Adaptive Cooperation Schemes for Energy Efficient Physical Layer Security

Li Wang*, Lie-Liang Yang†, Victor C.M. Schober* and Mei Song*
* School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, P.R. China.
Email: {*liwang@bupt.edu.cn*, *xmaeecs@gmail.com*, *songm@bupt.edu.cn*}
†School of ECS, University of Southampton, SO17 1BJ, UK. Email: {*lly@ecs.soton.ac.uk*}

***Abstract*—This work studies security-oriented cooperation schemes, addressing three possible cooperation scenarios, namely the *jammer only*, *relay only* and the *relay-jammer pair*. The cooperation scheme is adaptively selected according to the security requirement and network's operational conditions. The selection of a relay or/and a jammer as well as their transmit power are jointly optimized with the objective of attaining a good trade-off between security performance and energy consumption.**

I. Introduction

In literature, many cooperative schemes, including cooperative relay [1], [2] and cooperative jamming [3], [4], have been proposed for enhancing physical layer security. However, the existing studies mainly focus on the improvement of security performance, but often overlook the issue of energy efficiency.

In this paper, we consider a generalized cooperation scenario, where a relay or/and a jammer are selected in an adaptive way, in order to minimize the energy consumption while meeting the security requirement. Our generalized cooperation scenario may include three specific operational scenarios, namely, the *relay only* (RO), *jammer only* (JO) and the *relay-jammer pair* (RJP), one of which is adaptively selected at a time according to the security requirement and the related channel state information (CSI). Furthermore, the selection of relay or/and jammer nodes along with their transmit power are jointly optimized. The performance of the considered schemes is examined via simulations in terms of the *secrecy capacity* (SC) and network lifetime.

II. System Model

We consider a wireless network consisting of legitimate source and destination nodes, along with a set of candidate cooperative nodes and eavesdroppers. The network is divided to lattices, each of which is around a destination node. The cooperative nodes may be selected as relays to the destination node or helpful jammers to jam the eavesdroppers.

According to [5], the SC of a source-destination pair equals the difference between the capacity achieved at the destination and that atttainable at the eavesdropper, expressed as

$$SC = \left[\log_2\left(1+\mathsf{SINR}_D\right) - \log_2\left(1+\mathsf{SINR}_E\right)\right]^+, \quad (1)$$

where SINR_D and SINR_E represent the signal-to-interference-plus-noise ratio (SINR) attained at the destination and at the eavesdropper, respectively, while $[x]^+ = \max(0, x)$. In this paper, we consider the case that there is at most one eavesdropper associated with a destination.

This work was supported by the Natural Science Foundation of China under Grant 61201150, by the State Major Science and Technology Special Projects under Grant 2012ZX03004001, by the Science Technology Innovation Foundation for Young Teachers in BUPT under Grant 2013RC0202, and by the Beijing Higher Education Young Elite Teacher Project under Grant YETP0442.

III. Cooperation Schemes for Security

Let h_{SD}, h_{SE}, h_{RD}, h_{RE} and h_{JE} denote the pair-wise channel gains between two nodes including source (S), destination (D), relay (R), eavesdropper (E) and jammer (J). Let P_R be the relay transmit power, and P_J be the jamming power.

Jammer Only (JO): In JO mode, a jammer improves the SC by reducing the capacity of the S-E channel. When assuming that the jamming signal is focused only on the eavesdropper, for example, with the aid of beamforming technique [6], the SC of the JO mode can be expressed as

$$SC_{JO} = \frac{1}{2}\left[\log_2\left(1+\frac{P_S|h_{SD}|^2}{\sigma^2}\right) - \log_2\left(1+\frac{P_S|h_{SE}|^2}{P_J|h_{JE}|^2+\sigma^2}\right)\right]^+ \quad (2)$$

Relay Only (RO): In the RO mode, a relay is chosen to improve both the channel capacity and the SC of the S-D channel. The SC of the RO mode can be found to be

$$SC_{RO} = \frac{1}{2}\left[\log_2\left(1+\frac{P_R|h_{RD}|^2}{\sigma^2}\right) - \log_2\left(1+\frac{P_R|h_{RE}|^2}{\sigma^2}\right)\right]^+ \quad (3)$$

Relay-Jammer Pair (RJP): In the RJP mode, a relay and a jammer are simultaneously employed, which yields the SC

$$SC_{RJP} = \frac{1}{2}\left[\log_2\left(1+\frac{P_R|h_{RD}|^2}{\sigma^2}\right) - \log_2\left(1+\frac{P_R|h_{RE}|^2}{P_J|h_{JE}|^2+\sigma^2}\right)\right]^+ \quad (4)$$

