Increasing the Security of Wireless Communication Through Relaying and Interference Generation

Luca Rose, Elizabeth A. Quaglia, and Stefan Valentin
Mathematical and Algorithmic Sciences Lab, France Research Center,
Huawei Technologies Co. Ltd.
email: {luca.rose, elizabeth.quaglia, stefan.valentin}@huawei.com

***Abstract*—The exchange of confidential messages is an inherent problem in wireless communication due to the broadcast nature of the radio channel. In this paper, we enhance standard cryptography with information-theoretic techniques by exploiting relays to increase the confidentiality of wireless communication in the presence of one or more eavesdroppers with low-noise receivers. To achieve this, we present a protocol which makes use of relays in two ways. First, the relays re-transmit disjoint encrypted chunks of a message. Second, the relays utilize cooperative jamming techniques to generate pseudo-random signals in order to increase the interference level in the propagation domain. Chunks and interference levels are allocated over relays in such a way that the message can only be decoded within a critical area around the intended receiver. Our simulation results show that this area can be minimized under realistic assumptions on propagation environment and channel knowledge.**

***Index Terms*—Relays; Interference; Security.**

I. Introduction

In a world that is increasingly relying on wireless technologies, the need for secure communication through this medium is becoming paramount. Achieving this is considerably more challenging than in the wired setting, since information is naturally broadcast rather than sent through the wire, and it is generally considered easier for an attacker (A) to access wireless network communications than wired ones.

Message confidentiality is a fundamental aspect of secure communication and it is typically achieved by means of encryption, which ensures that no information about the encrypted message can be obtained without the appropriate decryption key. Although in theory there are many provably secure encryption schemes proposed in the cryptographic literature (RSA [1] being the most prominent), practice shows that unexpected vulnerabilities, such as the ones due to side-channels (as pioneered by [2]) and introduced through implementation (for instance, [3]), lead to a breach of confidentiality. While, on the one side, we have that the traditional way to provide security (i.e., cryptography) suffers from some practical shortcomings, on the other we have that an emerging approach, i.e., physical-layer security, is advancing in a promising way.

The concept of wiretap channel was introduced in [4], in which it was proved that messages can achieve perfect secrecy even in the absence of cryptographic protection, if the transmission rate is smaller than the secrecy capacity (SC). In [5], the SC of Gaussian channels was shown to amount to the difference of the capacities of the intended receiver (IR) and the A's channels. In practical terms, this means that to physically ensure the secrecy of a message it is sufficient to guarantee that the SINR level of any malicious transmission, i.e., the SINR of the message received by an A, is below a certain threshold. These results have originated a series of works and schemes that exploit the natural limitation of the physical medium to increase the secrecy of a message. In this line of research, works such as [6]–[9] aim, in general, at improving the SINR of the communication towards the intended receiver (IR), and reducing it towards the As.

As highlighted in [7], seeking solutions that combine the two approaches, i.e., cryptography and information theory, to improve the security of wireless communication is an interesting and challenging area of research. Our work represents a novel method in this direction.

A. Problem

In this paper, we consider the following problem: a base station (BS) wishes to confidentially communicate a message m to an IR over an open wireless channel. Contrary to standard systems, the message will not be sent directly from the BS to the IR; rather it will be transmitted via a set of available communication relays. (Indeed, the use of relays in wireless communication is rapidly increasing in order to better exploit radio spectrum[1].) Our goal is to ensure message confidentiality in the presence of an attacker A that wants to eavesdrop the communication. A can be located anywhere, and its location is *unknown* to both the BS and the relays. Furthermore, we allow A to be equipped with multiple antennas, as well as its level of receive noise to be equal to zero, as the worst case scenario. Note that our setting includes the case where multiple As are active, including malicious relays attempting to break message confidentiality.

B. Contributions

To solve this problem, we first introduce the concept of critical area (CA). The CA is an area situated in a neighborhood of the IR in which the secret capacity of the message is high enough to decode the transmitted message. In order to control the dimension of the CA we exploit the presence of relays and the concept of cooperative jamming [6]. Then, we propose a novel method to distribute the message over a selected subset of relays such that it can only be recovered in the

[1]Note that in 5G networks, also standard user equipment can be exploited as relay thanks to device-to-device (D2D) technologies [10].

