# Physical Layer Security in Wireless Cooperative Relay Networks: State of the Art and Beyond

*Leonardo Jiménez Rodríguez, Nghi H. Tran, Trung Q. Duong, Tho Le-Ngoc, Maged Elkashlan, and Sachin Shetty*

*Leonardo Jiménez Rodríguez and T. Le-Ngoc are with McGill University.*

*Nghi H. Tran is with the University of Akron.*

*Trung Q. Duong is with Queen's University Belfast.*

*Maged Elkashlan is with Queen Mary University of London.*

*Sachin Shetty is with Tennessee State University.*

## ABSTRACT

Cooperative relaying is an effective method of increasing the range and reliability of wireless networks, and several relaying strategies have been adopted in major wireless standards. Recently, cooperative relaying has also been considered in the context of PHY security, which is a new security paradigm to supplement traditional cryptographic schemes that usually handle security at the upper layers. In wireless PHY security, relay nodes can be used to exploit the physical layer properties of wireless channels in order to support a secured transmission from a source to a destination in the presence of one or more eavesdroppers. While some breakthroughs have been made in this emerging research area, to date, the problem of how to effectively adopt advanced relaying protocols to enhance PHY security is still far from being fully understood. In this article, we present a comprehensive summary of current state-of-the-art PHY security concepts in wireless relay networks. A case study is then provided to quantify the benefits of power allocation and relay location for enhanced security. We finally outline important future research directions in relaying topologies, full-duplex relaying, and cross-layer design that can ignite new interests and ideas on the topic.

## INTRODUCTION

Wireless communications has grown explosively and plays an important role in the daily life of human beings. Over the years, significant efforts have been made to address the primary challenge in the design of wireless communication systems: how to increase the data transmission rate over a bandwidth-limited wireless radio channel with high reliability and, at the same time, with as low power consumption as possible. Among various solutions, cooperative relaying has been considered as an effective method to increase the range and reliability in wireless networks. While research on cooperative relaying is still an active area, several relaying strategies have been adopted in major wireless standards because of the tremendous benefits that relaying offers.

Due to the broadcast nature of wireless channels, security and privacy are of utmost concern for future wireless technologies. However, securely transferring confidential information over a wireless network in the presence of adversaries still remains a challenging task. Although security was originally viewed as a high-layer problem to be solved using cryptographic methods, physical layer (PHY) security based on information theory has been gaining increasing research attention, especially for wireless networks [1]. In wireless PHY security, the breakthrough idea is to exploit the characteristics of wireless channels, such as fading or noise, to transmit a message from a source to an intended destination while trying to keep this message confidential from eavesdroppers. Different from cryptographic methods, no computational constraints are placed on the eavesdroppers. The theoretical foundations of PHY security were laid by Wyner [2], who introduced the wiretap channel shown in Fig. 1a. In this channel, a transmitter wants to send a confidential message to a receiver in the presence of an eavesdropper. Wyner characterized the trade-off between achievable rate at the destination and the level of ignorance at the eavesdropper. In particular, he showed that a non-zero rate can be achieved in perfect secrecy. Such a rate is defined as the secrecy rate, and the maximum secrecy rate is called the secrecy capacity. For instance, for a degraded channel, the secrecy capacity is given by

$$C_s = \max I(x, y) - I(x, z), \quad (1)$$

where $I(x, y)$ is the mutual information between the transmitted signal $x$ and the signal received at the legitimate receiver $y$, $I(x, z)$ is the mutual information between the transmitted signal and the signal overheard at the eavesdropper $z$, and the maximization is carried over the distribution of $x$.

Benefiting from information-theoretic studies in cooperative communications, relaying

0163-6804/15/$25.00 © 2015 IEEE

strategies have also recently received considerable attention in the context of PHY security over wireless networks [3]. As shown in Fig. 1b, in wireless PHY security, relay nodes can be deployed to support a secured transmission from a source to a destination in the presence of one or more eavesdroppers. For instance, similar to cooperative communications, relay nodes can be used as trusted nodes to retransmit an amplified version of the signal received from the source with a suitable power amplification coefficient, that is, amplify-and-forward (AF). The trusted relay can also transmit a weighted version of the decoded signal, that is, decode-and-forward (DF), or forward a compressed copy of the received signal, that is, compress-and-forward (CF). Another method is to generate a weighted jamming signal from the relay to confound the adversary. This technique is usually referred to as cooperative jamming. Different combinations of these techniques are also possible, as discussed later. In any case, the key issue is how to exploit channel characteristics, such as channel state information (CSI), to optimize the weighted signals so that the secrecy performance can be enhanced.

