ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

To Enhance Secrecy in Two Way Relay Network by Selecting Relay/Jamming Node Intelligently

Ganesh V. Kadam, Varsha Dahatonde

Head Of Department, Information Technology,Vishwabharati Academy's College Of Engineering, Pune University, Ahmednagar,Maharashtra, India.

Student, G.H. Raisoni College of Engineering andManagement, Ahmednagar, Maharashtra, India.

Abstract:It set up the utility of user support in assisting secure wireless communications against the malicious eavesdropper. In this paper, we consider joint relay and jammer selection in two-way cooperative networks. It mainly consisting of two sources, one is eavesdropper in communication channel for disturbing communication, and a number of intermediate nodes. These intermediate nodes having some constraints for secrecy about data.

While Conventional cryptography based approaches focus on hiding the meaning of the information being communicated from the eavesdropper, we consider a complimentary class of strategies that limit knowledge of the existence of the information from the eavesdropper.

We are selecting few intermediate nodes for our utility in which one of them operates in conventional relay mode which assist to another nodes for communicating with each other. The proposed scheme enables an opportunistic selection of few relay nodes to increase security against eavesdroppers in which first relay operates as a conventional mode and it assists to other nodes to deliver its data to a destination via Amplify-and-Forward strategy.

Three cooperative schemes we have considered here: decode-and-forward (DF), amplify-and-forward (AF), and cooperative jamming (CJ) for developing our utility.

The new approach is analysed for different complexity requirements based on instantaneous and average knowledge of the eavesdropper channels. In addition an investigation of an hybrid security scheme which switches between jamming and non-jamming protection is discussed in the paper. We find that in a scenario where the relay and jamming nodes are randomly and sparsely distributed, the proposed schemes with cooperative jamming outperform the conventional non-jamming schemes within a certain transmitted power range. We also find that, in a scenario where the intermediate nodes gather as a close cluster, the cooperative jamming schemes may be less effective than their non-jamming counterparts. Therefore, we introduce a hybrid scheme to switch between jamming and non-jamming modes.

Keywords: amplify-and-forward (AF), decode-and-forward (DF),and cooperative jamming (CJ)

I.INTRODUCTION

The broadcasting environment of wireless communicating channels, the problems of security and privacy have taken on an important role in wireless networks. To enable the genuine destination to effectively obtain source information, while the eavesdroppers (wire-tappers) are not able to interpret this information, we have to provide more security to the wireless communication.

Today wireless communication networks are widely used due to different applications is required that the data transmitted should be secure. So at the physical layer, we have to give more security for avoiding eavesdropper from decoding any message exchanged by legitimate user.

At the physical layer, the influential works by Wyner [7] and shortly afterwards by Csiszär and Körner [8] showed that by using channel codes and signal processing, secure communication is in fact possible without using key encryption in the presence of the eavesdropper.

Traditionally Information privacy in wireless networks takes place by using cryptography secure protocols at higher layer[1]. So it welcomes more attacks as the implementation of secrecy at higher layers, there has been a growing of interest in implementing security at the physical (PHY) layer as well [2]-[6].

Pioneered by Aaron Wyner's work [9], which established fundamental results of creating perfectly secure communications without relying on private keys, physical layer based security has drawn increasing attention recently. Later work in [10]– [12] studied the secrecy capacity of the Gaussian wiretap channel, and extended Wyner's approach to the transmission of confidential messages over the broadcast and wireless fading channels. In [13]–[15], several cooperative jamming schemes were investigated for different scenarios to increase the secrecy capacity of networks with secrecy constraints.

Recently, two-way relay channel [16]–[18] has been well studied for its potential application to cellular networks and peer-to-peer networks. In a cooperative network, the efficiency of relay or jammer selection has a great impact on the performance of the whole system.

In [19], a relay selection scheme was proposed for two-way networks with multiple relays, which maximized the worse receive signal-to-noise ratio (SNR) of the two sources. In [20], several relay selection techniques were proposed in one-way cooperative networks with secrecy constraints. Although cooperative networks have received much attention by far, the physical layer security issues with secrecy constraints in two-way relay networks have not yet been well investigated.

This paper proposes a scheme which can implement information exchange against eavesdroppers in two-way cooperative networks, consisting of two sources, one eavesdropper, and a number of intermediate nodes, with secrecy constraints.

Specifically, an intermediate node is selected to operate in the conventional amplify-and-forward (AF) relay mode and assists the sources to deliver data to the corresponding destinations.

