Secrecy Rate Optimization in Wireless Multi-hop Full Duplex Networks

FENG TIAN[1], (Member, IEEE), XIN CHEN[1], SHIDONG LIU[2], XU YUAN[3], (Member, IEEE), DAPENG LI[1,4], (Member, IEEE), XUEJUN ZHANG[1], AND ZHEN YANG[1]

[1] Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Ministry of Education, Nanjing 210003, China
[2] Department of information and communications, Global Energy Interconnection Research Institute, Nanjing 210003, China
[3] School of Computing and Informatics, University of Louisiana at Lafayette, Lafayette, LA 70504 USA
[4] National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China

Corresponding author: Zhen Yang (yangz@njupt.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61772287, Grant 61671252, and Grant 61471203, in part by the Key University of Science Research Project of Jiangsu Province under Grant 14KJA510003, in part by the Institute of Advance Technology Project, Nanjing university of posts and telecommunications, China, under Grant XJKY15008, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20161518, and in part by the open research fund of National Mobile Communications Research Laboratory, Southeast University under Grant 2018D05.

***Abstract*—Physical layer security and full duplex have been two widely applied techniques in wireless communications community, where the physical layer security can prevent eavesdropping without the upper layer data encryption while the full duplex can improve spectrum efficiency through simultaneous transmission and reception. In this paper, we jointly consider full duplex and security by investigating the cross-layer optimization problem to maximize the secrecy rate in the multi-hop wireless network. This combination aims to improve both spectrum efficiency and security of conventional wireless systems at the same time. We first construct a cross-layer secrecy rate model based on full duplex constraints, secrecy capacity constraints, and secrecy flow balance. Then, we formulate it into a Mixed Integer and Non-Linear Programming (MINLP) problem and reformulate it with Reformulation-Linearization Technique (RLT) and convex hull relaxation into the linear form. Finally, we validate our proposed optimization method and algorithm through comparing it with half duplex and jamming to demonstrate that the proposed combination of security and full duplex achieve the significant improvement of spectrum efficiency and security.**

***Index Terms*—Secrecy rate optimization, physical layer security, full duplex, wireless multi-hop network, convex hull relaxation**

I. INTRODUCTION

Due to the characteristics of wireless channels, it is particularly vulnerable for wireless networks to be attacked by an eavesdropper, which puts forward great challenges to secure communications. Traditional security approaches apply different cryptographic algorithm to achieving confidentiality and authentication in communications. Meanwhile, physical layer security (PLS) is applied by Shannon theory to exploring secrecy communication by coding. The basic idea of PLS is to explore the random nature of physical layer media to enhance the quality of legitimate channel while attenuating the quality of eavesdropping channel. Compared with traditional cryptographic technologies mainly at upper layers, PLS shows more security in some degree with its advantages, for example, applying proper coding and signal processing to guarantee message confidentiality, while traditional cryptographic methods can be broken by advanced computing technologies; PLS can be easily and conveniently achieved rather than massive resources and infrastructure exploited by sharing cryptographic materials among legitimate users; and the authentication of PLS for legitimate nodes is quick.

Hence, as an important and promising technique to prevent eavesdropping, it has attracted more attention in both industry and academic fields [1-5]. Related works in physical layer security were pioneered by Shannon's information theoretic secrecy analysis [1] and Wyner's discrete memory-less wiretap channel secrecy analysis [2]. Wyner proved that if it is a degraded version of the main channel for the eavesdropper's channel, the source and destination can achieve a positive perfect information rate, which is defined as the *secrecy rate*. And *secrecy capacity* is defined as the maximum secrecy rate from the source to the destination. In order to enhance physical layer security, there are numerous studies focused on node cooperation approaches, especially three-point cooperation mode with one source, one destination and one relay (or multiple relays) [3-5]. Relay nodes can be used to relay message or act as cooperative jammers to attenuate eavesdroppers' channel conditions, and thus increase the legitimate users' security transmission. In [6], it addressed secure communications of one source-destination and multiple cooperating relays with one or more eavesdroppers. Decode-and-forward (DF), amplify-and-forward (AF), and cooperative jamming (CJ) were considered for maximizing the achievable secrecy rate and minimizing the transmit power. In [7], it considered DF and CJ scheme to maximize the achievable secrecy rate subject to a total power and minimize the total transmit power with a secrecy rate constraint through semi-definite programming. In [8], it investigated the exact closed-form expressions of secrecy capacity and the secrecy outage probability, where a single antenna is employed for both the transmitter and legal receiver with a multiple antennas passive eavesdropper with either maximal-ratio combining or

Manuscript received December 15, 2017, accepted January 10, 2018.

selection combining reception. In [9], it constructed both the single-channel multi-jammer model and the multi-channel single-jammer model and formulated a Bertrand game based on price competition to achieve maximum profit with Bertrand Equilibrium and power allocation, respectively. In [10], it considered to select the jammer and relay nodes from the intermediate nodes to formulate a Bertrand Game based on price competition with power allocation, and applied a new particle swarm algorithm to achieve the maximum secrecy capacity in wireless cooperative networks.

Meanwhile, recently, several interesting works focus on artificial noise-aided directional modulation (DM) with robust synthesis scheme and antenna correlation for PLS enhancement [11-15]. In [11], it proposed a robust synthesis scheme, where the beamforming vector for the confidential message was developed to preserve its power in the desired directions as possible and the projection matrix of artificial noise (AN) was designed to minimize the effect on the desired directions. In [12], it considered a low-complexity dynamic DM synthesis method and developed a robust solution that combats the estimation errors of the direction angles for minimizing the distortion of the constellation points along the desired direction. In [13], it proposed a scheme of random frequency diverse array-based directional modulation with artificial noise, and optimized the transmission power allocation AN to pursue the optimal ergodic secrecy capacity. In [14], it investigated the performance of AN-aided secure transmission under the influence of transmitter-side correlation to develop a power allocation strategy and achieve the minimum secrecy outage probability. In [15], it proposed a new robust beamforming scheme that combines main-lobe-integration with leakage in directional modulation MU-MIMO systems to achieve simultaneous transmission of multiple different independent parallel confidential message streams. These studies explored the advanced security modulation techniques to promote PLS, which offered us significant reference to investigate cross-layer optimization on PLS.

Furthermore, instead of simply one hop or two hops, there are also some discussions on PLS for multi-hop networks [16-18]. In [16], with randomly distributed eavesdroppers, secure routing was studied through a homogeneous Poisson point process location model and the DF strategy to maximize secure connection probability approximation. In [17], it investigated the secure minimum energy routing to compute a minimum energy path between two nodes with the constraints on the secrecy and output over the path. In [18], it considered secure communications with one source–destination pair based on DF relay and multiple relays with cooperative beamforming to maximize achievable secrecy rates.

