Enforce Truth-Telling in Wireless Relay Networks for Secure Communication

Shuhang Liu*, Rongqing Zhang*, Lingyang Song*, Zhu Han†, and Bingli Jiao*
*School of Electronics Engineering and Computer Science, Peking University, Beijing, China.
†Electrical and Computer Engineering Department, University of Houston, Houston, TX, USA.

***Abstract*—To ensure security in data transmission is one of the most important issues for wireless relay networks. In this paper, we consider a cooperative network, consisting of one source node, one destination node, one eavesdropper node, and a number of relay nodes. Specifically, the source selects several relay nodes which can help forward the signal to the corresponding destination to achieve the best security performance. However, the relay nodes may have the incentive not to report their true private channel information in order to get more chance to be selected and gain more payoff from the source. We employ a self-enforcing truth-telling mechanism into the network to solve this cheating problem. By adding a transfer payoff to the total payoff of each selected relay node, we prove that each relay node would get its maximum expected payoff only when it tells the truth to the source. And then, an optimal secrecy capacity of the network can be achieved. Simulation results verify the efficiency of the proposed mechanism.**

I. Introduction

Security and privacy protection is one of the most important issues in wireless communications due to the broadcast nature of wireless channels. In recent years, besides traditional cryptographic mechanisms, information-theoretic-based physical layer security have been developing fast. The concept of wiretap channel was first introduced by Wyner [1], who showed that perfect secrecy of transmitted data from the source to the legitimate receiver is achievable in degraded broadcast channels. In follow-up work, Leung-Yan-Cheong and Hellman further investigated the secrecy capacity in the Gaussian wiretap channel [2]. Later, Csiszár and Körner extended Wyner's work to non-degraded broadcast channels and found an expression of secrecy capacity [3].

When considering a wireless relay network, the realization of secrecy capacity is much more complicated. In [4], [5], the authors demonstrated that cooperation among relay nodes can dramatically improve the physical layer security in a given wireless relay network. The channel state information (CSI) is assumed to be known at both the transmitter and the receiver in [6]. However, in practice, the relay node always measures its own channel gains and distributes the information to others through a control channel. There is no guarantee that it reveals its private information honestly. Hence, the most crucial problem is how to select efficient relay nodes to optimize the total secrecy rate in the network, while some selfish relay nodes may report false information to the source in order to increase their own utilities. In [7] truth-telling is assured by using the threat of punishment, and in [8], [9] reputation methods are designed to achieve this goal. However, all these methods need a delicate and complex detection scheme to monitor and catch the liar nodes, which is difficult to be realized because too much information needs to be exchanged.

With the help of game theory [10], [11] and its therein applications in wireless communications [12], [13], we propose a self-enforcing truth-telling mechanism to achieve the Bayesian Nash Equilibrium [14] and solve the possible cheating problem in relay networks. We focus on a system in which all the channels are orthogonal and each relay node's private channel information is unknown by others. After properly adding a transfer payoff function into the total payoff, each relay node would have no incentive to report false information which can lead to a loss in its own expected total payoff. We prove that the unique equilibrium is achieved on the condition that all the relay nodes report the truth. In other words, the competing relay nodes are enforced to obey the selection criterion and cooperate with each other honestly, and thus, no extra cost would be paid by the source since the total transfer payoff of all the relay nodes equals zero. Simulation results show that the relay nodes can get their maximum utilities when they all report their true channel information to the source and any cheating leads to a loss in the total secrecy rate of the system as well as the expected total payoff. We also observe that the more relays the source selects, the more expected total payoff each relay node can gain. In addition, we prove with simulations that the best strategy for each relay node is to improve its own physical channel condition to enlarge its secrecy rate and always report the truth to the source.

The remainder of this paper is organized as follows. In Section II, the system model for a relay network is described. In Section III, we propose a self-enforcing truth-telling mechanism to enforce relay nodes to reveal the true private information and prove that it is the unique equilibrium. Simulation results are shown in Section IV, and the conclusions are drawn in Section V.