While the use of relay nodes to transmit confidential information between the source and destination has gained considerable effort, attention has also been paid to untrusted relay networks in the context of PHY security. In this kind of network, a relay might attempt to try to decode the source's confidential signal. In this case, a very important question can be raised: Can cooperation with an untrusted relay be beneficial? Interestingly, the answer is positive [4]. Specifically, we can achieve a higher secrecy rate by treating the untrusted relay as both a helper to relay the information and an eavesdropper to overhear the information, rather than just considering the untrusted relay as an eavesdropper.

There is no doubt that benefits offered by cooperative relaying to enhance the security at the physical layer of wireless networks are significant. However, while quite a few advancements have been made recently in this emerging area, there are still a number of issues and challenges that need to be addressed for a novel PHY security treatment in a wireless relay network. For example, all current applications of relaying to secure communications assume that the source and relay transmit information over orthogonal channels. By allowing the source and relay(s) to transmit simultaneously in a non-orthogonal manner, the degrees of broadcasting and receiving collision are maximized, and security performance can be further improved. Unfortunately, adopting such advanced relaying protocols to enhance PHY security is not a straightforward task due to the fact that for quite a few non-orthogonal relaying protocols, the corresponding maximum achievable rates are still not known.

It is clear that research on PHY security for wireless relay networks is only at its early stage and the opportunity for innovation and research remains tremendous. Therefore, the aim of this article is two-fold:

- To present a comprehensive summary on current state of the art in this emerging research area
- To provide a high-level scope for future research directions.

In the remainder of the article, we first highlight the development of PHY security issues in untrusted relay networks. Then important issues and current state-of-the-art solutions in trusted relay networks are discussed. Following that we present a case study of AF relaying and jamming to illustrate in further detail the importance of power allocation and relay location for secrecy enhancement. Finally, we provide concluding remarks and outline important future research directions.

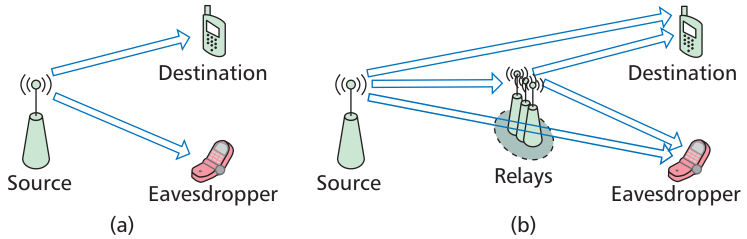

**Figure 1.** a) Wyner's wire-tap channel; b) wire-tap channel with cooperative relaying for enhanced security.

## Untrusted Relays

Untrusted relaying is motivated by several cooperative networks where the source $S$ and destination $D$ seek help from one or multiple relay nodes $R$ to relay the information, but at the same time, the source-destination pair wishes to keep the information confidential from these nodes. Examples of such a network include networks belonging to a government or a financial institution where not every node has the same level of security clearance. In a similar manner, in ad hoc networks, relay nodes are needed for connectivity, but they are not authenticated. In these networks, while the relay is willing to carry out the designated relaying scheme, the relay's observation should not be able to infer information about the message. Given the nature of the problem, AF and CF relaying are of particular interest. DF is precluded since it requires the relay to decode the message from its observation. Under this line of research, a very interesting question has been raised: Can we improve the security performance by exploiting relay cooperation with untrusted nodes?

Reference [4], which focuses on the secrecy capacity, appears to be one of the first studies tackling this issue. By considering a three-node model, as shown in Fig. 2a, which includes a source, a destination, and an untrusted relay, it was demonstrated in [4] that the untrusted relay can be beneficial for some specific relaying topologies. Specifically, when there is an orthogonal link in the second hop from the relay to the destination, one achieves higher secrecy rate by treating the relay as an eavesdropper $E$ as well as a helper rather than considering the relay as an eavesdropper only. This interesting result holds true for both AF and CF relaying. On the other hand, when the source and relay transmit to the destination via a multiple access channel, while

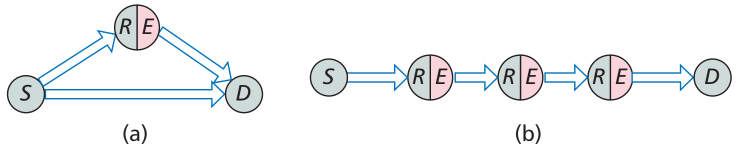

**Figure 2.** Wireless relay networks with untrusted relays where a relay $R$ acts as both a helper and an eavesdropper $E$: a) three-node model; b) multihop model.