However, all studies about PLS above focus on half duplex (HD). Based on the continuous improvement of the designs for full duplex (FD) transceivers, there have been lots of studies investigating the benefits of FD for cross-layer optimization problems [19-21]. It is found that there are few studies on combing PLS with FD scheduling in wireless multi-hop networks. Existing works for combining PLS with FD are as follows. In [22], it considered secure compute-and-forward strategy driven in bidirectional relaying and proposed a nested lattice based coding scheme to guarantee perfect or strong secrecy even in the absence of channel noise. In [23-24], they studied a three-hop relaying network for PLS, where each legitimate node simultaneously transmits a jamming signal when it receives the desired signal by using FD. Although it achieved cooperative jamming and needs no additional jammer, time slots were scarified. Therefore, in our paper, if a node in the multi-hop network is a destination node or an idle node without transmitting, it can be selected as a jammer to send jamming signal towards eavesdroppers for cooperative jamming on the network-level.

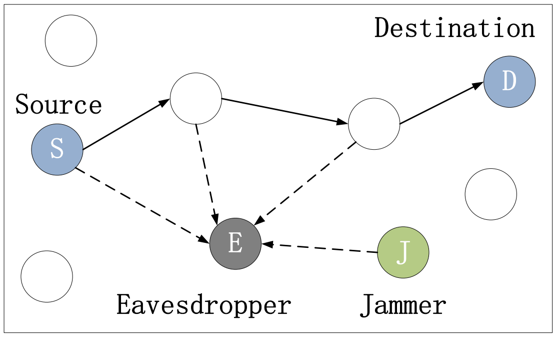

Fig. 1 Schematic illustration of security communication in a wireless full duplex multi-hop network, where S , D , E and J represent the source, destination, eavesdropper, and Jammer, respectively.

In this work, for the first time, we utilize full-duplex in physical layer security communication to maximize secrecy rate for cross-layer optimization of multi-hop networks. Firstly, a full-duplex scheduling model that enables transmitting and receiving simultaneously is constructed to promote spectrum efficiency in security communication. And security capacity model, where the achievable secrecy capacity (rate) is less than the difference between the achievable minimum link capacity under FD mode and the capacity of the eavesdropping channel from transmit nodes to eavesdropper nodes, is defined to offer a strong guarantee for security communication in wireless multi-hop FD Networks. Secondly, an optimization framework of mixed-integer nonlinear program (MINLP) is formulated to maximize the sum of secrecy rates for all sessions. RLT technique is utilized to transform the nonlinear product term into the linear one, and convex hull relaxation technique is applied to approximate the log function with a series of linear segments in the reformulation. Hence, the formulation of MILP is achieved and easily solved by CPLEX. Thirdly, numerical results are presented to characterize the secrecy rate in different cases. Our simulation firstly demonstrates that the security rate applying full duplex with eavesdropper and jammer is always better than the one applying FD with eavesdropper and HD with eavesdropper, while power, rate and time slot are varying respectively. Then, our results show that the secrecy rates decrease to a constant value with increasing of distance between one jammer and one eavesdropper either for FD or for HD. Furthermore, it reveals that the secrecy rate is not linearly improving while the numbers of jammers and eavesdroppers are increasing.

The remainder of this paper is organized as follows. In Section II, we give a secrecy rate model under FD scheduling and formulate the optimization problem. In Section III, we transform the nonlinear optimization problem into a linear one and solve it effectively. Section IV presents simulation results to validate model and algorithm. Section V concludes this paper.

II. Modelling And Formulation

In this section, we developed constraints for mathematical modeling and formulation to explore secrecy rate in a wireless FD multi-hop network. In a wireless multi-hop network as shown in Fig. 1, we suppose that there is a set of nodes $\mathcal{N}$ as legitimate users with the number of nodes $N=|\mathcal{N}|$. And a single antenna that can transmit and receive simultaneously is equipped in each node. There are also multiple eavesdroppers $\mathcal{E}$ with the number $E=|\mathcal{E}|$, which apply one antenna or multiple antennas to overhear the signals from legitimate uses and are randomly distributed in the range of wireless multi-hop network. Suppose that there is a set of active sessions $\mathcal{L}$ with the number $L=|\mathcal{L}|$ in the multi-hop network. $s(l)$ and $d(l)$ denote the source and destination nodes at session l, respectively. In our paper, if a node in the multi-hop network is a destination node or an idle node without transmitting, it can be selected as a jammer to send jamming signal towards eavesdroppers for cooperative jamming on the network-level. In general, we assume that all the legitimate nodes and jammer in the multi-hop network adopt the same power P. Now, we can focus on FD scheduling for secrecy communication in the wireless FD multi-hop network.

A. Full duplex scheduling constraints

The scheduling is selected as a time slot based one, which means there are T equal-length time slots in a frame. Within one time slot, for an FD scheduling, it means that a node may transmit and receive simultaneously not only at the same time but also at the same spectrum band. Note that each legitimate node will not be selected as a jammer and can only be used to transmit useful signals in FD scheduling for saving the limited resource of time slots.

Denote

$$x_{ij}^{l}(t)=\{\begin{array}{l}1\quad \text{If node } i \text{ transmits data to node } j\\ \quad\ \text{for session } l \text{ on time slot } t,\\ 0\quad \text{otherwise.}\end{array}$$

.Then, for FD scheduling, we have:

$$\sum_{l\in\mathcal{L}}\sum_{j\in T_i}x_{ij}^{l}(t)\le 1,\quad (i\in\mathcal{N},\ \ 1\le t\le T),\qquad (1)$$

$$\sum_{l\in\mathcal{L}}\sum_{i\in T_j}x_{ji}^{l}(t)\le 1,\quad (i\in\mathcal{N},\ \ l\in\mathcal{L},\ \ 1\le t\le T),\qquad (2)$$

$$\begin{gathered}\sum_{l\in\mathcal{L}}\sum_{j\in T_i}x_{ij}^{l}(t)=\sum_{l\in\mathcal{L}}\sum_{k\in T_i}x_{ki}^{l}(t),\\ (i,j,k\ne s(l),d(l)\in\mathcal{N},l\in\mathcal{L},\ 1\le t\le T).\end{gathered}\qquad (3)$$

where T_i is defined as the set of nodes located within node i 's transmission range on time slot t with $t\in T$ under the power P with $i\in\mathcal{N}$. And T_j can be also defined. Note that if $\sum_{l\in\mathcal{L}}\sum_{j\in T_i}x_{ij}^{l}(t)=1$, it means that node i transmits legitimate data to node j on time slot t only for session l.