II. System Model

Consider a cooperative network shown in Fig. 1, consisting of one source node, one destination node, one eavesdropper node, and I relay nodes, which are denoted by S, D, E, and R_i, $i = 1, 2, \ldots, I$, respectively. When the source node broadcasts a signal x, all the relay nodes in the network could receive it but only N $(N \leq I)$ nodes can decode this signal correctly due to their different geographical conditions. Then these N relay nodes report their own channel gains of both relay-destination and relay-eavesdropper links to the

978-1-4244-9920-5/11/$26.00 ©2011 IEEE

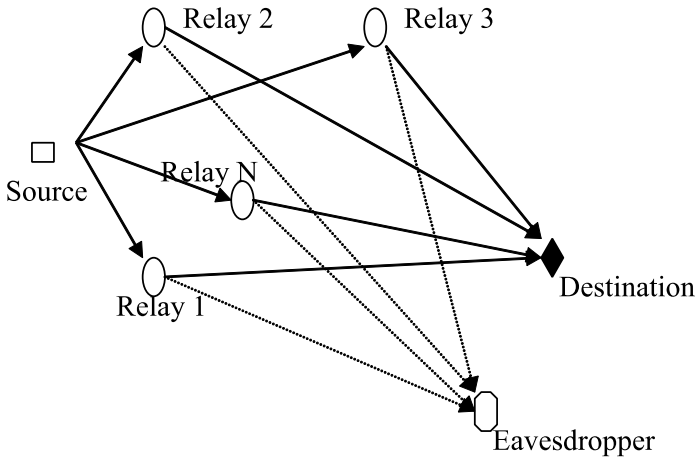

Fig. 1. System model for a relay network with one eavesdropper.

source node. We assume that all the channels in the network are orthogonal, and they have the same bandwidth, which is denoted by W. The source node wishes to gain the highest secrecy rate by properly selecting some efficient relay nodes based on their reported channel information. We denote the number of selected relay nodes by K $(K \leq N)$ and the set of K relay nodes by $\mathcal{K}$.

At the destination node the received signal from the i-th relay node $(R_i \in \mathcal{K})$ can be expressed as

$$y_{r_i,d} = \sqrt{P_{r_i}} h_{r_i,d} x + n_{r_i,d}, \tag{1}$$

and at the eavesdropper node the received signal can be expressed as

$$y_{r_i,e} = \sqrt{P_{r_i}} h_{r_i,e} x + n_{r_i,e}, \tag{2}$$

where P_{r_i} denotes the transmit power of relay node R_i under the power constraint $P_{r_i} \leq P_{max}$, $h_{r_i,d}$ is the channel gain between R_i and D, and $h_{r_i,e}$ is the channel gain between R_i and E. We assume that $h_{r_i,d}$ and $h_{r_i,e}$ contain both the path loss and the Rayleigh fading factor. Without loss of generality, we also assume that all the links have the same noise power which is denoted by σ^2. The decode-and-forward (DF) protocol is used for relaying.

The signal-to-noise-ratio (SNR) at the destination node is

$$\text{SNR}_{r_i,d} = \frac{P_{r_i} h_{r_i,d}^2}{\sigma^2}, \tag{3}$$

and the SNR at the eavesdropper node is

$$\text{SNR}_{r_i,e} = \frac{P_{r_i} h_{r_i,e}^2}{\sigma^2}. \tag{4}$$

The channel capacity for relay R_i to destination D is

$$C_{i,d} = W \log_2(1 + \text{SNR}_{r_i,d}). \tag{5}$$

Similarly, the channel capacity for relay R_i to eavesdropper E is

$$C_{i,e} = W \log_2(1 + \text{SNR}_{r_i,e}). \tag{6}$$

Then, the secrecy rate achieved by R_i can be defined as [15]

$$C_{i,s} = (C_{i,d} - C_{i,e})^+, \tag{7}$$

where $(x)^+ = \max\{x, 0\}$.