there is an orthogonal link from the source to the relay, the secrecy capacity is equal to zero [5]. It is because in this case, randomness at the source's encoder is not necessary, and the relay-destination link is not useful in improving the secrecy rate. The results in [4] have also been extended to multi-antenna setups in [6] where the source, destination, and relay are equipped with multiple antennas. In particular, by jointly optimizing the source beamforming vector and the relay beamforming matrix, the cooperative scheme achieves a better secrecy rate than the non-cooperative scheme. However, the proposed beamforming scheme can only be applied to AF relaying. To our knowledge, the corresponding problem associated with CF relaying remains a challenging task. The benefit of secure beamforming in multi-antenna systems was also investigated in [7] for two-way AF relaying. Recently, confidential message transfer over multihop communication with a chain of connected untrusted relays, as illustrated in Fig. 2b, was examined in [8]. Interestingly, under this line network model, end-to-end secrecy can still be achieved, and the secrecy rate has been shown to be independent of the number of hops. Specifically, in this network, interference is created for each relay from its next hop neighbor while it receives a confidential message from the previous hop neighbor. As such, each relay receives a superposition of the message and another signal that is intended for cooperative jamming. Via a coding scheme utilizing nested lattice codes, each relay cannot infer the message from the combination of the message and jamming that corresponds to another codeword.

The secrecy capacity relies on the assumption of ergodic channels and has been considered one of the foremost system benchmarks. However, in some certain fading scenarios, the channel gains change slowly over time. This corresponds to a situation where the coherent time of the channels is sufficiently long compared to the delay requirement. For such cases, the secrecy outage probability can be used as the main performance metric. In [9], the secrecy outage probability has been studied for a three-node non-regenerative AF relay network with an untrusted relay. It is then shown in [9] that secrecy can be achieved as long as the source and destination keep their CSI secret from the untrusted relay.

## Trusted Relays

We now turn our attention to the case of trusted nodes for security improvements. In trusted relay scenarios, the source is assisted by a single or multiple *trustworthy* relays to transmit confidential information to the destination in the presence of a passive eavesdropper, in addition to the legitimate parties. Different from the untrusted case, the relays are trusted nodes and can be fully exploited to significantly enhance security. This trusted scenario is of more interest and has received considerable attention in the literature. In the following, we introduce different ways that trusted relays can be used to enhance security.

### Strategies

For the scenario of trusted relays, several strategies to improve security have been proposed in the literature. The main techniques are schematically illustrated in Fig. 3 and explained in detail below.

***Relaying:*** Consider first the relaying strategy where the helper nodes aid in transmission by simply relaying information between legitimate nodes (e.g., [3, 10]). Depending on how the information flows, one-way (OW) and two-way (TW) relay protocols have been considered in the literature. In OW relaying, a source node wants to communicate to a destination node with the help of relays, so information flows in a unidirectional fashion (i.e., from source to destination). This is usually carried over two transmission phases: the source communicates with the relays in the first phase, and the relays communicate with the destination in the second one. In TW relaying, two nodes want to exchange data and information flows in a bidirectional manner. This is carried over two or three phases: the nodes communicate to the relay simultaneously or by turns in the first one or two phases, respectively, and the relay broadcasts in the third. An eavesdropper might overhear the information in one or multiple transmission phases.

When only one relay is available, the conventional DF or AF techniques are usually considered in the literature along with OW or TW relay protocols. On the other hand, when multiple relays are available, the most common relaying approach is *distributed beamforming*. In this approach, multiple relays transmit a weighted version of the decoded signal (for DF relays) or the noisy received signal (for AF relays). The weights are designed to steer the information vector away from the eavesdropper and in the direction of the intended destination. Assuming CSI of the links to the eavesdropper at the legitimate nodes, complete *nulling* of the information vector at the eavesdropper can be achieved. Such a beamforming/nulling scheme is applicable to both OW and TW relaying.

***Jamming:*** Consider now the strategy in which the helper nodes do not relay information but instead transmit jamming signals to confound the eavesdropper (e.g., [3]). This is commonly referred to as *cooperative jamming*. Generally speaking, in this approach, two nodes communicate directly with each other while the relays transmit jamming signals independent of the nodes' information. The objective of these signals is to degrade the signal-to-noise ratio at the eavesdropper without degrading that at the intended receiver. For instance, when multiple relays are available, complete *nulling* of the jam-