B. Secrecy capacity constraints

For FD communication in the wireless multi-hop network, global channel state information (CSI) and limited self-interference cancelation are considered. And we assume that multiple passive eavesdroppers apply maximal-ratio combining (MRC) receiver to overhear.

Denote C_s, C_{sd} and C_e the achievable secrecy capacity, the achievable minimum link capacity under FD mode, and the capacity of the eavesdropping channel from transmit nodes to eavesdropper nodes on time average, respectively. Denote $c_{ij}^{l}(t)$ and $c_{ie}^{l}(t)$ the instantaneous achievable link capacity (from Shannon's capacity formula) under FD mode and the instantaneous capacity of the eavesdropping channel from transmit node i to receive node e, for the session l. For $c_{ij}^{l}(t)$, we consider both self interference (due to FD) and mutual interference (from other links) as noise. Meanwhile, we consider applying decode-and-forward (DF) protocol in each relay of the multi-hop network, so that the eavesdroppers overhear all the messages from multiple hops and combine them by maximum ratio combination (MRC). Therefore, for $c_{ie}^{l}(t)$, received SINR from the legitimate users of all hops is combined at the eavesdroppers. And denote $f_{ij}(l)$ the average secrecy flow traffic on link (i,j) for session l. Since the average secrecy flow rate on each link cannot be larger than the link's achievable secrecy capacity, we obtain

$$\begin{aligned}\sum_{l\in\mathcal{L}}f_{ij}(l)&=C_s\le C_{sd}-C_e=\frac{1}{T}\sum_{t=1}^{T}\sum_{l\in\mathcal{L}}\left\{\min_{i\in\mathcal{N}}\ c_{ij}^{l}(t)-c_{ie}^{l}(t)\right\}\\
&=\frac{1}{T}\sum_{t=1}^{T}\sum_{l\in\mathcal{L}}\left\{\begin{array}{l}\min\limits_{i\in\mathcal{N}}\ W\log_2\left(1+\dfrac{g_{ij}x_{ij}^{l}(t)P}{\sum\limits_{a\in\mathcal{L}}\sum\limits_{m\ne i}\sum\limits_{n\in T_m}g_{mj}x_{mn}^{a}(t)P+\sum\limits_{b\in T_j}\theta x_{jb}^{l}(t)P+\eta W}\right)\\ -\,W\log_2\left(1+\sum\limits_{e\in\mathcal{E}}\sum\limits_{i\in\mathcal{N}}\dfrac{g_{ie}x_{ij}^{l}(t)P}{\sum\limits_{a\in\mathcal{L}}\sum\limits_{m\ne i}\sum\limits_{n\in T_m}g_{me}x_{mn}^{a}(t)P+\eta W}\right)\end{array}\right\}\\
&\le\frac{1}{T}\sum_{t=1}^{T}\sum_{l\in\mathcal{L}}\left\{\begin{array}{l}W\log_2\left(1+\dfrac{g_{ij}x_{ij}^{l}(t)P}{\sum\limits_{a\in\mathcal{L}}\sum\limits_{m\ne i}\sum\limits_{n\in T_m}g_{mj}x_{mn}^{a}(t)P+\sum\limits_{b\in T_j}\theta x_{jb}^{l}(t)P+\eta W}\right)\\ -\,W\log_2\left(1+\sum\limits_{e\in\mathcal{E}}\sum\limits_{i\in\mathcal{N}}\dfrac{g_{ie}x_{ij}^{l}(t)P}{\sum\limits_{a\in\mathcal{L}}\sum\limits_{m\ne i}\sum\limits_{n\in T_m}g_{me}x_{mn}^{a}(t)P+\eta W}\right)\end{array}\right\}.\end{aligned}$$

$$(i\in\mathcal{N},\ \ j\in T_i)\ (4)$$

i.e.,

$$\sum_{l\in\mathcal{L}}f_{ij}(l)\le\frac{1}{T}\sum_{t=1}^{T}\sum_{l\in\mathcal{L}}\left\{\begin{array}{l}W\log_2\left(1+\dfrac{g_{ij}x_{ij}^{l}(t)P}{\sum\limits_{a\in\mathcal{L}}\sum\limits_{m\ne i}\sum\limits_{n\in T_m}g_{mj}x_{mn}^{a}(t)P+\sum\limits_{b\in T_j}\theta x_{jb}^{l}(t)P+\eta W}\right)\\ -\,W\log_2\left(1+\sum\limits_{e\in\mathcal{E}}\sum\limits_{i\in\mathcal{N}}\dfrac{g_{ie}x_{ij}^{l}(t)P}{\sum\limits_{a\in\mathcal{L}}\sum\limits_{m\ne i}\sum\limits_{n\in T_m}g_{me}x_{mn}^{a}(t)P+\eta W}\right)\end{array}\right\}.$$

$$(i\in\mathcal{N},\ \ j\in T_i)\ (5)$$

where W denotes the bandwidth, g_{ij} denotes the path attenuation loss from transmit node i to receive node j, η

denotes the density of ambient Gaussian noise and θ denotes a performance parameter of self-interference cancellation.

Note that we should guarantee the minimum secrecy rate $R_{\min}$ for each session by the following constraints:

$$\mathrm{R}_{\min} \le \mathrm{r}(l), \quad (l \in L). \tag{6}$$

C. Secrecy flow balance constraints

In general, the flow splitting between a source node and its corresponding destination node for multi-path routing is allowed. Denote $r(l)$ the average secrecy rate (in b/s) of session l. Mathematically, we can easily model secrecy flow balance at each node. Hence, we can obtain the following secrecy flow balance constraints. While node i is the source node of session l, i.e., $i = s(l)$, then

$$\sum_{j \in T_i} f_{ij}(l) = r(l), \quad (i = s(l), l \in \mathcal{L}). \tag{7}$$

While node i is an intermediate relay node for session l, i.e., $i \neq s(l)$ and $i \neq d(l)$, then

$$\sum_{j \in T_i}^{i \neq s(l)} f_{ij}(l) = \sum_{k \in T_i}^{i \neq d(l)} f_{ki}(l), \quad (i \in \mathcal{N}, l \in \mathcal{L}). \tag{8}$$

While node i is the destination node of session l, i.e., $i = d(l)$, then

$$\sum_{k \in T_i} f_{ki}(l) = r(l), \quad (i = d(l), l \in \mathcal{L}). \tag{9}$$

It can be easily validated that if (7) and (8) are satisfied, (9) must also hold. Hence, it is sufficient to remain (7) and (8) in the formulation.