Therefore, the total secrecy rate achieved by the K selected relay nodes can be written as

$$C_s = \sum_{R_i \in \mathcal{K}} C_{i,s}. \tag{8}$$

III. Self-Enforcing Truth-Telling Mechanism

In this section, we propose a self-enforcing truth-telling mechanism to guarantee that each relay node reports its true information to the source during the process of relay selection. We define π as the price per unit of secrecy rate achieved by the relay node. The relay nodes in the network are assumed to be rational and fair-minded, which means that although they are selfish, none is malicious. The objective of the relay nodes is to maximize their own payoff under the payoff allocation scheme set by the source. The source selects K best relay nodes according to their reported channel information and the destination would calculate the payoff allocation of these relay nodes according to their real secrecy rate.

We assume that the channel gain is private information of each relay node, and thus, the source is unable to know whether the reported information is true or not. Since only the relay nodes selected by the source for secure data transmission could get the payoff, they may not report their true information to the source in order to win greater opportunity to be selected. In this condition, it may cause unfairness in selection and damage the expected payoff of those unselected. It also decreases the total secrecy rate of the system as well as the total payoff paid by the destination. It can be expressed as

$$\hat{C}_s \leq \tilde{C}_s, \tag{9}$$

and

$$\hat{D} \leq \tilde{D}, \tag{10}$$

where $\hat{C}_s$ and $\hat{D}$ represent the total secrecy rate and the total payoff calculated according to the information reported by the relay nodes, respectively, while $\tilde{C}_s$ and $\tilde{D}$ represent the total secrecy rate and the total payoff when all the relay nodes report the truth, respectively.

In the network, each relay node reports its own channel information $(h_{r_i,d}, h_{r_i,e})$ to the source. Assume

$$\left\{ \left(\tilde{h}_{r_1,d}, \tilde{h}_{r_1,e}\right), \left(\tilde{h}_{r_2,d}, \tilde{h}_{r_2,e}\right), \ldots, \left(\tilde{h}_{r_N,d}, \tilde{h}_{r_N,e}\right) \right\}$$

is a realization of channel gains at one time slot and the relay nodes report their information

$$\left\{ \left(\hat{h}_{r_1,d}, \hat{h}_{r_1,e}\right), \left(\hat{h}_{r_2,d}, \hat{h}_{r_2,e}\right), \ldots, \left(\hat{h}_{r_N,d}, \hat{h}_{r_N,e}\right) \right\}$$

to the source, which may not be the true information, but the source will make the selection based on it. Define R_i's private information as

$$g_i = \{h_{r_i,d}, h_{r_i,e}\}. \tag{11}$$

Due to the channel orthogonality, the payoff of R_i can be expressed as

$$D_i = \begin{cases} \pi C_{i,s}, & R_i \in \mathcal{K}, \\ 0, & \text{otherwise.} \end{cases} \tag{12}$$

The total payoff from the destination can be expressed as

$$D = \sum_{i=1}^{N} D_i. \tag{13}$$

Firstly, we prove that no equilibrium can be achieved under this situation.

Proposition 1: Assuming that R_i does not know other relays' secrecy rate, but knows that it obeys a certain probability density function defined as $p(\hat{C}_{j,s})$ $(0 \leq \hat{C}_{j,s} < \infty, j \neq i)$, then it has an incentive to exaggerate its $\hat{C}_{i,s}$ to ∞ to get the maximum expected total payoff.

Proof: R_i's expected payoff (12) can also be expressed as

$$D_i(\hat{g}_i) = \pi \tilde{C}_{i.s} P(R_i \in \mathcal{K}), \tag{14}$$

where $P(R_i \in \mathcal{K})$ represents the probability of $R_i \in \mathcal{K}$. Since $P(R_i \in \mathcal{K}) \propto \hat{C}_{i,s}$ and when $\hat{C}_{i,s} \to \infty$, $P(R_i \in \mathcal{K}) \to 1$, R_i gets its maximum payoff at infinity. This indicates that each relay node has an incentive to report false channel information, resulting in larger secrecy rate than reality, to the source, and thus, there is no equilibrium under this kind of payoff allocation. ■

To prevent relay nodes reporting distorted information, we can use either the reputation method or the threat of punishment [7]–[9]. However, it needs a delicate and complex detection scheme to catch the liar node. To this end, we propose a much easier and effective self-enforcing truth-telling mechanism to solve this problem. By using this mechanism, honest relay nodes gain the maximum payoff, as any cheating in the process would lead to a decrease in expected payoff.