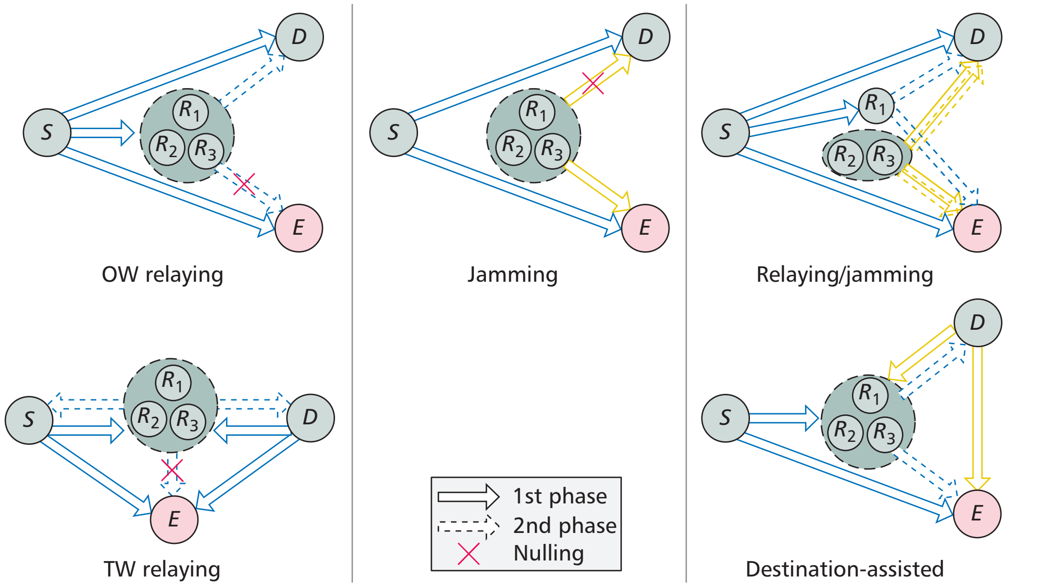

**Figure 3.** Relay-assisted techniques.

*Different from the untrusted case, the relays are trusted nodes and can be fully exploited to significantly enhance the security. This trusted scenario is of more interest and has received considerable attention in the literature. In the following, we introduce different ways that trusted relays can be used to enhance security.*

ming signal at the intended receiver is possible by proper weighting of the jamming signals. When information on the links to the eavesdropper can be acquired, the signal-to-noise ratio at the eavesdropper can be further degraded while still achieving nulling of the jamming signal at the destination. Note that different from relaying approaches, the relay nodes do not need to know any information about the signal being transmitted by the source node.

***Pure Relaying/Jamming Combinations:*** The above jamming and relaying approaches can also be combined into a single strategy (e.g., [11]). In this case, a subset of nodes act as relays, while another subset does jamming. Similar to the previous two strategies, beamforming and nulling can be used at any of the subsets for performance enhancement. However, different from jamming techniques, nulling of the jamming signal might be needed not only at the destination node, but also at the relay subset. One special case of relaying/jamming combinations is the so-called *destination-assisted* schemes. In these schemes, the destination node has the double duty of being a receiver and a jammer. Due to the half-duplex constraint, the destination cannot perform both tasks at the same time, and thus the source must communicate through relaying. Specifically, the source can transmit information to a relay subset in the first phase, while the destination and jamming subset transmits noise signals to the eavesdropper. In the second phase, the relay subset simply forwards the information to the destination, which must then remain silent and listen. Note that the techniques described here are referred to as "pure" combinations in that each node acts as either a jammer or a relay at any given time.

***Hybrid Relaying/Jamming Combinations:*** All the above techniques can be said to be part of a more general hybrid strategy in which all nodes are allowed to send superpositions of information and jamming signals, that is, the nodes can simultaneously perform jamming and relaying (e.g., [12, 13]). One of the most well-known hybrid schemes is perhaps the destination-assisted *artificial noise* protocol [12]. In this protocol, the source and destination send jamming signals in the first phase to the relays. In the second phase, the relays transmit a weighted version of the signal received in the previous phase. At the same time, the source sends a superposition of jamming and information signals. The jamming signal in this superposition is designed to cancel the jamming component due to the source at the destination, whereas the jamming component due to the destination can readily be cancelled off since it is known. This artificial noise concept has also been extended to TW relaying. Another destination-assisted hybrid protocol is the one in [13]. In that protocol, the source transmits a combination of data and jamming to the relay, while the destination cooperates with the source by also transmitting a jamming signal. The jamming signals from the source and destination are designed such that their addition will be cancelled at the relay. In the second slot, the relay sends a superposition of information and jamming signals, while the source transmits a different jamming signal. As in the first phase, the source and relay jamming signals are designed to be nulled at the destination. Hybrid protocols that do not require assistance from the destination have also been proposed.

### Criteria and Enhancements

Similar to the case of untrusted relays, different criteria have been considered in the literature to optimize the performance of the above strategies. Most works have concentrated on maximizing the secrecy rate, while fewer studies have been carried to minimize the outage performance. For either of these criteria, three aspects have been considered to enhance security.