D. Formulation

The objective function is defined as the sum of secrecy rates for all sessions. To sum up the objective function with all the constraints for FD scheduling, secrecy capacity, secrecy rate requirement and secrecy flow routing, we have the following formulation.

OPT-SC

max $\sum_{l \in \mathcal{L}} r(l)$

s.t FD scheduling constraints: (1), (2), (3);
Secrecy capacity constraints: (5);
Secrecy rate requirement constraints: (6);
Secrecy flow balance constraints: (7), (8);

where W, g_{ij}, θ, η, $r_{\min}$, and P are constants; $c_{ij}^{l}(t)$, $r(l)$, $f_{ij}(l)$ are continuous variables; and $x_{ij}^{l}(t)$ is a binary variable. Due to the log functions in constraints (5) and the nonlinear terms inside the log functions, the problem to be optimized is nonlinear, which is in the form of a mixed-integer nonlinear program (MINLP) [25]. We should linearize and solve the problem through reformulation and approximation.

III. Reformulation And Solution

In this section, we reformulate the nonlinear problem of maximizing secrecy rate in a wireless FD multi-hop network into the linear one and solve it.

A. Reformulation

Our reformulation method is presented as follows. Firstly, we apply Reformulation-Linearization Technique (RLT) [26, Chapter 6] to transform the nonlinear term (SINR) inside the logarithmic functions into the linear one. Then, we explore convex hull relaxation technique to substitute the log functions in (5) through a set of linear constraints. Finally, a linearized problem is achieved and solved, where its approximation error within ε is proved.

SINR reformulation. For (5), we substitute the nonlinear SINR term inside the log function with new variables $w_{ij,mn}^{l,sd}(t) = v_{ij}^{l,sd}(t) * x_{mn}^{l}(t)$ and $w_{ij,mn}^{l,e}(t) = v_{ij}^{l,e}(t) * x_{mn}^{l}(t)$. Therefore, we obtain that:

$$v_{ij}^{l,sd}(t) - 1 = \frac{g_{ij} x_{ij}^{l}(t) P}{\sum_{a \in \mathcal{L}} \sum_{m \neq i} \sum_{n \in T_m} g_{mj} x_{mn}^{a}(t) P + \sum_{b \in T_j} \theta x_{jb}^{l}(t) P + \eta W}, \tag{10}$$

$$w_{ij,mn}^{l,sd}(t) = v_{ij}^{l,sd}(t) * x_{mn}^{l}(t), \tag{11}$$

$$v_{ij}^{l,e}(t) - 1 = \sum_{e \in \mathcal{E}} \sum_{i \in \mathcal{N}} \frac{g_{ie} x_{ij}^{l}(t) P}{\sum_{a \in \mathcal{L}} \sum_{m \neq i} \sum_{n \in T_m} g_{me} x_{mn}^{a}(t) P + \eta W}, \tag{12}$$

$$w_{ij,mn}^{l,e}(t) = v_{ij}^{l,e}(t) * x_{mn}^{l}(t). \tag{13}$$

Since that $1 \le v_{ij}^{l,sd}(t) \le 40,\ 1 \le v_{ij}^{l,sd}(t) \le 40,$ and $0 \le x_{mn}^{l}(t) \le 1$, through RLT, we obtain the following linear constraints to substitute (10) and (11):

$$\begin{aligned} & v_{ij}^{l,sd}(t) * \eta w - \eta w - g_{ij} x_{ij}^{l}(t) P + \sum_{b \in T_j} \theta P * w_{ij,jb}^{l,sd}(t) - \sum_{b \in T_j} \theta x_{bj}^{l}(t) P \\ & + \sum_{a \in \mathcal{L}} \sum_{m \neq i} \sum_{n \in T_m} g_{mj} P * w_{ij,mn}^{a,sd}(t) - \sum_{a \in \mathcal{L}} \sum_{m \neq i} \sum_{n \in T_m} g_{mj} P * x_{mn}^{a}(t) = 0. \end{aligned} \tag{14}$$

$$x_{mn}^{l}(t) - w_{ij,mn}^{l,sd}(t) \le 1. \tag{15}$$

$$v_{ij}^{l}(t) - w_{ij,mn}^{l,sd}(t) \ge 1. \tag{16}$$

$$40 * x_{mn}^{l}(t) - w_{ij,mn}^{l,sd}(t) \ge 40. \tag{17}$$

$$v_{ij}^{l,sd}(t) + 40 * x_{mn}^{l}(t) - w_{ij,mn}^{l,sd}(t) \le 40. \tag{18}$$

Similarly, through RLT, we also obtain the following linear constraints to substitute (12) and (13):

$$\sum_{e \in \mathcal{E}} \sum_{i \in \mathcal{N}} \begin{bmatrix} v_{\overset{\wedge}{ij}}^{l,e}(t) * \eta w + \sum_{a \in \mathcal{L}} \sum_{m \neq i} \sum_{n \in T_m} g_{me} P * w_{\overset{\wedge}{ij},mn}^{a,e}(t) \\ -\eta w - g_{ie} x_{ij}^{l}(t) P - \sum_{a \in \mathcal{L}} \sum_{m \neq i} \sum_{n \in T_m} g_{me} P * x_{mn}^{a}(t) \end{bmatrix} = 0. \tag{19}$$

$$x_{mn}^{l}(t) - w_{\overset{\wedge}{ij},mn}^{l,e}(t) \le 1. \tag{20}$$

$$v_{\overset{\wedge}{ij}}^{l,e}(t) - w_{\overset{\wedge}{ij},mn}^{l,e}(t) \ge 1. \tag{21}$$

$$40 * x_{mn}^{l}(t) - w_{\overset{\wedge}{ij},mn}^{l,e}(t) \ge 40. \tag{22}$$

$$v_{\overset{\wedge}{ij}}^{l,e}(t) + 40 * x_{mn}^{l}(t) - w_{\overset{\wedge}{ij},mn}^{l,e}(t) \le 40. \tag{23}$$

Note that we define $\overset{\wedge}{ij}$ to distinguish the term ij from (12) to (14).