Meanwhile, another two intermediate nodes that perform as jamming nodes are selected and transmit artificial interference in order to degrade the eavesdropper links in the first and second phase of data transmission, respectively. Selection of the relay and the jamming nodes in order to provide more information security and protect the source message against eavesdroppers which is major issue. Several selection algorithms are then proposed, aiming at promoting the assistance to the sources and the interference to the eavesdropper. The proposed techniques with cooperative jamming can improve the secrecy rate of the system by a large scale within a certain transmitted power range. However, in some special scenarios, the proposed jamming schemes are less efficient than the non-jamming ones. Then we propose a hybrid scheme with intelligent switch mechanism between the jamming and non-jamming modes, which can overcome this problem.

The rest of this paper is organized as follows. In Section II we describe the system model and formulate the problem. In on III the selection techniques are presented. In Section IV, we provide qualitative analysis of the secrecy performance of different selection schemes in some typical configurations. Numerical results are shown in Section V, and the main conclusions are drawn in Section VI.

II. Literature Survey

The term refers to any kind of networking that does not involve cables. It is a technique that helps entrepreneurs and telecommunications networks to save the cost of cables for networking in specific premises in their installations. The transmission system is usually implemented and administrated via radio waves where the implementation takes place at physical level.

In [22], the scenario where multiple users communicate with a common receiver (i.e., multiple access) in the presence of an eavesdropper is considered, and the optimal transmit power allocation policy is chosen to maximize the secrecy sum-rate. A user that is prevented from transmitting basedon the obtained power allocation can help increase the secrecy rate for other users by transmitting artificial noise to the eavesdropper.

DF and AF cooperative schemes for improving transmission rate in the absence of an eavesdropper were studied in [23][24]. Cooperative schemes for improving communications in the presence of an eavesdropper can be grouped into three categories. In the first category, a relay plays a dual role, i.e., it acts as both a helper and an eavesdropper; in the second one, a relay helps the eavesdropper; in the third one, a relay or a helper helps the source-destination transmission.

In [25], a four-node system model is considered, (i.e., source, destination, eavesdropper and relay) in which the relay transmits a noise signal that is independent of the source signals in order to jam the eavesdropper. The rate-equivocation region is derived to show gains and applicable scenarios for cooperation. Since message secrecy is difficult to maintain.

In [26], inner and outer bounds on the rate-equivocation region are derived for the four-node model for both discrete memoryless and Gaussian channels. In [27], the secrecy rate of orthogonal relay eavesdropper channels is studied. In that scenario, relay and destination receive the source signals on two orthogonal channels, the destination also receives transmissions from the relay on its channel, and the eavesdropper overhears either one or both of the orthogonal channels. Secrecy rate maximization subject to a power constraint or power minimization subject to a secrecy rate restriction, and the obtained results is difficult.

Since we are contributing in this paper in terms of following aspects: i) The system models are different. Existing work has focused primarily on the case of one relay and one eavesdropper, while in this work the more general case of multiple relays and multiple eavesdroppers is considered and ii) The problems to be addressed are different. Existing work has focused primarily on the analysis of secrecy rate and the rate-achieving relaying strategy. In this paper, for each predefined cooperative scheme, we consider system design (relay weight design and power allocation)for secrecy rate maximization subject to a power constraint or power minimization subject to a secrecy rate constraint, and the obtained results are novel.

III.SYSTEM MODEL

Existing System:

In Existing System, we use one way co-operative network transmission. The nodes to be operate in the conventional relay mode and a number of intermediate nodes to be transmitted the signal, sometimes eavesdropper could be crash the transmission to hack the file.

Disadvantages:

1. Low Network Capacity.
2. Malicious Eaves Dropper

Proposed System:

In proposed system, we use two-way cooperative network transmission. A number of intermediate nodes with secrecy constraints transfer the files with enhance security against the malicious eavesdropper and to exchange the data with the amplify-and-forward protocol. In cellular network, and peer-to-peer network efficiency performance of the whole system. In a relay selection scheme was proposed for two-way networks with multiple relays, which maximized the worse receive signal-to-noise ratio (SNR) of the two sources.

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

Theoretical Foundation System Model:

We consider a distributed wireless network configuration as depicted in Fig. 1, with source, destination, eavesdropper and few relays. Here we represent different channels between the source and the eavesdropper, source and the destination, destination and the eavesdropper, the source and the relay, the relay and the eavesdropper, the relay and the destination etc. The eavesdropper is assumed to be passive, i.e., it listens only.

