Secure Communication via Untrusted Switchable Decode-and-Forward Relay

Haji M. Furqan*, Jehad.M. Hamamreh*, Huseyin Arslan*§
*School of Engineering and Natural Sciences, Istanbul Medipol University, Istanbul, Turkey, 34810
§Department of Electrical Engineering, University of South Florida, Tampa, FL, 33620
Email: {hamadni, jmhamamreh}@st.medipol.edu.tr, arslan@usf.edu

***Abstract*—In this paper, a practical power efficient technique is proposed for an untrusted decode-and-forward (DAF) based cooperative communication system to provide secure communication between the source and the destination. More specifically, a DAF relay, called switchable DAF (sDAF), is designed in such a way that it can be switched to amplify-and-forward (AAF) in certain predefined situations. The algorithm is based on destination-assisted jamming and comprised of two phases. The first phase securely shares the random manipulating sequence (RMS) through an untrusted relay, while the second phase uses this RMS for secure communication through untrusted relay. This algorithm not only provides secrecy, but also enhances the power efficiency as compared to other destination-assisted jamming techniques.**

***Index Terms*—Phy-security, jamming, untrusted relay, secure DAF**

I. Introduction

Due to the advantages of wireless communication over wired communication, wireless-based applications are becoming extremely pervasive in our daily life. Furthermore, with the advancement in high data-rate-based applications, the demand for bandwidth and power efficient transceivers is continuously increasing [1]. To this end, cooperative communication is a suitable candidate for providing bandwidth efficient transceivers, especially for handheld devices. More precisely, amplify-and-forward (AAF) and decode-and-forward (DAF) are the most popular techniques of cooperative communications [2]. In [3], the authors presented hybrid relaying scheme for Orthogonal Frequency Division Multiplexing (OFDM) system, which takes benefits of both DAF and AAF relaying by adaptively switching among AAF, DAF and non-relay modes on subcarrier basis. Although AAF and DAF are popularly used schemes in the literature, they have some problems related to noise enhancement and error propagation. These problems can be overcome by using efficient channel coding schemes [2], [4] such as convolutional encoding with Viterbi decoding [5], [6].

In addition, the security aspect of wireless communication is one of the most critical issues due to the broadcast nature of wireless communication [7]. The use of wireless communication for sharing sensitive information (e.g. financial transactions, personal information, etc.) makes security one of the most critical requirements for the current and future wireless systems [7]. Conventional techniques for security have mainly focused on cryptography but the key's establishment and management are very complex tasks in modern decentralized networks [8]. In order to solve this issue, the research on physical layer security (PLS) has drawn a lot of interest because of its ability to solve the challenges offered by the conventional cryptographic-based security techniques. The PLS techniques are capable of providing confidentiality by utilizing the impairments of wireless channel, such as noise, fading, interference, etc. [7], [8].

This study concerns about PLS techniques for cooperative communication systems. There is a variety of such PLS techniques [8], such as PLS-based secret key generation using relays [9], relay-based beamforming for PLS with and without cooperative jamming [10], relay selection for enhancing PLS [11], adaptive power allocation dependent PLS techniques [12], noise and cooperative jamming dependent PLS techniques with trusted and untrusted relay [13], [14], etc.

In this study, we mainly focus on cooperative jamming with untrusted relay. In [13], an untrusted relay was jammed with the help of an external node or the intended receiver in such a way that it helps in the reliability but cannot extract information from the signal. In [14], a technique composed of two phases was proposed to provide secrecy. In its first phase, the source transmits a signal towards relay, and simultaneously cooperates with the destination for jamming the eavesdropper. In its second phase, the decoded source signal is transmitted by the relay, and at the same time, this relay cooperates with the source to jam the eavesdropper.

In the case of untrusted AAF relay, destination-assisted jamming is an effective technique, which takes advantages of relay, while keeping information secure from the relay. However, in the case of untrusted DAF relay, the destination-assisted-jamming based security techniques do not work because jamming signals from destination affect the performance of DAF relaying [14]. Hence, DAF relaying had not been used in untrusted network as discussed in [15]. Although AAF's implementation is simple, it may amplify the noise [2], so coded DAF [5] is preferable. Motivated by [3] and destination-assisted jamming for AAF [14], a practical technique for secure communication via DAF untrusted relay is proposed. This technique allows the users to keep utilizing the benefits provided by DAF, while keeping the information secure from the untrusted relay.