CA. More specifically, we propose to 1) separate the message into *chunks* of bits which encode a subset of the message, 2) estimate the average channel gain between a set of potential relays and the IR, computing this estimation based on any available information, such as channel statistical knowledge or radio maps, 3) allocate the chunks to a set of relays, denoted signal-relays, selected in order to obtain a sufficiently small CA in which *all* of the chunks can be received at a signal strength above their decoding threshold, and 4) choose a set of relays, denoted interference-relays, to generate interference to guarantee the size and shape of the CA for an arbitrarily good receiver.

Our contributions are as follows. We propose and detail a wireless communication *protocol* that instructs us to encode a message m into several chunks, and to select a set of signal-relays, to which the chunks are distributed, and a set of interference-relays, which generate controlled noise. We present several set-selection *policies*, which differ according to various possible constraints, e.g., limit on the number of usable relays or restriction on the size of the CA. We propose *cryptographic solutions* to guarantee the confidentiality of the message in the presence of an attacker A. We test the proposed protocol through numerical *simulations*, confirming its capacity to reduce the CA even for a zero-noise A. The proposed protocol is a cross-layer solution that could be attractive in the following use-cases: (a) a cryptographic key needs to be established or renewed after a security leakage, (b) standard cryptographic techniques are too computationally cumbersome for an IR with limited computational capabilities, (c) a safety net for encrypted transmission needs to be established due to the importance of the message.

C. Related Work

Our work makes use of cooperative relays to enhance the security of wireless communication. This idea has been studied before. The interested reader can find in [7] an overview of the state of the art in this domain. In particular, in [9], the authors consider three schemes for secure message transmission using cooperative relays – decode-and-forward, amplify-and-forward, and cooperative jamming –, and for each scheme they propose a system design (which includes power allocation) for secrecy rate maximization. Their results assume that global channel state information (CSI) is available and, more importantly, that the eavesdropper's channel is known. Such strong assumptions reduce the practical viability of their solution. By contrast, our work only assumes an average CSI estimation and, more importantly, makes no assumption on the knowledge of the adversary's channel. In [11], wireless security is enhanced by adopting particular MIMO precoding techniques such as maximum ratio transmission and regularized zero-forcing. It is argued that with infinite antennas and perfect CSI, such system can delivered perfect security. However, imperfect CSI and pilot contamination [12] can completely compromise the secrecy of a message and this is almost impossible to detect. In [13], the security in cognitive radio systems using single and multiple relays is considered. In particular, the authors propose a multi-relay selection scheme, where each relay transmits the same message with different levels of power reducing the energy consumption and the area in which the message can be successfully decoded. We note however that it suffices for an eavesdropper to be sufficiently close to only one relay in order to decode the entire message. Our solution does not suffer from this drawback, since an A needs to recover *all* the message chunks distributed over the multiple relays in order to recover the original message. Finally, [6] proposes a cooperative transmission method which divides the message into blocks, and distributes each block to a different relay, similarly to what we do. The method's limitations mainly lie on the following assumptions: (a) A's hardware is identical to the IR's (same noise level and number of antennas); (b) the relays have perfect instantaneous channel information; (c) the relays must be all trusted. Conversely, our approach allows to relax all these assumptions.

II. Network Model

Consider a wireless system in which a BS wishes to transmit a message m to an IR, avoiding one or more As, as represented in Fig. 1. The BS is assumed to be aware of the position of the IR and the relays it communicates with, however it is unaware of the presence and the position of the eventual As. Denote as $p = (x, y)$ an arbitrary position on the map containing the BS, the IR, the relays and the As. Assume that a message is transmitted by a source with power P_T. Denote also by $P_R(r)$ the power received by a receiver r at position p. In the presence of interference, and assuming the absence of any form of interference cancellation, the capacity of the transmission from a relay T to a receiver r is given by:

$$C_T(r) = \frac{1}{2}\log_2\left(1 + \frac{P_R(r)}{\sigma_r^2 + I(r)}\right) \tag{1}$$

where σ_r^2 represents the thermal noise of receiver r and $I(r)$ the sum of all the interference received at receiver r. Under this conditions, it can be shown [5], [6], that the secrecy capacity can be expressed as:

$$C_{Sec} = \max\{C_T(IR) - C_T(A), 0\}. \tag{2}$$

It is easy to show that all the As for which it results that

$$\frac{P_R(IR)}{\sigma_{IR}^2 + I(IR)} < \frac{P_R(A)}{\sigma_A^2 + I(A)} \tag{3}$$

have zero secrecy capacity and cannot reliably decode the transmitted message if the transmission speed R is set sufficiently close to $R = WC_T(r)$ [6].

