A Review on Efficient Data Transmission in Wireless Relay Networks using Beamforming

Megha G. Paserkar, Shrikant D. Zade
Department of Computer Science & Engineering
Priyadarshini Institute of Engineering & Technology
Nagpur, India
e-mail: megha18deep@gmail.com
cdzshrikant@gmail.com

Abstract— The increased use of wireless networks for communication has grabbed the attention of many researchers in the recent years in order to find the actual techniques that are already used as well as the techniques that can be implemented in the wireless networks such as to provide highly efficient and secure data transmission with least data loss and to use the available resources in an effective manner. The main objective behind data exchange in such networks is to maintain the efficiency and secrecy capacity of the channels between the sources, destinations and the in-between relay nodes. This paper deals with the review on some of the well found existing methods and techniques that has been implemented on wireless networks under varying scenarios with consideration of various parameters aiming to improve the throughput of the network system. The varying scenarios may have inclusion of signal fading, representing coverage of each node, presence of relay nodes to further transmit the messages, power consumption, communication channels, eavesdropper nodes, encoding-decoding, use of antennas for bandwidth concerns and directing signals, all aiming at possibly increasing channel bandwidth and secrecy capacity assuming the channel state information of the network components to be known.

Keywords- *Relays, Wireless Networks, Beamforming, Secrecy Capacity, Eavesdropper.*

*****

I. INTRODUCTION

A Wireless Relay Networks (WRN) consists of many sensors some of which works as in-between nodes that are anonymously distributed spatially. These nodes not only monitor the physical conditions of the network but also the effective and efficient data traversal. Since the connectivity infrastructure is not pre-existing, these networks are also termed as ad-hoc networks. The in-between nodes are also called as relay nodes since they bridge gaps between the source and destination that are geographically separated and not within the range of each other following the principle of co-operative communication. So in this case, to complete the network, relay nodes acts as the medium through which connection of spatially distributed system is possible. These nodes, forming a complete route from transmitter to receiver, consist of sensors, some memory storage, microcontrollers and small battery for power source. Each time a node receives data from any other node, it processes it to get information regarding its destination and find the respective route through other relay nodes. The relay nodes do no keep data for a longer duration thus the temporary memory is present to store the data fro a while and then forward it towards its destination. At each time of processing the received data, some amount of power is consumed by the nodes. This power source is provided by the small battery present as a resource with the sensor nodes.

The communication in WRN's is broadcast in nature i.e. signal propagation is omni-directional by the antennas. This although being useful leads to non-uniform use of scarcely available resources since signal transmission by the antennas are propagated in all directions equally thus reducing the available bandwidth too. To overcome with this situation the concept of "beamforming" was brought into existence. Beamforming is a technique in which the transmitting antennas are directed towards the direction of the destined receiver thereby focusing complete signal propagation being focused towards the concerned receiver thereby saving power consumption and proper utilization of the limited bandwidth.

The use of beamforming techniques for communication in wireless networks has been considered as one of the most interesting paradigms in future of wireless networks. The Amplify and Forward (AF) and Decode and Forward (DF) procedures are very well known whenever communication in a wireless network is thought of. Also the main emphasis of the network designers, since the traditional times, has always been on increasing the system's throughput and secures transmission of data in packet switched peer networks minimizing the delay in communication. But since the transmission medium is broadcast nature and decentralized property, the outage probability poses a serious threat of eavesdropper and many such attacks directly or indirectly hampering the security in wireless communications in actual practice. The use of cryptography for encoding and decoding the transmitted messages has always been called for as the basic principle in secure communication in case of wireless networks. Thus by now it has been clear that guaranteeing secure transfer of the information over an ad-hoc wireless network is as important as reliability. One such approach to gain security in WRN's is to detect the suspicious eavesdropper nodes and then removing it from the network. Since it may not be practical in many cases to remove such malware nodes due to geographical spanning of the networks, measures can be taken to block message traffic of all future transmissions towards these nodes by deactivating the channels or causing interference in channels leading to such defaulter nodes. Thus many such technologies have been developed and are still under work, to cope up from the

various attacks that are to be encountered by these networks, by exploiting various means of diversities, including time, frequency, codes and space.