We assume a simple configuration consisting of two sources S1 and S2, one eavesdropper E and an intermediate node set Sin = {1, 2, ...,K} with K nodes and few relays nodes. As the intermediate nodes cannot transmit and receive simultaneously, the communication process is executed in two stages. In the broadcasting stage, S1 and S2 transmit their data to the intermediate nodes i.e. middle node. Meanwhile, one node J1 is selected from Sin to operate as a jammer and transmits intentional interference to corrupt the source-eavesdropper links in this phase. Since the jamming signal is unknown to the rest nodes in Sin, the interference will also corrupt the performance of the source-relay links, as shown in Figure 1. In the second stage, an intermediate node R is selected to operate as a conventional relay and forwards the source messages to the corresponding destinations. A second jammer J2 is selected from Sin, for the same reason as J1. Notice that S1 and S2 are not able to mitigate the artificial interference from the jammer, either [21].

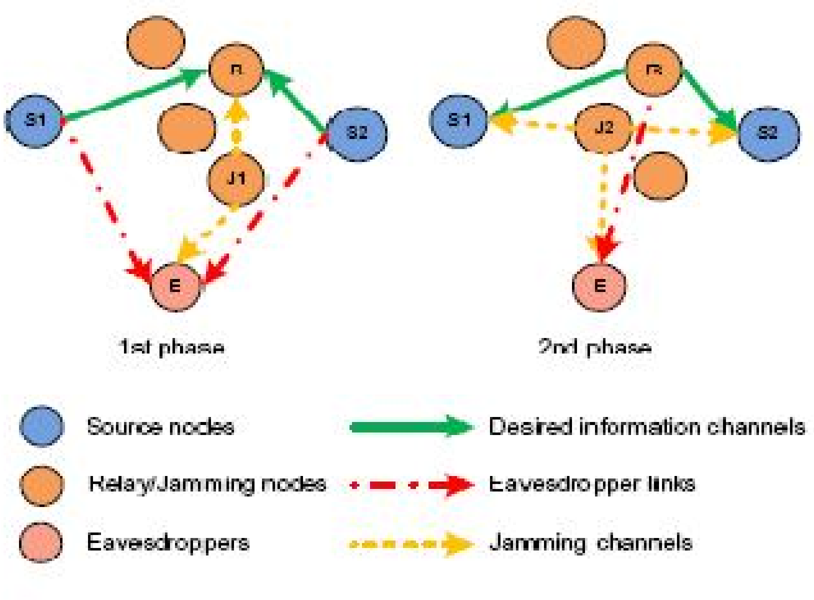

Fig. 1. System model for two-way cooperative network.

IV.IMPLEMENTATION DETAILS

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Following steps are included in our algorithm for sending file from source to destination with higher secrecy.

Step1. When source wants to transfer file to destination, enter system IP Address.
Step2. Select file which has to transfer.
Step3. Send it towards destination.
Step4. Client waiting for download the file and select the receiving path to download the file.
Step5. File transfer at that time jammer occur same time eavesdropper hack the file in two way transmission.
Step6. Security against malicious attack activates and transfer file via another path.
Step7. File received successfully.

Modules Description:

i. Two Ways Co-Operative network
ii. Conventional selection without jamming
iii. Optimal Switching
iv. Optimal Switching with jamming
v. Simulation Results

i. Two ways Co-Operative Network:

In this module, we can implement information exchange against eavesdroppers in two-way cooperative networks, consisting of two sources, one eavesdropper, and a number of intermediate nodes, with secrecy constraints.

Specifically, an intermediate node is selected to operate in the conventional amplify-and-forward (AF) relay mode and assists the sources to deliver data to the corresponding destinations.

Meanwhile, another two intermediate nodes that perform as jamming nodes are selected and transmit artificial interference in order to degrade the eavesdropper links in the first and second phase of data transmission, respectively.

ii. Conventional selection without jamming:

In this module, in a conventional cooperative network, the relay scheme does not have a jamming process. The conventional selection does not take the eavesdropper channels into account and the relay node is selected according to the instantaneous signal – to- noise ratio (SNR) of the links between Source 1 to Source 2.

iii. Optimal Switching:

In this module, the original idea of using jamming nodes is to introduce interference on the eavesdropper links. However, it simultaneously degrades the links between the relay R and the destinations. In some specific situation is close to one destination, continuous jamming may decreases secrecy seriously, and acts as a bottleneck for the system. In order to overcome this problem, we introduce the idea of intelligent switching between

iv. Optimal Switching with jamming:

In this module, the optimal selection with jamming assumes knowledge set and ensures a maximization of the sum of instantaneous to define as the overall signal -to- interference-and-noise-ratio (SINR) of the channel. The overall secrecy performance of the system is characterized by the ergodic secrecy rate that is the expectation of the sum of the two sources' secrecy rate for different types of channel feedback.

v. Simulation Results:

The intermediate nodes spread randomly within the square space. It is clear that selection with jamming outperform their non-jamming counterparts within a certain transmitted power range. Outside this range the secrecy rate of OSJ converges to a power-independent value. Whereas the ergodic secrecy rate of OS continues to grow with a slope. This validates the analysis the suboptimal scheme SSJ performs almost the same as the optimal scheme OSJ. Furthermore, it can be seen from that OW provides better performance than any other selection techniques with or without continuous jamming. Within this configuration, we also compare the performance of different selection techniques measured by secrecy outage probability.

