Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.53 – 59

RESEARCH ARTICLE

ENHANCING SECURITY IN TWO-WAY RELAY NETWORK BY USING COOPERATION JAMMING AND RELAY SELECTION APPROACH

[1]Ramya T V, [2]M. Madan Mohan

[1]PG scholar, Department of Computer Science and Engineering, Anna University Chennai, India

[2]Assistant Professor, Department of Computer Science and Engineering, Anna University Chennai, India

[1,2]Ranganathan Engineering College, Coimbatore

[1] ramyatv1991@gmail.com, [2] madhanaceit@gmail.com

Abstract* -*In wireless media, secure communication is one of the important concepts. We use Identity based cryptosystems in order to provide security in two-way relay networks. But due to the use of identity of a node as their public key, this scheme lacks the anonymity and privacy preservation. So, in order to solve this problem, propose a new approach in two-way relay networks by using cooperation jamming and relay selection approach for enhancing security. In this scheme, we propose a two-way relay network consisting of two sources, relays and an eavesdropper and there is a new relay chatting based on transmission scheme is proposed. It uses a single relay in order to forward the messages and the remaining relays transmit interference signals to confuse the eavesdropper by distributed beam forming.

Keywords –Jamming, Physical Layer Security, Relay Chatting, Secrecy Outage Probability, Two-way Relay Networks

I. INTRODUCTION

In wireless networks, security has been normally focused on higher layers by using cryptographic methods. Physical-layer security is to exploit the physical characteristics of the wireless channel in order to provide secure communications. In 1970s Wyner [1] introduced the wiretap channel , Which is a degraded version of the main

channel, so that the source and receiver can exchange secure messages at a non-zero rate. Cooperative jamming technique is used to improve the secrecy rate by causing interference to the eavesdropper with code words independent of the source messages. Yener and Tekin's [2] propose a scheme termed collaborative secrecy, which means a non-transmitting user is selected to increase the secrecy rate for a transmitting user by effectively "jamming" the eavesdropper.

The main purpose of physical-layer security is to exploit the physical characteristics of the wireless channel for providing secure communications. The security is defined in terms of *secrecy capacity*, which is the maximum rate of reliable information sent from the source to the appropriate destination in the presence of eavesdroppers. Wyner showed that the wiretap channel is a degraded version of the main channel, so that the source and the destination can exchange secure messages at a nonzero rate**.**

In Secure Wireless Communications via Cooperation [3]**,** Source and relays are in the same cluster, whereas, destination and eavesdropper are far away from this cluster. Global channel state information (CSI) is maintained for this approach. In this case, Stage1 is secure, while stage 2 is not secure. There are several schemes [4]-[17] has been proposed to overcome this limitation with the help of *cooperative relaying* [3], [4], and *cooperative jamming* [5]–[7]. In [3] and [4], authors proposed effective decode-and-forward (DF) and amplify-and-forward (AF)-based cooperative relaying protocols for physical-layer security. Cooperative jamming is an approach to improve the secrecy rate by interfering the eavesdropper with codeword's independent of the source messages.

In Opportunistic relay selection for one-way relay networks with secrecy constraints was addressed in [9], where the proposed scheme involved the joint selection of a relay and a jamming node to enhance the security. Following a similar idea in joint relay and jammer selection for two-way cooperative networks were investigated in [11]. Different from [9], the proposed algorithms in [11] select three relay nodes to enhance security, where the first selected node operated in the conventional relay mode and forwarded the sources' signals, and the second and third nodes act as jammers to degrade the eavesdropper links in the first and second phase, respectively. However, when the transmit power increases the secrecy outage probability would converge to a fixed value as the since the selected single-antenna jammer nodes introduced interference to the legitimate receiver [9,11]. Most recently, a relay chatting based on transmission scheme was proposed to enhance security in one-way relay networks introduced in [11], where a best relay is used to forward the source's signal using an amplify-and-forward (AF) protocol, and the remaining relays transmitted a jamming signal to confuse the eavesdropper and causing artificial interference via distributed beam forming. In this case, opportunistic relay chatting guaranteed that the secrecy outage probability converged to zero at high transmit power.