This means that, for a fixed transmission rate R and bandwidth W for the transmission to the IR, it is possible to define a decoding threshold, denoted by Γ as the minimum value of $\frac{P_R(r)}{I(r)+\sigma^2}$ for which an A can eavesdrop the message, i.e., $\Gamma = 2^{\frac{R}{W}-1}$. The name decoding threshold is justified by the fact that if a receiver has an SINR below such threshold it cannot decode the message with 0 probability of error, even if no cryptography is adopted, no matter what decoding technique it adopts.

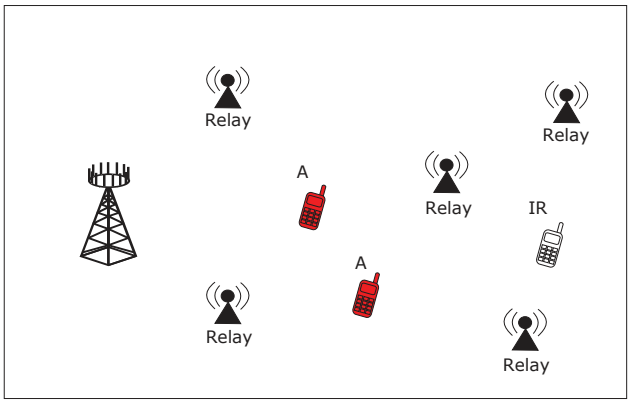

Fig. 1. Basic scenario depicting the BS, the relays, the IR, and the As.

The value of the power received by a receiver r, i.e, $P_R(r)$, depends on many factors such as distance from the transmitter, presence of objects between the transmitter and the receiver, fading and antenna gain. In the following, we refer to the ratio between the transmit power P_T and the received power $P_R(r)$ as the *channel gain* $G_R(r) = \frac{P_T}{P_R(r)}$. Note that, if the BS had beforehand (a) the value of $G_R(r)$ for each point in space and each receiver; (b) the value of the thermal noise power for each receiver σ_r^2; and (c) the level of power of the interference received $I(r)$, then it could establish where, and which receiver, is able to decode the message.

A. Channel Gain Estimation

The channel between the IR and the available relays is supposed known (or estimated up to some uncertainty) by the BS. In order to estimate such a value, a channel estimation scheme can used, in particular in TDD systems where the training sequences transmitted by the IR are exploited by the relays to estimate the channel gains. This would yield almost perfect instantaneous channel knowledge at the cost of high signaling between the relays and the BS. A more practical approach would encompass the adoption of statistical channel knowledge or of radio maps. In particular, radio maps are a viable way to achieve a sufficiently precise and cheap estimation of the channel gain. Radio maps report for every point in the cell, and every transmitter, the average channel gain. This information is measured once and then updated when new measures are available [14].

III. Wireless communication protocol

We propose a wireless communication protocol which makes use of cooperative relays. The main idea behind our protocol is as follows. First, split the original message into smaller chunks with no redundancy, i.e., all the chunks are necessary to recover the original message m. Second, assign each chunk to a different relay in such a way that the area in which it is possible to correctly decode all the chunks (denoted as critical area (CA)) is centered around the IR and is sufficiently small. Third, in order to prevent an arbitrarily powerful A to see an increased CA, select a number of relays to transmit a pseudo-random noise of controlled power.

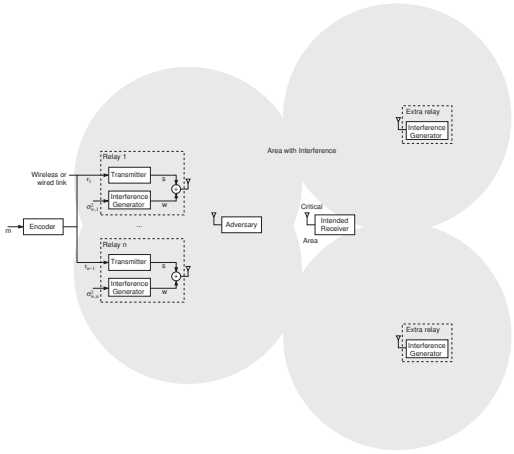

Fig. 2. Interactions between the entities in the system. Here, it is highlighted the role of the interference-relays.