We can see the different kind of functionality by using case diagram of our proposed system:

So it shows, intermediate node is selected to operate in the conventional amplify-and-forward (AF) relay mode and assists the sources to deliver data to the corresponding destinations.

Meanwhile, another two intermediate nodes that perform as jamming nodes are selected and transmit artificial interference in order to degrade the eavesdropper links in the first and second phase of data transmission, respectively. The conventional selection does not take the eavesdropper channels into account and the relay node is selected according to the instantaneous signal – to- noise ratio (SNR). Therefore the proposed hybrid scheme which switches intelligently between jamming and non-jamming modes is efficient in providing the highest secrecy rate in almost the whole transmitted power regime in two-way cooperative networks.

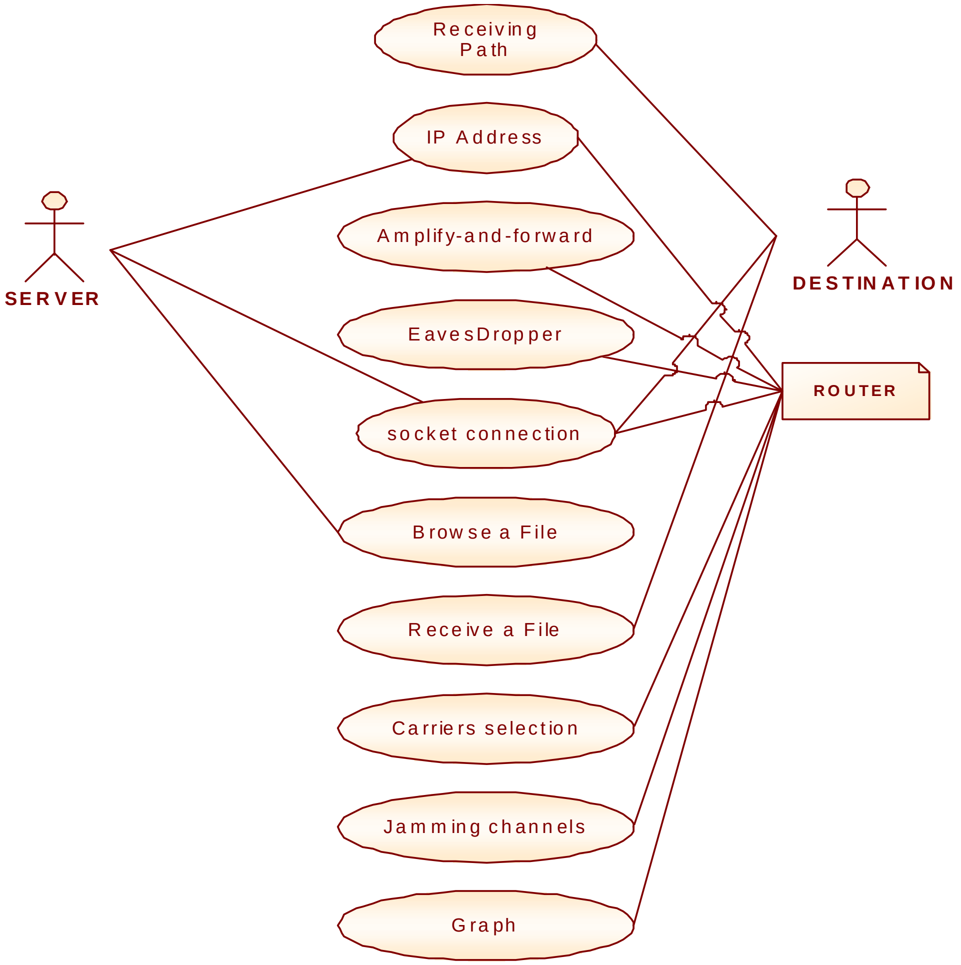

Fig. 2. Use Case Diagram.

