Secure Communications with D2D Cooperation

Samah A. M. Ghanem*, Munnujahan Ara†,
* Mobile Communications Department, Eurecom, Sophia Antipolis, France
Email: samah.ghanem@eurecom.fr

† Khulna University, Khulna-9208, Bangladesh
Email: munnujahan@gmail.com

***Abstract*—Device to Device (D2D) communication provides a promising technique for 5G wireless networks, supporting higher data rates. Security of data transmission over wireless clouds could put constraints on devices; whether to cooperate or not. Therefore, our aim is to provide analytical framework for the security at the physical layer and to define the constraints embodied with cooperation in wireless clouds[1]. In this paper, two legitimate transmitters Alice and John cooperate to increase the reliable transmission rate received by their common legitimate receiver Bob, where one eavesdropper, Eve exists. We propose a distributed algorithm that allows the devices to select whether to cooperate or not and to adapt their optimal power allocation based on the cooperation framework selected. Moreover, we define distance constraints to enforce the benefits of cooperation between devices in a wireless cloud.**

I. Introduction

The Wiretap channel models scenarios of the data transmission under security attacks on the physical layer [1]. Several optimal power allocation interpretations that aim to maximize the secure and reliable information rates exist in the literature. Such designs were done for different channel models, for example, for the two user MAC Gaussian channel [2], or for cooperative virtual MIMOs [3] by directly maximizing the mutual information, or via optimizing other design criterion such as, minimizing the mean square error [4], or minimizing the bit error rate [5]. In [6], the authors address secure communications of one source-destination pair with the help of multiple cooperating relays in the presence of one or more eavesdroppers with different cooperative schemes. In [7], the authors devise several cooperation strategies. They consider a deaf helper phenomenon, where the relay is able to facilitate secure communications while being totally ignorant of the transmitted messages. In [8], the author studied the security of communication for the relay channel under the situation that some of the transmitted messages are confidential to the relay. Moreover, in [9], the authors considered cooperative jamming where a relay equipped with multiple antennas transmits a jamming signal to create interference at the eavesdropper. They proposed design methods to determine the antenna weights and transmit power of source and relay, so that the system secrecy rate is maximized. In [10], the authors studied three opportunistic relay selection approaches under security constraints. They show that optimal relay selection outperforms conventional and minimum selection methods in terms of secure achievable rates. Optimal power allocation strategies were derived for a zero sum game with an unfriendly jammer in [11]. In [12], the authors propose a distributed game-theoretic method for power allocation in bi-directional cooperative communication. They proved the benefits of bi-directional cooperation between nodes closer to each other.

In this paper, we focus on a wireless communications scenario where transmitting devices cooperate, while an eavesdropper device overhears their transmissions, assuming that this eavesdropper is only overhearing their own direct transmissions. In fact, this assumption is basically based on the lack of knowledge of the eavesdropper - who aims to decode their transmitted messages - that a message of one transmitter could be mixed over time or that any cooperation could exist. Of particular relevance are the benefits of D2D cooperation to secure data transmission, and more relevant is to study when and where cooperation should exist, building a framework of distance constraints which could allow devices in a cloud to decide to go for cooperation, to cooperate from one side, not to cooperate, or to change location avoiding any distance attacks. We mean by a distance attack, is the capability of one eavesdropper device to experience a better version of the transmitted message than the legitimate receiving device. Under such distance constraints, the legitimate transmitters and receivers could choose to move far from an attacking device as a defense strategy.

In this paper, we consider a scenario which is more of practical relevance where two side cooperation exists. The usual assumption of one side cooperation is addressed for analytical purposes only. However, we consider cooperation of bi-directional two relay devices to show that 'a real egoistic behavior is to cooperate', [13]. Our work differs from other works not only on this assumption, but we have also considered that the devices under certain distance constraints switch their mode of cooperation from Relay to MAC or vice versa or choose not to cooperate. This assumption is of particular relevance in a D2D cooperation within a wireless cloud to assure that cooperation will not harm one or the other device reliable and secure transmission rates. We are interested in optimal power allocation strategies under different scenarios, when two legitimate transmitters/receivers Alice and John cooperate in a bi-directional way to increase their secrecy rate, i.e., to increase the secure and reliable transmission rate

[1] A wireless cloud is a small fixed size wireless network with known cooperative devices. Such devices define jointly their system configuration and schedule their transmission in a certain mode of cooperation.

received by Bob, their common legitimate receiver during which an eavesdropper, Eve tries to eavesdrop both.