Our protocol can be considered a wireless communication *framework*, and can be schematized as follows.

- **Setup phase**

The BS first locates the IR and the available relays. It then selects two sets R_S and R_I of relays: R_S are the signal-relays for message transmission and R_I are the interference-relays for noise generation. Such selection is based on criteria such as those detailed in Section III-A.

- **Transmit phase**

Message transmission: The BS separates message m into chunks which are distributed to the signal-relays in R_S. It also transmits values for interference to relays in R_I.
Interference Generation: While the signal-relays simply forward the chunks to the IR, as per standard relay, interference-relays in R_I, equipped with an interference generator, emit a pseudo-random sequence emulating Gaussian noise, which creates an artificial noise floor in accordance with the BS's instructions. The interference generated to the IR from the interference-relay is henceforth denoted as $\bar{I}_{IR}$.

- **Receive phase**

The IR retrieves *all* the chunks to recover the message.

The key interactions between the entities in our protocol are depicted in Fig. 2. We next provide details to illustrate how to implement our protocol in practice.

A. *Setup Phase*

- *Position retrieval*

At first, the BS needs to retrieve the position of the IR and the relays. Some relays are infrastructure relays, and their position is known *a priori*. Consider, however, that in LTE-A and 5G even mobile devices can be used by the BS as a potential relay. In this case their position needs to be acquired. The position of the IR can also be determined by means of GPS or similar location sensors and signaled to the BS by the device.

- *Relay discard*

The BS has now a list of available relays in the area of interest of the BS. However, this list can be cumbersome,

especially if D2D relaying is admitted. In order to reduce the list dimension, it is possible to discard the relays that do not respect a minimal set of features. Instances of such features are: minimum transmit power, available battery, proximity to known malicious users.

- *Relay ranking*

The relays now present in the list are ranked from the one requiring the least amount of power to the one requiring the most amount of power to transmit to the IR. The amount of power is estimated through standard transmission techniques or by means of link budget based on a known path-loss measurement, e.g., present in a radio map.

- *Area drawing*

In this step, the BS computes for each relay the area in which the respective chunk can be decoded. This area can be drawn using two different proposed approaches: geometrical (GB) and radio-map-based (RMB). The GB method requires the BS to compute the maximal receiver radius within which the message can be detected. This can be obtained from conventional path-loss equations and channel modeling. A circle of equal radius is hence drawn around each relay. Conversely the RMB approach requires the BS to use image processing techniques on top of the radio map in order to estimate the channel gain between the relays and each point of the map.

- *Relay Selection*

Relay set R_S. In order to select the signal-relays we propose three different strategies. In the first one, the BS fixes a number number of relays and an exhaustive search is run through the relays in order to minimize the critical area. The purpose is to minimize the geographical zones in which an A can decode all the messages for a given amount of network resource.

In a second strategy, the BS fixes a threshold area and an exhaustive search algorithm is run in order to minimize the number of relays used. Here, the purpose is to minimize the relay usage (and corresponding resource exploitation) guaranteeing that the critical area is below a given threshold.

In a third strategy, the BS fixes a threshold area, and the relays are ranked from the one with the highest channel gain to the one with the lowest channel gain with respect to the IR. Then the BS starts from the first relay in the list, and it adds relays until the critical area falls below the fixed threshold. The purpose is to adopt a minimum amount of power in order to achieve a target CA.

Relay set R_I. The interference creating relays are selected as follows. First, a total interference factor I_R is established. This is the largest interference level that can be created to the IR, and that will need to be compensated by the power at the signal transmitting relays. As a rule of thumb, one can take $I_R = \sigma_r^2$, that is a degradation of 3 dB of SINR for the IR. Relays are thus ranked from the one showing the smallest channel gain to the one with the largest channel gain towards the IR, and are added to the list correspondingly computing the level of total interference created to the IR, until the total interference reaches the threshold I_R.