Two-way communication is a common scenario in which two nodes can transmit and receive the information simultaneously. Joint relay and jammer selection for two-way cooperative networks selected three relay nodes to enhance security, where the first selected node operated in a conventional relay mode and forwarded the source signals by the use of an AF protocol, and the second and third nodes acted as jammers in order to confuse the eavesdropper during the first and second phase of transmission. But the major problem associated with this technique is that the interference from jammers also degrades the information channels.

In the proposed system, a relay chatting scheme is introduced to enhance security where a best relay selected to forward message using an amplify-and-forward (AF) protocol, and the remaining relays used to cause artificial interference across the eavesdropper via distributed beam forming. Two chatting groups are formed from

the relays to transmit artificial interference to degrade the eavesdropper in the first and second phase, respectively. It obtains better secrecy performance than the joint relay and jammer selection scheme introduced before.

II. SYSTEM MODEL

The diagram shows the system model. In this fig.1, there are two sources S1 and S2, one eavesdropper E, and a relay node set $S_{in} = \{1,2,\ldots..K\}$ with K nodes. The relay nodes cannot transmit and receive simultaneously, so that the total communication process is performed in two phases. In the first phase, S1 and S2 broadcast their messages and the best relay transmits the message. The remaining relays forms a relay chatting group and causing artificial interference across the eavesdropper. The chatting group with size *N1*, is denoted as

$R1 = \{R_1, R_2 \ldots\ldots R_{N1}\}$

This is formed from the remaining K-1 relays and transmits a random message x1 via distributed beam-forming.

During second phase, the best relay node forwards the source messages to the corresponding destinations based on AF protocol while a new chatting group of size *N2* is denoted as

$R2 = \{R_1, R_2 \ldots\ldots R_{N2}\}$

This transmits a random message x2 by using a new beam forming vector. We can assume that the eavesdropper E can overhear the signals from the two phases.

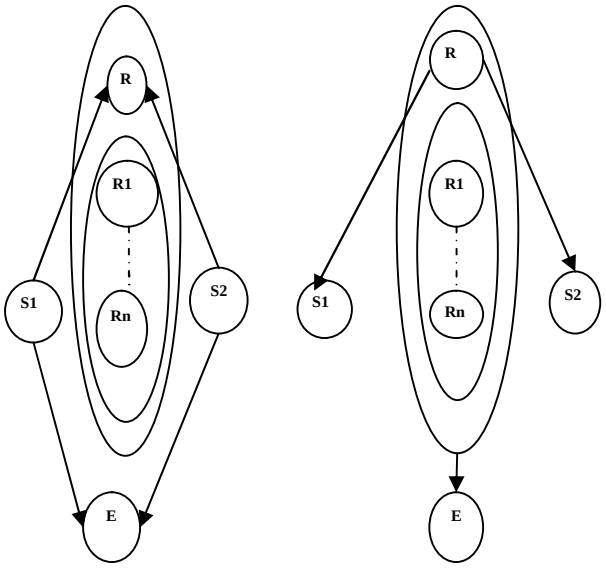

Fig.1 System model for relay chatting

The channel gain from node i to node j is denoted by $h_{i,j}$ which means an independent ,zero-mean, circularly symmetric Gaussian random variable with the variance $\sigma_{i,j}^2$ .Where as, $\sigma_{i,j}^2 = d_{i,j}^{-\beta}$, $d_{i,j}$ represents the Euclidean distance between node i and node j, whereas β represents the path-loss exponent. Furthermore, additive white Gaussian noise (AWGN) with zero mean and unit variance is assumed at each receiver.

III. SIGNAL MODEL

During the first phase, the two sources send the information symbols *s1* and *s2* , respectively, which are mapped to a PSK set. The received signals at the best relay node R and eavesdropper *E* can be, respectively, expressed as ,

$$y_R = \sqrt{P_S} h_{S1,R} s1 + \sqrt{P_S} h_{S2,R} s2 + \sqrt{P_J} h_{J1,R} j1 + v_R$$
$$y_{E1} = \sqrt{P_S} h_{S1,E} s1 + \sqrt{P_S} h_{S2,E} s2 + \sqrt{P_J} h_{J1,E} j1 + v_E \quad (1)$$

where $\{E\{|S_i|^2 = 1$ whereas i=1,2. v_R and v_E denote the noise at relay and the eavesdropper E, respectively.

$$h_{E1} = \left[h_{R1,E}, h_{R2,E} \dots \dots h_{R_{N1},E}\right]^T$$

With $h_{R_i,E}$ denoting the channel gain from the relay node *Ri* of the chatting group R1 to the eavesdropper E. And

$$h_R = [h_{R1R}, h_{R2R} \dots \dots h_{R_{N1}E}]^T$$

With, $h_{R_i,R}$ denoting the channel R1 gain from the relay node *Ri* of the chatting group to the best relay node R.