II. System Model

We consider a model that includes two legitimate transmitters Alice and John, and one common legitimate receiver, Bob. One eavesdropper Eve tries to decrease the security of both transmitters trying to decode the messages received by both transmitters. The communications between different parties are done over a point to point bi-directional links. The transmitted message from transmitter i is defined as x_i, and the received message by the receiver k is defined as y_k. Considering that Alice and John are relay devices who cooperate in relaying each others data to Bob who receives two vectors from Alice and from John, assuming that each will relay a replica of the other's main message as follows,

$$y_{ab} = G_{ab}\sqrt{P_a}x_a + G_{ab}\sqrt{P_{ab}}x_j + n_1 \tag{1}$$

$$y_{jb} = G_{jb}\sqrt{P_j}x_j + G_{jb}\sqrt{P_{jb}}x_a + n_2 \tag{2}$$

Eve receives two vectors from Alice and John; assuming that Eve will receive the main message of each via overhearing, and will not be aware of the relayed part, this assumption is done for the sake of simplicity, as follows,

$$y_{ae} = G_{ae}\sqrt{P_a}x_a + \bar{n}_1 \tag{3}$$

$$y_{je} = G_{je}\sqrt{P_j}x_j + \bar{n}_2 \tag{4}$$

$y_{ab} \in \mathbb{C}^n$ and $y_{jb} \in \mathbb{C}^n$ represent the received vectors of complex symbols at Bob's side from Alice and John; respectively, $y_{ae} \in \mathbb{C}^n$ and $y_{je} \in \mathbb{C}^n$ represent the received vectors of complex symbols at Eve's side from Alice and John; respectively. $x_a \in \mathbb{C}^n$ and $x_j \in \mathbb{C}^n$ represent the vectors of complex transmit symbols with zero mean $\mathbb{E}[x_a x_a^T], \mathbb{E}[x_j x_j^T]$ and identity covariance $\mathbb{E}[x_a x_a^\dagger], \mathbb{E}[x_j x_j^\dagger]$, respectively. $n_1 \in \mathbb{C}^n$, $n_2 \in \mathbb{C}^n$, $\bar{n}_1 \in \mathbb{C}^n$, and $\bar{n}_2 \in \mathbb{C}^n$ represent vectors of circularly symmetric complex Gaussian noises with zero mean and identity covariance. G_{ik} represents the complex gains[2] of the channels between transmitter i and receiver k. $\sqrt{P_{jb}}$ and $\sqrt{P_{ab}}$ represent the relay power used by John and Alice respectively to relay each others data. $\sqrt{P_a}$ and $\sqrt{P_j}$ represent the transmitted power for Alice and John used respectively to transmit their own data[3]. If relaying is precluded, the terms including $\sqrt{P_{ab}}$ and $\sqrt{P_{jb}}$ will be omitted from (1) and (2), respectively. The achievable secrecy rate that each of the legitimate devices will try to maximize is called (Cs), assuming Maximum Ratio Combiner (MRC) at Bob's side.

III. D2D Cooperation Framework and Problem Formulation

A. D2D Cooperation Framework

The cooperation setup in this paper is between two parties who cooperate to reach their optimum strategies in service request way, such that the one who request the relay service will follow a strategy of cooperation defined by the other device, where both devices at the end cooperate in relaying each others data, or not, in different cooperation levels. Based on the objective functions defined for each device, the devices choose the optimal power allocation, that may correspond to a cooperation decision when cooperation is of benefit, to minimal cooperation in a multiple access channel (MAC) mode, or no cooperation when there is no benefits expected. Therefore, first, we consider the scenario where there is cooperation with relaying. Second, we consider the scenario where there is cooperation without relaying data. Third, we consider a scenario where no cooperation exists. Fourth, we consider a scenario when there is cooperation from one side and without relaying data. The later two scenarios considered give insightful solutions through which secure communication via D2D cooperation in a wireless cloud can be evaluated.

B. Problem Formulation

Consider the objective functions per cooperative device, Alice with $Cs1$, and John with $Cs2$. The maximum achievable secrecy rate for Alice,

$$Cs1 = max\ R_{ajb} - R_{ae} \tag{5}$$

$$Subject\ \ to,\ P_j + P_{jb} \leq P_J \tag{6}$$

$$Therefore,\ \ {P_{jb}}^* = arg \max_{\zeta P_{jb}, P_{ab}/\zeta} R_{ajb} - R_{ae}, \tag{7}$$

with ${P_j}^* = P_J - {P_{jb}}^*$, and $0 \leq \zeta \leq 1$. $R_{ajb} = log(1 + SNR_{ab} + f(SNR_{aj}, SNR_{jb}))$, when John is relaying Alice data, [14]. When no relaying is considered R_{ajb} is the same as,

