



## ASSORTMENT OF JAMMERS FOR SHELTERED TWO-WAY COMPLEX

S.M.Kulkarni<sup>1</sup>, S.A.Khaliq<sup>2</sup>, S.Srilakshmi<sup>3</sup>

<sup>1</sup>M.Tech Student, Dept of CSE, Al-Habeeb College of Engineering and Technology, Chevella (M),  
R.R Dist, A.P, India

<sup>2</sup>Associate Professor, Dept of CSE, Al-Habeeb College of Engineering and Technology, Chevella (M),  
R.R Dist, A.P, India

<sup>3</sup>Associate Professor, Dept of CSE, Al-Habeeb College of Engineering and Technology, Chevella (M),  
R.R Dist, A.P, India

### ABSTRACT:

In a cooperative network, the efficiency of relay or jammer selection has a great impact on the performance of the entire system. Even though cooperative networks enclosed much concentration by far, the security issues of physical layer with confidentiality constraints in two-way relay networks have not so far been well examined. Two-way relay channel in the recent times has been well considered for its possible application to cellular networks and networks of peer-to-peer. Numerous algorithms of selection are then proposed, intending at promoting the support to the sources and the intrusion to the eavesdropper. Two to three intermediate nodes were selected in the proposed system for improving security against the hateful eavesdropper. Selection of the first node makes it to operate in the conservative transmit mode and makes the other two sources for exchanging data connecting each other in the protocol of amplify-and-forward. A hybrid system was introduced for switching between jamming and non-jamming modes for a situation where the intermediate nodes gets together as a close cluster and the cooperative jamming systems will be less effectual than their equivalents of non-jamming. The hybrid system switches smartly between jamming and non-jamming modes and is well-organized for providing the high privacy rate in the entire transmitted power organization in networks of two-way cooperative networks.

*Keywords: Cooperative Networks, Jamming Modes, Hybrid System, Physical layer.*

## 1. INTRODUCTION:

Even though supportive networks have established much consideration by distant, the physical layer security issues with secrecy constraints in two-way transmit networks have not been found out. In a cooperative network, the efficiency of relay or jammer selection has a great impact on the performance of the entire system [4]. A transmit selection scheme was proposed intended for networks of two-way by means of multiple transmits that make the most of the worse receiving signal-to-noise ratio of the two sources. Many transmit selection techniques were proposed in one-way cooperative networks with confidentiality restrictions. Numerous algorithms of selection are then proposed, intending at promoting the support to the sources and the intrusion to the eavesdropper [8]. Two-way relay channel in the recent times has been well considered for its possible application to cellular networks and networks of peer-to-peer. An intermediate node is selected principally for operating in the conventional amplify-and-forward transmit mode and assists the sources to allocate the data to the equal destinations [1]. The examination and results of simulation expose the proposed techniques by means of cooperative

jamming which can get better the rate of secrecy of the system by means of a large scale within a convinced transmitted power range. For the time being, other two intermediate nodes which perform as jamming nodes are selected for transmitting simulated interference in turn for degrading the eavesdropper links in the initial and subsequent phase of data transmission [11]. The unique idea of using jamming nodes is for introduction of interference on the eavesdropper links is the purpose of using jamming nodes. The node of selected relay helps to improve the information transmission connecting the two sources by means of strategy of an amplify-and-forward, whereas the jamming nodes are used in the direction of creating intended interference at the eavesdropper [3].

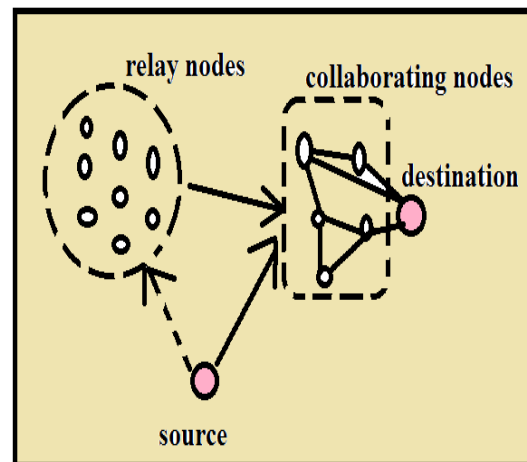


Fig 1: An overview of cooperative network system.

## 2. METHODOLOGY:

A simple design containing two sources  $U_1$  and  $U_2$ , one eavesdropper  $D$  and an intermediate node set  $U_{in} = \{1, 2, \dots, M\}$  with  $M$  nodes was assumed in the representation of system. In the propagation phase,  $U_1$  and  $U_2$  transmit their data to the intermediate nodes. For the meantime, one node  $E_1$  is selected from  $S_{in}$  to function as a jammer and transmits intended interference for degrading the source-eaves dropper links [9]. The contact process is performed in two phases as the intermediate nodes cannot pass on and receive at the same time. The interference will degrade the presentation of the source-relay links, because the jamming signal is unknown to the rest nodes in  $U_{in}$  [8] [10]. In the second phase, an intermediate node  $I$  is selected to function as a conservative relay and ahead the source communication to the corresponding destinations [7]. Throughout the two phases, a slow, plane and block Rayleigh fading atmosphere is recognized, the channel remains stationary for one consistency interval and changes separately in dissimilar coherence intervals with a variance  $\sigma^2$ .

