A REVIEW ON DISTRIBUTED BEAM FORMING TECHNIQUES -AN APPROACH IN WIRELESS RELAY NETWORKS

Megha G. Paserkar[1], Shrikant D. Zade[2]

[1]*Research Scholar, Department of Computer Science and Engineering, Priyadarshini Institute of Engineering and Technology, Nagpur, Maharashtra, India*
[2]*Assistant Professor, Department of Computer Science and Engineering, Priyadarshini Institute of Engineering and Technology, Nagpur, Maharashtra, India*

Abstract

Physical layer security can be considered to solve the security problem from the point of view of information theory in wireless networks. The combination of cryptographic schemes with channel coding techniques is called for in the basic principle of information-theoretic security. Due to the presence of one or more eavesdropper in wireless relay networks, secrecy of communication is in jeopardy. For such a scenario secrecy rate of the network provide a good measure of performance of the system. In this paper our focus is on secrecy capacity and its optimization with appropriate weight designs of relays taking into consideration the channels through which the eavesdroppers are connected to the relays. We propose the AF and DF based optimal beam forming scheme to improve the wireless security against eavesdropping attack by detecting and removing the eavesdroppers from the wireless relay networks and thus finding measures to maximize the efficiency, response time and the throughput of the system It includes an auto-regression technique as first approach and the use of RC6 algorithm for encrypting the confidential messages. The scheme is a two way approach that will not only provides security to the confidential messages, to be communicated within a wireless relay network in presence of multiple relays and eavesdroppers, but also it will deal with the saving the consumed power by detecting and removing the nodes which are malicious or defected which in turn will consume more power in order to perform malicious activity on the messages or may try to create interferences in the network. The eavesdropper nodes in the proposed system are considered to be working as relays so it may either be connected to source or destination directly or in between the relays.

Keywords: *Beamforming, Channel State Information, Eavesdropper Attack, Power Consumption, Secrecy Capacity.*

----------***----------

1. INTRODUCTION

Recently a significant amount of research is going on to ensure secure communication in wireless networks. The implementation of security schemes at physical layer becomes a hotspot, as the high-layer secure protocols have attracted growing attacks in recent years. Due to broadcast nature of wireless transmission, the transmitted messages are susceptible to be intercepted by eavesdroppers. However, due to the fading effect and the broadcast property of radio transmission, wireless communication are always vulnerable to eavesdropping which consequently makes security schemes of great importance in it as a promising approach to communicate confidential messages and so the secrecy capacity is severely limited in wireless communications. If the eavesdropper node is not detected within appropriate time then the messages transmitted in the network could be read and used for malicious activities. To that end, user cooperation as an emerging spatial diversity technique can effectively combat wireless fading and thus improves the secrecy capacity of wireless transmissions in the presence of eavesdropping attack. In particular, node cooperation via relays can increase the achievable secrecy rate by exploiting/mitigating the channel effects. There are mainly two relaying protocols for the cooperative secure transmission: decode and-forward (DF) and amplify-and-forward (AF). The secrecy rate based on single-antenna systems is hampered by channel conditions.

Cooperative communications uses multiple nodes which help each other to transmit messages and has been widely acknowledged as an effective way to improve system performance. Beamforming is an attempt to achieve spatial diversity through the use of the partner's antenna. Apart from the cellular scenario, user cooperation diversity has the potential to be successfully used in wireless ad hoc networks also. Typically, the main channel capacity with multiple relays can be significantly increased by using cooperative beam forming. More specifically, multiple relays can form a virtual antenna array and cooperate with each other to perform transmit beam forming such that the signals received at the intended destination experience constructive interference while the others (received at eavesdropper) experience destructive interference. With the cooperative beam forming, the received signal strength of destination will be much higher than that of eavesdropper. In DF relaying protocol the relay first decodes its received signal from source and then re-encodes and transmits its decoded outcome to the destination. In an AF protocol, the source broadcasts message in the form of signal in the first hop where the information symbol is selected from a codebook and is normalized. The received signal at relay is the actual

message with additive noise. In the second hop, each relay forwards a weighted version of the noisy signal it just received. Amplify and forward relay networking scheme is simplest among them where each node transmits the message it has received after amplification (scaling). Though simplest in nature but the significance of this scheme lies in its low cost implementation and effectiveness against fading.