$$R_{ab} = I(x_a; y_{ab}) = log(1 + SNR_{ab}) \tag{8}$$

$$R_{ae} = I(x_a; y_{ae}) = log(1 + SNR_{ae}) \tag{9}$$

The maximum achievable secrecy rate for John,

$$Cs2 = max\ R_{jab} - R_{je} \tag{10}$$

$$Subject\ \ to,\ P_a + P_{ab} \leq P_A \tag{11}$$

$$Therefore,\ \ {P_{ab}}^* = arg \max_{Pab/\zeta, \zeta P_{jb}} R_{jab} - R_{je}, \tag{12}$$

with ${P_a}^* = P_A - {P_{ab}}^*$, and $0 \leq \zeta \leq 1$. $R_{jab} = log(1 + SNR_{jb} + f(SNR_{ja}, SNR_{ab}))$, when Alice is relaying John data, [14]. When no relaying is considered R_{jab} is the same as,

$$R_{jb} = I(x_j; y_{jb}) = log(1 + SNR_{jb}) \tag{13}$$

$$R_{je} = I(x_j; y_{je}) = log(1 + SNR_{je}) \tag{14}$$

[2] Notice that the channel gains are considered to be fixed over the transmission time of (x_a, x_j). Therefore, $G_{ab}(\sqrt{P_a}x_a + \sqrt{P_{ab}}x_j)$ and $G_{jb}(\sqrt{P_{jb}}x_a + \sqrt{P_j}x_j)$ are associated to the transmission of the main and relayed transmitted symbols over each link.

[3] Notice that the model considers that the power P_A, P_J for Alice and John, respectively is divided between the main transmitted signals and the relayed ones.

Where SNR_{ik} is the received signal to noise ratio between transmitter i and receiver k.

$$SNR_{ik} = \frac{G_{ik}P_i}{\sigma^2} \tag{15}$$

G_{ik} is the channel gain between different devices, and σ^2 is the noise power, considered as fixed over all links. Given that the framework will include bi-directional cooperation, and including relaying with ζ cooperation level between Alice and John. The received SNR via the path of transmitter i, relay point r, and receiver k will be considered as follows, [12], [14]

$$f(SNR_{ir}, SNR_{rk}) = \frac{G_{ir}G_{rk}P_iP_{rk}}{\sigma^2(G_{ir}P_i + G_{rk}P_{rk} + \sigma^2)} \tag{16}$$

Therefore, we need to analyze a set of scenarios where we can derive the optimal power allocation required to maximize the achievable secrecy rates, and therefore to get insights on the effect of cooperation and relaying on the secrecy rates. In particular, we will devise the optimal power allocation set $({P_{ab}}^*, {P_{jb}}^*)$ used for relaying, and $({P_a}^*, {P_j}^*)$ used for main data transmission. Where ${P_a}^* = P_A - {P_{ab}}^*$, and ${P_j}^* = P_J - {P_{jb}}^*$.

IV. Cooperative Relays

We consider the scenario where John is trying to relay Alice data with power P_{jb} and Alice is trying to relay John data with power P_{ab} using the shared bi-directional link between them. Both relays utilize Amplify and Forward (AF) protocol for cooperation. The cooperation level defines the main cooperation point in the mathematical formulation of the optimization problem. The achievable secrecy rate and their corresponding optimization problem can be written as follows,

$$\begin{aligned} Cs1_{\zeta P_{jb}} = &\max_{\zeta P_{jb}} \; log(1 + SNR_{ab} + f(SNR_{aj}, SNR_{jb})) \\ &- log(1 + SNR_{ae}) \end{aligned} \tag{17}$$

$$Subject \;\; to, \; P_j + P_{jb} \leq P_J \tag{18}$$

$$\begin{aligned} Cs2_{\frac{P_{ab}}{\zeta}} = &\max_{\frac{P_{ab}}{\zeta}} \; log(1 + SNR_{jb} + f(SNR_{ja}, SNR_{ab})) \\ &- log(1 + SNR_{je}) \end{aligned} \tag{19}$$

$$Subject \;\; to, \; P_a + P_{ab} \leq P_A \tag{20}$$

Since the one who is providing the service first dictates the cooperation level, the formulation is defined as in (17) and (19). Let Alice be the one who first request the relay service from John. Therefore, the power John decides to cooperate with will dictate the response of Alice. Hence, the first objective (utility) $Cs1$ will lead to the optimal relay power P_{jb}: John uses to relay Alice data. On the other hand, the second objective (utility) $Cs2$ is to maximize John achievable secrecy rate by letting Alice relay the data of John to Bob, thus we derive the optimal relay power P_{ab}: Alice uses to relay John data to Bob. λ is the Lagrange multiplier. Thus, applying the Karush-Kuhn-Tucker (KKT) conditions, it follows an optimal power allocation policy, see [15]. Assuming that John will be more cooperative with Alice; the power cooperation is defined as,

$$P_{ab} = \zeta P_{jb} \tag{21}$$

Solving (17), the cooperative optimal power allocation for the cooperative scenario through relaying which increases the secrecy rate for Alice is as follows,

$$\psi_1 {P_{jb}}^3 + \psi_2 {P_{jb}}^2 + \psi_3 P_{jb} + \psi_4 = 0 \tag{22}$$

where ψ_i are variables with respect to the channel gains and the power P_a.