**Selection Techniques without Jamming:** In a conservative cooperative network, the relay systems do not have a

jamming method. For the same reason as  $E_1$  a second jammer  $E_2$  is selected from  $U_{in}$ . Observe that  $U_1$  and  $U_2$  are not capable to mitigate the artificial interference from the jammer, moreover. We have the following solutions

**Conventional Selection:** The conventional selection do not take the eavesdropper channels into consideration and selects the relay node according to the immediate signal-to-noise ratio of the links between  $U_1$  and  $U_2$  [2].

**Optimal Selection:** This solution takes into account the relay-eavesdropper links were taken into account by the solution and decides the relay node according to the knowledge set [11] [15].

**Optimal Selection with Jamming:** The most excellent potential assortment with jamming imagines knowledge set  $\psi_0$  and ensures a maximized summation of immediate privacy rate of node  $U_1$  and node  $U_2$ .

**Optimal Switching:** The unique idea of using jamming nodes is for introduction of interference on the eavesdropper links is the purpose of using jamming nodes [5] [12]. On the other hand, it degrades the links between the relay  $I$  and the destinations at the same time. In some detailed circumstances constant jamming will decrease privacy critically and acts as a blockage for the system [12]. The scheme of

hybrid which switches sharply connecting modes of jamming and non-jamming is competent in providing the uppermost rate of secrecy in almost the entire transmitted power administration in networks of two-way cooperative system [10]. Selection of suboptimal with Jamming: we can get some best possible selection metrics on the basis of the theory of  $\psi_0$ . On the other hand, only a standard knowledge of these links  $\psi_1$  can be obtainable. A system was proposed for applying information replacing in opposition to eavesdroppers in two-way cooperative networks, containing two sources such as one eavesdropper in addition to a number of intermediate nodes, through confidentiality limitations [13]. A two-way transmit channel was well studied for their possible application to cellular networks where the efficiency of transmit or jammer selection has a strong impact on the presentation of the system in a cooperative network shown in fig1 containing two sources one eavesdropper, and many intermediate nodes with privacy constraints. Numerous selection algorithms were proposed, for promoting the support to the interference to the eavesdropper and increasing the information security and protect the source message against eavesdroppers [6]. In

several situations, the proposed blocking systems are less capable than the non-jamming ones. Subsequently a proposed hybrid system with intellectual switch method between the jamming and non-jamming modes was proposed.

### 3. RESULTS:

The examination and results of simulation expose the proposed techniques by means of cooperative jamming which can get better the rate of secrecy of the system by means of a large scale within a convinced transmitted power range. The node of selected relay helps to improve the information transmission connecting the two sources by means of strategy of an amplify-and-forward, whereas the jamming nodes are used in the direction of creating intended interference at the eavesdropper. The scheme of hybrid which switches sharply connecting modes of jamming and non-jamming is competent in providing the uppermost rate of secrecy in almost the entire transmitted power administration in networks of two-way cooperative system.

### 4. CONCLUSION:

In a cooperative network, the competence of relay or selection of jammer has an immense

impact on the performance of the whole system. In the recent times a two-way transmit channel was well studied for their possible application to cellular networks where the efficiency of transmit or jammer selection has a strong impact on the presentation of the system in a cooperative network. Numerous algorithms of selection are then proposed, intending at promoting the support to the sources and the intrusion to the eavesdropper. On the basis of both instant and normal knowledge of the eavesdropper channels the proposed system has done the selection of one conservative transmit node and two jamming nodes for increasing security against eavesdroppers. The hybrid system switches smartly between jamming and non-jamming modes and is well-organized for providing the high privacy rate in the entire administration of transmitted power in two-way cooperative networks. Though the jamming nodes are used for making intentional interference at the eavesdropper the selected transmit node helps for enhancing the information transmission between the two sources.

#### REFERENCES:

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] Mugen Peng and Wenbo Wang. "Technologies and standards for TDSCDMA evolutions to IMT-Advanced," *IEEE Communications Magazine*, vol. 47, no. 12, pp. 50–58, Dec. 2009.

[11] 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.

[12] 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.

[13] Lingyang Song and A. G. Burr, "Successive interference cancellation for space-time block codes over time-selective channels," *IEEE Communications Letter*, vol. 10, no. 12, pp. 837–839, Dec. 2006.