V. Conclusion

Security is one of the major issues in MANETs. Their natural characteristics make them vulnerable to passive and active attacks, in which misbehaving nodes can eavesdrop or delete packets, modify packet contents, or impersonate other nodes. It is widely acknowledged that public key cryptographic mechanisms can provide some of the strongest techniques against most vulnerability.

These mechanisms use public/private key pairs to encrypt and decrypt messages. However, the use of traditional public key cryptography over MANETs can cause severe computational, memory, and energy overhead. The proposed hybrid scheme which switches intelligently between jamming and non-jamming modes is efficient in providing the highest secrecy rate in almost the whole transmitted power regime in two-way cooperative networks.

This correspondence has studied the Cooperative Jamming via distributed relays to increase the physical layer security. The conditions for positive secrecy rate have been derived and we have shown that the optimal Cooperative Jamming solution can be obtained by secure Two-Way Relay Networks by Joint Relay and Jammer Selection so it is efficient in providing the highest secrecy rate in almost the whole transmitted power regime in two-way cooperative networks.

REFERENCES

[1] E. D. Silva, A. L. D. Santos, L. C. P. Albini, and M. Lima, "Identitybased key management in mobile ad hoc networks: techniques and applications," IEEE Wireless Commun., vol. 15, pp. 46-52, Oct. 2008.
[2] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, pp. 1355-1387, Jan. 1975.
[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," IEEE Trans. Inform. Theory, vol. 24, pp. 451-456, July 1978.
[4] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," IEEE Trans. Inform. Theory, vol. 54, pp. 2493-2507, June 2008.
[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," IEEE Trans. Inform. Theory, vol. 54, pp. 2515-2534, June 2008.
[6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in Proc. IEEE Int. Symp. Inf. Theory, Seattle, USA, pp. 356-360, July 2006.
[7] A. D.Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, 1975.
[8] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.
[9] A. D. Wyner, "The wire-tap channel," Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[10] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," IEEE Transactions on Information Theory, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[11] I. Csisz´ar and J. K¨orner, "Broadcast channels with confidential messages," IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 339–348, May 1978.
[12] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in Proceedings of IEEE International Symposium on Information Theory, Adelaide, Australia, Sep. 2005.
[13] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," IEEE Transactions on Information Theory, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
[14] 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.
[15] Jingge Zhu, Jianhua Mo, and Meixia Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," IEEE Communications Letters, vol. 14, no. 10, pp. 885–887, Oct. 2010.
[16] B. Rankov and A. Wittneben, "Achievable rate regions for the twoway relay channel," in Proceedings of IEEE International Symposium on Information Theory, Seattle, USA, Jul. 2006.
[17] B. Rankov and A. Wittneben, "Spectral efficient protocols for half-duplex fading relay channels," IEEE Journal on Selected Areas in Communications, vol. 25, no. 2, pp. 379–389, Feb. 2007.
[18] Lingyang Song, Yonghui Li, Anpeng Huang, Bingli Jiao, and A. V. Vasilakos, "Differential modulation for bidirectional relaying with analog network coding," IEEE Transactions on Signal Processing, vol. 58, no. 7, pp. 3933–3938, Jul. 2010.
[19] Yindi Jing,"A relay selection scheme for two-way amplify-and-forward relay networks," in Proceedings of International Conference on Wireless Communications & Signal Processing, Nov. 2009.
[20] I. Krikidis, J. Thompson, and S. Mclaughlin,"Relay selection for secure cooperative networks with jamming," IEEE Transactions on Wireless Communications, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.
[21] Jingchao Chen, Rongqing Zhang, Lingyang Song, Zhu Han, Bingli Jiao "Joint Relay and Jammer Selection for SecureTwo-Way Relay Networks" IEEE ICC 2011.
[22] E. Tekin and A. Yener, "The general Gaussian multiple access andtwo-way wire-tap channels: Achievable rates and cooperative jamming,"IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2735–2751, Jun.
2008.
[23] J. N. Laneman, D. N. C. Tse, and G. W.Wornell, "Cooperative diversityin wireless networks: Efficient protocols and outage behavior," IEEETrans. Inf. Theory, vol. 50, pp. 3062–3080, Dec. 2004.
[24] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity Part I: System description," IEEE Trans. Commun., vol. 51, no.11, pp. 1927–1938, Nov. 2003.
[25] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperationfor secrecy," IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005–4019,Sep. 2008.
[26] M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," inProc. 41st Annu. Conf. Inf. Sci. Syst., Baltimore, MD, Mar. 2007.
[27] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, "Secrecycapacity of a class of orthogonal relay eavesdropper channels,"EURASIP J. Wireless Commun. Netw., vol. 2009, 2009, Article ID494696, 14 pp.