P^*_{jb} is the solution of the third order equation, which is the optimal power allocation John will decide to cooperate with Alice to relay her data in order to increase her secrecy.

Similarly, solving (19), the cooperative optimal power allocation for the cooperative scenario through relaying which increases secrecy rate for John is as follows,

$$\beta_1 {P_{ab}}^3 + \beta_2 {P_{ab}}^2 + \beta_3 P_{ab} + \beta_4 = 0 \tag{23}$$

where β_i are variables with respect to the channel gains and the power P_j.

P^*_{ab} is the solution of the third order equation, which is the optimal power allocation Alice will use to cooperate with John to relay his data in order to increase his secrecy. Therefore, the optimal power allocation will be as provided in the following Theorem.

Theorem 1: The optimal power allocation that maximizes the achievable secrecy rate of the cooperative scenario with relaying is the solution of (17) subject to (18) and (19) subject to (20) identified with the optimal set (P^*_{ab}, P^*_{jb}) in (22) and (23) respectively with ${P_{ab}}^* = \zeta P_{jb}$

V. Cooperative MAC

A. Cooperative Scenario without Relaying

In this scenario, the devices will not work as relays, so both devices will cooperate in their own transmissions power to maximize the secrecy rate of the other. Note that this scenario is a special case of the previous one, where the SNR that contributes to the extra rates through relayed data will disappear from the equation. The achievable secrecy rates are defined as follows,

$$Cs1_{\zeta P_j} = \max_{\zeta P_j} \; log(1 + SNR_{ab}) - log(1 + SNR_{ae}) \tag{24}$$

$$Subject \;\; to, \; P_j \leq P_J \tag{25}$$

$$Cs2_{\frac{P_a}{\zeta}} = \max_{\frac{P_a}{\zeta}} \; log(1 + SNR_{jb}) - log(1 + SNR_{je}) \tag{26}$$

$$Subject \;\; to, \; P_a \leq P_A \tag{27}$$

Therefore, the optimal power allocation will be as provided in the following Theorem.

Theorem 2: The optimal power allocation that maximizes the achievable secrecy rates of the cooperative scenario without relaying is the solution of (24) subject to (25) and (26) subject to (27) identified with the optimal set (P^*_a, P^*_j) given by the following closed forms,

$$P_a{}^* = \frac{\zeta}{2}\sqrt{\frac{\lambda^2\sigma^4(G_{jb}+G_{je})^2 + 4\lambda G_{jb}G_{je}(\sigma^2 G_{jb} - \sigma^2 G_{je} - \lambda\sigma^4)}{(\lambda G_{jb}G_{je})^2}} - \sigma^2(\frac{1}{G_{je}} + \frac{1}{G_{jb}}) \quad (28)$$

$$P_j{}^* = \frac{1}{2\lambda\zeta}\sqrt{\frac{(\sigma^2 G_{ab}+\sigma^2 G_{ae})^2 + 4\lambda G_{ab}G_{ae}(\sigma^2 G_{ab} - \sigma^2 G_{ae} - \lambda\sigma^4)}{(G_{ab}G_{ae})^2}} - \sigma^2(\frac{1}{G_{ae}} + \frac{1}{G_{ab}}) \quad (29)$$

Notice that the optimal cooperation level can be derived finding out $\frac{\partial P_j}{\partial \zeta}$ or $\frac{\partial P_a}{\partial \zeta}$. On the other hand, we can derive also the SNR over each link at which the cooperation is optimal.

B. Cooperation from one side

This scenario consider that John helps Alice, while Alice does not help John. So, this scenario considers a cooperation at which Alice and John are concerned to maximize her own secrecy rate, since Eve is targeting Alice only. However, no relaying is considered here.

We define the optimization problem for the scenario of cooperation from one side as follows,

$$Cs1_{P_a} = \max_{P_a} \; log(1 + SNR_{ab}) - log(1 + SNR_{ae}) \quad (30)$$

$$Subject \;\; to, \; P_a \leq P_A \quad (31)$$

$$Cs2_{\zeta P_j} = \max_{\zeta P_j} \; log(1 + SNR_{ab}) - log(1 + SNR_{ae}) \quad (32)$$

$$Subject \;\; to, \; P_j \leq P_J \quad (33)$$

Such scenario will be a mixed scenario from the previous scenario and the one in the next section. Therefore, the optimal power allocation will be as provided in the following Theorem.