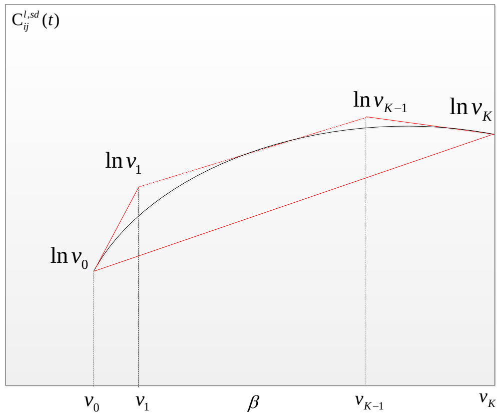

Fig. 2 A convex hull for $\ln(\cdot)$ function.

Convex hull relaxation of ln function. In this section, we apply a convex hull relaxation [27] to approximate the nonlinear $\log(\cdot)$ term in the constraint (5) with the linear one and guarantee the performance as shown in Fig. 2. For the nonlinear terms $\ln\left(v_{ij}^{l,sd}(t)\right)$ and $\ln\left(v_{ij}^{l,e}(t)\right)$, we select new variables $C_{ij}^{l,sd}(t)$ and $C_{ij}^{l,e}(t)$ to substitute them, respectively. Therefore, we can obtain the following new constraints from (5):

$$\sum_{l\in\mathcal{L}} f_{ij}(l) \le \frac{W}{\ln 2T}\sum_{t=1}^{T}\sum_{l\in\mathcal{L}}\left(C_{ij}^{l,sd}(t)-C_{ij}^{l,e}(t)\right) \quad (24)$$

$v_{ij}^{l,sd}(t)\in\{v_0,v_1,\dots,v_K\}$ denotes each horizontal coordinate of possible points of tangency on $\ln(\cdot)$ curve, which corresponds to its tangent curve for $\ln(\cdot)$ curve. For any horizontal coordinate v_k in interval $[v_0,\dots,v_K]$, unless the approximation error between its corresponding vertical coordinate on convex hull and $\ln(\cdot)$ curve is less than or equal to δ, it will stop calculating new tangent points based on the intersection point between two tangent curves on last time (iteration). Therefore, we can obtain the approximation relationship between them as follows:

$$C_{ij}^{l,sd}(t)-\frac{\ln v_K-\ln v_0}{v_K-v_0}v_{ij}^{l,sd}(t)-\frac{v_K\ln v_0-v_0\ln v_K}{v_K-v_0}\ge 0. \quad (25)$$

$$C_{ij}^{l,sd}(t)-\frac{\ln v_k-\ln v_{k-1}}{v_k-v_{k-1}}v_{ij}^{l,sd}(t)-\frac{v_k\ln v_{k-1}-v_{k-1}\ln v_k}{v_k-v_k}\le 0 \quad (26)$$

where $1\le k\le K=\{1,2,3,5,9,\dots,33,\dots\}$. It is similar to construct convex hull constraints for $\ln\left(v_{ij}^{l,e}(t)\right)$ with a new variable $C_{ij}^{l,e}(t)$.

For a given error bound δ between $C_{ij}^{l,sd}(t)$ .and $\ln\left(v_{ij}^{l,sd}(t)\right)$ or $C_{ij}^{l,e}(t)$ .and $\ln\left(v_{ij}^{l,e}(t)\right)$, the values of v_0, $v_1,\dots v_{k-1}$, $v_k,\dots v_K$ and the number K of terminal points v_K can be found iteratively by the following convex hull relaxation process:

Initialization: set $v_0\leftarrow V^L$, $v_K\leftarrow V^H$, $v_k\in\{v_0,v_K\}$, and $K\leftarrow 1$

For v_0 and v_K, calculate their corresponding tangent curves on $\ln(\cdot)$ curve for the intersection point $(\beta=\dfrac{[\ln v_k-\ln v_{k-1}]\cdot v_k\cdot v_{k-1}}{v_k-v_{k-1}},\ln\beta)$ of tangent curves and add β to the set $\{v_0,v_K\}$ to obtain $\{v_0,v_1,v_K\}$, and set $K\leftarrow 2$.

While

$$\left(\ln\beta-\frac{\ln v_k-\ln v_{k-1}}{v_k-v_{k-1}}\beta-\frac{v_k\ln v_{k-1}-v_{k-1}\ln v_k}{v_k-v_k}\ge\delta,\right)$$

$for\ v_k\in\{v_0,\dots,v_K\}$.

{

1. Choose each point of $(\beta,\ln\beta)$ as a new point of tangency for $\ln(\cdot)$ curve to calculate its corresponding tangent curve;

2. Calculate each new intersection point $(\beta,\ln\beta)$ from the new tangent curve and its neighboring tangent curve (generated in last iteration), and replace $v_k\in\{v_1,\dots,v_{K-1}\}$ with all new β in the set of $v_k\in\{v_0,v_1,\dots,v_K\}$ and set $(K-1)\leftarrow 2(K-1)$ based on bisection method;

3. Recalculate

$$\ln\beta-\frac{\ln v_k-\ln v_{k-1}}{v_k-v_{k-1}}\beta-\frac{v_k\ln v_{k-1}-v_{k-1}\ln v_k}{v_k-v_k},$$

$for\ v_k\in\{v_0,\dots,v_K\}\ and\ \beta;$

4. If the results are all less than or equal to δ, exist; Otherwise, go to step 1.

}.

B. Solution and Approximation Error

Therefore, we can obtain the final $v_k\in\{v_0,v_1,\dots,v_K\}$ and the value of K. Finally, we achieve the following linear relaxation formulation OPT-SC$_L$.

OPT-SC$_L$

max $\sum_{l\in\mathcal{L}} r(l)$

s.t FD scheduling constraints: (1), (2), (3);
Secrecy capacity constraints: (14-23), (25), (26);
Secrecy rate requirement constraints: (6);
Secrecy flow balance constraints: (7), (8);

where W, g_{ij}, θ, η, $r_{\min}$, and P are constants; $v_{ij}^{l,sd}(t)$, $w_{ijmn}^{l,sd}(t)$, $v_{ij}^{l,e}(t)$, $v_{ij}^{l,e}(t)$, $C_{ij}^{l,sd}(t)$, $C_{ij}^{l,e}(t)$, $r(l)$, $f_{ij}(l)$ are continuous variables; and $x_{ij}^{l}(t)$ is a binary variable. OPT-SC$_L$ is in the form of *mixed integer linear program* (MILP), which can be solved through commercial software CPLEX efficiently. Based on (24-25), we can prove that the approximation error of optimal objective is $\varepsilon\le 2\delta * W * L/\ln 2$.

Lemma 1: The gap between the optimal objective values of OPT-SC and OPT-SC$_L$ is upper bounded by $\varepsilon=\dfrac{LW}{\ln 2}\cdot 2\delta$.