The rest of the paper is organized as follows. The system model is presented in Section II, followed by the proposed

978-1-5090-4372-9/17/$31.00 ©2017 IEEE

algorithm in Section III. Section IV presents simulation results, while Section V offers practical insights on the proposed scheme, and the paper is concluded in Section VI.

II. System Model and Preliminaries

The system model, presented in Fig. 1, consists of a source, a destination, and a relay in a two-hop half-duplex relay-aided system. In this system, an untrusted switchable DAF (sDAF) relaying based cooperative communication is considered. Its normal/actual operation is DAF but it can be switched to AAF relaying in certain predefined switching conditions because of simplicity of AAF relaying.

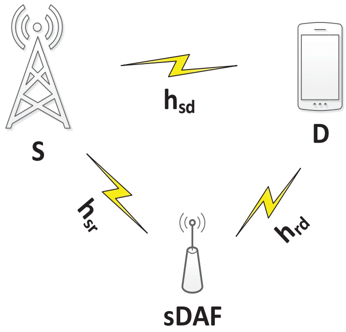

Fig. 1. Basic system model for cooperative communication system.

The relay is assumed to be passive and it can only store one frame at a time, which means that it must forward the current frame in order to get a new frame. It is also assumed that each node can either transmit or receive a signal at a given time slot. In Fig. 1, the notations h_{sd}, h_{sr} and h_{rd} denote Rayleigh fading coefficients from source to destination, source to relay and relay to destination, respectively. All of these coefficients are modeled as zero mean complex Gaussian random variables [2].

III. Proposed Method

In this section, the proposed algorithm is explained. The algorithm is based on TDMA protocol and it is divided into two phases.

(A) Phase 1: In the first phase, the source shares RMS with destination through untrusted sDAF relay in the presence of interference signal from destination.

(B) Phase 2: In the second phase, the shared RMS is used for establishing secure cooperative communication through untrusted sDAF.

The process of phase switching is explained at the end of this section. For reliability improvement and efficiency, coded cooperative communication system is considered in this protocol. The explanation details of two phases of this algorithm are as follows:

A. Phase 1

In this phase, our system is in AAF mode. In the first time slot, T0, of phase 1, the source encodes RMS [6], modulates it and sends a frame X_{RMS} of QPSK modulated signal, while at the same time the destination transmits the jamming signal X_j [14] as presented in Fig. 2. It is assumed that the destination can either transmit or receive signal at a given time slot, so in T0, it is only transmitting interference signal. The received signal at the relay in the time slot T0 is given by

$$Y_{r1} = h_{sr}X_{RMS} + h_{rd}X_j + n_{sr}, \tag{1}$$

where Y_{r1} is the received signal and n_{sr} represents additive white gaussian noise (AWGN) with the variance σ^2 at source to relay link. The Signal to inteference ratio (SINR) at relay is given by

$$SINR^R_{p1} = \frac{|h_{sr}|^2}{\sigma^2 + |h_{rd}|^2} \tag{2}$$

where $|h_{rd}|^2$ is the interference due to the jamming signal from destination.

The mutual information M^R_{p1} at relay in phase 1 is given by

$$M^R_{p1} = \frac{1}{2}\log_2\left(1 + \frac{|h_{sr}|^2}{\sigma^2 + |h_{rd}|^2}\right), \tag{3}$$

where we assume the transmission power at the destination and the source to be the same. In the second time slot, T1, the relay amplifies the mixed signal and forwards it to the destination. The transmitted signal at T1 is given by

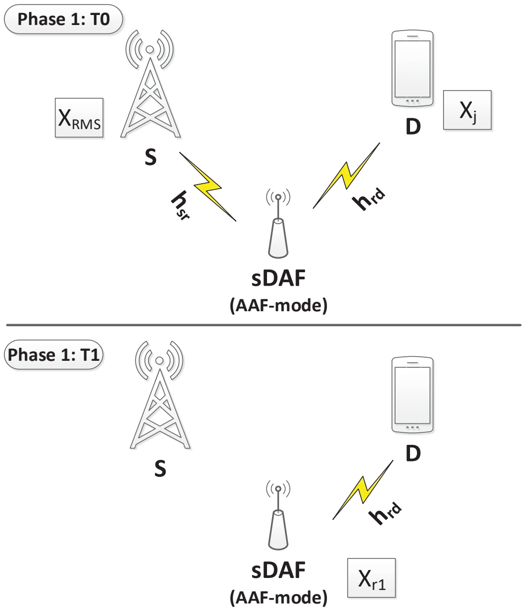

Fig. 2. Phase 1 (RMS sharing)