II. Overview of Existing Methods

This section describes the comprehensive review of the existing techniques and algorithms and methods related to confidential message transmission in wireless relay networks based on published research on various techniques using multiple relays for providing security and efficiency improvement in the WRN's taking various parameters into consideration.

A design of beamforming in WRN's for improvement of security in physical layer, is given by author in [1]. Beamforming solutions have been proposed for amplify-and-forward (AF) and decode-and-forward (DF) relay networks for secrecy capacity in presence of several eavesdroppers. It has been shown in the results that as the distance between eavesdropper and the relays increases or as total relay transmit power increases in an AF network; the secrecy capacity does not always grow. Also, it was found in that if the distance between destination and the relays is less than that of the eavesdropper, a suboptimal power can derived in closed form through monotonicity analysis of the secrecy capacity. Whereas, for DF network, secrecy capacity was shown in [1] 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 consideration of the eavesdropper in the DF network seemed to be unnecessary.

The design of distributed position based protocol i.e. a self-reconfiguring network protocol is developed in [2] for a stationary ad hoc network in order to find the minimum power topology that consumes the least possible amount of energy. Each node is both an information source and an information sink in a peer to peer network. This means that each node wishes to both send and receive messages to and from any other nodes. An important requirement of such communications is strong connectivity of the network. A network graph is said to be "strongly connected" if there exists a path from any node to any other node in the graph [12]. A peer-to-peer communications protocol must guarantee strong connectivity. Since the position of each node changes over time in mobile networks, the protocol must be able to dynamically update its links to maintain strong connectivity.

Combined use of wiretap codes, lattice codes and a network coding scheme in [3] shows that the information theoretic end-to-end secure communication is possible over a chain of non-trustworthy relay nodes. Each relay has the ability to remove the channel noise from its received signal, thus alleviating the degradation in rate due to noise accumulation over the hops, but cannot separate the confidential message from the structured interference. The concept of rely channel was introduced in [14]. It is proved that the source and destination .can securely communicate despite of the fact that the signals transmitted by the source can reach the destination only through the route using these untrusted relay nodes. For this, a multi-hop line network is considered, where each node can receive the transmitted signals by its two adjacent neighbours. The model embodies both the interference and broadcast aspects of wireless networks as such. The fact that the network has interference was utilized as the main idea behind the achievability scheme. The achievable secrecy rate is independent of the number of hops through relay nodes.

Two different beamforming design approaches are proposed in [4]. A common assumption is used regarding the availability of perfect instantaneous channel state information (CSI) at the receiver as well as relay nodes. A wireless network consisting of a source, a destination and multiple relay nodes is considered where each relay has a single antenna for sending and receiving the information. As first approach a beamformer is designed through minimization of the total transmit power subject to a constraint guaranteeing the quality of service to the receiver. Whereas, as the second approach, beamforming weights have been designed through maximizing the signal-to-noise ratio (SNR) at the receiver subject to total transmit power constraint and individual relay power constraints. And also as the CSI becomes more uncertain, the quality of service constraint becomes harder to satisfy, i.e., more power is required to satisfy these constraints.

The behavior of block space-time code in wireless channel dynamics is observed in [5]. A slow fading channel environment is considered for optimally constructing the block space-time code. Although some space-time codes have been developed for fast fading channels [13], assuming the low data rates and low signal-to-noise ratios. A base station and mobile is considered, both of them equipped with multiple antennas. It has been shown that as compared to the conventional channel coding, the block space-time coding gain can be degraded below using a single transmit antenna for some characteristics of channel With the uncertain and rapidly changing channels in wireless communication, a robust space-time code is very much needed. Each symbol encoded are converted first from serial to parallel and then fed to the modulator, later on which the convolutional coding is applied on each stream of data.