Proof: Assuming that an optimal solution of OPT-FD-EE is ζ_{OPT}^{*} and its objective value is $\left(\sum_{l\in L} r^{*}(l)\right)_{OPT}$. A feasible solution to OPT-SC$_L$ is defined as ζ_{OPT-L} based on ζ_{OPT}^{*}, and ζ_{OPT-L} can hold all the constraints in OPT-SC$_L$. Assuming that

$v_{ij}^{l,sd}(t)$ and $v_{ij}^{l,e}(t)$ falls in the interval $[v_{k-1}, v_k]$. Then $\ln\left(v_{ij}^{l,sd}(t)\right)$ and $\ln\left(v_{ij}^{l,e}(t)\right)$ can achieve maximization only if $\left|C_{ij}^{l,sd}(t)-\ln\left(v_{ij}^{l,sd}(t)\right)\right|\le\delta$ and $\left|C_{ij}^{l,e}(t)-\ln\left(v_{ij}^{l,e}(t)\right)\right|\le\delta$ in (24) while $x_{ij}^{l}(t)=x_{ij}^{l*}(t)$. Denote $\left(\sum_{l\in L} r(l)\right)_{OPT-L}$ the objective value in OPT-SC$_{\mathrm{L}}$. Then we have

$$\left(\sum_{l\in L} r(l)\right)_{OPT-L}-\left(\sum_{l\in L} r^*(l)\right)_{OPT}$$

$$=\sum_{l\in\mathcal{L}}\frac{W}{\ln 2TL}\left(\begin{array}{l}\sum_{t=1}^{T}\sum_{l\in\mathcal{L}}\left(\ln\left(v_{ij}^{l,sd}(t)\right)-\ln\left(v_{ij}^{l,e}(t)\right)\right)\\ -\sum_{t=1}^{T}\sum_{l\in\mathcal{L}}\left(\ln\left(v_{ij}^{l,sd*}(t)\right)-\ln\left(v_{ij}^{l,e*}(t)\right)\right)\end{array}\right)$$

$$=\sum_{l\in\mathcal{L}}\frac{W}{\ln 2T}\left(\begin{array}{l}\sum_{t=1}^{T}\left(C_{ij}^{l,sd}(t)-C_{ij}^{l,e}(t)\right)\\ -\sum_{t=1}^{T}\sum_{l\in\mathcal{L}}\left(\ln\left(v_{ij}^{l,sd*}(t)\right)-\ln\left(v_{ij}^{l,e*}(t)\right)\right)\end{array}\right)$$

$$=\frac{LW}{\ln 2}\left(\begin{array}{l}\left|C_{ij}^{l,sd*}(t)-\ln\left(v_{ij}^{l,sd*}(t)\right)\right|\\ +\left|C_{ij}^{l,e*}(t)-\ln\left(v_{ij}^{l,e*}(t)\right)\right|\end{array}\right)$$

$$\le\frac{LW}{\ln 2}\cdot 2\delta$$

Let $\varepsilon=\frac{LW}{\ln 2}\cdot 2\delta$. Denote ζ_{OPT-L}^{*} an optimal solution to OPT-SC$_{\mathrm{L}}$ and its objective value is $\left(\sum_{l\in L} r^*(l)\right)_{OPT-L}$. As $\left(\sum_{l\in L} r(l)\right)_{OPT-L}$ is merely the objective value of an infeasible solution, we have $\left(\sum_{l\in L} r^*(l)\right)_{OPT-L}\le\left(\sum_{l\in L} r(l)\right)_{OPT-L}$. Then $\left(\sum_{l\in L} r^*(l)\right)_{OPT-L}-\left(\sum_{l\in L} r^*(l)\right)_{OPT}\le\left(\sum_{l\in L} r\ (l)\right)_{OPT-L}-\left(\sum_{l\in L} r^*(l)\right)_{OPT}\le\varepsilon.$ We complete the proof.

IV. Numerical Simulation

In this section, we conduct numerical studies to explore security rate performance under FD through comparing with half duplex and jamming in the multi-hop wireless networks.

A. Simulation Setting

A 20-user multi-hop wireless network is with users randomly distributed in an $100m\times100m$ area. The bandwidth is normalized to one unit (i.e., $W=1$). For each node, the transmission power set to $P=30dBm$. The path loss parameter $g_{ij}=d^{-4}$, where d is the distance between nodes i and j. The self-interference cancellation parameter is $\theta=-50dB$ and ambient noise is $\eta W=-20dBm$. Assuming that there is 2 sessions coexisting in the network and the number of time slots in a frame is $T=4$. The number of eavesdroppers and jammers are all set to 1, respectively. The target approximation error is $\varepsilon=0.05$.

B. Secrecy rate versus power P

Note that secrecy rate in the following simulations refers to the sum of all the links' average secrecy rate, i.e., $\sum_{l\in\mathcal{L}} r(l)$. In Fig. 3, we compare three different cases for secrecy rate versus power P, where minimum secrecy rate is set to $R_{\min}=0.5$ and the total time slots is set to $T=4$. These three cases are applying full duplex with eavesdropper and jammer (as the first case), full duplex with eavesdropper (as the second case), and half duplex with eavesdropper (as the third case) in a multi-hop network, respectively. In Fig. 3, it shows that the variation trends of these three cases are similar, where the achievable secrecy rates of three cases are all monotonically increasing corresponding to the increase of power P. No matter which case in these three is adopted, it demonstrates that the achievable secrecy rates can be increased once the power increase. However, for the same power P, the achievable secrecy rates of three cases are different. Due to jamming, the performance of the first case is better than the second case to achieve bigger secrecy rate on the same power P. Due to FD, the performance of the first case is better than the third case to achieve larger secrecy rate on the same power P. Also, due to FD, the performance of the second case is better than the third case to achieve larger secrecy rate on the same power P. The results validate the benefits of combining full duplex with security to achieve the best cross-layer optimization performance in a multi-hop network.

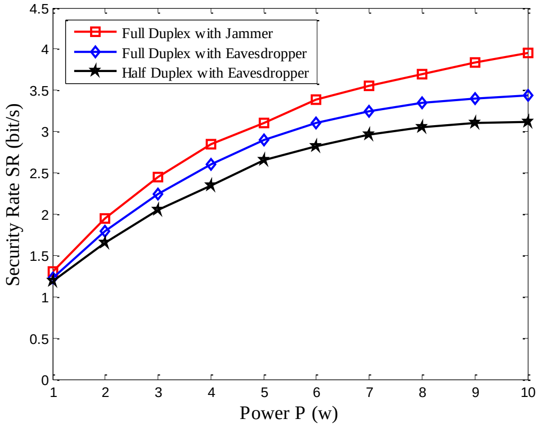

Fig. 3 Results of secrecy rate versus power P in the multi-hop network.

