Enhancing Security In Two-Way Communicate Network by Using Collaboration Congestion and Transmit Selection Approach

[1]Hasina A. Razzak. A. Karim, [2]Prof. S S Handa, [3] Prof. M V Ramana Murthy
[1]Research Scholar, Dept of Computer Science & Engg, Manav Rachna International University, Faridabad, India.
[2] Professor in Dept. of Computer Science and Engg, Manav Rachna International University, Faridabad, India.
3 Professor, Dept. of Math & Computer Science, Osmania University, Hyderabad

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 Transmit 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 Transmit networks by using Collaboration Congestion and Transmit selection approach for enhancing security. In this scheme, we propose a two-way Transmit network consisting of two sources, Transmits and an eavesdropper and there is a new Transmit chatting based on transmission scheme is proposed. It uses a single Transmit in order to forward the messages and the remaining Transmits transmit interference signals to confuse the eavesdropper by distributed beam forming.

Keywords –Congestion, Physical Layer Security, Transmit Chatting, Secrecy Outage Probability, Two-way Transmit Networks

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 Congestion 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 "Congestion" 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.

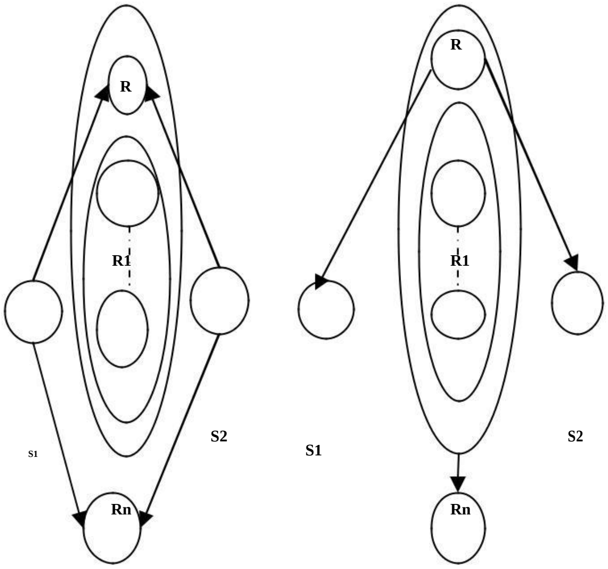
In Secure Wireless Communications via Collaboration [3]**,** Source and Transmits are in the same cluster, whereas, destination and eavesdropper are far away from this cluster. Global channel state information (CSI) is maintained for this approach. In this case, Stage1 is secure, while stage 2 is not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

In Opportunistic Transmit selection for one-way Transmit networks with secrecy constraints was addressed in [9], where the proposed scheme involved the joint selection of a Transmit and a Congestion node to enhance the security. Following a similar idea in joint Transmit and jammer selection for two-way cooperative networks were investigated in [11]. Different from [9], the proposed algorithms in [11] select three Transmit nodes to enhance security, where the first selected node operated in the conventional Transmit 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 Transmit chatting based on transmission scheme was proposed to enhance security in one-way Transmit networks introduced in [11], where a best Transmit is used to forward the source's signal using an amplify-and-forward (AF) protocol, and the remaining Transmits transmitted a Congestion signal to confuse the eavesdropper and causing artificial interference via distributed beam forming. In this case, opportunistic Transmit chatting guaranteed that the secrecy outage probability converged to zero at high transmit power.

In the proposed system, a Transmit chatting scheme is introduced to enhance security where a best Transmit selected to forward message using an amplify-and-forward (AF) protocol, and the remaining Transmits used to cause artificial interference across the eavesdropper via distributed beam forming. Two chatting groups are formed from the Transmits to transmit artificial interference to degrade the eavesdropper in the first and second phase, respectively. It obtains better secrecy performance than the joint Transmit and jammer selection scheme introduced before.

SYSTEM MODEL

The diagram shows the system model. In this fig.1, there are two sources S1 and S2, one eavesdropper E, and a Transmit node set = {1,2, … . . } with K nodes. The Transmit 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 Transmit transmits the message. The remaining Transmits forms a Transmit chatting group and causing artificial interference across the eavesdropper. The chatting group with size *N1*, is denoted as



Data Transmitting in Network with Congestion – Fig. 1

R1= { , ... }

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

During second phase, the best Transmit 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= { , ... }

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.

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

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 Transmit node is selected from the intermediate node set to forward the messages from source to destination. The remaining intermediate nodes form a Transmit chatting group causing artificial interference across the eavesdropper in the first and second phase of data transmission.

EAVESDROPPER ATTACKING AND PREVENTION

In the two-way Transmit 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

Transmit chatting is introduced in the two-way system. Whereas, secrecy outage probability as the metric of the secrecy performance.

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. Eavesdropper applies maximal ratio combining (MRC), so in order to examine the efficiency of the proposed scheme.

SIMULATION RESULTS

The intermediate nodes spread out randomly within a square space. When we are comparing the Transmit chatting scheme with joint Transmit 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 Transmit chatting scheme, it avoids those difficulties introduced before.

Two-way communication is a common scenario in which two nodes can transmit and receive the information simultaneously. Joint Transmit and jammer selection for two-way cooperative networks selected three Transmit nodes to enhance security, where the first selected node operated in a conventional Transmit 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.

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.

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.

CONCLUSION

This paper has studied a new Transmit chatting transmission scheme for secure communications in two-way Transmit networks. In this scheme, it does not require the knowledge of the eavesdropper’s channel and it uses of a Transmit chatting scheme. It uses a single Transmit in order to forward the messages and the other Transmits 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 Transmit 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, "Transmit selection for secure cooperative networks with Congestion," *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 Collaboration," 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 Collaboration 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 Congestion," 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, "Transmit Selection for Secure Cooperative Networks With Congestion," *IEEE Transactions on Wireless Communications*, Vol. 8, No. 10, 2009,

[10]. E. Ekrem and S. Ulukus, "Secrecy in cooperative Transmit 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 Transmit and Jammer Selection for Secure Two-Way Transmit Networks,"

[12]. X. He and A. Yener, "On the equivocation region of Transmit 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 Transmit 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 Transmits is possible," in *Proc. 42nd Ann. Asilomar Conf.Signals, Systems, and Computers*, Pacific Grove, CA, Nov. 2008.

[15]. Y. Oohama, "Coding for Transmit channels with confidential messages, "in *Proc. IEEE Information Theory Workshop*, Cairns, Australia, Sep.2001.

[16]. Y. Oohama, "Capacity theorems for Transmit 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.