Secrecy Capacity Optimization via Cooperative Relaying and Jamming for WANETs

Biao Han, *Member, IEEE*, Jie Li, *Senior Member, IEEE*, Jinshu Su, *Member, IEEE*, Minyi Guo, *Senior Member, IEEE*, and Baokang Zhao, *Member, IEEE*

Abstract—Cooperative wireless networking, which is promising in improving the system operation efficiency and reliability by acquiring more accurate and timely information, has attracted considerable attentions to support many services in practice. However, the problem of secure cooperative communication has not been well investigated yet. In this paper, we exploit physical layer security to provide secure cooperative communication for wireless ad hoc networks (WANETs) where involve multiple source-destination pairs and malicious eavesdroppers. By characterizing the security performance of the system by secrecy capacity, we study the secrecy capacity optimization problem in which security enhancement is achieved via cooperative relaying and cooperative jamming. Specifically, we propose a system model where a set of relay nodes can be exploited by multiple source-destination pairs to achieve physical layer security. We theoretically present a corresponding formulation for the relay assignment problem and develop an optimal algorithm to solve it in polynomial time. To further increase the system secrecy capacity, we exploit the cooperative jamming technique and propose a smart jamming algorithm to interfere the eavesdropping channels. Through extensive experiments, we validate that our proposed algorithms significantly increase the system secrecy capacity under various network settings.

Index Terms—Cooperative communication, physical layer security, secrecy capacity, relay assignment, cooperative jamming

1 Introduction

Cooperative wireless networking, which exploits the relaying capability of other wireless devices, has received significant attentions recently as an emerging network design strategy for future wireless networks. Successful cooperative networking is potential to prompt the development of advanced emergency-oriented wireless applications such as disaster recovery, connectivity maintain, interactive multimedia communication, real-time rescue, etc. [1], [2]. Although cooperative networking promises to provide performance enhancements in terms of spatial diversity, increased capacity and improved reliability, it also brings potential security crisis while exploiting the benefits of cooperative communication (CC).

One of the most significant vulnerabilities of cooperative communication is the disclosure of messages while transmission performs cooperatively. It becomes extremely critical for the environments where involve undesired receivers with eavesdropping capabilities. Take the illustrative network in Fig. 1 as an example, where the eavesdropper can overhear the cooperative transmitting signals generated from the source node and forwarded by the relay node. Secure communication can be achieved by using classical measures, such as the cryptographic methods at higher layers [3]. However, the emergence of large-scale, dynamic, and decentralized cooperative wireless networks imposes new challenges on classical security measures [4], [5]. Besides, due to the additional computational overhead associated with the key distribution and management process, it becomes extremely challenging for the energy-limited wireless devices to handle. For this reason, researchers have sought novel information techniques that can secure wireless networks *without* the need of secret keys. One of the most promising ideas is to exploit the wireless channel physical layer characteristics for improving the reliability of wireless transmission against eavesdropping attacks, named as *physical layer security* [6], [7]. Recently, physical layer security has emerged as a key technique for providing trustworthy and reliable future wireless networks and has witnessed a significant growth in the past few years.

This line of work is pioneered by Wyner [8], who introduced the wire-tap channel and established fundamental results of creating perfectly secure communications without relying on secret keys. Wyner showed that when the eavesdropper's channel is a degraded version of the main source-destination channel, the source and destination can exchange perfectly secure messages at a non-zero rate, while the eavesdropper is unable to decode any information. The maximum transmission rate of reliable information secretly sent from the source to the intended destination with the presence of eavesdroppers is termed as *secrecy capacity*. Following Wyner's work, Leung-Yan-Cheong and Hellman in [9] studied the secrecy capacity of the Gaussian wiretap channel. Csiszar and Korner in [10] extended Wyner's approach to the transmission of

- *B. Han, J. Su, and B. Zhao are with the School of Computer, National University of Defense Technology, 410073 Changsha, China. E-mail: nudtbill@nudt.edu.cn, sjs@nudt.edu.cn, bkzhao@nudt.edu.cn.*
- *J. Li is with the Faculty of Engineering, Information and Systems, University of Tsukuba, Tsukuba Science City, Ibaraki 305-8573, Japan. E-mail: lijie@cs.tsukuba.ac.jp.*
- *M. Guo is with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China. E-mail: guo-my@cs.sjtu.edu.cn.*

Manuscript received 15 July 2013; revised 3 Mar. 2014; accepted 11 Mar. 2014. Date of publication 7 Apr. 2014; date of current version 6 Mar. 2015. Recommended for acceptance by E. Leonardi.
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TPDS.2014.2316155

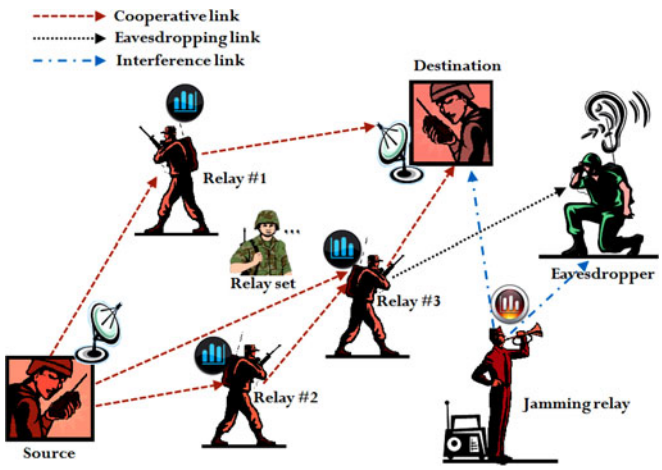


Fig. 1. Illustrative topology for a cooperative ad hoc network with a malicious eavesdropper.

confidential messages over broadcast channels, which showed that when the destination and the eavesdropper have separate channels, secret communication is possible if the source-eavesdropper channel has a smaller capacity than the source-destination channel. There have been considerable efforts devoted to generalizing physical layer security to the wireless fading channel and to various multi-user scenarios (see e.g., ch. 6-8 in [6] for an overview). Among these literatures, secrecy capacity can be computed by $\max\{(\mathcal{C}_{\mathcal{P}} - \mathcal{C}_{\mathcal{E}}), 0\}$, where $\mathcal{C}_{\mathcal{P}}$ denotes the capacity of the primary channel between source and destination, $\mathcal{C}_{\mathcal{E}}$ denotes the capacity of the eavesdropping channel between source and eavesdropper. Notice that if the eavesdropping channel happens to be better than the primary channel, e.g., $\mathcal{C}_{\mathcal{E}} \geq \mathcal{C}_{\mathcal{P}}$, positive secrecy capacity cannot be achieved. In other words, secret communication cannot be guaranteed.

Recently, the interaction of cooperative diversity concept [11], [12] with secret communication opens opportunity for overcoming this limitation by cooperation, mainly *cooperative relaying* and *cooperative jamming*. By cooperative relaying, a relay node locates closer to the destination provides a higher capacity to the primary channel than the eavesdropping one, which boosts the capacity of the primary channel and decreases the capacity of the eavesdropping channel simultaneously by the assignment of cooperative relays [13], [14], [15]. However, most of the prior works are from the information theoretic point of view and the relationship between secrecy capacity enhancement and relay assignment process has not been well investigated yet. On the other hand, in order to increase the secrecy capacity, cooperative jamming technique which introduces intentional interference to the eavesdropping channel has also been developed as an interesting approach for recent secure applications [16], [17], [18]. As far as we know, joint cooperative relaying and jamming techniques with the presence of multiple eavesdroppers under cooperative communication aware wireless ad hoc networks (WANETs) have not been studied yet.

In this paper, we aim to provide secure cooperative communication for wireless ad hoc networks where involve multiple unicast sessions and eavesdroppers. The objective of our design is to maximize the system secrecy capacity through cooperative relaying and cooperative jamming techniques. Take the illustrative network in Fig. 1 as an example, in order to protect the broadcast message and achieve secure cooperative communication, source node can exploit the relay nodes set and choose one or more relays to cooperatively beam-form towards the destination and enable a greater capacity gain in the primary channel than the eavesdropping channel. Thus, the relays that are assigned to help the source-destination pairs have a great impact on the system security performance. One can enhance the system security against eavesdroppers by boosting the capacity of the primary channel and simultaneously decreasing the capacity of the eavesdropping one with an efficient relay assignment procedure. Besides, for the relay nodes which are not assigned to help the transmission between sources and destinations, they can act as friendly jammers to the source-destination pairs and generate intentional interference to the eavesdroppers. Therefore, the secrecy capacity can be further increased. Motivated by this scenario, we characterize the security performance of the system by secrecy capacity and study the secrecy capacity optimization problem. This paper offers an extension of our previous work [19] in cooperative wireless ad hoc environments. In contrast to [19], in which one relay node is assigned to at most one source-destination pair to exploit physical layer security, here, we propose a more general model where a relay node can be shared by multiple source-destination pairs.