C. Secrecy rate versus minimum secrecy rate $R_{\min}$

Similarly, we consider the same three cases in Fig. 3 to investigate secrecy rate versus minimum secrecy rate $R_{\min}$, where the power is set to $P=1$ and the total time slots is set to $T=4$. In Fig. 4, we find that the achievable secrecy rates for three cases always show a line with their constant values, respectively, while minimum secrecy rate constantly increases. Unless minimum secrecy rate is set larger than its maximum achieved value, all secrecy rates of three cases will stop keeping this constant value and be infeasible. Meanwhile, for a fixed minimum secrecy rate, the case of full duplex with jammer has the best performance, the case of full duplex with eavesdropper is better, and the case of half duplex with eavesdropper is worst. The results also validate our proposition.

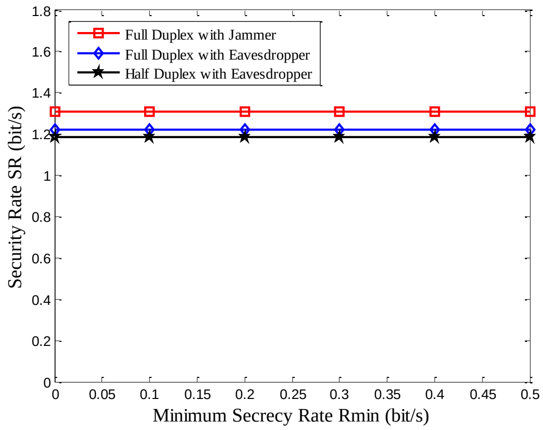

Fig. 4 Results of secrecy rate versus minimum secrecy rate $R_{\min}$ in the multi-hop network.

D. Secrecy rate versus time slot T

Similar to Fig. 3 and Fig. 4, Fig. 5 demonstrates the same three cases in Fig. 3 and Fig. 4 to explore secrecy rate versus time slot T, where the power is set to $P=1$ and minimum secrecy rate is set to $R_{\min}=0.5$. From Fig. 5, we can find three cases have the similar variation trends. While the time slot T increases, the achievable secrecy rates of three cases are all increasing monotonically. Meanwhile, for a fixed time slot, the performance of the first case is the best, the performance of the second case is better, and the performance of the third case is the worst. Also, the results validate the benefits of combining full duplex with security to achieve the best cross-layer optimization performance in a multi-hop network.

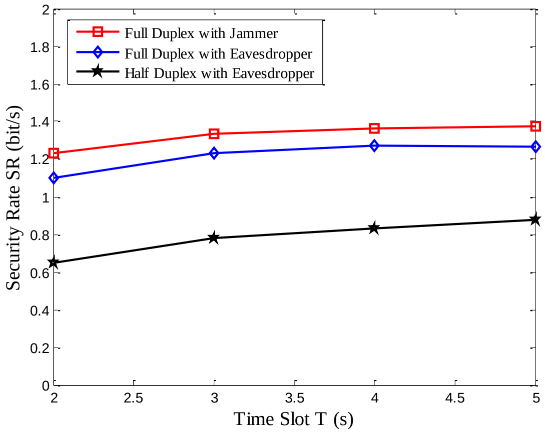

Fig. 5. Results of secrecy rate versus time slot T in the multi-hop network.

E. Secrecy rate versus distance D_{JE}

In Fig. 6, the effects on the achievable security rate of the distance D_{JE} between one moving jammer and one fixed eavesdropper is explored, where the minimum secrecy rate is set to $R_{\min}=0.1$, the power is set to $P=1$, and the total time slots is set to $T=4$. The achievable security rate about the distance D_{JE} is the average value obtained from all directions. Fig. 6 shows that the variation trends of the full-duplex case and the half duplex case are similar, where the achievable secrecy rates are all monotonically decreasing corresponding to the distance between the jammer and the eavesdropper, and finally to be constant values, respectively. Due to FD, the performance of full-duplex case is better than the half-duplex case to achieve larger secrecy rate on the same distance D_{JE}. The results also validate our method.

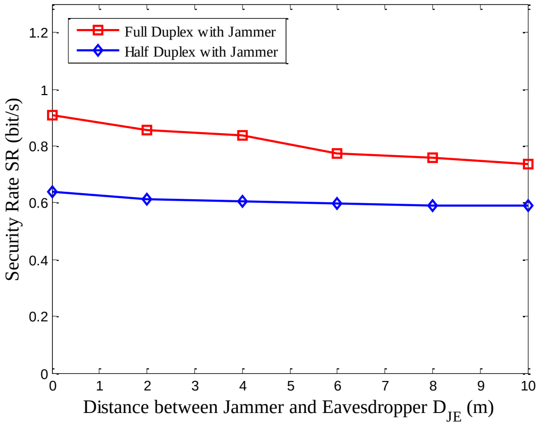

Fig. 6 Results of secrecy rate versus distance D_{JE} between jammer and eavesdropper in the multi-hop network.

F. Secrecy rate versus multi-jammer and multi-eavesdropper.

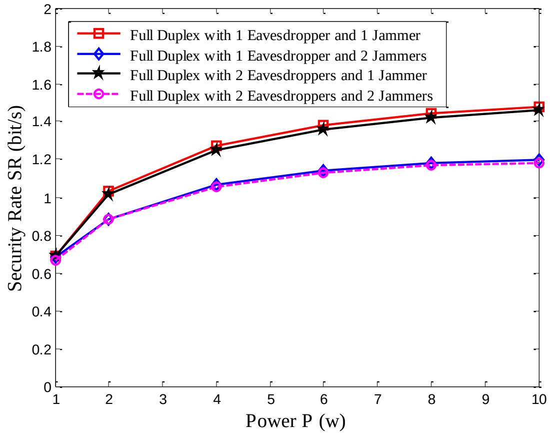

Fig. 7 Results of secrecy rate versus multi-jammer and multi-eavesdropper in the multi-hop network.