IV. Energy Efficient Cooperation

A. Reward Function with Energy Consideration

Let set $\mathcal{C}$ collect the nodes that are legitimate for acting as cooperative nodes. In order to determine the set of candidates for cooperation by jointly considering the security level, the remaining energy of the nodes and the reliability of communications, we propose a *reward function* for node $N \in \mathcal{C}$ as

$$W_N = \xi_1 f\left(|h_{ND}|, |h_{NE}|\right) + \xi_2\left(\frac{z_N}{z_{max}}\right) + \xi_3\left(\frac{P_{e,\max}}{P_{e,N}}\right) \quad (5)$$

where $P_{e,N}$ denotes the bit-error rate (BER) at a receiving node N and $P_{e,\max}$ is the maximum BER of the nodes in $\mathcal{C}$; the function $f(|h_{ND}|, |h_{NE}|)$ indicates the security level; z_{max} is the maximum remaining energy of the nodes in $\mathcal{C}$, while z_N

978-1-4799-3088-3/14/$31.00 ©2014 IEEE

represents the remaining energy of node N. In addition, the weight coefficients $\sum_{i=1}^{3}\xi_i = 1$.

From (2) and (3), it is not difficult to derive that $SC_{RO} \propto |h_{RD}|/|h_{RE}|$ and $SC_{JO} \propto |h_{JE}|$. These results provide hints in the design of $f(|h_{ND}|, |h_{NE}|)$, so that we can derive the rewards $W_N^{(R)}$ for the relays in the relay set $\mathcal{R}_C$ and the rewards $W_N^{(J)}$ for the jammers in the jammer set $\mathcal{J}_C$. Here the detailed derivation is omitted due to the space limit. With the reward function, the prospective relay set $\mathcal{R}_C$ and the prospective jammer set $\mathcal{J}_C$ can be found to be $\mathcal{R}_C = \left\{N \in \mathcal{C},\ W_N^{(R)} > \rho_R\right\}$ and $\mathcal{J}_C = \left\{N \in \mathcal{C},\ W_N^{(J)} > \rho_J\right\}$, where ρ_R and ρ_J are two preset thresholds for guaranteeing the required system rewards, when the nodes are chosen as relays or jammers. Correspondingly, the candidate node set $\mathcal{N}_C$ is the union of $\mathcal{R}_C$ and $\mathcal{J}_C$, i.e., $\mathcal{N}_C = \mathcal{R}_C \bigcup \mathcal{J}_C$.

B. Selection of Cooperation Scheme

1) Jammer Only Selection: The JO mode is employed, when the capacity C_{SD} of the S-D channel is higher than the required channel capacity C_{req}, while the threshold of required SC, SC_{th}^{JO}, is below the maximum SC, expressed as $SC_{\lim}^{(1)}$. Here, $SC_{\lim}^{(1)}$ represents the capacity of the S-D channel when there is no interception.

2) Relay Only Selection: The RO mode is employed when $C_{SD} < C_{req}$ without the help of a relay. In this case, the threshold of required SC, SC_{th}^{RO}, should be up-bounded by the limit $SC_{\lim}^{(2)} \approx \log_2\left(\frac{|h_{RD}^{opt}|}{|h_{RE}^{opt}|}\right)$, which can be obtained from (3).

3) Relay-Jammer Pair Selection: The RJP mode is employed when neither JO nor RO alone can achieve the required SC. In this case, the threshold of required SC, SC_{th}^{RJP}, is up-bounded by $SC_{\lim}^{(3)}$ with the optimal power allocation.

C. Optimal Node Selection and Power Allocation

Under the general RJP mode, the optimal relay and jammer selection as well as the associated power allocation can be determined according to the optimization of

$$[(P_R^*, P_J^*); (R^*, J^*)] = \underset{R,J\in\mathcal{N}_C;P_R,P_J}{\arg\max} \frac{\left[(1-\varsigma)SC_{RJP} - SC_{th}^{RJP}\right]^+}{P_R + P_J} \quad (6)$$

subject to $C_{SD} \geq C_{req}$. In (6) ς denotes a correction factor, which is introduced for correcting the deviations caused by channel estimation errors and for reducing the outage probability of achieved SC.