1.1 Summary of Main Contributions

Our main contributions are summarized as follows:

- We exploit the secure cooperative communication issue with the presence of *multiple* eavesdroppers in WANETs. The secrecy capacity optimization problem is addressed in which security enhancement is achieved by cooperative relaying and cooperative jamming. We first model the relay assignment problem for secrecy capacity maximization, and make comprehensive investigations on the secrecy capacity gain brought by the relay assignment procedure.
- An optimal relay assignment algorithm is first developed, which solves the secrecy capacity maximization problem in polynomial time. Then the advantages of cooperative jamming technique is exploited and a smart jamming algorithm is proposed to further increase the system secrecy capacity.
- Extensive experimental results validate that our proposed algorithms significantly improve the system secrecy capacity under various network settings.

1.2 Paper Organization

The rest of this paper is organized as follows. In Section 2, we briefly survey the related work. In Section 3, we describe the architecture of our system model and formulate the problem under consideration. We exploit the opportunities of secrecy capacity enhancement brought by relay assignment in Section 4. We develop an optimal relay assignment algorithm in Section 5. A smart jamming algorithm is presented in Section 6. In Section 7, we evaluate

the efficiency of our proposed algorithms through experiments. Finally, Section 8 concludes the paper and points out the future work.

2 Related Work

Cooperative wireless networking with the objective to improve the system capacity has attracted extensive attentions during the past half-decade. For instance, in [2], [20] and [21], authors tended to enhance the system capacity through efficient cooperative relay assignment. With the objective to support emergency services in WANETs, Han et al. proposed two novel networking framework for cooperative and non-cooperative WANETs in [2] and [22], respectively.

Considering physical layer security for secure cooperative communication, Dong et al. proposed effective decode-and-forward (DF) and amplify-and-forward (AF) based cooperative relaying protocols for physical layer security in [23] and [24], respectively. Recently, there have been considerable efforts devoted to generalizing physical layer security to the wireless fading channel and to various multi-user scenarios [6]. Aggarwal et al. studied the secrecy capacity of a class of orthogonal relay eavesdropper channels in [25]. Tekin and Yener in [26] considered the scenario where multiple users communicate with a common receiver in the presence of an eavesdropper, and the optimal transmission power allocation policy is chosen to maximize the secrecy sum-rate. Dong et al. in [13] used cooperative relays to improve wireless physical layer security in the presence of multiple eavesdroppers. Literature [16] and [17] investigated the joint relay and jammer selection problem for one-way and two-way cooperative relay networks with secrecy constraints, where one or more jammer nodes transmitting simultaneously with the relaying link in order to create artificial interference to degrade the eavesdropper links was analyzed. In [19], we first investigated the secrecy capacity maximization problem via cooperative relaying and jamming, in which the system model is restricted to guarantee there are sufficient relays for all *s-d* pairs.

3 System Description and Problem Formulation

3.1 Network Model

In this paper, we investigate the secure cooperative communication issue for wireless ad hoc networks with the presence of multiple malicious eavesdroppers. Specifically, we consider a WANET consisting of N individual nodes, with each node being either a source node, a destination node, a potential relay node or an eavesdropping node. We assume that there are N_s source nodes forming the source set $S = \{s_1, s_2, \ldots, s_{N_s}\}$. Each source node is required to transmit packets to its respective destination. Denote $D = \{d_1, d_2, \ldots, d_{N_d}\}$ as the set of destination nodes. We consider the traffic in the WANET performs as a number of unicast sessions and each source node s_i is paired with a destination node d_i.[1] Thus, we have $N_s = N_d$. Besides, there

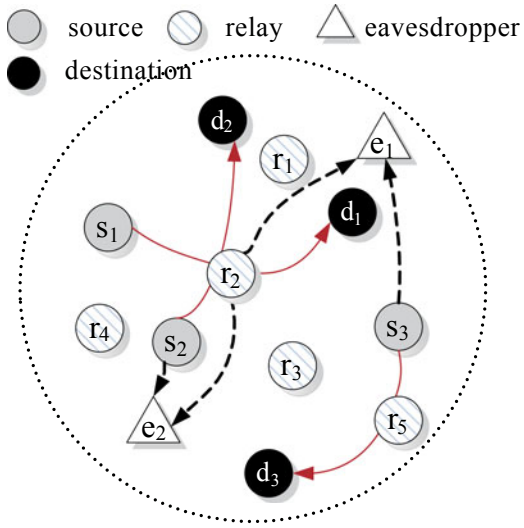


Fig. 2. A cooperative ad hoc network consisting of 3 *s-d* pairs, 5 relay nodes and 2 eavesdropping nodes, in which solid line represents the cooperative link and dash line is the eavesdropping link.

are N_r relay nodes forming the relay set $R = \{r_1, r_2, \ldots, r_{N_r}\}$ and N_e $(\leq N_s)$ eavesdropping nodes $E = \{e_1, e_2, \ldots, e_{N_e}\}$ forming the eavesdropper set.[2] We assume that each node is equipped with a single transceiver and can transmit/receive within one channel at a time. In addition, each node can only serve a unique role of source, destination, relay, or eavesdropper at a time, i.e., $N = 2N_s + N_r + N_e$. The eavesdropping nodes are assumed to be *passive* so they do not transmit any signal with the intention of jamming the destinations and only eavesdrop the information transmitted by the sources and relays. We assume that the WANET is cooperative communication aware, that is, the distance between any two nodes in the network is less than the transmission range so that each *s-d* pair can use direct transmission (DT) or cooperative communication. In other words, each transmission can be overheard by all the eavesdropping nodes. An example of a cooperative ad hoc network is shown in Fig. 2, which will be used for investigation throughout this paper. For clarity purpose, we only indicate part of the links in the figure.

A flat, block Rayleigh fading environment is applied [14]. That is, the wireless channel remains static for one coherence interval (one slot) and changes independently in different coherence intervals with a variance $\sigma_{i,j}^2 = l_{i,j}^{-\alpha}$, where $l_{i,j}$ is the euclidean distance between node i and j, and α is the pass loss exponent. The channel gain between node i and j is denoted as $h_{i,j}$, which is modeled as a zero-mean, independent, circularly-symmetric complex Gaussian random variable with variance $\sigma_{i,j}^2$. Additive white Gaussian noise (AWGN) with power spectral density N_0 (in Watt/Hz) is assumed [17]. The *fixed-channel-bandwidth* model is adopted where the bandwidth of each channel is assumed to be W in *Hz*. Thus, when node i transmits a signal to node j with power P_i, the instantaneous signal-to-noise ratio (SNR) seen

1. The terms source-destination pair s_i and d_i, *s-d* pair s_i and d_i, and $\langle s_i, d_i \rangle$ will be used interchangeably throughout this paper.

2. In [19], we assume $N_r > N_s$ to guarantee there are sufficient relays for all the sessions. Here, we relax this constraint and allow multiple source-destination pairs can share a common relay node. Besides, the spare relays can act as friendly jammers, which will be discussed in Section 6.

by node j, denoted by $\gamma_{i,j}$, is $\gamma_{i,j} \triangleq \frac{P_i|h_{i,j}|^2}{N_0 W}$. We assume that the transmission power for all source nodes and relay nodes are P_s and P_r in Watt, respectively. In order to mitigate interference, we make the same assumption as in [20] and [21], where the orthogonal channels are available in the network, e.g., different sources can communicate with their respective destinations at their assigned channels with orthogonal frequency division multiple access (OFDMA) technique, which is proposed for cooperative communication [29]. Furthermore, we assume that the overall bandwidth of all *s-d* pairs will not exceed the bandwidth allocated to the network.

