two-hop buffer-aided networks, IEEE Trans. Commun. 66 (3) (2018) 972–985.

[14] X. Liu, Z. Li, C. Wang, Secure decode-and-forward relay swipt systems with power splitting schemes, IEEE Trans. on Veh. Commun. 67 (8) (2018) 7341–7354.