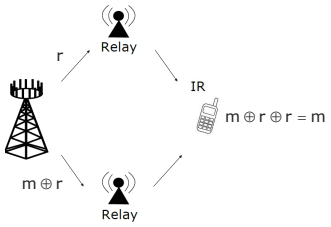

Fig. 3. We depict here a simple run of our protocol. It is designed so that only the IR receives both chunks, namely r and $m \oplus r$, from which the message m can be recovered. Either chunk alone leaks nothing about m, ensuring confidentiality of the message.

B. *Transmit Phase*

- *Message transmission*

Let m be the message BS wishes to deliver to the IR. Let us assume that the message space consists of bit-strings of length n, i.e., $m \in \{0,1\}^n$. If that is not the case, we can find a mapping from the message space to bit-strings of a fixed length. Let ℓ be the number of relays in R_S selected in the Setup phase. The core idea is to split the message into ℓ chunks such that 1) BS distributes one chunk per relay and 2) all chunks are needed to recover message m. The choice of relays in our proposed protocol ensures that the recovery of all ℓ chunks is only possible if a user is in the critical area. If such area surrounds the IR and is small enough, we are guaranteed that only the IR recovers all the chunks. We note that message m represents the information BS wishes to confidentially communicate to IR. We do not limit its nature, i.e., it could be raw content as well as cryptographic key material exchanged for further purposes.

We propose to deliver message m in the following way. BS generates $\ell - 1$ random bit-strings of length n, namely $r_1, r_2, \ldots, r_{\ell-1}$. It then computes $r_\ell = m \oplus r_1 \oplus r_2 \oplus \cdots \oplus r_{\ell-1}$ and, for all i from 1 to ℓ, sends r_i to relay $\mathrm{R}_i \in R_S$. Each relay transmits the received chunk to the IR.

- *Interference Generation*

As can be easily deduced from (3) the critical area dimension strongly depends on the variance of the noise σ_r^2. If an A is equipped with particularly sophisticated hardware, it can be subject to a reduced level of noise and hence observe an increased CA [15]. In this step, the interference-relays attempt to reduce the critical area against an A equipped with a zero-noise receiver. This is done by creating a certain level of fictional interference that behaves as additive noise for all the receivers. In principle, this disturbs in a controlled way also the reception of the IR. However, since the noise is controlled, its negative effect can be compensated by a higher transmission power. For A, on the other hand, the extra interference will drastically reduce the reception capability.

C. *Receive Phase*

The IR computes $r_1 \oplus r_2 \oplus \cdots \oplus r_{\ell-1} \oplus r_\ell$ and recovers the message. Note that only by receiving *all* $r_1, r_2, \ldots, r_{\ell-1}, r_\ell$ can the message m be reconstructed. A simplified instance of this phase is depicted in Fig.3.

IV. Protocol Analysis

In this section, we present an analysis of our protocol. More specifically, we first provide measurements for its performance in terms of the dimension of the CA, showcasing the value of a higher number of signal-relays as well as the need for interference-relays to guarantee that the CA remains sufficiently small. We then discuss the security of our protocol in the presence of an eavesdropper, and suggest possible extensions to account for more powerful, i.e. active, attackers.

A. Simulations

We consider a simple example of a rectangular cell of sides equal to 200m and 300m. The IR is set at the center of the cell, whereas 40 relays are randomly positioned inside the borders. For simplicity, perfect CSI information between each relay and the IR is assumed, and an exponential model of exponent $\alpha = 2$ is considered. All the devices in the network are assumed to be equipped with an isotropic single-antenna, hence the antenna gains are normalized at one. Each relay has a maximum transmit power of 23 dBm, the IR and A noise variances are set to $\sigma^2_{IR} = -90$ dBm and $\sigma^2_A = 120$ dBm, respectively. It is assumed that each message can be correctly decoded if the SINR level is above a threshold $\Gamma = 10$ dB.

The protocol implemented in the simulation operates as follows. First, a fixed predefined number of signal-relays are selected starting from the closest to the IR to the farthest. Each of these relays is assigned a transmission power equal to the minimum necessary power to respect the SINR threshold condition at the IR position, that is

$$P_T = \frac{\sigma^2_{IR} + \bar{I}_{IR}}{G_{IR}} 10^{\frac{\Gamma}{10}}. \quad (4)$$

Note that, under the simplified channel model considered in this experiment, this policy also minimizes the power consumed by the relays. Second, the interference-relays are selected going from the farthest to the closest to the IR. Each relay is assigned its maximum transmit power, and relays are added to the list as long as (i) the interference generated to the IR is below the interference threshold I_{IR}, and (ii) there are available relays that are not already selected as signal-relays.