In Fig. 7, the achievable security rates for multi-jammer and multi-eavesdropper with the increasing power P are compared, where the minimum secrecy rate is set to $R_{\min}=0.1$, and the total time slots is set to $T=4$. The locations of eavesdropper 1, eavesdropper 2, jammer 1, and jammer 2 are (25, 30), (35, 30), (30, 35), (30, 25), respectively. While the power is changing, the achievable security rate of 2 eavesdroppers and 1 jammer is always smaller than the one of 1 eavesdropper and 1 jammer since more eavesdroppers reduce the choice of nodes for routing and deteriorate the achievable security rate. And the achievable security rate of 2 eavesdroppers and 2 jammers (or 1 eavesdropper and 2 jammers) is always smaller than the one of 2 eavesdroppers and 1 jammer (or 1 eavesdropper and 1 jammer) since more jammers may generate a worse effect on the achievable security rate in a limited communication range.

Therefore, the achievable security rate cannot be increased through purely increasing jammers, which also depends on the selection of the new jammers' location and the nodes' density of the whole network.

V. CONCLUSION

In multi-hop networks, the benefits of combining full duplex and security were rarely explored. Through rigorous cross-layer optimization modeling, formulating and reformulating, we investigate secrecy rate optimization in wireless multi-hop full duplex networks. Numerical results validate the proposed optimization methods.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Technol. J., vol. 28, pp. 656-715, 1949.

[2] A. D. Wyner, "The wire-tap channel," Bell Syst. Technol. J., vol. 54, no. 8, pp. 1355-87, 1975.

[3] Y. Liu, H. H. Chen, L. Wang, "Physical layer security for next generation wireless networks: theories, technologies, and challenges," IEEE Communications Surveys and Tutorials, vol. 19, no. 1, pp. 347-376, 2017.

[4] Y. P. Hong, P. C. Lan, C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," IEEE Signal Process Magazine, vol. 30, no. 5, pp. 29-40, 2013.

[5] L. Zhou, D. Wu, B. Zheng, M. Guizani, "Joint physical-application layer security for wireless multimedia delivery," IEEE Communications Magazine, vol. 52, pp. 3, pp. 66-72, 2014.

[6] L. Dong, Z. Han, A. P. Petropulu, H. V. Poor, "Improving wireless physical layer security via cooperating relays," IEEE Trans. Signal Processing, vol. 58, no. 3, pp. 1875-1888, 2010.

[7] J. Li, A. P. Petropulu, S. Weber, "On cooperative relaying schemes for wireless physical layer security," IEEE Trans. Signal Processing, vol. 59, no. 10, pp. 4985-4997, 2011.

[8] D. D. Tran, D. B. Ha, V. T. Ha, and E. K. Hong, "Secrecy analysis with MRC/SC-based eavesdropper over heterogeneous channels," IETE Journal of Research, vol. 61, no. 4, pp. 363-371, 2015.

[9] K. Wang, L. Yuan, T. Mizayaki, Y. Sun, and S. Guo, "Anti-eavesdropping with selfish jamming in wireless networks: a bertrand game approach," IEEE Transactions on Vehicular Technology, vol.66, no.7, pp. 6268-6279, 2017.

[10] K. Wang, L. Yuan, T. Miyazaki, D. Zeng, S. Guo, and Y. Sun, "Strategic anti-eavesdropping game for physical layer security in wireless cooperative networks," IEEE Transactions on Vehicular Technology, vol. 66, no. 10, pp. 9448-9457, 2017.

[11] F. Shu, X. Wu, J. Li, R. Chen, B. Vucetic, "Robust beamforming scheme for secure multi-beam directional modulation in broadcasting systems," IEEE Access, vol. 4, no.99, pp. 6614-6623, 2016.

[12] J. Hu, F. Shu, J. Li, "Robust synthesis method for secure directional modulation with imperfect direction angle," IEEE Communications Letters, vol. 20, no. 6, pp. 1084-1087, 2016.

[13] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation," IEEE Trans. Wireless Communications, vol. 15, no. 12, pp. 8286-8297, 2016.

[14] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays", IEEE Access, vol. 5, pp. 1658-1667, 2017.

[15] F. Shu, W. Zhu, X. Zhou, J. Li, J. Lu, "Robust secure transmission of using main-lobe-integration-based leakage beamforming in directional modulation MU-MIMO systems," IEEE Systems Journal, vol. PP, no. 99, pp. 1-11, 2017.

[16] J. Yao, S. Feng, X. Zhou, Y. Liu, "Secure routing in multihop wireless Ad-Hoc networks with decode-and-forward relaying," IEEE Trans. Communications, vol. 64, no. 2, pp. 753-764, 2016.

[17] M. Ghaderi, D. Goeckel, A. Orda, M. Dehghan, "Minimum energy routing and jamming to Thwart wireless network eavesdroppers," IEEE Trans. Mobile Computing, vol. 14. no. 7, pp. 1433-1448, 2015.

[18] J. Lee, "Optimal power allocation for physical layer security in multi-hop DF relay networks," IEEE Trans. Wireless Communications, vol. 15, no. 1, pp. 28-38, 2016.

[19] Z. Zhang, K. Long, A. V. Vasilakos, L. Hanzo, "Full-duplex wireless communications: challenges, solutions, and future research directions," Proceedings of the IEEE, vol. 104, no. 7, pp. 1369-1409, 2016.

[20] X. Xie and X. Zhang, "Does full duplex double the capacity of wireless networks," in Proc. IEEE INFOCOM, Toronto, Canada, Apr. 2014, pp. 253–261.

[21] X. Qin, H. Zeng, X. Yuan, B. Jalaian, Y. T. Hou, W. Lou, and S. F. Midkiff, "Impact of full duplex scheduling on end-to-end throughput in multi-hop wireless networks," IEEE Trans. Mobile Computing, vol. 16, no. 1, pp. 158-171, 2017.

[22] S. Vatedka, N. Kashyap, A. Thangaraj, "Secure compute-and-forward in a bidirectional relay," IEEE Trans. Information Theory, vol. 61, no. 5, pp. 2531-2556, 2015.

[23] J. Yao, S. Feng, Y. Liu, "Secure routing in full-duplex jamming multihop relaying," IEEE GLOBECOM, Washington, DC, USA, Dec. 2016, pp. 1-6.

[24] J. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," IEEE Communications Letters vol. 19, no. 4, pp. 525-528, 2015.

[25] M. R. Garey and D. S. Johnson, "Computers and intractability: a guide to the theory of NP-completeness," W. H., Freeman and Company, pp. 245–248, 1979.

[26] Y. T. Hou, Y. Shi, and H. D. Sherali, "Applied optimization methods for wireless networks," Cambridge, Cambridge Univ. Press, 2014.

[27] Y. Shi, Y. T. Hou, S. Kompella, and H. D. Sherali, "Maximizing capacity in multi-hop cognitive radio networks Under the SINR model," IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 954-967, 2011.