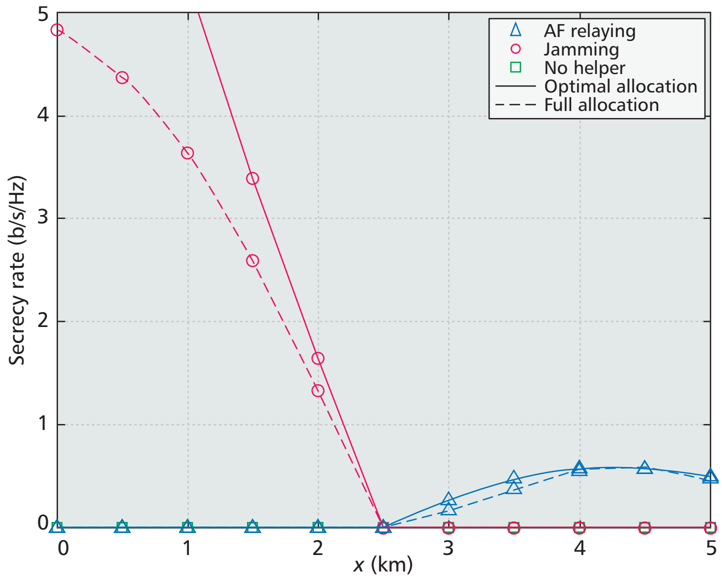

**Figure 4.** Secrecy rate of different jamming and AF relaying schemes.

The first aspect is *power allocation*, where the total system power must be optimally shared among the nodes (i.e., sum power constraint scenario) or where each node has an individual power budget (i.e., per-node power constraint scenario). In the latter case, we should mention that using full power at any of the nodes might not always be beneficial in certain configurations. For instance, full power at a relay could result in too much information being leaked to the eavesdropper, whereas full power at a jammer might cause too much interference at the destination. For hybrid protocols, further splitting the power between information and jamming signals at a given node is also of great importance.

The second aspect considered in the literature is *weight optimization* at the relays. As discussed above, such optimization is needed for beamforming or nulling of the relaying and jamming signals. It should be emphasized that complete nulling of the jamming vector at the destination or of the information vector at the eavesdropper is in general not always optimal. This is because such a tight constraint could potentially limit the degrees of freedom and the overall performance of the system.

The third and final aspect is *relay selection*, where a subset of all available nodes must be selected for relaying or jamming. Generally speaking, the nodes that increase the interference to the eavesdropper while protecting the destination must be selected for jamming. Likewise, the nodes that improve the quality of the signal received at the destination without increasing that at the eavesdropper must be selected for relaying. Different selection techniques can be applied depending on the availability of the channel information at the controller.

## A Case Study

Most of the strategies presented in the previous section require the network to have multiple friendly relays. However, the benefits offered by such multi-relay techniques might be severely undermined by coordination, synchronization, and heavy signaling/feedback issues. This is especially true for techniques in which the channel information among all the links in the network is required at all legitimate nodes. Although the single-relay schemes are simpler to study, their analysis is still very challenging, and such networks have not been thoroughly investigated in the literature, especially for jamming or AF relaying. For instance, although power allocation schemes have been derived in closed form for some DF networks, the globally optimal power allocation schemes at the source and relay that maximize the secrecy rate for the jamming or AF relaying strategies have not been addressed in the literature. This is due to the difficulty in solving the related non-convex optimization problems. Given that jamming and AF relaying present reduced complexity, and the latter has been shown to provide larger secrecy service areas than DF [10], a thorough investigation of these schemes is required.

In this case study, we quantify the gain that can be achieved using optimal power allocation in single-relay networks. We also investigate the effect of relay location on security. Both the jamming and AF relaying strategies according to Fig. 3 are adopted. Specifically, for the jamming strategy, the source communicates directly to the destination while the jammer sends Gaussian noise to both the eavesdropper and the destination. For AF relaying, the source transmits a signal to the relay and destination in the first phase. In the second phase, the relay amplifies what it received in the previous phase and forwards it to the destination. The eavesdropper overhears in both phases. In this case study, the source, eavesdropper, and destination are placed at the corners of a square with sides of 5 km, while the relay can be anywhere inside the square. Specifically, the source, destination, eavesdropper, and relay have coordinates of (0, 0), (5 km, 0), (0, 5 km), and ($x$, $y$), where $0 <= x, y <= 5$ km. In addition, the source and relay have a power budget of 40 dBm and 30 dBm, respectively, and the noise power at all nodes is –100 dBm. A path loss model is considered such that the power received at any node is given by $P_{\text{Rx}} = P_{\text{Tx}}/d^{\alpha}$, where $P_{\text{Tx}}$ is the transmitted power, $d$ is the distance between the transmitter and the receiver, and $\alpha$ is the path loss exponent, which is set to 3.

To analyze the effect of power allocation on security, Fig. 4 shows the secrecy rate of the jamming and AF relaying strategies when the relay moves along the diagonal of the square from eavesdropper to destination. Two power allocation schemes are considered in this figure: full power at both nodes and the optimal power allocation scheme. The optimal power allocation maximizes the instantaneous secrecy rate for the considered protocols under per-node power constraints and under the assumption of full channel information at the legitimate nodes (similar to [3, 10, 11, 13]). First, note from Fig. 4 that using full power at source and relay is not necessarily optimal. For instance, when the jammer is close to the eavesdropper, a small amount of power is needed to jam it, and further increasing the power affects the destination and thus the overall performance. Similarly, when the relay is close to the destination, using full power might lead to too much information leakage. From this example, power control appears to be more beneficial for the jamming strategy. As expected, it can be seen from Fig. 4 that jamming is preferred when the relay is closer to the eavesdropper, whereas relaying is a better choice when it is closer to the destination. It should also be noted from Fig. 4 that the secrecy rate for AF relaying is zero when the relay is closer to the eavesdropper, whereas that for jamming is zero when the relay is closer to the destination.