Theorem 3: The optimal power allocation that maximizes the achievable secrecy rates of the cooperative scenario from one side is the solution of (30) subject to (31) and (32) subject to (33) identified with the optimal set (P_a^*, P_j^*) given by the following closed forms,

$$P_a{}^* = \frac{1}{2}\sqrt{\frac{\lambda^2\sigma^4(G_{ab}+G_{ae})^2 + 4\lambda G_{ab}G_{ae}(\sigma^2 G_{ab} - \sigma^2 G_{ae} - \lambda\sigma^4)}{(\lambda G_{ab}G_{ae})^2}} - \sigma^2(\frac{1}{G_{ae}} + \frac{1}{G_{ab}}) \quad (34)$$

$$P_j{}^* = \frac{1}{2\lambda\zeta}\sqrt{\frac{(\sigma^2 G_{ab}+\sigma^2 G_{ae})^2 + 4\lambda G_{ab}G_{ae}(\sigma^2 G_{ab} - \sigma^2 G_{ae} - \lambda\sigma^4)}{(G_{ab}G_{ae})^2}} - \sigma^2(\frac{1}{G_{ae}} + \frac{1}{G_{ab}}) \quad (35)$$

VI. No-Cooperation

In this scenario, no cooperation exists, thus every device wants to maximize its own utility with its own resources. The reasoning behind considering this scenario is to study the implications of cooperation in the solution; i.e., to provide analytical insight when the cooperation is of benefit.

We define the optimization problem for the scenario of no cooperation as follows,

$$Cs1_{P_a} = \max_{P_a} \; log(1 + SNR_{ab}) - log(1 + SNR_{ae}) \quad (36)$$

$$Subject \;\; to, \; P_a \leq P_A \quad (37)$$

$$Cs2_{P_j} = \max_{P_j} \; log(1 + SNR_{jb}) - log(1 + SNR_{je}) \quad (38)$$

$$Subject \;\; to, \; P_j \leq P_J \quad (39)$$

Therefore, the optimal power allocation will be as provided in the following Theorem.

Theorem 4: The optimal power allocation that maximizes the achievable secrecy rates for the non-cooperative scenario is the solution of (36) subject to (37) and (38) subject to (39) identified with the optimal set (P_a^*, P_j^*) given by the following closed forms,

$$P_a{}^* = \frac{1}{2}\sqrt{\frac{\lambda^2\sigma^4(G_{ab}+G_{ae})^2 + 4\lambda G_{ab}G_{ae}(\sigma^2 G_{ab} - \sigma^2 G_{ae} - \lambda\sigma^4)}{(\lambda G_{ab}G_{ae})^2}} - \sigma^2(\frac{1}{G_{ae}} + \frac{1}{G_{ab}}) \quad (40)$$

$$P_j{}^* = \frac{1}{2}\sqrt{\frac{\lambda^2\sigma^4(G_{jb}+G_{je})^2 + 4\lambda G_{jb}G_{je}(\sigma^2 G_{jb} - \sigma^2 G_{je} - \lambda\sigma^4)}{(\lambda G_{jb}G_{je})^2}} - \sigma^2(\frac{1}{G_{je}} + \frac{1}{G_{jb}}) \quad (41)$$

Notice that the solution set of this scenario is a special case of the solution set of the previous scenario when the cooperation level $\zeta = 1$, as well as the constant $\lambda = 1$. In fact, in a non-cooperative scenario, with per device total power constraint, it can be easily shown through the Lagrangian and the KKT conditions that the optimal strategy for each device is to allocate their own total maximum power, i.e., $(P_a^*, P_j^*) = (P_A, P_J)$.

VII. D2D Cooperative Distance

Cooperation may be not beneficial for both parties, so no-cooperation will be one response from one or both devices if the cooperation will adversely affect its secrecy. Hence, it follows the importance of the distance considerations between cooperating parties. Thus, we consider the distance between Alice and John so that cooperation beneficially exists; otherwise John will adversely affect Alice. The distances between different devices are considered such that d_{ik} is the distance between transmitter i and receiver k. Then, using the relation between the path loss exponent $d_{ik}^{-\eta}$ which relates the loss of the transmitted power over the distance of the transmission path, we can substitute the distance corresponding to the SNR in the defined optimization problems. In fact, inducing the distances between Alice, Eve, and Bob, or John, Eve, and Bob is not enough to make D2D cooperation exit. Therefore, we need to consider the distance between Alice and John in the cooperation problem. Consider the effect of Alice on John and vice versa as an interference effect, thus the cooperative optimization problem in scenario-A, section-V is such that the information rate from Alice to John and vice versa will influence one another in a positive way, i.e., it is used to cancel the rate decay (leakage) to Eve. Thus, the optimization problem can be written as follows,