3.2 Transmission Model

Following our network model and the discussions in [20] and [32], each source-destination pair can use either direct transmission or cooperative communication with the help of the best relay to achieve full diversity. We define the channel between s_i and d_i (with or without cooperative relay) as *primary channel*, and the channel between s_i and e_u (with or without cooperative relay) as *eavesdropping channel*. When the direct transmission is applied, the transmission between s_i and d_i can also be overheard by the eavesdroppers. The capacity of the primary channel from s_i to d_i and that of the eavesdropping channel from s_i to e_u under DT can be computed by:

$$C^P_{DT}(s_i, d_i) = \frac{W}{2}\log_2(1+\gamma_{s_i,d_i}), \tag{1}$$

$$C^E_{DT}(s_i, e_u) = \frac{W}{2}\log_2(1+\gamma_{s_i,e_u}). \tag{2}$$

$$C^P_{AF}(\mathcal{R}(s_i)) = \frac{1}{|\mathcal{S}(\mathcal{R}(s_i))|}\frac{W}{2}\log_2 \left(1+\gamma_{s_i,d_i}+\frac{\gamma_{s_i,\mathcal{R}(s_i)}\gamma_{s_i,d_i}}{\gamma_{s_i,\mathcal{R}(s_i)}+\gamma_{\mathcal{R}(s_i),d_i}+1}\right), \tag{3}$$

$$C^E_{AF}(\mathcal{R}(s_i), e_u) = \frac{1}{|\mathcal{S}(\mathcal{R}(s_i))|}\frac{W}{2}\log_2 \left(1+\gamma_{s_i,e_u}+\frac{\gamma_{s_i,\mathcal{R}(s_i)}\gamma_{s_i,e_u}}{\gamma_{s_i,\mathcal{R}(s_i)}+\gamma_{\mathcal{R}(s_i),e_u}+1}\right), \tag{4}$$

$$C^P_{DF}(\mathcal{R}(s_i)) = \frac{1}{|\mathcal{S}(\mathcal{R}(s_i))|}\frac{W}{2} \min\{\log_2(1+\gamma_{s_i,\mathcal{R}(s_i)}), \log_2(1+\gamma_{s_i,d_i}+\gamma_{\mathcal{R}(s_i),d_i})\}, \tag{5}$$

$$C^E_{DF}(\mathcal{R}(s_i), e_u) = \frac{1}{|\mathcal{S}(\mathcal{R}(s_i))|}\frac{W}{2} \min\{\log_2(1+\gamma_{s_i,\mathcal{R}(s_i)}), \log_2(1+\gamma_{s_i,e_u}+\gamma_{\mathcal{R}(s_i),e_u})\}. \tag{6}$$

When the cooperative communication is applied, we adopt the model proposed in [12] where transmission proceeds in a frame-by-frame basis and each frame is divided into two time slots: (a) broadcast phase in the first time slot, and (b) cooperative phase in the second time slot. During the broadcast phase, source s_i transmits the signal to its dedicated destination d_i. Due to the broadcast nature of wireless communication, this transmission can also be overheard by the relay nodes in R and eavesdropping nodes in E. During the cooperative phase, at most one relay node is assigned to source-destination pair $\langle s_i, d_i\rangle$. The assigned relay node forwards the data to d_i using different techniques depending on different CC modes: Amplify-and-Forward or Decode-and-Forward. Under AF mode, the relay node amplifies the signal received from the source node in the first time slot and then transmits the amplified signal to the destination in the second time slot. Under DF mode, the relay node decodes and estimates the signal received from the source node in the first time slot and then transmits the estimated data to the destination node in the second time slot.

In contrast to [19], where we assume that each source-destination pair is assigned a different relay node. Here, we extend the model and analyze the situation when multiple source-destination pairs share a common relay node. We say that relay node r_j is *assigned* to source-destination pair $\langle s_i, d_i\rangle$ if r_j helps s_i to achieve cooperative communication from s_i to d_i. Denote the relay node assigned to source-destination pair $\langle s_i, d_i\rangle$ in the cooperative phase by $\mathcal{R}(s_i)$. Let $\mathcal{S}(\mathcal{R}(s_i))$ denote the set of *s-d* pairs to which $\mathcal{R}(s_i)$ is assigned for cooperative communication. For the case when multiple *s-d* pairs share one relay node, i.e., $|\mathcal{S}(\mathcal{R}(s_i))| > 1$, where $|X|$ is the cardinality of set X, we assume that each relay node equally provides service to all the *s-d* pairs employing it. This can be achieved, for example, by using a reservation-based TDMA scheduling and the shared relay node serves each *s-d* pair in a round-robin fashion [21]. According to the analysis in [17] and [14], the achievable capacity of the primary channel between s_i and d_i with an assigned AF or DF relay $\mathcal{R}(s_i)$ can be expressed as Eqn. (3) and Eqn. (5). During cooperative communication, the eavesdropping nodes can also overhear the transmitting signals in both of the two phases. Similarly, the achievable capacity of the eavesdropping channel between s_i and e_u with an assigned AF or DF relay $\mathcal{R}(s_i)$ can be expressed as Eqn. (4) and Eqn. (6), respectively.

Secrecy capacity is defined as the maximum transmission rate of the involved *s-d* pair at which the eavesdropper is unable to decode any information. For our predefined model, secrecy capacity can be computed by the differences between the Shannon capacity of primary channel and that of the eavesdropping channel [27]. Let $C^S_{DT}(s_i, e_u)$ denote the secrecy capacity between *s-d* pair $\langle s_i, d_i\rangle$ and eavesdropping node e_u under direct transmission, it can be computed by:

$$C^S_{DT}(s_i, e_u) = \left[C^P_{DT}(s_i, d_i) - C^E_{DT}(s_i, e_u)\right]^+, \tag{7}$$

where $[x]^+ \triangleq \max\{0, x\}$. Similarly, the secrecy capacity between *s-d*pair $\langle s_i, d_i\rangle$ and eavesdropping node e_u with an assigned AF or DF relay $\mathcal{R}(s_i)$ can be expressed as:

$$C^S_{AF}(\mathcal{R}(s_i), e_u) = \left[C^P_{AF}(\mathcal{R}(s_i)) - C^E_{AF}(\mathcal{R}(s_i), e_u)\right]^+, \tag{8}$$

$$C^S_{DF}(\mathcal{R}(s_i), e_u) = \left[C^P_{DF}(\mathcal{R}(s_i)) - C^E_{DF}(\mathcal{R}(s_i), e_u)\right]^+. \tag{9}$$

3.3 Problem Formulation

Following the previous definitions, we first give the secrecy capacity expression between an *s-d* pair $\langle s_i, d_i \rangle$ and an eavesdropper e_u, denoted by $C^S(s_i, e_u)$:

$$C^S(s_i, e_u) = \delta_{i,j} \cdot C^S_{CC}(\mathcal{R}(s_i), e_u) + \big(1 - \delta_{i,j}\big) \cdot C^S_{DT}(s_i, e_u), \tag{10}$$

where $\delta_{i,j} \in \{0, 1\}$ is a binary variable to characterize whether a cooperative relay r_j is assigned to $\langle s_i, d_i \rangle$, i.e., if $\mathcal{R}(s_i) = r_j$, $\delta_{i,j} = 1$, otherwise, $\delta_{i,j} = 0$, and $C^S_{CC}(\mathcal{R}(s_i), e_u)$ is the secrecy capacity between $\langle s_i, d_i \rangle$ and e_u under AF or DF mode, i.e., $C^S_{CC}(\mathcal{R}(s_i), e_u) = C^S_{AF}(\mathcal{R}(s_i), e_u)$ if AF is used and $C^S_{CC}(\mathcal{R}(s_i), e_u) = C^S_{DF}(\mathcal{R}(s_i), e_u)$ if DF is used.

As there are multiple eavesdroppers in the network, the transmission rate between an *s-d* pair is restricted by the minimum secrecy capacity among the *s-d* pair and all eavesdroppers. It is reasonable to focus on the *minimum* secrecy capacity between the dedicated *s-d* pair and all the eavesdroppers.

Definition 3.1 (Secrecy capacity for a single pair). *The secrecy capacity for* s-d *pair* $\langle s_i, d_i \rangle$ *is the minimum secrecy capacity between* $\langle s_i, d_i \rangle$ *and all eavesdroppers, which is the maximum transmission rate at which all eavesdroppers are unable to decode any transmitting information from* s_i *to* d_i*:*

$$C^S(s_i) = \min_{e_u \in E} \big\{ C^S(s_i, e_u) \big\}. \tag{11}$$

Therefore, the secrecy capacity for the predefined ad hoc network consisting of N_s *s-d* pairs, N_r relay nodes and N_e eavesdropping nodes with relay assignment profile δ is defined as the total secrecy capacity of all *s-d* pairs:

$$C^S_{sum}((S, D), R, E, \delta) \ = \sum_{s_i \in S} C^S(s_i). \tag{12}$$

Next we address the **R**elay **A**ssignment **P**roblem for secrecy capacity maximization in **S**ecure **C**ooperative **A**d hoc **N**etworks (**RAP-SCAN**) as follows.