The exploitation of multi-element array (MEA) technology is examined in [6]. The ultimate limits of bandwidth efficient delivery of digital signals with high bit rate in presence of MEA's have been estimated in wireless communication networks. The narrow bandwidth is analyzed such that the channel can be treated as flat over frequency and then the capacity is computed. As the number of antennas increases the capacity is seen to be increasing drastically. However, there have been some limitations exposed. First limitation being the strong correlation of the field transmission matrix elements as the antenna spacing drops below certain level. The second limitation being the introduction of mutual coupling between antennas as the spacing between antennas reduces even more. In many cases, the CSI are assumed to be available.

The capacities of the certain discrete relay channels and the Gaussian relays are evaluated in [7]. For this an encoding scheme viz., Superposition block Markov encoding scheme is used to show achievability of channel capacity and its converses have been established for capacity for degraded, reversely degraded and feedback relay channels. The relay channel in this case is considered to be including an input, a relay output, a channel output and the relay sender. The channel is assumed to be memoryless. A lower bound to the capacity of the channel of the general relay channel is achieved.

A two-way relay network consisting of two sources, multiple relays cooperate with each other for communication and an eavesdropper is investigated in [8].]. A network is

configured in such a way that the created scenario, consists of two sources, one eavesdropper, and a set of relay nodes, is altogether considered. Multiple antennas may not be available at network nodes and therefore cooperative relays were used due to the limitations in their cost and size. A relay chatting based transmission scheme to two-way relay networks is extended motivated by the work done in [16]. The proposed scheme is found to achieve better performance than the joint relay and jammer selection scheme. Also the knowledge of the eavesdropper's channel did not seem to be necessary. As the transmit power increases the outage probability secrecy of the proposed scheme approaches to zero level. The secrecy outage probability is used as the metric of secrecy performance. The outage probability of secrecy not only provides outage probability for the case where the intended destinations are unable to decode the messages reliably from the sources, but also it gives the metric for the case where some information leakage to the eavesdropper node exists during the message transmission. For proposing secure scheme with relay chatting, a method for selecting optimal relay [15] for communication is needed. The first relay operates as a conventional node assists a source to deliver its data to a destination via a DF strategy and the second relay is used in order to create intentional interference at the eavesdropper nodes [15].

Opportunistic relay selection with secrecy constraints in cooperative networks is studied in [9]. Three opportunistic relay selection schemes are considered to deal with the problems of overhearing of confidential messages by the eavesdroppers in the network. The first scheme deals with selection of the relays with lowest instantaneous signal-to-noise ratio (SNR) to eavesdropper nodes so as to reduce the overhearing of information at the eavesdroppers site. Conventional selection relaying that seeks the relay having the highest SNR to the destination is dealt with in the second scheme. Whereas in the third scheme, ratio between the SNR of a relay and the maximum among the corresponding SNR's to the eavesdroppers is considered, and then based on its output the optimal relay is selected to forward the signal to the destination node. The performances of the three relay selection schemes in terms of the probability of non-zero achievable rate of secrecy, the outage probability of secrecy and achievable secrecy rate of the three schemes are studied. The system model possesses a single source and destination and a set of decode-and-forward (DF) relays [17] that help the transmission between the source and the destination to avoid overhearing attacks of malicious eavesdroppers.

The Gaussian wiretap channel model in [18], in which there is no interference in the main channel, is extended to the Gaussian wiretap channel with side information by introducing additive white Gaussian interference in the main channel in [10], which is available in advance to the encoder. A leakage function is introduced and used for node selection as a criterion. Based on the value of this leakage function, the mode of operation is selected. In addition to the transmit power, the power of the interference, is used to confuse the wire-tapper even though the interference cannot be controlled by the encoder. The limited power available to the encoder is used for two purposes viz., so that perfect secrecy can be achieved by confusing the adversary, and to mitigate the interference effect in the main channel so that the high rate message transmission can be made possible.