$$Cs1_{\zeta P_j} + log(1 + SNR_{ja}) \quad (42)$$

$$Cs2_{P_a/\zeta} + log(1 + SNR_{aj}) \tag{43}$$

From a power allocation perspective, this formulation means that, $log(1 + SNR_{ja})$ would substitute for $log(1 + SNR_{ae})$ and $log(1 + SNR_{aj})$ would substitute for $log(1 + SNR_{je})$ as well, otherwise cooperation will not exist. Substitute the distances into the conditions discussed we get the following,

$$\frac{\zeta G_{aj}}{{d_{ab}}^2\sigma^2 + \zeta G_{aj}P_j} \leq \frac{\zeta G_{ae}}{{d_{ae}}^2\sigma^2 + \zeta G_{ae}P_j} \tag{44}$$

and,

$$\frac{G_{ja}}{\zeta {d_{ab}}^2\sigma^2 + G_{ja}P_a} \leq \frac{G_{je}}{\zeta {d_{je}}^2\sigma^2 + G_{je}P_a} \tag{45}$$

This leads to the condition that, if we need the cooperation to be of benefit for one or both parties, then the following distance constraints should exist. Similar analysis of the effect of the distance between different devices in a wiretap setup without cooperative scenarios has concluded that there is a distance consideration for which the secrecy can exist, otherwise not, and they call it secrecy coverage distance, [16]. Therefore, the distance between Alice and Eve should be,

$${d_{ae}}^\eta \leq \frac{G_{ae}}{G_{aj}}{d_{aj}}^\eta, \tag{46}$$

and the distance between John and Eve should be,

$${d_{je}}^\eta \leq \frac{G_{je}}{G_{ja}}{d_{aj}}^\eta \tag{47}$$

If such distance considerations are met, then the cooperative power allocation strategies are optimal in the sense of optimal cooperation level. Hence, Eve can try to break such distance constraints going more near to one or both devices she wants to eavesdrop, i.e., moving the cooperation level into less cooperative and so the achievable secure and reliable rates into lower bounds.

VIII. Algorithm

We introduce a distributed algorithm that finds the optimal power allocation set that secures the data transmission in our model. First, the devices will check the distance constraints to test if cooperation is of benefit. If yes, then the devices will initiate the cooperation and will decide to cooperate jointly, to cooperate from one side, if not, the devices will chose not to cooperate. Therefore, the optimal power allocation for Alice and John will follow the solution set of the scenarios discussed.

IX. Simulation Results

We shall now present a set of illustrative results that cast further insights to the problem. We choose a cooperation level $\zeta = 0.8$, channels gains are $G_{ab} = 0.4$, $G_{ae} = 0.3$, $G_{ja} = 0.2$, $G_{jb} = 0.5$, and $G_{je} = 0.3$. We now analyze the set of scenarios considered. Notice that we have chosen channel gains for a non-degraded case, where the channels between legitimate transmitters and the legitimate receiver are stronger than those between legitimate transmitters and the illegitimate receiver. Figure 1 illustrates the achievable secrecy rate for Alice with respect to the main power P_a and the power P_{jb} used to relay her data. Figure 2 illustrates the achievable secrecy rate for John with respect to the main power P_j and the power P_{ab} used to relay his data. As expected, the framework of cooperation via relaying adds significantly to the achievable secure data rates of each device compared to the data rates achieved without cooperation. The difference between the gains in the data rates for Alice and John is due to the stronger channel gain that John enjoys between his device and the receiver device, Bob.

Algorithm 1: Optimum Cooperative Power Allocation.

```
Alice→initiates cooperation mode; Alice→requests relay service
Input : distance $d_{ab}$, $d_{ae}$, $d_{jb}$, $d_{je}$, $d_{aj}$.
if $\frac{\zeta G_{aj}}{{d_{ab}}^2\sigma^2+\zeta G_{aj}P_j} \leq \frac{\zeta G_{ae}}{{d_{ae}}^2\sigma^2+\zeta G_{ae}P_j}$ and
$\frac{G_{ja}}{\zeta {d_{ab}}^2\sigma^2+G_{ja}P_a} \leq \frac{G_{je}}{\zeta {d_{je}}^2\sigma^2+G_{je}P_a}$ and
${d_{ae}}^2 \leq \frac{G_{ae}}{G_{aj}}{d_{aj}}^2$ and ${d_{je}}^2 \leq \frac{G_{je}}{G_{ja}}{d_{aj}}^2$ then
John→accepts to cooperate and decide cooperation with level $\zeta$ and request Alice
relay service.  if Alice accepts to cooperate; then
    $Output$ : 1 is executed.

else if John→rejects to relay data and devices go to MAC cooperative mode; then
    $Output$ : 2 is executed.

else if John→accepts to cooperate from one side; then
    $Output$ : 3 is executed.

else if John→rejects to cooperate and devices go to non-cooperative mode; then
    $Output$ : 4 is executed.

else
    $Output$ : 4 is executed.

Output: 1
The optimal cooperative relay power:
$({P_{ab}}^*, {P_{jb}}^*)$ solving (22) and (23), respectively
Output: 2
The optimal cooperative main power:
$({P_a}^*, {P_j}^*)$ in (28) and (29)
Output: 3
The optimal cooperative / non-cooperative main power:
$({P_a}^*, {P_j}^*)$ in (34) and (35)
Output: 4
The optimal non-cooperative main power:
$({P_a}^*, {P_j}^*)$ in (40) and (41)
Devices keep checking distance constraint and adaptively allocate their optimal
power based on the cooperation scenario selected.
```