Definition 3.2 (RAP-SCAN). *Given a set of source-destination pairs* (S, D)*, a set of relay nodes* R *and a set of eavesdropping nodes* E*, RAP-SCAN seeks for a relay assignment profile such that the system secrecy capacity* $C^S_{sum}((S, D), R, E, \delta) = \sum_{s_i \in S} C^S(s_i)$ *is maximized among all the possible relay assignment profiles.*

According to the above definitions and discussions, we theoretically formulate RAP-SCAN as the following optimization problem:

$$(\mathbf{RAP-SCAN}) \text{ Maximize } C^S_{sum}((S, D), R, E, \delta) \tag{13}$$

subject to:

$$\delta_{i,j} = \begin{cases} 1, & \text{if } \mathcal{R}(s_i) = r_j, \\ 0, & \text{otherwise.} \end{cases} \tag{14a}$$

$$\text{Given } \mathcal{R}(s_i) = r_j, \mathcal{S}(\mathcal{R}(s_i)) = \sum_k \delta_{k,j} (s_i, s_k \in S, r_j \in R), \tag{14b}$$

$$\sum_{j=1}^{N_r} \delta_{i,j} \le 1 (s_i \in S, r_j \in R), \tag{14c}$$

$$\Phi_{CSI} = \{\gamma_{s_i,d_i}, \gamma_{s_i,r_j}, \gamma_{r_j,d_i}, \gamma_{s_i,e_u}, \gamma_{r_j,e_u}\} \quad (\forall s_i \in S, d_i \in D, r_j \in R, e_u \in E), \tag{14d}$$

where Eqn. (14a) specifies the binary variable $\delta_{i,j}$, Eqn. (14b) specifies that each relay node can be assigned to multiple *s-d* pairs, Eqn. (14c) specifies that each *s-d* pair can only choose at most one relay node for cooperative communication, Eqn. (14d) indicates that the global Channel State Information (CSI) is available [16], [17]. Φ_{CSI} includes all channel information between sources and destinations, sources and relays, relays and destinations, sources and eavesdroppers, and relays and eavesdroppers.

4 Secrecy Capacity Gain from Cooperative Relay Assignment

The basic idea of secure CC is that after amplifying or decoding the signals, the cooperative relay and source can *beam-form* towards the destination to enable a greater capacity gain in the primary channel than the eavesdropping one. According to the previous formulations, it is not easy to observe whether cooperative relay assignment can benefit the secrecy capacity. In this section, we analyze the secrecy capacity gain brought by cooperative relay assignment and exploit the opportunities of secrecy capacity enhancement.

4.1 Maximum Primary Channel Capacity under CC

Secrecy capacity is defined as the difference between the capacity of the primary channel and that of the eavesdropping channel. Intuitively, one wants to obtain the maximum secrecy capacity can exploit maximizing the achievable capacity of the primary channel and minimizing that of the eavesdropping channel at the same time. Here, we first derive the achievable upper bound of the primary channel under cooperative AF and DF mode.

Lemma 4.1 (Maximum capacity of the primary channel). *When relay node* r_j *involves in the cooperative transmission between* s-d *pair* s_i *and* d_i*, the maximum capacity of the primary channel can be achieved by solving the following optimization problems, under AF and DF mode, respectively:*

$$\text{AF mode} : \max C^S_{AF} \Leftrightarrow \max \left\{ \frac{\gamma_{s_i,r_j} \gamma_{r_j,d_i}}{\gamma_{s_i,r_j} + \gamma_{r_j,d_i} + 1} \right\}, \tag{15}$$

$$\text{DF mode} : \max C^S_{DF} \Leftrightarrow \max\{\min\{\gamma_{s_i,r_j}, \gamma_{s_i,d_i} + \gamma_{r_j,d_i}\}\}, \tag{16}$$

Proof. It is not hard to notice that the above objective formulations are derived from the capacity expressions of the primary channel in Eqn. (3) and Eqn. (5). □

According to the above Lemma, we can obtain the maximum capacity of the primary channel be solving the formulated sub-problems. Unfortunately, as the relay nodes are randomly distributed in the network, a source node can not always exploit the *best located* relay to assist its transmission towards the dedicated destination in order to achieve maximum cooperative link capacity. On the other hand, one can

observe that the capacity expression of the eavesdropping channel under cooperative mode have a similar form as that of the primary channel. It is hard to obtain the optimum secrecy capacity by maximizing Eqn. (3) and (5), and minimizing Eqn. (4) and (6) at the same time. Therefore, an efficient relay assignment procedure is required and the secrecy capacity gain brought by the cooperative relay assignment should be well investigated.

4.2 Secrecy Capacity Gain under CC-AF Mode

Under cooperative Amplify-and-Forward mode, the relay node first amplifies the received signals from the source and then cooperates with the source to transmit the secret information to the destination. According our previous discussions, the secrecy capacity between *s-d* pair $\langle s_i, d_i \rangle$ and eavesdropping node e_u with an assigned AF relay is expressed in Eqn. (8). It is not obvious to observe the benefits brought by the involved AF relay. We first consider the case when the secrecy capacity between *s-d* pair $\langle s_i, d_i \rangle$ and eavesdropping node e_u under direct transmission is zero, i.e.,the eavesdropping channel is better than the primary channel ($\gamma_{s_i,e_u} > \gamma_{s_i,d_i}$). The following lemma indicates the opportunities of secrecy capacity enhancement brought by the assigned AF relay node $\mathcal{R}(s_i) = r_j$.

Lemma 4.2. *In the case that the secrecy capacity between* s-d *pair* $\langle s_i, d_i \rangle$ *and eavesdropping node* e_u *under direct transmission is zero, i.e.,* $C^S_{DT}(s_i, e_u) = 0$, positive *secrecy capacity can be achieved if the involved AF relay node satisfies the following channel condition:*

$$\frac{\gamma_{s_i,r}(1+\gamma_{s_i,r})(\gamma_{r,d}-\gamma_{r,e_u})}{(1+\gamma_{s_i,r}+\gamma_{r,d})(1+\gamma_{s_i,r}+\gamma_{r,e_u})} > \gamma_{s_i,e_u}-\gamma_{s_i,r}. \quad (17)$$

Proof. The proof of the above lemma can be obtained by calculating $C^S_{AF}(\mathcal{R}(s_i), e_u) > 0$ in Eqn. (8). □

The above lemma indicates that the involved AF relay not only provides additional channel to transmit the secret information, but it also compensates the secret information loss at the source [31]. We can achieve nonzero secrecy capacity under AF mode with large γ_{s_i,r_j} and enough secret information compensation, i.e., $\gamma_{r_j,d_i} - \gamma_{r_j,e_u} \gg \gamma_{s_i,e_u} - \gamma_{s_i,d_i}$.

4.3 Secrecy Capacity Gain under CC-DF Mode

Under cooperative Decode-and-Forward mode, the relay node first decodes the received signals from the source and then cooperates with the source to transmit the secret information to the destination. Similar as the analysis under AF mode, we consider the secrecy capacity brought by the involvement of DF relay when $\gamma_{s_i,e_u} > \gamma_{s_i,d_i}$.

Lemma 4.3. *In the case that the secrecy capacity between* s-d *pair* $\langle s_i, d_i \rangle$ *and eavesdropping node* e_u *under direct transmission is zero, i.e.,* $C^S_{DT}(s_i, e_u) = 0$, positive *secrecy capacity can be achieved if the involved DF relay node* r_j *satisfies the following channel conditions:*

$$\begin{cases} \gamma_{r_j,d_i} - \gamma_{r_j,e_u} > \gamma_{s_i,e_u} - \gamma_{s_i,d_i}, \\ \gamma_{s_i,r_j} > \gamma_{s_i,e_u} + \gamma_{r_j,e_u}. \end{cases} \quad (18)$$

The proof to the above lemma can be found in Appendix A in the supplementary file, which can be found on the Computer Society Digital Library at http://doi.ieeecomputersociety.org/10.1109/TPDS.2014.2316155. To this end, let us look back into the formulated problem. From the above two lemmas, we observe that whether the cooperative relay assignment benefits the secrecy capacity greatly depends on the involved relay nodes.

5 An Optimal Relay Assignment Algorithm

Advanced cooperative wireless applications calls for time-efficient and effective networking strategies to improve the system operation efficiency and reliability. In this section, by discussing with the case of multi-pair cooperative communication, we develop an optimal relay assignment algorithm, which is able to solve RAP-SCAN in polynomial time.

5.1 Multi-Pair Cooperative Communication

For the case that multiple *s-d* pairs share a common relay, we are more interested in whether this sharing will deteriorate the system secrecy capacity. The following lemma indicates us how we can improve the system secrecy capacity if there exists a relay node shared by multiple *s-d* pairs.