$$X_{r1} = \frac{Y_{r1}}{amp}, \tag{4}$$

$$amp = \sqrt{|h_{sr}|^2 + |h_{rd}|^2 + \sigma^2}, \tag{5}$$

where amp is the normalization coefficient for power. It should be mentioned that due to the jamming signal from the destination, the untrusted relay cannot decode it successfully, even if it tries. In the time slot T1, the received signal at destination from relay is given by

$$\begin{aligned} Y_{1d} = &\frac{1}{amp} h_{rd} h_{sr} X_{RMS} + \frac{1}{amp} h_{rd}^2 X_j \\ &+ \frac{1}{amp} h_{rd} n_{sr} + n_{rd}, \end{aligned} \tag{6}$$

where Y_{1d} is the received signal at the destination and n_{rd} is the AWGN at the relay to destination link.

The SINR at destination

$$SINR_{p1}^{D} = \frac{\frac{1}{amp^2}|h_{sr}|^2|h_{rd}|^2}{\frac{1}{amp^2}|h_{rd}|^2\sigma^2 + \sigma^2} \tag{7}$$

Since X_j was generated by destination, such jamming signal will not degrade the performance at destination. The mutual information M_{p1}^{D} at destination in phase 1 is given by

$$M_{p1}^{D} = \frac{1}{2}\log_2\left(1 + \frac{\frac{1}{amp^2}|h_{sr}|^2|h_{rd}|^2}{\frac{1}{amp^2}|h_{rd}|^2\sigma^2 + \sigma^2}\right), \tag{8}$$

The destination can remove the interference from received signal because it knows the interference signal that it has sent in the time slot T0. So, at the end of phase 1, the destination demodulates and decodes the RMS.

The achievable secrecy rate with sDAF in phase 1 for is given by

$$\begin{aligned} SR = &\frac{1}{2}\log_2\left(1 + \frac{\frac{1}{amp^2}|h_{sr}|^2|h_{rd}|^2}{\frac{1}{amp^2}|h_{rd}|^2\sigma^2 + \sigma^2}\right) \\ &- \frac{1}{2}\log_2\left(1 + \frac{|h_{sr}|^2}{\sigma^2 + |h_{rd}|^2}\right). \end{aligned} \tag{9}$$

It should be noted that at high SNR the factor $\frac{|h_{sr}|^2}{\sigma^2+|h_{rd}|^2}$ in M_{p1}^{R} is constant and the value of M_{p1}^{R} is negligible which ensure that RMS can not be intercepted at sDAF. The reason of negligible value of M_{p1}^{R} at relay is due to fact that interference from destination degrades the performance of signal at relay.

B. Phase 2

In the second phase of our algorithm, the cooperative system switches back to its normal (DAF) operation. In this phase, the source uses the RMS (from phase 1) for data manipulation, and then encodes it, modulates it, and finally transmits a frame of secure symbols X_s in the first time slot, T0, of phase 2, that will be received by relay and destination as presented in Fig. 3. The received signals at relay and destination in time slot T0 are given by

$$Y_{r2} = h_{sr} X_s + n_{sr}, \tag{10}$$

$$Y_{d2_1} = h_{sd} X_s + n_{sd}, \tag{11}$$

where Y_{r2} and Y_{d2_1} are the signals received at relay and destination, respectively, while, n_{sd} is AWGN at source to destination link. In the second time slot, T1, the relay will decode and then re-encode the data, modulate it, and then forward it to the destination. The received signal at destination in time slot T1 is given by

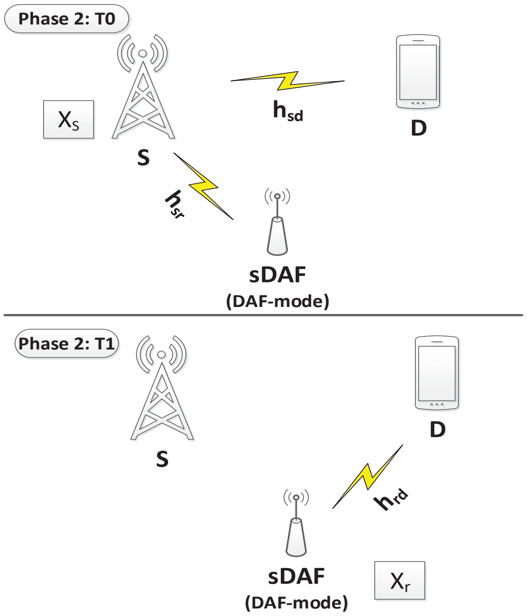

Fig. 3. Phase 2 (Secure DAF)

$$Y_{d2_2} = h_{rd} X_r + n_{rd}, \tag{12}$$

where Y_{d2_2} is the received signal at destination in slot T1. The destination will use the signals from T0 and T1 for final decoding. After decoding, the receiver will extract information by using RMS signal.