Monte Carlo simulations are run in order to average among the different possible relay positions. The results of this experiment are reported in Fig. 4 and Fig. 5. Fig. 4 plots the ratio between the CA and the total cell area corresponding to IR's noise level, as a function of the amount of signal-relays. We remark the following.

Remark 1: The dimension of the CA strongly decreases as the number of selected signal-relays increases. This is due to the fact that the CA is the intersection among all the areas in which the single chunks are received with a sufficient SINR.

Remark 2: The correct number of selected signal-relays depends on the precision of the estimated average CSI and the desired CA dimension. In more realistic settings, it is not possible to exploit perfect CSI, hence a certain tolerance on the dimension of the CA should be accounted for.

Fig. 5 plots the dimension of the ratio between the CA and the total cell area corresponding to the A's noise level, as a function of the ratio between the allowed interference level $\bar{I}_{IR}$ and the IR noise level σ^2_{IR}, for three different sets of signal-relays.

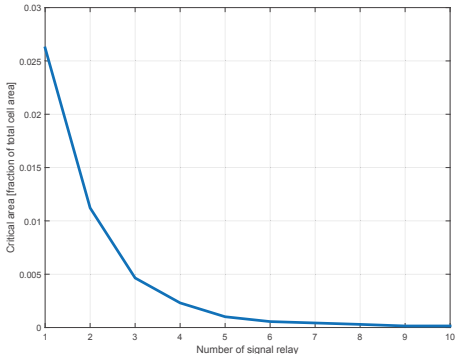

Fig. 4. CA of the IR as a function of the number of the signal-relays.

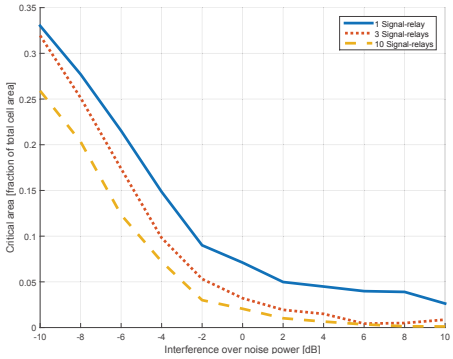

Fig. 5. CA of the A as a function of the number of the signal-relays and the interference generated to the IR.

Remark 3: From Fig. 5 we see that increasing the number of signal-relays does not reduce efficiently the CA from A's point of view. This demonstrates that policies based only on distributing the message among different relays are unable to guarantee the privacy of a message.

Remark 4: The level of interference generated to the IR strongly impacts the A's ability to eavesdrop a message. However one should consider that the interference also deteriorates the performance of the IR, and needs to be compensated by a higher transmission power as indicated in (4). Moreover, such a technique potentially deteriorates the performance of other receivers present in the same cell. As a consequence, too high levels of interference are undesirable. As a rule of thumb, a level of $\bar{I}_{IR} = \sigma^2_{IR}$ appears as a good tradeoff between security and performance.

B. Security analysis and extensions

Since receiving *all* the chunks can only happen inside the critical area, our protocol provides message confidentiality against passive attacks, i.e., eavesdropping, whenever the adversary is outside of the critical area. Furthermore, the adversary recovers no partial information on the message even if it recovers some of the chunks. In particular, r_1, r_2,..., $r_{\ell-1}$ are random bit-strings and therefore do not contain any information on m, and r_ℓ is a one-time pad for m and therefore

information-theoretically hides the message. So, as long as we can ensure a sufficiently small CA, our protocol provides confidentiality to wireless communication.

We can envisage to enhance the security of our protocol by considering the following extensions.

Let Π be a public-key encryption scheme consisting of algorithms GenKey, Enc and Dec, as per standard definition [16]. Let each possible receiver IR be equipped with a public key pk and a corresponding secret key sk, obtained by running Π's key generation algorithm GenKey. Let BS split the message m into chunks as in Section III-B. Further, for all i from 1 to ℓ, let BS encrypt r_i with pk, and send $\mathsf{c}_i = \mathsf{Enc}(\mathsf{pk}, r_i)$ to relay R_i. Each relay transmits the received ciphertext to the IR, who runs Dec using sk on each received ciphertext and reconstructs the message. Note that only the IR can decrypt using sk, and message m can be reconstructed only upon receiving all ciphertexts encrypting the r_is. By adding encryption, we strengthen the security of our protocol against passive attacks to hold end-to-end (as opposed to just *outside* the critical area). This means that even if the eavesdropper receives all the encrypted chunks, i.e., the adversary is in the critical area, it cannot recover m since it does not hold the secret key needed for decryption.