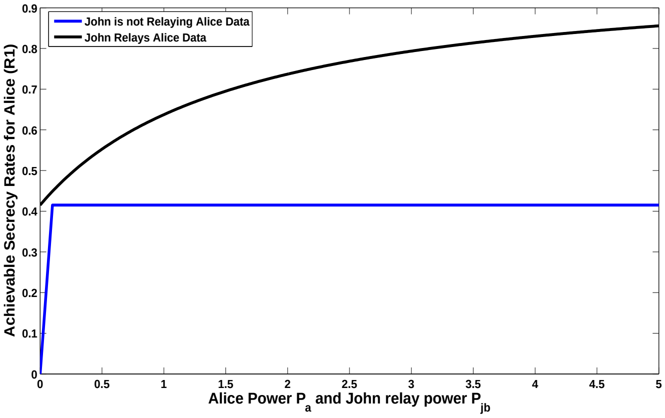

Fig. 1. Secure data rates achievable ($bits/sec/Hz$) by Alice (with and without relaying) with respect to the main power P_a, (when no cooperation exists) and the relay power P_{jb} (when $P_a = P_A$ is fixed and equals 5 and cooperative relaying is active).

Figure 3 illustrates the achievable secrecy rates of Alice with respect to her distance from Bob, when $\eta = 2$ for free

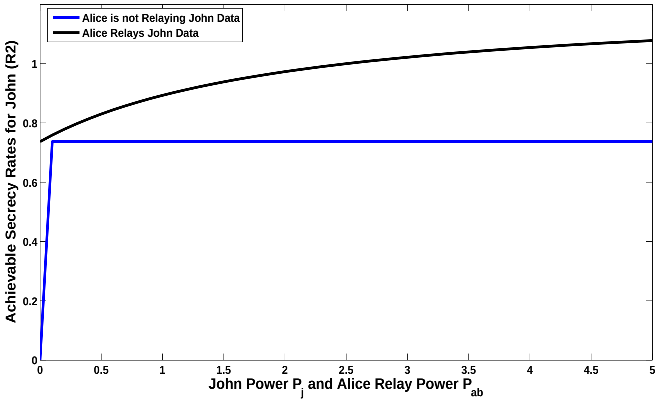

Fig. 2. Secure data rates achievable $(bits/sec/Hz)$ by John (with and without relaying) with respect to the main power P_j, (when no cooperation exists) and the relay power P_{ab} (when $P_j = P_J$ is fixed and equals 5 and cooperative relaying is active).

space path loss. The secrecy rates has been simulated under different distances between Alice and Eve d_{ae} and between John and Bob d_{jb}. As already explained analytically in the previous sections, such distances are associated to the SNRs obtained without and with relaying. Therefore, it is of particular relevance to observe that the distance of the eavesdropper and the transmitter has fundamental role in deciding whether the cooperation is of benefit or not. This result shows that as long as the distances between the legitimate transmitters and the legitimate receiver are smaller than the distances between the legitimate transmitters and the eavesdropper, the achievable secrecy gains are noticeable, and as expected with relaying, the secrecy rates are higher. Therefore, cooperative relaying is of benefit. However, its interestingly shown that if John is too much far from Bob, the gains expected from relaying are very limited, and at some point going into no cooperation could be of more benefit to the legitimate transmitter. Similar analysis applies to the achievable secrecy rates of John with respect to his distance from Bob.