A special case of partially cooperating encoders from a security perspective with Willems's two-user multi-access channel is studied in [11]. Two encoders are considered in the setup of system model. In this, only one among the two encoders is used to confer with the transmission in the network and a passive eavesdropper is considered from which the communication is to be kept secret so that the transmission is not overheard by it. Two cases are illustrated where first is the discrete memoryless case for which inner and outer bounds on the capacity-equivocation region is established and second case is for memoryless Gaussian model for which lower and upper bounds on the secrecy capacity is established. A multi-access channel is considered in which the two users can cooperate partially through a unidirectional noiseless bit-pipe of finite capacity. If the capacity of noiseless bit-pipe is increased, the achievable secrecy rate increases. The inner bound here is based on a combination of Willems's coding scheme, noise injection and additional binning that provides security randomization.

III. CONCLUSION

Since its first introduction, communication over wireless network has been remarkably skyrocketing for the past few decades and as a result of this, wireless communication is one of the fast innovating technologies. The study focused only on the review of wireless communication networks to forecast the future of wireless mobile communication technologies with detailed consideration of the other related factors so as to reflect adoption of future technologies indirectly into the wireless network model. Even though with some limitations, this study provides a useful survey, of wireless mobile communication networks and the additional technologies, protocols and schemes, through a quantitative analysis. Base on the study done for the review it can be concluded that many procedures have been implemented since now on wireless scenario, each of them having main focus on improving the overall efficiency and response time of the system thereby leading to increased throughput. It is because the security of confidential messages transmitted over the network is always the main priority thereby also maintaining and effectively and efficiently managing the available resources without much loss in such networks.

ACKNOWLEDGMENT

I sincerely acknowledge the teaching staffs of the department and authors of the corresponding references for their guidance and being an inevitable part of this review article.

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] Volkan Rodoplu and Teresa H. Meng, "Minimum energy mobile wireless networks", IEEE Journal on Selected Areas in Communications, Vol. 17, No. 8, August 1999.

[3] 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.

[4] Veria Havary-Nassab, Shahram Shahbazpanahi, Ali Grami and Zhi-Quan Luo, "Distributed beamforming for relay networks based on second-order statistics of the channel state information", IEEE Transactions on Signal Processing, Vol. 56, NO. 9, September 2008.

[5] Won Mee Jang, Jong Hak Jung, " Performance of block space-time code in wireless channel dynamics", Int. J. Communications, Network and System Sciences, Scientific Research, 2009, 6, 461-468.

[6] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas", Wireless Personal Communications 6: 311–335, 1998.Kluwer Academic Publishers. Printed in the Netherlands.

[7] Thomas M. Cover and Abbas A. El Gamal, "Capacity theorems for the relay channel", IEEE Transactions on Information Theory, Vol. IT-25, No. 5, September 1979.

[8] Jun Xiong, Dongtang Ma, Chunguo Liu, Xin Wang, " Secure communications for two-way relay networks via relay chatting", Communications and Network, 2013, 5, 42-47 http://dx.doi.org/10.4236/cn.2013.53B2009, Scientific Research, Published Online September 2013.

[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) 6076 - 6085" DOI : 10.1109/TWC.2013.110813.121671.

[10] Chaichana Mitrpant, A. J. Han Vinck and Yuan Luo "An achievable region for the gaussian wiretap channel with side information", IEEE Transactions on Information Theory, Vol. 52,No.5,May2006.

[11] Zohaib Hassan Awan, Abdellatif Zaidi and Luc Vandendorpe, "Multiaccess channel with partially cooperating encoders and security constraints", In Press.

[12] N. A. Lynch, "Distributed Algorithms", San Mateo, CA: Morgan Kaufmann, 1996, pp. 51–80.

[13] V. Tarokh, N. Seshadri and A. R. Calderbank, "Space-time codes for high data rate wireless communi-cation: Performance criterion and code construction," IEEE Transactions on Information Theory, Vol. 44, No. 2, pp. 744–765, March 1998.

[14] E. C. van der Meulen, "Three-terminal communication channels," Adv. Appl. Prob., vol. 3, pp. 120-154, 1971.

[15] 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.

[16] Z. Ding, K. K. Leung, D. L. Goeckel and D. Towsley. "Opportunistic relaying for secrecy communications: cooperative jamming vs. relay chatting," IEEE Transactions on Wireless Communication. 2011, pp. 1725-1729. doi: /10.1109/TWC.2011.040511.101694.

[17] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behaviour," IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

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