In this paper, we propose an auto regression technique and RC6 algorithm for maximizing the secrecy capacity of message being transmitted within a wireless relay network. For this, assuming that the global channel state information (CSI) is available, we consider a multi-hop network consisting of a single source and a single destination along with multiple relay nodes in between. However, due to the presence of one or more eavesdropper, secrecy of communication is in jeopardy. For such a scenario secrecy rate of the network provide a good measure of performance of the system. Unlike some previous works where only total relay power constraints are assumed, we consider the individual relay power constraint also. Generally, in practice, the relay nodes are powered by their individual power source without any means to share their power sources (e.g. battery). Therefore, individual relay constraint is more relevant in practical situations and general.

Auto regression technique here takes power consumption constraint into consideration. The proposed system is considered to be an ergodic system which is based only on past or present values of each node within a wireless relay network that participates in data transmission. In order to gain high efficiency this strategy of auto regression can be very helpful since it deals with power consumption in this paper. At each moment while transmitting message or signal the sensor's power consumption output will be compared to an already set threshold value. If the threshold value exceeds, it can be easily possible to detect an eavesdropper node since it may consume more power in order to process or observe the data for its malicious use.

The RC6 algorithm on the other hand provides a way to secure the transmission by encoding the message in such a way that if any other node except the trusted ones tries to decode the message by applying a random incorrect key, then the message will be destroyed and will not be available again to that suspicious eavesdropper node. Now since the feedback is included in the network due to cooperative relays. The missing packet can be recognized and resent from a different route. In this way, the proposed paper provides a 2- way secure approach for achieving secrecy in confidential message transmission in wireless relay networks using beamforming.

2. OVERVIEW OF EXISTING METHODS

In this paper we provide a comprehensive review of the published research on beamforming techniques using multiple relays, focusing to maintain secrecy capacity of the message. This section describes the existing techniques and algorithms related to confidential message transmission in wireless relay networks using relays and beamforming techniques for providing security and efficiency improvement in the relay nodes considering various parameters.

For improving security in physical layer, a design of beamforming in wireless relay networks is given by author in [1]. Beamforming solutions for amplify-and-forward (AF) and decode-and-forward (DF) relay networks have been proposed for secrecy capacity in presence of multiple eavesdroppers. It shows that the secrecy capacity does not always grow as the eavesdropper moves away from the relays or as total relay transmit power increases in an AF network. Also, if the destination is nearer to the relays than the eavesdropper, a suboptimal power is derived in closed form through monotonicity analysis of secrecy capacity. Whereas, in DF network, secrecy capacity is shown to be a single Rayleigh quotient problem that can be solved easily and if the relay-eavesdropper distances are nearly same, then in this case it is unnecessary to consider the eavesdropper in a DF network.

Author in [2] has worked on theoretical aspect of the system for obtaining new forms of transmit diversities so that the limitations in mobile user's data rate and quality of service can be overcome. The technique of user cooperation is implemented in a conventional low-rate code-division multiple-access (CDMA) system. In this, active mobile users are observed in CDMA implementation under consideration of information theoretic channel capacity , signal outage and cellular coverage and the gains obtained from user cooperation technique was found to be two pronged i.e. the higher data rate and decrement in sensitivity to channel variations. User cooperation strategy for mobile users in this case necessitates the need of ability to detect the uplink signals. The implementation of system in this involved increased complexity in the mobile receiver. The cooperative strategy in some sense, involves resending, of information using a cooperative signal. Another possibility for the two users involved in communication is to always transmit new information, even during the cooperative periods, thus necessitating the use of sequence detection due to the inter-symbol interference that would result from such a strategy.