One of the important factors in this algorithm is the relay mode switching. In the literature, switching is controlled by SNR based algorithm [6], but in this work, a simple case for switching, which is referred to as hard switching, is considered. In hard switching, the system goes through phase 1 at the start of the communication (once or for a certain predefined number to minimize errors), and then it switches back to normal phase 2. In our system, the RMS can be updated by switching back to phase 1 from phase 2 after a certain predefined number of frames, which completely depends on the required security level, complexity and delay. The relay mode switching can also be done by sending a feedback from destination to relay and source.

In comparison to the conventional cooperative jamming techniques introduced in the literature [13-15], in which continuous jamming signal is required to be sent from source, helping relay or destination, the proposed algorithm does not require continuous jamming signal. Instead, it requires jamming signal only during phase 1 of the algorithm for sharing RMS. So, this fact makes the proposed algorithm more power efcient as compared to others jamming based security schemes.

It should be mentioned that the proposed algorithm can also be applied in the scenarios where there is no direct path between source and destination.

IV. Simulation Results

In this section, simulation results are presented by using bit error rate (BER) as a metric to analyze the effectiveness of our proposed security method [16]. In this study, the effects of imperfect channel estimation, that may occur due to interference, synchronization and noise errors are taken into account by adding intentional independent estimation errors at the destination and the relay. These estimations errors are based on values of mean square error (MSE) of a least square estimator (LSE) [16], [17].

The estimated erroneous channels at destination can be modeled as $\hat{h}_{sd} = h_{sd} + \Delta h_{sd}$, where h_{sd} is the perfect channel and Δh_{sd} is modeled as independent complex Gaussian noise vector with zero mean and error variance $\sigma^2 = e \times 10^{\frac{-SNR_{dB}}{10}}$, where, $e = 0.2$ is considered here. It should be noted that the value of error variance can be improved by using estimators of good quality. For the case of h_{sr} and h_{rd}, similar assumptions for imperfect channel estimation are made as described above. The basic parameters for both encoder and decoder for phase 1 and phase 2 are presented in Table 1.

TABLE I
Simulation parameters

No. of bits per frames	1000
Modulation	BPSK
Channel encoding	1/2 Convolution Codes
Channel Decoder	Viterbi Decoder
Code rate	1/2
Memory	2
Channel	Rayleigh fading channel

In phase 1, sDAF is in AAF-mode with destination-assisted interference to secure RMS from untrusted relay as explained in Section III. The BER performance of AAF-mode (phase 1) for both perfect channel estimation (PCE) and imperfect channel estimation (IPCE) is presented in Fig. 4 by abbreviation "sDAF-P1(PCE)" and "sDAF-P1(IPCE)", respectively. It is observed that IPCE leads to a small degradation in BER that can be overcome by using training sequence of larger length and higher power.

As explained in section III, phase 1 is used to transmit RMS that will be used in phase 2 for secure communication. It should be noted that errors in RMS are minimized to a negligible value by sending multiple interleaved copies of RMS frames in phase 1 at high SNR, and by comparing different copies. The significance of interference from destination in phase 1 is that even if relay tries to decode the signal, it cannot decode it properly, as presented by abbreviation "R-P1(PCE)" in Fig. 4. This is due to fact that at approximately high SNR values the value of M_{p1}^{R} is negligible which ensure that RMS can not be intercepted at sDAF. The securely transmitted RMS will be used in phase 2 for manipulating data. Fig. 5 presents results for phase 2. In the first time slot of phase 2, the relay and the destination receive RMS-manip ulated encoded data from the source. The relay first decodes the received data by using the Viterbi decoder and then re-encodes the data, modulates it and transmits it to the destination in the next slot. The destination uses symbols from time slot 1 and time slot 2 to apply Viterbi decoder after demodulation. After decoding the data, the destination will extract information