Let Σ be a digital signature scheme consisting of algorithms Gen, Sign and Ver, as per standard definition [16]. Let (sigk, vk) be, respectively, the signature and verification keys BS is equipped with by running Gen. This method is as above where additionally BS signs each ciphertext with sigk before distributing them to the relays, which forward each received signed ciphertext to the IR. The IR first verifies with the verification key vk each ciphertext it receives from the relays, and then, if all verifications succeed, decrypts and recomputes the message as usual. By adding a signature to the sent encrypted chunks we provide message authentication, i.e., the IR is guaranteed that, if the signature verifies, the signed material originates from the BS. This addition is a security enhancement since the resulting protocol resists passive attacks and a class of active attacks, namely pollution attacks. Indeed, failure of a signature to verify allows the IR to detect that the attacker has injected a malicious packet so as to prevent the IR from reconstructing the correct message.

V. Conclusions

This papers proposes a method to increase the confidentiality of wireless communication between a base station and a receiver, when multiple attackers with unknown positions are present in the network. The main idea is to exploit cooperative transmission via signal-relays to create an exclusive geographical zone, denoted critical area (CA), in which the message can be correctly decoded. However, the dimension of such zone is shown to be dependent on the noise floor at the receiver. To guarantee that the size of the CA remains sufficiently small, even in the presence of attackers equipped with enhanced hardware (at the limit with noiseless receivers), a selected set of interference-relays appropriately transmits a pseudo-random noise. Different relay-selection policies are proposed, and numerical simulations show that, if perfect channel state information (CSI) is available, it is possible to arbitrarily reduce the dimension of the CA. It is argued that, when only imperfect statistical CSI is available, a certain tolerance in the dimension of the CA has to be accounted for. This reduces the secrecy level with respect to the case with perfect CSI, but does not compromise it. A specific cryptographic technique, tailored for creating different enciphered chunks, is argued to protect the confidentiality of the message in the presence of passive as well as active attackers.

References

[1] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern, "RSA-OAEP is secure under the RSA assumption," *J. Cryptology*, vol. 17, no. 2, pp. 81–104, 2004.

[2] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, 1996, pp. 104–113.

[3] J. Manger, "A chosen ciphertext attack on RSA optimal asymmetric encryption padding (OAEP) as standardized in PKCS #1 v2.0," in *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, 2001, pp. 230–238.

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

[5] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul 1978.

[6] T. D. Stojanovski and N. Marina, "Secure wireless communications via exhaustive cooperative jamming against a single eavesdropper," in *Telecommunications Forum (TELFOR), 2012 20th*, Nov 2012, pp. 384–387.

[7] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: state of the art and beyond," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 32–39, Dec 2015.

[8] V. Pellegrini, F. Principe, G. de Mauro, R. Guidi, V. Martorelli, and R. Cioni, "Cryptographically secure radios based on directional modulation," in *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, May 2014, pp. 8163–8167.

[9] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, March 2010.

[10] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5g cellular networks: challenges, solutions, and future directions," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 86–92, May 2014.

[11] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 6, pp. 2006–2021, Jun. 2014.

[12] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive mimo: An overview on passive eavesdropping and active attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[13] Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 215–228, Jan 2015.

[14] K. Connelly, Y. Liu, D. Bulwinkle, A. Miller, and I. Bobbitt, "A toolkit for automatically constructing outdoor radio maps," in *International Conference on Information Technology: Coding and Computing (ITCC'05)*, vol. 2, Apr. 2005, pp. 248–253.

[15] V. Volkov, D. Vavriv, E. Bulakh, and A. Kravtsov, "A broadband low-noise receiver front-end with ultrawide bandwidth," in *International Conference on Microwaves, Radar, and Wireless Communication (MIKON)*, Jun. 2014, pp. 1–4.

[16] J. Katz and Y. Lindell, *Introduction to modern cryptography*. Chapman & Hall/CRC, 2008.