To analyze the joint effect of relay location and optimal power allocation, Fig. 5 shows the contour of the secrecy rate when the helping node acts as a relay and is placed at a given ($x$, $y$) location. Only the optimal power allocation is considered in Fig. 5. Note from this figure that relaying can achieve a positive rate when the node is closer to the destination than to the eavesdropper. More importantly, the optimal relay location appears to be on the line from source to destination. This is because in this location, the relay is far from the eavesdropper while still being relatively close to the source for listening and the destination for forwarding.

To analyze the optimal location for the jamming strategy, Fig. 6 shows a similar contour plot as above but now assuming that the helping node is a jammer. The optimal power allocation at the jammer is again considered. We can see in Fig. 6 that a positive rate is achieved when the jammer is closer to the eavesdropper than to destination. In this case, the performance of jamming improves as the jammer approaches the eavesdropper.

By comparing the rates in Figs. 5 and 6, we observe that relaying is again preferable when the helping node is closer to the destination ($x > y$), whereas jamming is better when the node is closer to the eavesdropper ($y > x$). Similar trends have also been observed when the eavesdropper moves closer to the destination while keeping the same distance from the source. Finally, it is important to note that using a helping node in this configuration is crucial to achieving a positive secrecy rate. This is because the destination and eavesdropper are at the same distance from the source, so the secrecy capacity without such help would be zero.

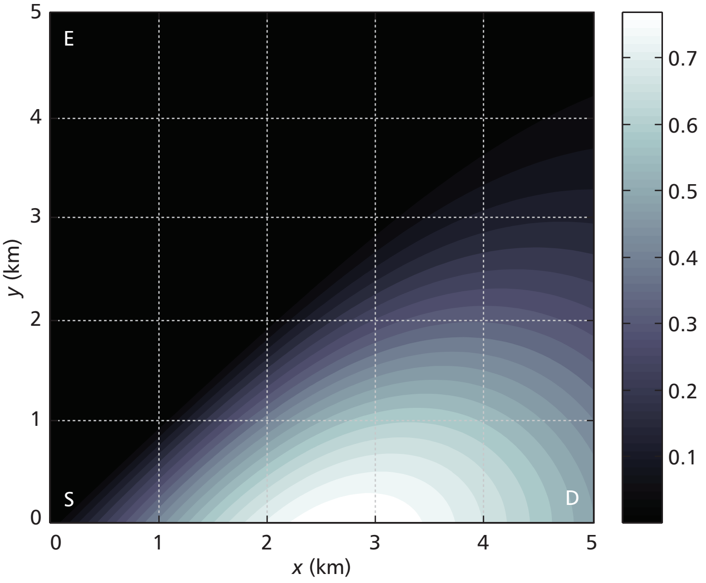

**Figure 5.** Secrecy rate of AF relaying with different locations.

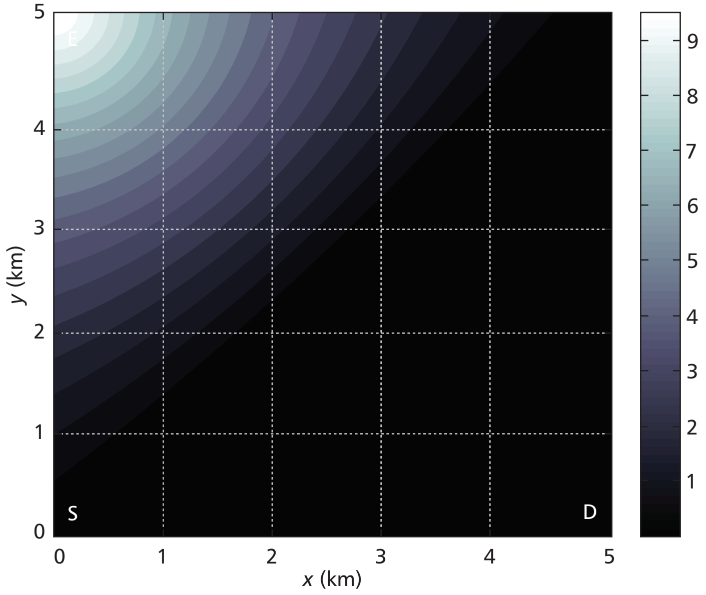

**Figure 6.** Secrecy rate of jamming with different locations.

## Concluding Remarks and Future Research Directions

This article has provided a comprehensive overview of the area of physical layer security in wireless cooperative relay networks. The focus was on both untrusted and trusted relay networks to illustrate that cooperative relaying plays an important role in enhanced security. While the discussion has been at a high level, we hope that the article can motivate further research on PHY security for such important networks. The scope of future research in this direction is broad, and we have no doubt that novel relaying topologies and scenarios along with the corresponding security schemes shall be developed. Therefore, in the following, we would like to present only a few interesting and challenging research topics we believe are worth further investigation.