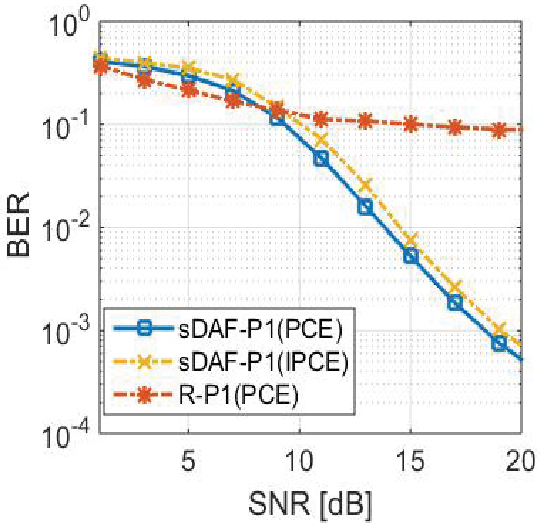

Fig. 4. BER performance for phase 1.

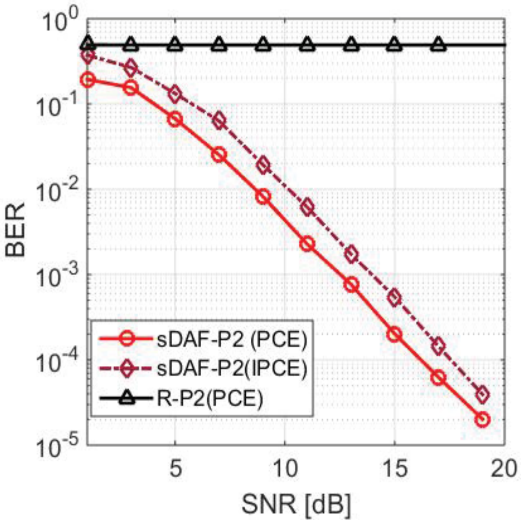

Fig. 5. BER performance for phase 2.

from decoded data by using RMS as explained in Section III. The performance of RMS-manipulated DAF versus average SNR for PCE and IPCE of our algorithm is presented in Fig. 5 by abbreviation “sDAF-P2(PCE)” and “sDAF-P2(IPCE)”, respectively. The performance of RMS-manipulated DAF is better than AAF relaying in the presence of effective channel coding scheme as presented in Fig. 5. The BER versus SNR performance at relay in phase 2 is presented by abbreviation “R-P2(PCE)”. Due to RMS manipulation the relay is not able to decode the data properly. Hence, this algorithm provides secure communication in the presence of untrusted DAF relay.

V. Practical Insights on the Proposed Scheme

It is important to mention that unlike many of the existing physical layer security techniques, whose design is channel-dependent, making them extremely prone and vulnerable to channel reciprocity mismatch and estimation errors, our proposed security technique is channel-independent. This merit helps ease and facilitate the practical implementation of the proposed security technique, making it hardware-friendly. Accordingly, a simple prototype can easily be built by using some affordable SDR devices. More specifically, a testbed of the proposed method can be implemented by utilizing only three USRP-devices controlled by LabVIEW or MATLAB software as presented in Fig. 5. Consequently, the presented work not only offers a power-efficient security technique but also hardware-friendly and easy to implement technique. The details of the implementation are left for future work.

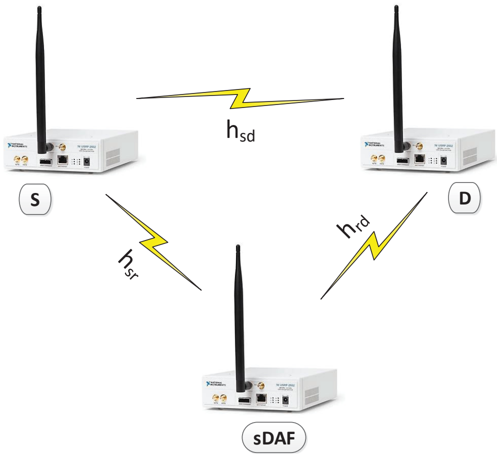

Fig. 6. Basic Hardware setup.

VI. Conclusion

In this paper, a reliable and power efficient security technique for an untrusted DAF based cooperative communication is proposed. The technique enables us to keep utilizing the benefits provided by DAF relay, while keeping information secure from it. The proposed technique is more power efficient as it does not require continuous power for jamming signal. The simulation results are provided to demonstrate the effectiveness of the proposed algorithm for both perfect and imperfect channel estimation cases. Future studies can examine untrusted-relay-assisted D2D based heterogeneous networks and untrusted secondary users in cognitive communication.