We add another part of payoff, defined as the transfer payoff

$$t_i(\hat{g}_1, \hat{g}_2 \cdots \hat{g}_N) = \Phi_i(\hat{g}_i) - \frac{1}{N-1} \sum_{j=1, j\neq i}^{N} \Phi_j(\hat{g}_j) \tag{15}$$

to make the total payoff of R_i as

$$U_i(\hat{g}_i) = D_i(\hat{g}_i) + t_i(\hat{g}_1, \hat{g}_2 \cdots \hat{g}_N), \tag{16}$$

where

$$\Phi_i(\hat{g}_i) = \sum_{j=1, j\neq i}^{N} E[D_j(\hat{g}_i)] \tag{17}$$

represents the sum of the other relay nodes' expected payoff given the reported information $\hat{g}_i$.

We calculate the total transfer payoff and get

$$\begin{aligned} &\sum_{i=1}^{N} t_i(\hat{g}_1, \hat{g}_2 \cdots \hat{g}_N) \\ =&\sum_{i=1}^{N} \Phi_i(\hat{g}_i) - \frac{1}{N-1} \sum_{i=1}^{N} \sum_{j=1, j\neq i}^{N} \Phi_j(\hat{g}_j) \\ =&0. \end{aligned} \tag{18}$$

This implies that the proposed scheme can realize a payoff reallocation among the relay nodes, and no extra cost requires to be paid by the system.

If one relay node claims a higher $\hat{h}_{r_i,d}$ or a lower $\hat{h}_{r_i,e}$ than the reality to make its secrecy rate larger, it may get larger chance to be selected by the source, but also will pay a higher transfer payoff to those unselected. On the contrary, if one relay node reports a lower secrecy rate than reality it will receive the compensation from other relay nodes at the cost of smaller chance to be selected. By adding this transfer function, we can prove that only when the relay nodes report the true information of their channels, they can gain the largest expected payoff. There is only one equilibrium under this kind of payoff allocation.

Proposition 2: By using the transfer function (15) to balance the payoff allocation, relay node R_i can gain its largest expected total payoff when it reports its true private channel information:

$$\hat{g}_i = \tilde{g}_i(\hat{h}_{r_i,d} = \tilde{h}_{r_i,d}, \hat{h}_{r_i,e} = \tilde{h}_{r_i,e}). \tag{19}$$

Proof: Without loss of generality, we consider the total expected payoff of R_1. Since R_1 only knows its own channel information, its expected total payoff can be expressed as

$$\begin{aligned} E[U_1(\hat{g}_1)] =&E[D_1(\hat{g}_1) + t_1(\hat{g}_1, \hat{g}_2 \cdots \hat{g}_N)] \\ =&E[D_1(\hat{g}_1)] + E[\sum_{j=1, j\neq i}^{N} D_j(\hat{g}_1)] \\ &- \frac{1}{N-1} \sum_{j=1, j\neq i}^{N} \Phi_j(\hat{g}_j) \\ =&E[\sum_{i=1}^{N} D_i(\hat{g}_1)] - \frac{1}{N-1} \sum_{j=1, j\neq i}^{N} \Phi_j(\hat{g}_j). \end{aligned} \tag{20}$$

We can see that there are two terms in the right side of (20). The first one represents the total expected payoff paid by the destination when R_1 reports $\hat{g}_1$ as its channel information (The expectation is calculated by R_1 itself). Since the other term being independent of $\hat{g}_1$, only this one decides the expected total payoff of R_1. As we have discussed above, the total payoff paid by the destination is based on the real secrecy rate and the maximum payoff can be achieved when the best K relay nodes are selected by the source. That is to say, only when all the relay nodes tell the truth, the source can select the best K relay nodes and the destination pays the maximum payoff. Any cheating leads to a decrease in the relay nodes' total payoff, which means $\hat{D} \leq \tilde{D}$. Therefore, $E[U_1(\hat{g}_1)]$ could reach the maximum when R_1 reports its true channel information. Then, we can conclude that R_1 will report $\hat{g}_1 = \tilde{g}_1$ to maximize its own expected total payoff. Similarly, each relay node in the system has an incentive to report its true channel gain ($\hat{g}_i = \tilde{g}_i$) to the source. Thus, the unique equilibrium is achieved in this condition. ■