In the JO (RO) mode, for optimal jammer (relay) selection and power allocation, in (6), we need to replace $\mathcal{N}_C$ using $\mathcal{J}_C$ ($\mathcal{R}_C$), to replace the subscript and superscript "RJP" by "JO" ("RO"), and to replace $P_R + P_J$ by P_J (P_R), respectively.

V. Performance Evaluation

In our simulations, data are transmitted in blocks. Each data block consists of two stages. Pilot frames are sent in stage 1 for CSI estimation and data frames are sent in stage 2.

Fig. 1 shows the network's lifetime versus the threshold of the percentage of exhausted nodes, Ex_{th}, which makes the network incapable of working properly. In our simulations, the optimal JO (OJO) mode is compared to the random jammer selection (RJS) approach. As shown in Fig. 1, the OJO approach has much longer lifetime than the RJS approach, especially when Ex_{th} takes a small value, owing to its capability of considering the remaining energy of the candidate nodes. In Fig. 2, we depict the SC performance, when the system is operated under the optimal JO (OJO) mode or the optimal RJP (ORJP) mode. As expected, the SC of both the OJO mode and the ORJP mode increases, as the transmit power of the jammer increases, and the cooperation schemes switching boundaries have also been marked.

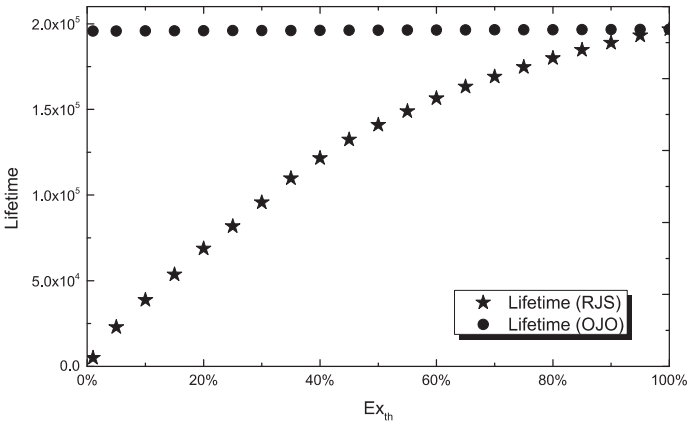

Fig. 1. The network lifetime versus the threshold of the percentage of exhausted nodes, Ex_{th}. Here the network's lifetime is denoted by the number of loops that our programme runs, and the results were obtained from the averages of 5000 realizations.

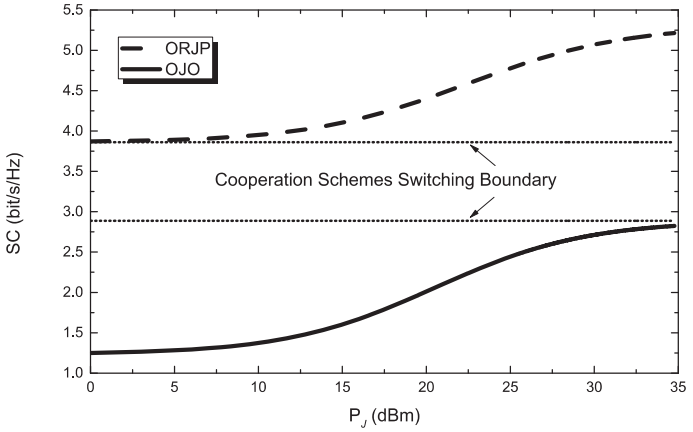

Fig. 2. Secrecy capacity performance of the OJO and ORJP modes versus the jamming power P_J.

References

[1] D. S. Michalopoulos, H. A. Suraweera, G. K. Karagiannidis, and R. Schober, "Amplify-and-forward relay selection with outdated channel estimates," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1278–1290, May 2012.

[2] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Selected Area Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.

[3] R. Negi and S. Goel, "Secret communication using artificial noise," in *2005 IEEE 62nd Vehicular Tech. Conf. (VTC-2005-Fall)*, Dallas, U.S.A., Sept. 2005, pp. 1906–1910.

[4] L. Dong, H. Yousefiźadeh, and H. Jafarkhani, "Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper," in *2011 IEEE Int'l Conf. Commun. (ICC)*, Kyoto, June 2011, pp. 1–5.

[5] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE Int'l. Symposium Info. Theory (ISIT 2006)*, Seattle, WA, July 2006, pp. 356–360.

[6] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *2009. SSP '09. IEEE/SP 15th Workshop on Statistical Signal Processing*, Cardiff, Sept. 2009, pp. 417–420.