The practical implementation aspect of diversity in user cooperation and analysis of its performance dealing with in-cell user cooperation is made in [3]. In particular, the optimal and suboptimal receiver design, the benefits of user cooperation technique of [2] and practical issues within the CDMA framework is extended and investigated. In this, the user cooperation in absence of the channel state information for high rate CDMA whereas the suboptimal reception and performance related issues for conventional CDMA is investigated. The reduced susceptibility to Rayleigh fading due to cooperation is attested to by a "smoother" data rate as a function of time, which can be measured by calculating the variance of the effective data rate.

To combat signal outage for cooperative diversity in wireless networks, low-complexity cooperative diversity protocol, selection and incremental relaying protocols has been introduced in [4]. Incremental relaying protocol exploits limited feedback to overcome bandwidth inefficiency by rare repetition of message to be transmitted thereby improving spectral efficiency of both fixed as well as selection relaying. For fixed relaying, the relays are allowed to either amplify their received signals subject to their power constraints, or to decode, re-encode and retransmit the messages. Analytically it has been shown that, except for fixed decode-and-forward, cooperative protocols achieves full diversity, i.e., outage probability decays with inverse proportion to square of signal to noise ratio (SNR), whereas without cooperation it decays with inverse proportion to SNR.

Gaussian wire-tap channel with feedback in [5] is an extension to the Wyner's results of achievable region for discrete memoryless wire-tap channels in [14]. Using converse theorem and time sharing curve the results obtained in [5] therefore, shows the secrecy capacity as the difference between the capacities of the main and wiretap channel, considering the uncertainties of the signal to noise ratios of the corresponding channels.

In [6], the authors have considered a collaborative use of AF relays in order to form beamforming system and to provide security at physical layer for a wireless machine to machine system taking power constraint into consideration. For several optimization problems various beamforming schemes have been proposed viz., secrecy rate maximization (SRM), semi-definite relaxation (SDR), virtual eavesdropper-based SRM (VE-SRM), relay power minimization (RPM) and virtual eavesdropper-based RPM (VE-RPM) beamforming scheme. Each of these schemes combats the complexities of its predecessor. SRM has been developed to maximize the secrecy rate at relays under total power constraint but it is difficult to implement SRM due to the existence of multiple semi-definite programs (SDPs). A two-level optimization problem can be formed by the problem of secrecy rate maximization in SRM and to solve it SDR technique was introduced. The VE-SRM beamforming scheme relaxes the constraint of selecting the eavesdropper with the highest eavesdropping rate. The power constraints consideration of the RPM beamforming scheme is relaxed by introducing the virtual eavesdropper-based RPM (VERPM). All these beamforming schemes do not rely on the null space conditions.

In order to increase secrecy of message in cooperative wireless communication via relays, it is important to have a method that helps selecting an optimal relay. One such method of AF and DF based optimal relay selection schemes are explored in [7]. And also the multiple relay combining MRC framework has been investigated in which signals from multiple relays are combined at destination node in presence of single eavesdropper. Unlike traditional approach in which only the CSI of two-hop relay links are considered, additional CSI is also considered along with. In order to evaluate the diversity order performance of optimal relay selection schemes in comparison with traditional schemes, an asymptotic intercept probability analysis has been carried out. And it has been found that intercept probability of proposed scheme is always smaller than traditional scheme.

Author in [8] provides three cooperative schemes for improving physical layer security while using cooperative relays. These schemes are: a) decode-and-forward (DF), b) amplify-and-forward (AF) and c) cooperative jamming (CJ). System design in this is determined in such a way that the achievable secrecy rate maximizes subject to a transmit power constraint, or, the transmit power minimizes with respect to a secrecy rate constraint. Each node is assumed to carry a single omni-directional antenna, i.e. beamforming scheme and that global CSI is available. For AF and DF, the message broadcasting stages are as explained in [1], whereas in CJ the relays transmit a weighted jamming signal with the purpose of prohibiting the eavesdroppers while the source broadcasts its message in the network. For designing relay weights and allocating the transmit power separate methods are carried out for DF and CJ. In CJ, complete nullification of the total jamming signal sent from relays is done at destination whereas in DF a closed form optimal solution for the relay weights, in presence of an eavesdropper, is derived.