IV. Simulation Results

In this section, we provide simulation results of the proposed self-enforcing truth-telling mechanism. Specifically, to simplify the calculation and simulation, we assume that each relay node first calculates its own secrecy rate according to its channel information and then reports it to the source. Not considering the process of calculating $\pi C_{i,s}$, we give random values x_i to indicate $\pi C_{i,s} (i = 1, 2, \ldots, N)$, which

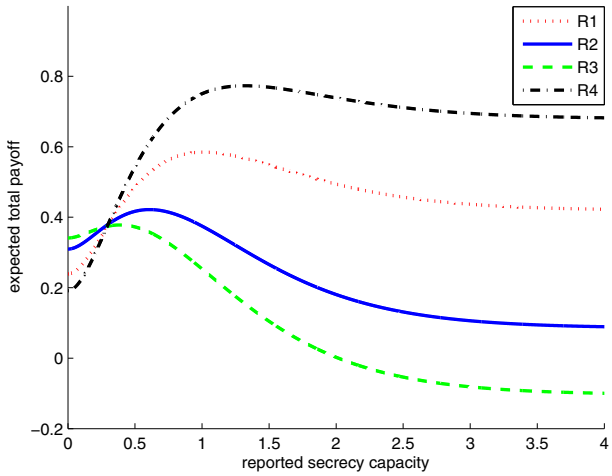

Fig. 2. Expected total payoff when different secrecy capacities are reported.

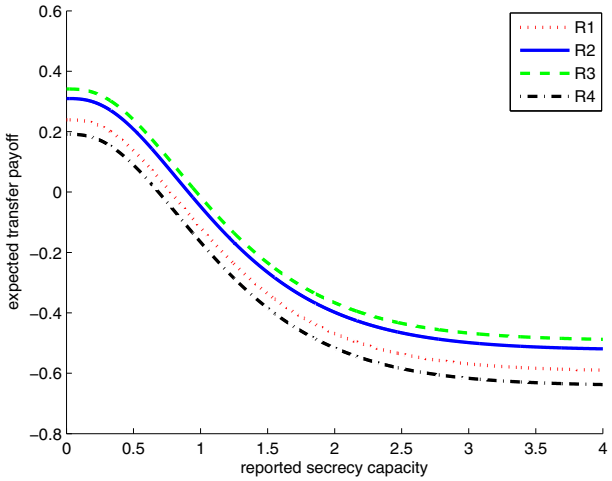

Fig. 3. Expected transfer payoff when different secrecy capacities are reported.

would not affect the source's selection result. Furthermore, we assume that though R_i does not know other relay nodes' channel information, it knows that each reported value obeys the probability density function: e^{-x_i} ($x_i \in [0, \infty)$ and $\int_0^{+\infty} e^{-x_i} dx_i = 1$).

Firstly, we consider a system with $N = 4$ relay nodes and from which the source chooses $K = 2$ relay nodes for data transmission. A random sample of these relay nodes' secrecy rate is obtained as $1.0132, 0.6091, 0.3885, 1.3210$ and the price per unit of secrecy rate $\pi = 1$ is assumed.

Fig. 2 shows the variation of R_i's expected total payoff when the reported values change. Given that the other three nodes are honest, $R_i (i = 1, 2, 3, 4)$ could get its maximum total payoff when reporting the truth. From Fig. 2 we can observe that when they all tell the truth, the larger the true value of secrecy rate one relay node has, the more the expected total payoff it gains. For example, R_4 has the largest secrecy rate ($\tilde{C}_{4,s} = 1.3210$) and its expected total payoff is the largest and up to 0.7732 when it reports the true value. It is higher than the other three relay nodes' payoff even though it is not as much as $\pi C_{4,s} = 1.3210$, which is paid by the destination.