Acknowledgment

This work has been supported by The Scientific Research Council of Turkey (TUBITAK) under grant No. 114E244.

References

[1] L. Hanzo, L. L. Yang, E. L. Kuan and K. Yen, “Single-and multi-carrier DS-CDMA: multi-user detection, space-time spreading, synchronisation, standards and networking”, John Wiley & Sons, 2003.

[2] K. J. K. Liu, A. K. Sadek, W. Su and A. Kwasinski, “Cooperative communications and networking,” Cambridge University Press, 2009.

[3] B. Can, H. Yomo and E. D. Carvalho, “Hybrid Forwarding Scheme for Cooperative Relaying in OFDM Based Networks,” Proc. IEEE Int. Conf. Commun. (ICC), Istanbul, pp. 4520–4525, 2006.

[4] M. Fadhil, M. Ismail, A. Saif, N. S. Othman and M. Khaleel, “Cooperative communication system based on convolutional code CDMA techniques,” 2014 IEEE REGION 10 SYMPOSIUM, Kuala Lumpur, pp. 594–599, 2014

[5] Z. Si, R. Thobaben, M. Skoglund, “Bilayer LDPC convolutional codes for decode-and-forward relaying,” IEEE Transactions on Comm., vol. 61, no. 8, pp. 3086–3099, Aug. 2013.

[6] A. Rawat, “Implementation of a Forward Error Correction Technique using Convolutional Encoding with Viterbi Decoding,” M.S. thesis, Dept. Electron. Eng., Ohio Univ., Athens, 2004

[7] H. M. Furqan, J. M. Hamamreh and H. Arslan, “Secret key generation using channel quantization with SVD for reciprocal MIMO channels,” International Symposium on Wireless Communication Systems (ISWCS), Poznan, pp. 597–602, 2016

[8] J. M. Hamamreh and H. Arslan, “Secure Orthogonal Transform Division Multiplexing (OTDM) Waveform for 5G and Beyond,” in IEEE Communications Letters , vol.PP, no.99, pp.1–1, 2017.

[9] T. Shimizu, H. Iwai, and H. Sasaoka, “Physical-Layer Secret Key Agreement in Two-Way Wireless Relaying Systems,” IEEE Trans. Inf. Forensics Secur., vol. 6, no. 3, pp. 650–660, 2011.

[10] C. Jeong, I. M. Kim, and D. I. Kim, “Joint Secure Beamforming Design at the Source and the Relay for an Amplify-and-Forward MIMO Untrusted Relay System,” IEEE Trans. Signal Process., vol. 60, no. 1, pp. 310–325, 2012.

[11] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, “Relay Selection for Security Enhancement in Cognitive Relay Networks,” IEEE Wirel. Commun. Lett., vol. 4, no. 1, pp. 46–49, 2015.

[12] A. H. A. El-Malek, A. M. Salhab and S. A. Zummo, “Optimal Power Allocation for Enhancing Physical Layer Security in Opportunistic Relay Networks in the Presence of Co-Channel Interference,” in IEEE Global Communications Conference (GLOBECOM), San Diego, CA, pp. 1–6, 2015.

[13] X. He and A. Yener, “Two-Hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming,” in IEEE Global Communications Conference (GLOBECOM), New Orleans, LO, pp. 1–5, 2008.

[14] Y. Liu, J. Li, and A. P. Petropulu, “Destination Assisted Cooperative Jamming for Wireless Physical-Layer Security”, IEEE Trans. Inf. Forensics Secur., vol. 8, no. 4, pp. 682–694, 2013.

[15] X. Zhou, L. Song, and Y. Zhang,“Physical Layer Security in Wireless Communications”, CRC Press, 2013.

[16] J. M. Hamamreh, E. Guvenkaya, T. Baykas, and H. Arslan, “A Practical Physical-Layer Security Method for Precoded OSTBC-Based Systems”, in IEEE Wireless Communications and Networking Conference (WCNC), pp.1651–1656, 2016.

[17] J. M. Hamamreh, M. Yusuf, T. Baykas and H. Arslan, “ Cross MAC/PHY layer security design using ARQ with MRC and adaptive modulation,”IEEE Wireless Communications and Networking Conference, Doha, 2016, pp. 1–7, 2016.