Thus far, all current relaying strategies considered under the context of PHY security are based on orthogonal or multihop mechanisms. That is, the source and relay transmit information over orthogonal channels. By using this "cake-cutting" approach, only a fraction of the channel degrees of freedom can be exploited. As a consequence, it might fail to realize the full benefits offered by cooperative relaying for enhanced secrecy. To understand the true limitation of cooperative relaying to improve security, more advanced non-orthogonal relay protocols in which the source and relay transmit information simultaneously should be considered. Such

*Another research challenge is to define a totally new security metric that has both information-theoretic and cryptographic flavor [15] that might lead to a more efficient encryption scheme using cooperative relaying. This research direction shall certainly offer a rich set of challenges.*

a study will certainly result in a more complete picture of the benefits of relaying for security enhancement in wireless networks. Besides relaying, strategies such as jamming or jamming/relaying combinations can also be adopted. Among all these strategies, it is in general not clear which one is better for a given topology. Thus, another interesting research direction is to provide a comparative study to analyze the circumstances under which any one transmission strategy is preferable. Lastly, security enhancements such as power allocation, weight optimization, and relay selection require channel knowledge. Therefore, investigating enhancements that rely on partial or statistical channel information is also of great importance.

Current relaying technologies in wireless communications have been developed under the constraint of half-duplex (HD) communication, where a relay node can either transmit or receive on a single channel, but not both simultaneously. This is because the transmitted signal power in wireless systems is usually many orders of magnitude larger than the received signal power, thus rendering simultaneous transmission and reception over the same frequency band impractical. This HD constraint results in inefficient use of resources as a dedicated bandwidth or time slot is required for relay transmissions. Recently, a number of encouraging full-duplex (FD) designs have been proposed to overcome the self-interference problem using novel combinations of antenna, analog, and digital cancellations. As one important aspect of FD transmission, FD relaying can be exploited to enhance secrecy. For instance, an FD relay node can generate a jamming signal to degrade the eavesdropper channel, while at the same time assisting the transmission from the source to destination. While the potential benefits of FD relaying for enhanced security are undoubted, it is important to investigate jointly cooperative relay and jamming protocols to optimize the secrecy capacity of wireless FD relay networks. To this end, the residual self-interference of FD operation must also be taken into account, which makes the related problems much more challenging [14].

Finally, we note that while PHY security techniques are promising, the security of communication networks has traditionally relied on cryptographic schemes in upper layers, such as the application and presentation layers. Therefore, cross-layer analysis of secrecy to find how best to combine the PHY security and cryptographic schemes in wireless relay networks to guarantee the security of the whole system is another interesting research area. To find such a combination approach, it is important to investigate how the PHY security and traditional cryptographic methods interact with each other to enhance the security of the system. For example, one interesting question is how to combine PHY security techniques in cooperative relaying and cryptographic techniques to build a secret-key agreement protocol, which is to generate a secret key that can be used in a cryptosystem at an upper level. Another research challenge is to define a totally new security metric that has a both information-theoretic and cryptographic flavor [15] that might lead to a more efficient encryption scheme using cooperative relaying. This research direction shall certainly offer a rich set of challenges.

## References

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

[2] A. Wyner, "The Wire-Tap Channel," *Bell Sys. Tech. J.*, vol. 54, no. 87, Oct. 1975, pp. 1355–87.

[3] L. Dong *et al.*, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Trans. Signal Processing*, vol. 58, no. 3, Mar. 2010, pp. 1875–88.

[4] X. He and A. Yener, "Cooperation with an Untrusted Relay: A Secrecy Perspective," *IEEE Trans. Info. Theory*, vol. 56, no. 8, Aug. 2010, pp. 3807–27.

[5] L. Sun *et al.*, "Performance Study of Two-Hop Amplify-and-Forward Systems with Untrustworthy Relay Nodes," *IEEE Trans. Vehic. Tech.*, vol. 61, no. 8, Oct. 2012, pp. 3801–07.

[6] 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 Processing*, vol. 60, no. 1, Jan. 2012, pp. 310–25.

[7] J. Mo *et al*., "Secure Beamforming for MIMO Two-Way Communications with an Untrusted Relay," *IEEE Trans. Signal Processing*, vol. 62, no. 9, May 2014, pp. 2185–99.

[8] X. He and A. Yener, "End-to-End Secure Multi-Hop Communication with Untrusted Relays," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, Jan. 2013, pp. 1–11.