Fig. 3 shows the expected transfer payoff of R_1, R_2, R_3, and R_4. They are all monotone decreasing because the larger the reported value is, the more transfer payoff should be paid to others. From Fig. 3 we also find that R_1's and R_4's transfer payoffs are negative while the other two's are positive when they tell the truth. This is because R_1 and R_4 are actually selected by the source and get payoff from the destination while R_2 and R_3 are not. By using the self-enforcing truth-telling mechanism, the relay nodes which have smaller secrecy rate will get compensations from those which have larger ones. It can balance the payoff allocation of the system and benefit those in worse channel conditions. Furthermore, we calculate the expected transfer payoff of R_i when they all report the truth: $t_1 = -0.1247, t_2 = 0.1570, t_3 = 0.2831, t_4 = -0.3154$ and $t_1 + t_2 + t_3 + t_4 = 0$, which is in accord with (18):

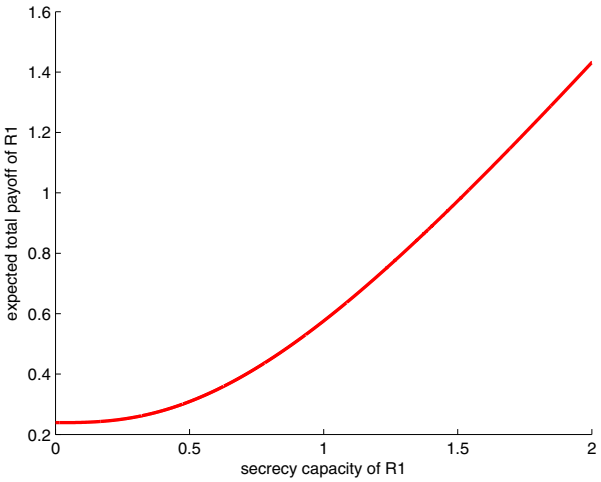

Fig. 4. Expected total payoff of R_1.

$$\sum_{i=1}^{N} t_i(\hat{g}_1, \hat{g}_2 \cdots \hat{g}_N) = \sum_{i=1}^{N} \Phi_i(\hat{g}_i) - \frac{1}{N-1} \sum_{i=1}^{N} \sum_{j=1, j\neq i}^{j=N} \Phi_j(\hat{g}_j) = 0.$$

Secondly, we consider that when R_1 enlarges its real secrecy rate by some methods, while R_2, R_3, and R_4 hold the same value as we have assumed above. From Fig. 4 we can see that when R_1's real secrecy rate increases, the total payoff it could get will increase at the same time. As the value of $C_{1,s}$ changes from 0 to 2, the total payoff changes from 0.2391 to 1.4316. Therefore, R_1 has a strong inclination to increase its own real secrecy rate even though it has to pay more transfer payoff to other relay nodes then.

Lastly, we focus on the effect of the value K on the expected total payoff. From Fig. 5 we can observe that when the value K increases, the expected total payoff of R_1 also increases. The larger K is, the lower the decline rate of the expected total payoff becomes, which makes the curves smoother. Considering the transfer payoff of R_1 shown in Fig. 6, we find that when K is smaller ($K = 1$), the transfer

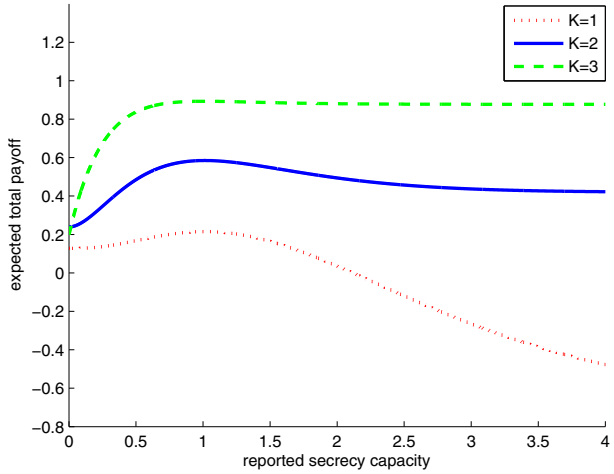

Fig. 5. Expected total payoff of R_1 at different K.