Lemma 5.1. *If a relay node* r_j *is shared by multiple* s-d *pairs, we can improve the system secrecy capacity by the following* double-step*adjustment: i) let the* s-d *pair with the minimum secrecy capacity among all the pairs sharing* r_j *use direct transmission; ii) keep other* s-d *pairs' relay assignment profile the same.*

The proof to the above lemma can be found in Appendix B in the supplementary file, available online.

Following our predefined system model, each source node will be either assigned a relay node for cooperative transmission or transmit to the destination directly. On the other hand, based on Lemma 5.1, we can always improve the system secrecy capacity by applying the double-step adjustment. Thus, each relay node will be assigned to at most one s-d pair in order to achieve maximum total secrecy capacity. This one-to-one matching relation indicates that we can relaxed the constraint in Eqn. (14b) to:

$$\text{For each } r_j \in R, \sum_{i=1}^{N_s} \delta_{i,j} \leq 1 (s_i \in S). \quad (19)$$

5.2 Motivating Example

Considering the cooperative ad hoc network in Fig. 2, the secrecy capacity between each *s-d* pair and eavesdropping node e_1 under the direct transmission and the cooperative communication are illustrated in Tables 1 and 2, respectively. Under direct transmission, the secrecy capacity between $\langle s_1, d_1 \rangle$ and e_1 is 0, between $\langle s_3, d_3 \rangle$ and e_1 is 1. After a random relay assignment, e.g., $\mathcal{R}(s_1) = r_2$, $\mathcal{R}(s_2) = r_1$ and $\mathcal{R}(s_3) = r_5$, the secrecy capacity between $\langle s_1, d_1 \rangle$ and e_1 increases to 3, between $\langle s_3, d_3 \rangle$ and e_1 increases to 7. However, the secrecy capacity between $\langle s_2, d_2 \rangle$ and e_1 decreases from 2 to 0. In other words, this relay assignment profile benefits *s-d* pair $\langle s_1, d_1 \rangle$ and $\langle s_3, d_3 \rangle$, but harms $\langle s_2, d_2 \rangle$.

TABLE 1
Secrecy Capacity under Direct Transmission (*Mbps*)

	$C^P_{DT}(s_i,d_i)$	$C^E_{DT}(s_i,e_1)$	$C^S_{DT}(s_i,e_1)$
$< s_1,d_1 >$	8	9	0
$< s_2,d_2 >$	10	8	2
$< s_3,d_3 >$	10	9	1

Although it is hard to evaluate whether such an assignment profile is good or not, it inspires us to seek for an optimal relay assignment profile that the system secrecy capacity can be maximized.

In Table 3, we list the secrecy capacity between all *s-d* pairs and eavesdropping nodes for the sample network in Fig. 2. Secrecy capacity is denoted as a two dimensional vector, $(C^S(s_i,e_1), C^S(s_i,e_2),)$ $(1 \le i \le 3)$. Notice that the dimension of the vector here is the number of eavesdropping nodes N_e. Each highlighted cell represents the secrecy capacity under the current assignment, which is the minimum one among all of the N_e results. For example, $C^S(s_1,e_1) = 0$ (under direction transmission) and $C^S(s_1,e_1) = 2$ (with assigned relay r_1). With the secrecy capacity for each *s-d* pair in mind, any relay assignment algorithms with the objective to maximize the system secrecy capacity seek for an optimum assignment profile for each *s-d* pair. Following our predefined system model and Lemma 5.1, each source node will be either assigned a relay node for cooperative transmission or transmit to its destination directly. This one-to-one matching relation indicates that we can map any instance of RAP-SCAN into that of the *Maximum Weighted Bipartite Matching (MWBM)* problem [30] and use corresponding algorithms to solve it.

5.3 Algorithm Details

For any instance $((S,D),R,E)$ of RAP-SCAN, we construct an instance $G=(U,V,w)$ of the MWBM problem as follows. Let a set U of vertices represents the source nodes set S, and a set V of vertices represents $D \cup R$. Then we set $w(s_i,r_j) = \min_{e_u \in E}\{C^S_{CC}(s_i,e_u)\}(r_j = \mathcal{R}(s_i))$, and set $w(s_i,d_i) = \min_{e_u \in E}\{C^S_{DT}(s_i,e_u)\}$ for all $s_i \in U$, $d_i \in V$. The corresponding MWBM instance for Fig. 2 is shown in Fig. 3. In order to have a clear view of the conversion, we also label the involved eavesdropping node with the minimum secrecy capacity together with the weight on the edge, e.g., e^*_u is the labeled eavesdropping node and $e^*_u = \arg\min_{e_u \in E}\{C^S(s_i,e_u)\}$.

We present our proposed **O**ptimal **R**elay **A**ssignment algorithm for **S**ecure **C**ooperative **A**d hoc **N**etworks, named

TABLE 2
Secrecy Capacity with an Assigned Cooperative Relay (*Mbps*)

	$\mathcal{R}(s_i)$	$C^P_{CC}(\mathcal{R}(s_i))$	$C^E_{CC}(\mathcal{R}(s_i),e_1)$	$C^S_{CC}(\mathcal{R}(s_i),e_1)$
$< s_1,d_1 >$	r_2	13	10	3
$< s_2,d_2 >$	r_1	14	15	0
$< s_3,d_3 >$	r_5	15	8	7

TABLE 3
Secrecy Capacity under Cooperative Communication (*Mbps*)

s-d pair	$\mathcal{R}(s_i)$					
	$\emptyset$	r_1	r_2	r_3	r_4	r_5
$< s_1,d_1 >$	(0, 2)	(2, 4)	(3, 3)	(0, 0)	(1, 0)	(0, 0)
$< s_2,d_2 >$	(2, 1)	(0, 0)	(3, 2)	(0, 0)	(4, 0)	(0, 0)
$< s_3,d_3 >$	(1, 4)	(0, 0)	(0, 0)	(2, 3)	(0, 0)	(7, 5)

ORA-SCAN, as illustrated in Appendix C in the supplementary file, available online. The proposed ORA-SCAN first constructs a set U of N_s vertices corresponding to S and a set V of $N_s + N_r$ vertices corresponding to $D \cup R$. After labeling the weight of each edge in the constructed graph, i.e., $w(s_i,d_i) = \min_{e_u \in E}\{C^S_{DT}(s_i,e_u)\}$, we apply an MWBM algorithm to find a maximum weighted matching M^* for $G=(U,V,w)$. Next we prove the correctness and analyze the computational complexity of it by the following theorem.

Theorem 5.1. *The proposed ORA-SCAN algorithm guarantees to find an optimal cooperative relay assignment profile for RAP-SCAN in time bounded by* $O(N_s^2 N_r)$.

Proof. We prove the correctness of ORA-SCAN by contradiction. Following the formulated RAP-SCAN and our previous discussions, each optimal relay assignment profile for RAP-SCAN can be mapped to a matching in the graph $G=(U,V,w)$, as described from Lines 1 to 11. Assume that there exists another relay assignment profile δ' which resulting in a higher secrecy capacity than δ^* returned by ORA-SCAN. In other words, there exists another matching M' for G, which has a higher weight than that of M^*. It contradicts the fact that M^* is a maximum weight matching for G. Therefore, it is an optimal relay assignment algorithm.

For the computational time of ORA-SCAN, it is consisted of three parts: mapping time from RAP-SCAN to MWBM (from Lines 1 to 11), the running time of the corresponding MWBM algorithm (Line 12) and the resulting variable resetting (from Lines 13 to 20). For the first part, the computational time of the secrecy capacity for all *s-d* pairs is $O(N_s N_r N_e)$. For the second part, many algorithms have been developed to solve the MWBM problem in polynomial time, such as Dijkstra algorithm with Fibonacci heap and Kuhn-Munkres algorithm [30]. If the Dijkstra algorithm with Fibonacci heap is used, the running time is bounded by $O(N_s^2 N_r)$. For the third part, the running time is bounded by $O(N_s N_r)$. Therefore, the running time of ORA-SCAN is bounded by $O(N_s N_r N_e + N_s^2 N_r + N_s N_r)$. For our system model, as we assume that $N_e \le N_s$, the running time of ORA-SCAN is bounded by $O(N_s^2 N_r)$. □

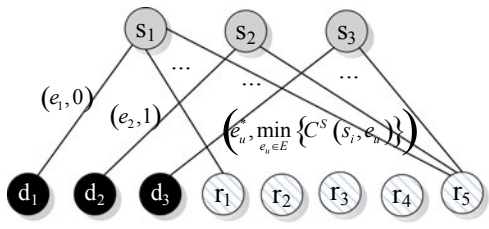


Fig. 3. Mapping RAP-SCAN to the MWBM problem.