[9] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure Communication via an Untrusted Non-Regenerative Relay in Fading Channels," *IEEE Trans. Signal Processing*, vol. 61, no. 10, May 2013, pp. 2536–50.

[10] P. Zhang *et al*., "Analyzing Amplify-and-Forward and Decode-and-Forward Cooperative Strategies in Wyner's Channel Model," *Proc. IEEE WCNC*, Apr. 2009, pp. 1–5.

[11] J. Chen *et al.*, "Joint Relay and Jammer Selection for Secure Two-Way Relay Networks," *IEEE Trans. Info. Forensics Security*, vol. 7, no. 1, Feb. 2012, pp. 310–20.

[12] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, June 2008, pp. 2180–89.

[13] Y. Liu, J. Li, and A. Petropulu, "Destination Assisted Cooperative Jamming for Wireless Physical-Layer Security," *IEEE Trans. Info. Forensics Security*, vol. 8, no. 4, Apr. 2013, pp. 682–94.

[14] S. Parsaeefard and T. Le-Ngoc, "Improving Wireless Secrecy Rate via Full-Duplex Relay-Assisted Protocols", *IEEE Trans. Info. Forensics & Security*, vol. 10, no. 10, Oct. 2015, pp. 2095-2107.

[15] M. Bellare, S. Tessaro, and A. Vardy, "Semantic Security for the Wiretap Channel," *Advances in Cryptology—CRYPTO 2012*, Lecture Notes in Computer Science, vol. 7417, Springer-Verlag, pp. 294–311.

## Acknowledgment

The work of Nghi H. Tran and Sachin Shetty was partially supported by the Office of Naval Research, under Grant No. N00014-15-1-2444.

## Biographies

Leonardo Jiménez Rodríguez (S'09) received his B.Eng. degree (with honors) in electrical engineering from Ryerson University, Toronto, Ontario, Canada, in 2008, and his M.Eng. and Ph.D. degrees in electrical engineering from McGill University, Montreal, Quebec, Canada, in 2010 and 2014, respectively. His research interests include cooperative communications, physical layer security, full-duplex transmission, and coded modulation techniques.

Nghi H. Tran (S'05, M'08, SM'15) received a B.Eng. degree from Hanoi University of Technology, Vietnam, in 2002, and M.Sc. (with Graduate Thesis Award) and Ph.D. degrees from the University of Saskatchewan, Saskatoon, Canada, in 2004 and 2008, respectively, all in electrical and computer engineering. Since August 2011, he has been an assistant professor with the Department of Electrical and Computer Engineering, University of Akron, Ohio. His research interests include signal processing, communication, and information theories for wireless systems and networks.

TRUNG Q. DUONG (S'05, M'12, SM'13) received his Ph.D. degree in telecommunications systems from Blekinge Institute of Technology, Sweden in 2012. In 2013, he joined Queen's University Belfast, United Kingdom as a lecturer (assistant professor). His current research interests include cooperative communications, cognitive radio networks, physical layer security, massive MIMO, cross-layer design, mmWave communications, and localization for radios and networks.

THO LE-NGOC (F'97) is a professor in the Department of Electrical and Computer Engineering at McGill University. His research interest is in the area of broadband access communications. He is a Fellow of the Engineering Institute of Canada, the Canadian Academy of Engineering, and the Royal Society of Canada. He was the recipient of the 2004 Canadian Award in Telecommunications Research and the IEEE Canada Fessenden Award 2005. He holds a Canada Research Chair (Tier I) on Broadband Access Communications.

MAGED ELKASHLAN (M'06) received a Ph.D. degree in electrical engineering from the University of British Columbia, Canada, in 2006. From 2007 to 2011, he was with the Wireless and Networking Technologies Laboratory at Commonwealth Scientific and Industrial Research Organization, Australia. During this time, he held an adjunct appointment at the University of Technology Sydney, Australia. In 2011, he joined the School of Electronic Engineering and Computer Science at Queen Mary University of London, United Kingdom, as an assistant professor. He serves as an Editor of *IEEE Transactions on Wireless Communications*, *IEEE Transactions on Vehicular Technology*, and *IEEE Communications Letters*. His research interests fall into the broad areas of communication theory, wireless communications, and statistical signal processing for distributed information processing, security, cognitive radio, millimeter wave communications, and 5G HetNets.

SACHIN SHETTY received a Ph.D. degree in modeling and simulation from Old Dominion University. He also serves as director of the Cyber Security Laboratory and the associate director of the TSU Interdisciplinary Graduate Engineering Research Institute. His research interests lie at the intersection of computer networking, network security, and machine learning. He has published over 70 refereed conference, workshop, and journal articles, and book chapters in research and pedagogical techniques. He has secured over $5 million external funding from several federal agencies. He is the recipient of a DHS Scientific Leadership Award and a TSU Research Mentorship Award.