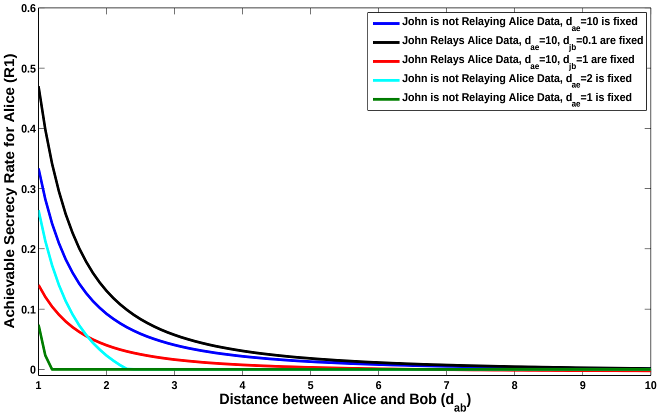

Fig. 3. Secure data rates achievable $(bits/sec/Hz)$ by Alice, with and without relaying, with respect to the distance between Alice and Bob (d_{ab}), and under different distances (d_{ae}, d_{jb}) between Alice and Eve and John and Bob, respectively.

X. Conclusions

Different optimal cooperative power allocation strategies that aim to maximize the achievable secrecy rates for the devices cooperating in a wireless cloud have been derived. We compare cooperation frameworks to the non-cooperative ones. We define distance constraints that allow for adaptive modes of D2D cooperation and adaptive power allocation accordingly. We show that such distance constraints answers the question: when the D2D cooperation is of benefit.

Finally, we establish that although D2D cooperation seems very promising and appealing for next generation wireless networks, however, to secure data transmission, such D2D cooperation should be associated with adaptive and distributed algorithms that constraint the global cloud cooperation when cooperating devices will cause interference and jam the main transmission or when possible common or active eavesdroppers exist. From a security perspective, there should be a framework for cooperation that can be customizable to the application.

References

[1] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[2] S. Ghanem, “MAC Gaussian Channels with Arbitrary Inputs: Optimal Precoding and Power Allocation,” *IEEE International Conference on Wireless Communications Signal Processing (WCSP), Huangshan, China*, pp. 1–6, Oct. 1-6 2012.

[3] ——, “Optimal Power Allocation and Optimal Precoding with Multi-Cell Processing,” *IEEE* 77^{th} *Vehicular Technology Conference: VTC-Spring, Dresden, Germany*, pp. 1–5, Jun. 2-5 2013.

[4] H. Reboredo, M. Ara, M. R. D. Rodrigues, and J. Xavier, “Filter Design with Secrecy Constraints: The Degraded Multiple-Input Multiple-Output Gaussian Wiretap Channel,” *IEEE* 73^{rd} *Vehicular Technology Conference: VTC-Spring, Budapest, Hungrary*, pp. 1–5, May 15-18 2011.

[5] J. Barros and M. R. D. Rodrigues, “Secrecy Capacity of Wireless Channels,” *IEEE International Symposium on Information Theory*, pp. 356–360, Jul. 2006.

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

[7] Lifeng Lai and El Gamal, H., “The Relay-Eavesdropper Channel: Cooperation for Secrecy,” *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[8] Oohama, Y., “Coding for relay channels with confidential messages,” *IEEE Information Theory Workshop*, pp. 87–89, 2001.

[9] L. Dong, Z. Han, A. Petropulu, and H. Poor, “Cooperative jamming for wireless physical layer security,” in *Statistical Signal Processing, 2009. SSP ’09. IEEE/SP 15th Workshop on*, Aug 2009, pp. 417–420.

[10] Vo Nguyen Quoc Bao and Linh-Trung, N. and Debbah, M., “Relay Selection Schemes for Dual-Hop Networks under Security Constraints with Multiple Eavesdroppers,” in *IEEE Transactions On Wireless Communications*, vol. 12, no. 12, Dec. 2013, pp. 6076–6085.

[11] M. Ara, H. Reboredo, S. Ghanem, and M. Rodrigues, “A Zero-sum Power Allocation Game in the Parallel Gaussian Wiretap Channel with an Unfriendly Jammer,” *International Conference on Communication Systems (ICCS), Singapore*, pp. 60–64, 21-23 Nov. 2012.

[12] M. Janzamin and M. R. Pakravan and H. Sedghi, “A Game Theoritic Approach for Power Allocation in Bidirectional Cooperative Communication,” *IEEE Wireless Communication and Networking Conference (WCNC)*, pp. 1–6, Apr. 18-21 2010.

[13] Fitzek, FrankH.P. and Katz, MarcosD., *Cooperation in Wireless Networks: Principles and Applications*. Netherlands: Springer, 2006.

[14] Laneman, J.N. and Tse, D.N.C. and Wornell, Gregory W., “Cooperative diversity in wireless networks: Efficient protocols and outage behavior,” in *IEEE Transactions on Information Theory*, vol. 50, no. 12, Dec. 2004, pp. 3062–3080.

[15] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge University Press, 2004.

[16] J. P. Vilela and M. Bloch and J. Barros and S. W. McLaughlin, “Wireless Secrecy Regions with Friendly Jamming,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.