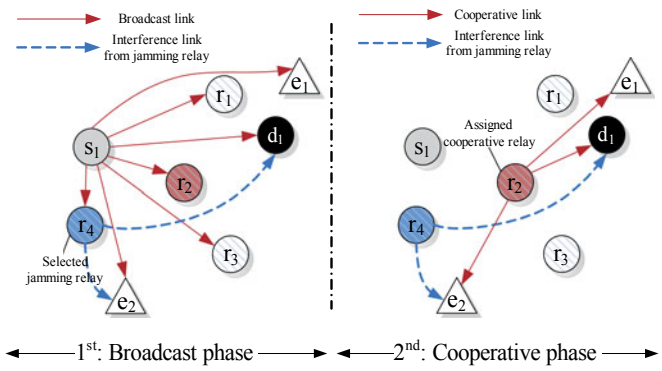


Fig. 4. Communication phases with a selected friendly jammer.

6 Proposed Smart Jamming Algorithm

In order to reduce the capacity of the eavesdropping channel, cooperative jamming technique which encourages one or more involved nodes to generate artificial interference towards the eavesdropping nodes is of great interests recently. It has been shown that, by carefully scheduling the interaction between relay nodes and jamming nodes, substantial secrecy improvements can be achieved [16], [18]. In this section, we exploit the advantages of cooperative jamming technique and propose a smart jamming algorithm to further increase the system secrecy capacity.

6.1 Transmission Model with Cooperative Jamming

We modify the two-phase cooperative communication transmission model presented in Section 3.2 and the communication phases are shown in Fig. 4. Under the modified model, one or more relays that were not assigned to any *s-d* pairs during the assignment procedure can be selected to act as friendly jammer(s) to further increase the system secrecy capacity. During the *broadcast* phase, in order to protect the source's broadcast message, a relay node is selected to act as the friendly jammer, which generates intentional interference towards the eavesdropping nodes. During the *cooperative* phase, the assigned cooperative relay transmits the source's message towards the destination. The selected jamming relay node acts as a friendly jammer to the *s-d* pair it is serving, and continues to generate intentional interference towards the eavesdropping nodes. Take the scenario in Fig. 4 (part of Fig. 2) as an example, relay node r_4 is not assigned to any *s-d* pairs after the relay assignment procedure, so it can be selected to serve as a friendly jammer for $\langle s_1, d_1\rangle$. During the cooperative phase, the assigned cooperative relay node r_2 transmits the data from s_1 to d_1 . r_4 acts as a friendly jammer to $\langle s_1, d_1\rangle$ and generates intentional interference towards eavesdropper e_2. One should also notice that the interference signal generated by the selected jamming relay node can also affect the cooperative links, for example, there is interference from r_4 to d_1 during both phases.

Following our system model, orthogonal channels are applied to all *s-d* pairs, the jamming relay can use the same channel as the *s-d* pair it is serving but just generating artificial interference. Thus, the interference signal generated by the jamming relay will not affect the transmission of other *s-d* pairs. Furthermore, we assume that the jamming relay selected in the two communication phases is the same, the selection methodology with involvement of two different jamming nodes in two phases is out of the scope of this paper.

6.2 Algorithm Description

Under the predefined cooperative Decode-and-Forward mode, if the maximum ratio combiner (MRC) technique [28] is used to combine the two-phase transmissions at the destination, the instantaneous secrecy capacity between $\langle s_i, d_i\rangle$ and e_u with a cooperative jamming relay j_v can be expressed as [17]:

$$C^S_{DF}(s_i, e_u, j_v) = \frac{W}{2}\left[\log_2\left(1+\frac{\gamma_{s_i,d_i}}{1+\beta^{(1)}\gamma_{j_v,d_i}}+\frac{\gamma_{\mathcal{R}(s_i),d_i}}{1+\beta^{(2)}\gamma_{j_v,d_i}}\right) -\log_2\left(1+\frac{\gamma_{s_i,e_u}}{1+\beta^{(2)}\gamma_{j_v,e_u}}+\frac{\gamma_{\mathcal{R}(s_i),d_i}}{1+\beta^{(2)}\gamma_{j_v,e_u}}\right)\right]^+, \quad (20)$$

where $\beta^{(t)} \in \{0, 1\}$ is a binary variable to indicate whether the jamming relay is activated during the tth phase, t=1 denotes the broadcast phase and t=2 is the cooperative phase, respectively.

As all relay nodes have the global channel state information, the following lemma indicates the condition for an *s-d* pair to select an unassigned relay as a friendly cooperative jammer.

Lemma 6.1. *A relay node that was not assigned to any* s-d *pairs, denoted by r_v, can be selected to act as a friendly cooperative jammer for $\langle s_i, d_i\rangle$ if $\gamma_{r_v,e_u} > \gamma_{r_v,d_i}$.*

Proof. It can be derived from comparing Eqn. (20) and Eqn. (9). The improvement on secrecy capacity when a cooperative jamming relay involves can be expressed as $C^S_{DF}(s_i, e_u, r_v) - C^S_{DF}(\mathcal{R}(s_i), e_u) > 0$. Hence, we have $\gamma_{r_v,e_u} > \gamma_{r_v,d_i}$. □

The above lemma implies whether an unassigned relay can be selected to act as a friendly jammer for an *s-d* pair. The friendly jammer selection procedure is presented in Appendix D in the supplementary file, available online. After running the proposed algorithm, a jamming relay selection profile is obtained, in which the selected relay nodes are associated with different *s-d* pairs. As the smart jamming procedure follows with the the optimal relay assignment process, an efficient transmission scheduling is necessary.

7 Performance Evaluation

7.1 Experiment Setup

In this section, we verify our analysis and evaluate the efficiency of the proposed algorithms through extensive experiments.

To evaluate the effect of relay location on the primary channel capacity, we conduct experiments on a network consisting of a source node, a relay node and a destination node. Details of the experimental results can be found in Appendix E in the supplementary file, available online.

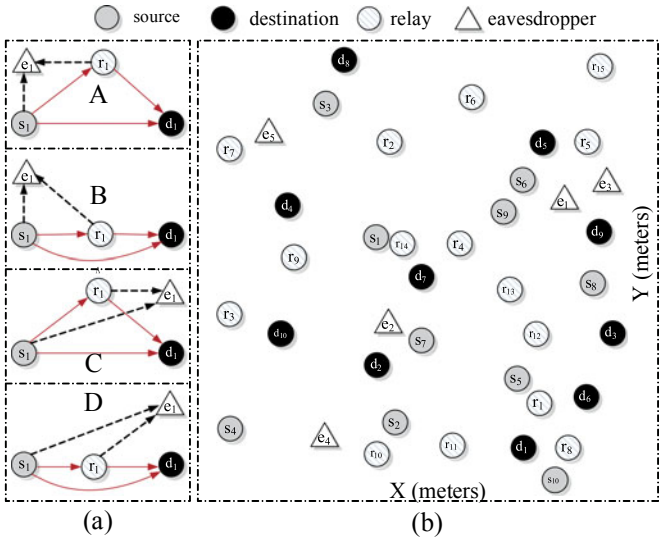


Fig. 5. Experimental scenarios: (a) Four secure cooperative ad hoc network scenarios each with one *s-d* pair, one relay node and one eavesdropping node. (b) Topology for a 40 nodes cooperative ad hoc network where $N_s = 10$, $N_r = 15$ and $N_e = 5$.

To evaluate the secrecy capacity gain brought by the cooperative relay assignment, experiments are first conducted in four sub-scenarios where the location of relay and eavesdropper varies, corresponding to different assignment choices, as shown in Fig. 5a. The distance from source and destination is $1{,}000$ meters and the location of relay and eavesdropper varies in different scenarios, e.g., $l_{s_1,e_1} = l_{r_1,e_1} = 500$ m, $l_{s_1,r_1} = l_{r_1,d_1} = 707$ m in Scenario A, $l_{s_1,e_1} = l_{s_1,r_1} = l_{r_1,d_1} = 500$ m, $l_{r_1,e_1} = 707$ m in Scenario B, etc. In the experiments, we set $W = 22$ MHz for the channel. We vary the path loss exponent, the transmission power of relay, and the transmission power of source to compare the secrecy capacity under different scenarios.