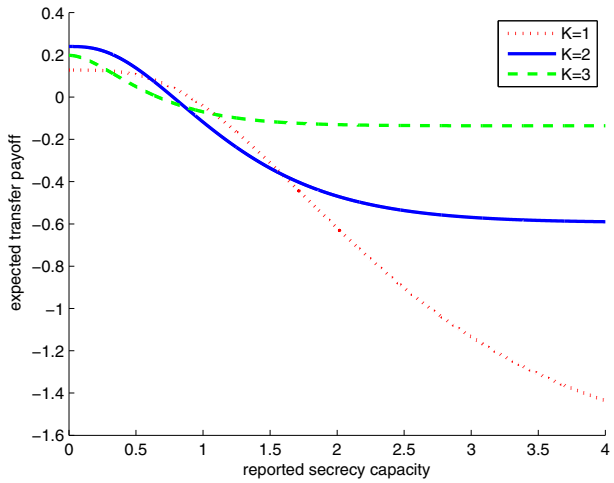

Fig. 6. Expected transfer payoff of R_1 at different K.

payoff decreases faster and gets a larger negative value quickly. This explains why R_1's expected total payoff decreases faster when K decreases. So if the source increases the number of relays which are selected to forward signals, all the relay nodes in the system could gain larger utilities.

V. Conclusions

In this paper, we have proposed a self-enforcing truth-telling mechanism to guarantee that each relay node tells the truth during the process of relay selection taking secure data transmission into consideration. By adding a transfer payoff we found that each relay node gets its maximum utility only when it reports its true channel information, and any deviation from the truth will lead to a loss in its own expected total payoff as well as the total secrecy rate of the network. Simulation results verify that the relay nodes have no incentive to report false information after adding the transfer payoff. We also observed that increasing the number of relay nodes selected by the source and increasing one relay node's real secrecy rate are two ways to increase the expected total payoff, which also indicates that trying to improve one's own condition but not cheating the source is able to get more payoff.

Acknowledgment

This work was partially supported by the US NSF CNS-0953377, CNS-0905556, and CNS-0910461, and also by the National Nature Science Foundation of China under grant number 60972009 and 61061130561, as well as the National Science and Technology Major Project of China under grant number 2009ZX03003-011, 2010ZX03003-003, 2010ZX03005-003, and 2011ZX03005-002.

References

[1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jul. 1975.

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

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] N. Marina, R. Bose, and A. Hjørungnes, "Increasing the secrecy capacity by cooperation in wireless networks," in *Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Sep. 2009.

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

[6] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels" *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 2470–2492, Sep. 2009.

[7] R. Etkin, A. Parekh, and D. Tse, "Spectrum sharing for unlicensed bands," *IEEE Journal on selected areas in communications*, vol. 25, no. 3, pp. 517–528, Apr. 2007.

[8] A. Josang and R. Ismail, "The beta reputation system," in *Proc. Bled Electronic Commerce Conference e-Reality: Constructing the e-Economy*, Bled, Slovenia, Jun. 2002.

[9] Y. Rebahi, V. E. Mujica-V and D. Sisalem, "A reputation-based trust mechanism for ad-hoc networks," in *Proc. IEEE Symposium on Computers and Communications*, Jun. 2005.

[10] D. Fudenburg and J. Tirole, *Game Theory*, MA: MIT Press, 1993.

[11] Z. Han, D. Niyato, W. Saad, T. Basar, and A. Hjørungnes, *Game Theory in Wireless and Communication Networks: Theory, Models and Applications*, in print, Cambridge University Press, UK, 2011.

[12] A. B. MacKenzie and S. B. Wicker, "Game theory in communications: Motivation, explanation, and application to power control," in *Proc. IEEE Global Telecommunications Conference*, Nov. 2001.

[13] J. Neel, A. B. Mackenzie, R. Menon, L. A. Dasilva, J. E. Hicks, J. H. Reed, and R. P. Gilles, "Using game theory to analyze wireless ad-hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 7, no. 4, pp. 46–56, Apr. 2005.

[14] E. Dekel, D. Fudenberg, and D. K. Levine, "Learning to play Bayesian games," *Games and Economic Behavior*, vol. 46, pp. 282–303, Feb. 2004.

[15] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE International Symposium in Information Theory*, Jul. 2006.