IV. CONSTRUCTION OF A TWO-WAY RELAY NETWORK

This module implements the information exchange against eavesdroppers in two-way cooperative networks, which usually consisting of two sources, one eavesdropper, and a collection of intermediate nodes. A relay node is selected from the intermediate node set to forward the messages from source to destination. The remaining intermediate nodes form a relay chatting group causing artificial interference across the eavesdropper in the first and second phase of data transmission.

V. EAVESDROPPER ATTACKING AND PREVENTION

In the two-way relay network if there is a presence of eavesdropper, it will degrade the performance of the network. The main purpose of the eavesdropper is to degrade the data from source to destination. So, to prevent this problem there several node selection techniques via relay chatting is introduced in the two-way system. Whereas, secrecy outage probability as the metric of the secrecy performance.

VI. SECURE COMMUNICATIONS VIA RELAY CHATTING

Define Γ_j as the signal to interference-plus-noise ratio (SINR) of the virtual channel *Si to Sj*.

$$\Gamma_1 = \frac{\alpha^2 P s_2 \left|h_{R^*,s1}\right|^2 \left|h_{s2,R^*}\right|^2}{\alpha^2 \left|h_{R^*,s1}\right|^2 + 1} \qquad (2)$$

$$\Gamma_2 = \frac{\alpha^2 P s_1 \left|h_{R^*,s2}\right|^2 \left|h_{s1,R^*}\right|^2}{\alpha^2 \left|h_{R^*,s2}\right|^2 + 1} \qquad (3)$$

The best relay can be selected based upon the following equation. In this case, we do not want to gain the global channel state information (CSI), only local CSI is needed.

$$\{R^*\} = \arg\max_{R \in S_{in}} \{(1 + \Gamma_1)(1 + \Gamma_2)\} \qquad (4)$$

The SINR of *S*i to *E* can be calculated as

$$\Gamma_{E_i} = \frac{P s_i \left|h_{Si,E}\right|^2}{P s_j \left|h_{sj,E}\right|^2 + P R_1 \left|h_{E_1}^T f_1\right|^2 + 1} + \frac{\alpha^2 P s_i \left|h_{R^*,E}\right|^2 \left|h_{si,R^*}\right|^2}{\alpha^2 P s_j \left|h_{R^*,E}\right|^2 \left|h_{sj,R^*}\right|^2 + P R_2 \left|h_{E_2}^T f_2\right|^2 + \alpha^2 \left|h_{R^*,E}\right|^2 + 1} \qquad (5)$$

The instantaneous secrecy rate for relay node set can be calculated as,

$$R_{s_i} = \left[\frac{1}{2} log_2(1 + \Gamma_i) - \frac{1}{2} log_2\left(1 + \Gamma_{E_j}\right)\right] \qquad (6)$$

Where *i,j*=1,2, i≠j

The overall secrecy performance of the two-way relay network is characterized by the sum of the two sources secrecy rate, which is represented as

$$R_s = R_{s1} + R_{s2}$$

$$= \left[\frac{1}{2} log_2 \frac{1+\Gamma_1}{1+\Gamma_{E_2}} + \frac{1}{2} log_2 \frac{1+\Gamma_2}{1+\Gamma_{E_1}}\right]$$

$$= 1/2 \left[log_2 \frac{(1+\Gamma_1)(1+\Gamma_1)}{(1+\Gamma_{E_2})\left((1+\Gamma_{E_1})\right)}\right] \qquad (7)$$

VII. SECRECY OUTAGE PROBABILITY

We use the secrecy outage probability as the metric of the secrecy performance. The probability is the providability for the case where the intend destinations are unable to decode the messages from the sources reliably. It also gives the metric for the case where the message transmission is not perfectly secure, which means there exists

some information leakage to the eavesdropper E . In order to calculate the secrecy outage probability, we firstly have to get the SINR of the links from *Si* to *E* for *i*=1,2. Eaves-dropper applies maximal ratio combining (MRC), so in order to examine the efficiency of the proposed scheme.