To evaluate the efficiency of our proposed relay assignment algorithm and the smart jamming algorithm, we carry out comprehensive experiments by studying various cooperative ad hoc network scenarios. We first varied the number of source-destination pairs N_s, the number of relay nodes N_r and the number of eavesdropping nodes N_e to evaluate the efficiency of our proposed relay assignment algorithm. Nodes are randomly distributed in a 500×500 m square. For each setting, we randomly generate 10 instances and the average result is presented with a 95 percent confidence interval. Experiments are conducted by comparing the total secrecy capacity under direct transmission, a random cooperative relay assignment, and our proposed relay assignment algorithm, ORA-SCAN. We set 22 MHz as the bandwidth for the channels. The transmission power for all sources and relays is set to 1 Watt and the ambient noise is 10^{-9} Watt/Hz. Lastly, we evaluate our proposed algorithms by studying a 40 nodes cooperative ad hoc network as shown in Fig. 5b. Nodes are randomly distributed in a 500×500 m square. There are 10 source-destination pairs which represent the unicast sessions, 15 relay nodes and five eavesdroppers. Experiments are conducted by comparing the total secrecy capacity under direct transmission, CC with ORA-SCAN, and CC with ORA-SACN and the smart jamming algorithm.

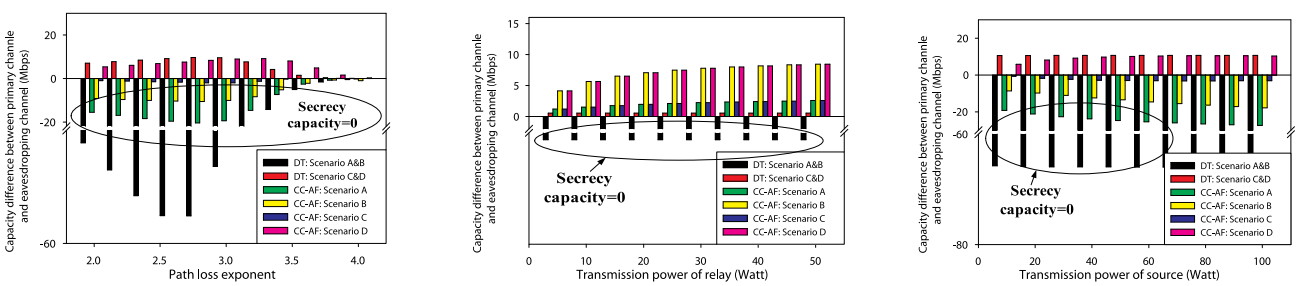
7.2 Experimental Results

7.2.1 Secrecy Capacity Gain from Relay Assignment

We evaluate the secrecy capacity under four different scenarios in Fig. 5a by varying the network settings, as shown in Figs. 6a, 6b and 6c. For clarify purpose, we also provide the secrecy capacity that is below zero. From the three sub-figures, we observe that the network settings (e.g., path loss exponent and the transmission power of source and relay) have less impact on the secrecy capacity than the assignment of relays. For example, sub-scenario-D always achieves nonzero secrecy capacity as the involvement of relay improves the capacity of the primary channel and simultaneously decrease the capacity of the eavesdropping one. Another observation is that the location of cooperative relay and eavesdropper has great impact on the secrecy capacity.

7.2.2 Efficiency of the Proposed Algorithms

We compare the performance of our proposed relay assignment algorithm (ORA-SCAN) with direct transmission and a random relay assignment algorithm, by varying the number of relay nodes, *s-d* pairs and eavesdropping nodes, as shown in Figs. 7a, 7b and 7c. In Fig. 7a, we fix the number of *s-d* pairs to 20 and the number of eavesdropping nodes to 5. ORA-SCAN achieves a much greater secrecy capacity gain than the random assignment when the number of relay nodes increases. Then we fix the number of relay nodes to 20 and the number of eavesdropping nodes to 5, we calculate the total secrecy capacity by varying the number of *s-d* pairs, as shown in Fig. 7b. Although ORA-SCAN still outperforms the other two algorithms, the secrecy capacity

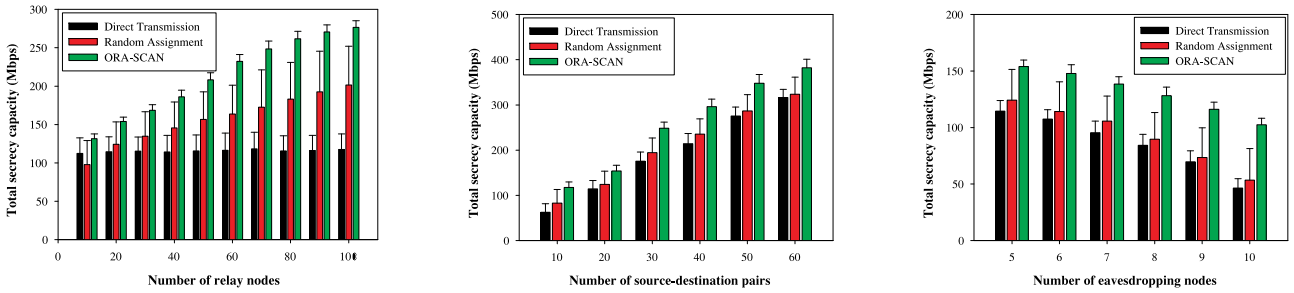


(a) Secrecy capacity vs. path loss exponent α

(b) Secrecy capacity vs. transmission power of relay P_r

(c) Secrecy capacity vs. transmission power of source P_s

Fig. 6. Secrecy capacity under four different scenarios in Fig. 5a.

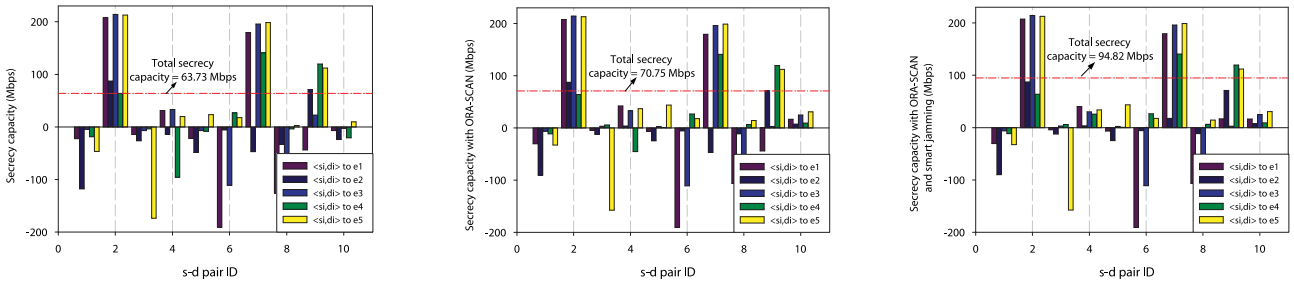


(a) Total secrecy capacity vs. number of relay nodes with 20 *s-d* pairs and 5 eavesdroppers

(b) Total secrecy capacity vs. number of *s-d* pairs with 20 relay nodes and 5 eavesdroppers

(c) Total secrecy capacity vs. number of eavesdropping nodes with 20 *s-d* pairs and 20 relay nodes

Fig. 7. Efficiency of proposed relay assignment algorithm.



(a) Secrecy capacity under direct transmission

(b) Secrecy capacity wih ORA-SCAN

(c) Secrecy capacity with ORA-SCAN and smart jamming

Fig. 8. Secrecy capacity of different *s-d* pair in Fig. 5b.

gain increase much slower as there are limited set of relay nodes to be exploited. In Fig. 7c, we vary the number of eavesdropping nodes which indicates for different security requirements. For each of the algorithms under consideration, the secrecy capacity gain from ORA-SCAN is much better than the other two algorithms.

Consider the network topology in Fig. 5b, we generate the secrecy capacity for each *s-d* pair under our proposed ORA-SCAN algorithm, as shown in Fig. 8b, and compare it with the secrecy capacity under direct transmission in Fig. 8a. The total secrecy capacity increases from 63.73 to 70.75 Mbps. This benefit is from the optimal relay assignment process. Further, we exploit the jamming technique and select one or more unassigned relay nodes to act as friendly jammer for some of the *s-d* pairs. We compute the secrecy capacity after running ORA-SCAN and the smart jamming algorithm altogether, which receives considerable improvement on the total secrecy capacity from 70.75 to 94.82 Mbps, as shown in Fig. 8c. The reason is that some spare relays can act as friendly jammer and serve for some transmitting sessions, e.g., jamming relay is selected to serve $\langle s_4, d_4\rangle$, $\langle s_7, d_7\rangle$ and $\langle s_9, d_9\rangle$ and to combat the dedicated eavesdropping nodes, which increases the secrecy capacity for each of the above *s-d* pairs.