3. CONCLUSION

Data security has always been a very important issue while transmitting data in a wireless relay networks. So to deal with this, various beamforming techniques as well as cryptographic methods has been used but it worked for two hop message transmission process and also it did not provide the efficient security in case when the number of relays increased, thereby increasing the number of hops and demanding measures for increased secrecy of confidential message. Beamforming enables the pair of wireless terminals, each with a single antenna, to fully exploit spatial diversity in the channel by focussing its complete signal array in the direction of the receiver node directly. Relay nodes uses amplify and forward and decode-and-forward relaying to convey the source message to the destination via the relays. The alternate solution is the use of auto-regression technique and RC6 algorithm which therefore provides two way security and so is power saving. The different parameters used are time consumption, power consumption and cryptography to produce result. Since, managing the limited resources along with increased security is an important issue to be dealt in the wireless networks, appropriate techniques and system design modifications providing higher system throughput and efficiency can be made in the system as future scope.

REFERENCES

[1] Mujun Qian, Chen Liu and Youhua Fu, "Distributed beamforming designs to improve physical layer security in wireless relay networks", EURASIP Journal on advances in signal processing 2014, 2014:56.

[2] Andrew Sendonaris, Elza Erkip and Behnaam Aazhang, "User cooperation diversity—part I: system description", IEEE transactions on communications, vol. 51, no. 11, November 2003.

[3] Andrew Sendonaris, Elza Erkip and Behnaam Aazhang, "User cooperation diversity—part II: implementation aspects and performance analysis", IEEE transactions on communications, vol. 51, no. 11, November 2003.

[4] J. Nicholas Laneman, David N. C. Tse and Gregory W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior", IEEE transactions on information theory, vol. 50, no. 12,December 2004.

[5] S. K. Leung, Yan-Cheong and Martin E. Hellman, "The gaussian wire-tap channel", IEEE transactions on information theory, vol. IT-M, no. 4, July 1978.

[6] Zhongjian Liu, Xiaoning Zhang, Lin Bai, Chen Chen and Haige Xiang, "Secure beamforming via amplify-and-forward relays in machine-to-machine communications", International journal of distributed sensor networks volume 2013, Article ID 728532, 11 pages.

[7] Yulong Zou, Xianbin Wang and Weiming Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks", IEEE journal on selected areas in communications (In press).

[8] Lun Dong, Zhu Han, Athina P. Petropulu and H. Vincent Poor, "Improving wireless physical layer security via cooperating relays", IEEE transactions on signal processing, vol. 58, no. 3, March 2010.

[9] Vo Nguyen Quoc Bao, Nguyen Linh-Trung and M´erouane Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers", IEEE transactions on wireless communications 12, 12 (2013).

[10] Xiang He and Aylin Yener, "End-to-end secure multi-hop communication with untrusted relays", IEEE transactions on wireless communications, vol. 12, no. 1, January 2013.

[11] Ioannis Krikidis, John S. Thompson and Steve McLaughlin, "Relay selection for secure cooperative networks with jamming", IEEE transactions on wireless communications, vol. 8, no. 10, October 2009.

[12] A H M Kamal, "Steganography: securing message in wireless network", International journal of computers & technology volume 4 No. 3, March-April, 2013.

[13] Jun Xiong, Dongtang Ma1, Chunguo Liu, Xin Wang, "Secure communications for two-way relay networks via relay chatting", communications and network, September 2013.

[14] A. D. Wyner, 'The wire-tap channel," Bell Cyst. Tech. Journal, vol. 54, pp. 1355-1387, Oct. 1975.