VIII. SIMULATION RESULTS

The intermediate nodes spread out randomly within a square space. When we are comparing the relay chatting scheme with joint relay and jammer selection scheme [11].It can be found that optimal selection with Maximum sum instantaneous secrecy rate (OS-MSISR)requires the knowledge of the eavesdropper channel and it is very difficult to obtain. When we are introducing the relay chatting scheme, it avoids those difficulties introduced before.

IX. CONCLUSION

This paper has studied a new relay chatting transmission scheme for secure communications in two-way relay networks. In this scheme, it does not require the knowledge of the eavesdropper's channel and it uses of a relay chatting scheme. It uses a single relay in order to forward the messages and the other relays are used to cause artificial interference across the eavesdropper. The secrecy outage probability of previous schemes converges to a fixed value as the transmitted power increases because single antenna jammer nodes causing interference to the sources. In the proposed work, the secrecy outage probability converges to zero as the transmitted power increases. This scheme achieves better performance by than the joint relay and jammer selection scheme.

REFERENCES

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

[2]. I. Krikidis, J. 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.

[3]. L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. 46th Ann. Allerton Conf.Communication, Control, and Computing, UIUC*, Illinois, Sep. 2008.

[4]. 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, and Signal Processing*, Taipei, Taiwan, Apr. 2009.

[5]. E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy," in *Proc. 44th Ann. Allerton Conf. Communication, Control, and Computing*, Monticello,IL, Sep. 2006.

[6]. E. Tekin and A. Yener, "The multiple access wire-tap channel: Wireless secrecy and cooperative jamming," in *Proc. Information Theory and Applications Workshop*, San Diego, CA, Jan. 2007.

[7]. E. Tekin and A. Yener, "Achievable rates for two-way wire-tap channels," in *Proc. IEEE Int. Symp. Information Theory*, Nice, France, Jun. 2007.

[8]. E. Ekrem and S. Ulukus, "Cooperative secrecy in wireless communications," in *Securing Wireless Communications at the Physical Layer*,W. Trappe and R. Liu, Eds. New York: Springer-Verlag, 2009.

[9]. I. Krikidis, J. S. Thompson and S. McLaughlin, "Relay Selection for Secure Cooperative Networks With Jamming," *IEEE Transactions on Wireless Communications*, Vol. 8, No. 10, 2009,

[10]. E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels,"*IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137–155, Jan. 2011.

[11]. J. Chen, R. Zhang, L. Song, Z. Han and B. Jiao, "Joint Relay and Jammer Selection for Secure Two-Way Relay Networks," *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 1, Jan. 2012

[12]. X. He and A. Yener, "On the equivocation region of relay channels with orthogonal components," in *Proc. 41st Ann. Asilomar Conf. Signals, Systems, and Computers*, Pacific Grove, CA, Nov. 2007.
[13]. X. He and A. Yener, "The role of an untrusted relay in secret communication,"in *Proc. IEEE Int. Symp. Information Theory*, Toronto, Canada, Jul. 2008.
[14]. X. He and A. Yener, "End-to-end secure multi-hop communication with untrusted relays is possible," in *Proc. 42nd Ann. Asilomar Conf.Signals, Systems, and Computers*, Pacific Grove, CA, Nov. 2008.
[15]. Y. Oohama, "Coding for relay channels with confidential messages, "in *Proc. IEEE Information Theory Workshop*, Cairns, Australia, Sep.2001.
[16]. Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proc. IEEE Int. Symp. Information Theory*, Nice, France,Jun. 2007.
[17]. E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy," in *Proc. 44th Ann. Allerton Conf. Communication, Control, and Computing*, Monticello,IL, Sep. 2006.

Ramya T V – Currently pursuing her M.E in Computer Science and Engineering from Ranganathan Engineering College, Coimbatore. Her areas of interest are network security, and Mobile computing.

M. Madan Mohan – He is working as an Assistant Professor in Dept.of Computer Science and Engineering in Ranganathan Engineering College, Coimbatore, India. His areas of interest are network security, Mobile computing, and Cloud computing.