8 Conclusion and Future Work

This paper aims to provide secure cooperative communication for WANETs via cooperative relaying and jamming. We theoretically formulate the secrecy capacity maximization problem and develop an optimal relay assignment algorithm to solve it in polynomial time. Then we propose a smart jamming algorithm to further increase the system secrecy capacity. Extensive experimental results reveal that our proposed algorithms can achieve high secrecy capacity under various network settings. For a future work, we will exploit the secrecy capacity optimization problem with imperfect channel state information. We provide a sketch of further discussions in Appendix F of the supplementary file, available online.

Acknowledgments

The authors would like to thank the editor and the anonymous reviewers, whose insightful comments helped us to improve the quality of the paper. This work was partially supported by Grant-in-Aid for Scientific Research of Japan Society for Promotion of Science (JSPS), Japan. This work also is partially support by the National Natural Science Foundation of China (NSFC) with Grants no. 61202488, no. 61373156 and no. 91438121, Key Basic Research Project of the Science and Technology Commission of Shanghai Municipality no. 12JC1405400, Shanghai Pujiang Program no.13PJ1404600, and Shanghai Branch of Southwest Electron and Telecom Technology Research Institute Project no. 2013008. An bridged version of this paper was accepted in the main conference of IEEE INFOCOM'2013 under the title "Secrecy Capacity Maximization for Secure Cooperative Ad-hoc Networks". Jie Li is the corresponding author.

References

[1] X. Shen, A. Hjrungnes, Q. Zhang, P. R. Kumar, and Z. Han, "Guest editorial: Cooperative networking - challenges and applications (Part 1)," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 241–244, Feb. 2012.

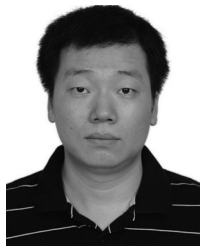
[2] B. Han, J. Li, J. Su, and J. Cao, "Self-supported cooperative networking for emergency services in multi-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, p. 450–457, Feb. 2012.
[3] Y. Sun, W. Trappe, and K. J. R. Liu, *Network-Aware Security For Group Communications*. New York, NY, USA: Springer, 2007.
[4] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun. Mag.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.
[5] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE Conf. Comput. Commun.*, 2011, pp. 1422–1430.
[6] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*. Delft, The Netherlands,Now Publishers, 2009.
[7] Y. Liang, H. V. Poor, and L. Ying, "Wireless broadcast networks: Reliability, security, and stability," in *Proc. IEEE Inf. Theory Appl. Workshop*, Feb. 2008, pp. 249–255.
[8] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[9] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[10] I. Csiszar and J. Korner, "Broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[11] A. Bletsas, H. Shin, and M. Z. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 3450–3460, Sep. 2007.
[12] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, pp. 3062–3080, Dec. 2004.
[13] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperative relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
[14] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
[15] J. Zhang, L. Fu, and X. Wang, "Impact of secrecy on capacity in large-scale wireless networks," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2012, pp. 3051–3055.
[16] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensic Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.
[17] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.
[18] T. Wang and G. B. Giannakis, "Mutual information jammer-relay games," *IEEE Trans. Inf. Forensic Security*, vol. 3, no. 2, pp. 290–303, Jun. 2008.
[19] B. Han and J. Li, "Secrecy capacity maximization for secure cooperative ad-hoc networks," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2013, pp. 2796–2804.
[20] S. Sharma, Y. Shi, Y. T. Hou, and S. Kompella, "An optimal algorithm for relay node assignment in cooperative ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 19, no. 3, pp. 879–892, Jun. 2011.
[21] D. Yang, X. Fang, and G. Xue, "HERA: An optimal relay assignment scheme for cooperative networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 245–253, Feb. 2012.
[22] B. Han, J. Li, and J. Su, "Self-supported congestion-aware networking for emergency services in WANETs," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2011, pp. 891–899.
[23] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, UIUC, Illinois, USA, Sep. 2008, pp. 1132–1138.
[24] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Process.*, Taipei, Taiwan, Apr. 2009, pp. 2613–2616.
[25] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," *EURASIP J. Wireless Commun. Netw.*, doi:10.1155/2009/494696, vol. 2009, 2009.
[26] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.
[27] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, July 2006, pp. 356–360.
[28] Y.-W. P. Hong, W.-J. Huang, and C.-C. J. Kuo, *Cooperative Communications and Networking: Technologies and System Design*. New York, NY, USA: Springer, 2010.
[29] H. Liu and G. Li, *OFDM-Based Broadband Wireless Networks: Design and Optimization*. Hobken, NJ, USA: Wiley 2005.
[30] D. B. West, *Introduction to Graph Theory*. 2nd ed. Englewood Cliffs, NJ, USA: Prentice Hall, 2001.
[31] P. Zhang, J. Yuan, J. Chen, J. Wang, and J. Yang, "Analyzing amplify-and-forward and decode-and-forward cooperative strategies in Wyner's channel model," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2009, pp. 1–5.
[32] Y. Zhao, R. S. Adve, and T. J. Lim, "Improving amplify-and-forward relay networks: Optimal power allocation versus selection," in *Proc. IEEE Int. Symp. Inf. Theory*, 2006, pp. 1234–1238.

Biao Han (M'13) received the BE and master's degrees in computer science in 2007 and 2009 respectively, both from National University of Defense Technology (NUDT), China, where he is currently an assistant professor. He received the PhD degree from the University of Tsukuba, Japan, in 2013. From January 2012 to April 2012, he has been a visiting scholar in the Department of ECE at the University of Florida. His research interests are in software defined networks (SDN), cooperative wireless communication, and network security. He is a member of the IEEE.

Jie Li (M'94-SM'04) received the BE degree in computer science from Zhejiang University, Hangzhou, China, and the ME degree in electronic engineering and communication systems from the China Academy of Posts and Telecommunications, Beijing, China. He received the DrEng degree from the University of Electro-Communications, Tokyo, Japan. He has been with the University of Tsukuba, Japan, where he is a full professor. His research interests are in mobile distributed multimedia computing and networking, OS, network security, modeling, and performance evaluation of information systems. He received the Best Paper Award from IEEE NAECON'97. He is a member of Information Processing Society of Japan (IPSJ). He has served as a secretary for Study Group on System Evaluation of IPSJ and on several editorial boards for IPSJ Journal and so on, and on Steering Committees of the SIG of System Evaluation (EVA) of IPSJ, the SIG of DataBase System (DBS) of IPSJ, and the SIG of MoBiLe computing and ubiquitous communications of IPSJ. He has been a co-chair of several international symposia and workshops. He has also served on the program committees for several international conferences such as IEEE ICDCS, IEEE INFOCOM, IEEE GLOBECOM, and IEEE MASS. He is a senior member of the IEEE and the ACM.

Jinshu Su (M'05) received the BS degree in mathematics from Nankai University, 1985, and the MS and PhD degrees from the National University of Defense Technology (NUDT) in 1988 and 2000, respectively, both in computer science. He is a full professor with the School of Computer at National University of Defense Technology. His research interests include internet architecture, internet routing, security, and wireless networks. Currently, he leads the Distributed Computing & High performance Router (DCHR) Lab and the Computer Networks & Information Security (CNIS) Lab, both are key Labs of National 211 and 985 projects of China. He also leads the High performance computer networks (HPCN) Lab, which is a key Lab of Hunan Province, China. He is a member of the ACM and IEEE, a senior member of China Computer Federation (CCF).

Minyi Guo received the BSc and ME degrees in computer science from Nanjing University, China, and the PhD degree in computer science from the University of Tsukuba, Japan. He is currently a Zhiyuan chair professor and a chair of the Department of Computer Science and Engineering, Shanghai Jiao Tong University (SJTU), China. Before joined SJTU, he had been a professor of the school of computer science and engineering, University of Aizu, Japan. He received the national science fund for distinguished young scholars from NSFC in 2007, and was supported by g Recruitment program of Global Experts in 2010. His present research interests include parallel/distributed computing, compiler optimizations, embedded systems, pervasive computing, and cloud computing. He has more than 250 publications in major journals and international conferences in these areas. He received five Best Paper Awards from international conferences. He is on the editorial board of *IEEE Transactions on Parallel and Distributed Systems* and *IEEE Transactions on Computers*. He is a senior member of the IEEE, member of the ACM, IEICE IPSJ, and CCF.



Baokang Zhao recevied the BS and PhD degrees in computer science from the National University of Defense Technology. He is an assistant professor in the School of Computer Science, National University of Defense Technology. He served as a program committee member for several international conferences and a reviewer for several international journals (including TCAD, etc.). He serves on the editor board of *Journal of Internet Sevices and Information Security (JISIS)*. His current research interests include system design, protocols, algorithms, and security issues in computer networks. He is a member of the ACM, IEEE, and CCF.