International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.2., 2016
(Mar-Apr)

REVIEW ARTICLE

ISSN: 2321-7758

A SECURE TRANSMISSION SCHEME FOR MIMO TECHNIQUE WITH TRANSMIT ANTENNA SELECTION

KEERTHIGA.K[1], RAMACHANDIRAN.K[2]
[1]Student, [2]Senior Assistant Professor,
Department of ECE, IFET College of Engineering,Villupuram.

ABSTRACT

The proposed system is a secure transmission scheme in the multi-input multi-output multi-eavesdropper wiretap channel. The transmit antenna selection with maximal-ratio combining (TAS/MRC) is adopted in user-destination and relay-destination links where a single transmit antenna that maximizes the instantaneous received signal-to-noise ratio is selected and fed back to transmitter by receiver and all the receive antennas are combined with MRC. In practice, the signal-to-noise ratios (SNRs) of all branches need to be known for optimal antenna selection. However, it is indeed challenging to know these SNRs when there is only one radio frequency (RF) chain at the transmitter.This proposed system mainly used data encryption and decryption of transfer data in the network. To thoroughly assess the secrecy performance achieved by the proposed scheme, we derive new closed-form expressions for the exact secrecy outage probability and the probability of non-zero secrecy capacity for arbitrary SNRs.

Keywords: Transmit antenna selection, Maximal ratio combing, Channel state information, Data encryption and decryption.

INTRODUCTION

Wireless networks involve multiple limitations and complexities. Wireless devise always face constraints with regard to their size and number of antenna, along with the transmission power, power consumption, and data capacity. To solve the problems, different multiple input multiple output(MIMO) technologies have been proposed, which introduce works and the devices.

Sharing local resources of other nodes in the network helps propagation of information from the source to the destination. This exploitation of the spatial diversity by relaying overheard signals is the signal is the main concept underlying cooperative communication[1]. This method requires the cooperation of a partner in a wireless network and recently attracted considerable attention in emerging wireless applications due to their advantage of network coverage extension and capacity expansion. A spatially replicated packet propagates through multiple nodes from the source to the destination. A node may or may not be in an active session itself, but simultaneously, can act as a cooperating peer for another node. We note that most research contribution in cooperative communications assumed perfect synchronization[3].In some times synchronization imperfect means, it cannot applicable for the transmission of networks.

To overcome the problem caused by imperfect synchronization, the space-time network coding(STNC) scheme was used[5]. This method used time division multiple access(TDMA) to deal with the imperfect synchronization issues. Importantly, this scheme achieves the full diversity order. STNC combines information from different sources at each relay mode and transmits the combined signal in dedicated time slots. Which jointly exploit the benefits of both network coding and space-time coding. To quantify the benefit offered by STNC, the symbol error rates of STNC over Rayleigh and nakagami-m fading channel were investigated in [6][9],respectively, and the outage probability of STNCin Rayleigh fading channel analyzed in[6]. In [10] it was assumed that the channel state information is known at the receivers. To avoid the requirement of channel estimation, the differential space-time network coding(DSTNC) and distributed differential space-time frequency network coding(DSTFNC) schemes were designed for narrowband and broadband cooperative communication system, respectively, in8. Similarly to STNC, both the DSTNC and DSTFNC scheme provide the full diversity. STNC scheme was proposed to achieve a better tradeoff between diversity gain and bandwidth efficiency. The primary analytical contributions of this paper are summarized as follows.

- We integrate cascaded TAS/MRC into STNC as a solution to preserve full transmit and receive diversity with low computational complexity and reduced feedback overheard.
- We drive new closed form exact and asymptotic expressions for the OP and SER. These results are valid for general operating scenarios with arbitrary number of antennas and arbitrary number of relays.
- Based on our results. It is demonstrated that the transmit diversity vanishes and that the diversity order is entirely independent of the number of transmit antennas.

These are advantage present in this method. But some of the disadvantages are, it cannot provide secure data transmission in network. So, we go for secure data transmission in the network. In our proposed scheme used same method for full diversity order and reduce overheard in the network. But, we use cryptography method for data encryption and decryption.In conventional communication systems, various cryptographic schemes have been designed and applied to guarantee the information transmission security in the upper layers assuming an error-free link in the physical layer. However, traditional cryptographic schemes based on complex mathematical functions have become increasingly unreliable when the computational ability of eavesdropper becomes more powerful. Based on this important observation, from the information theoretic point of perspective, physical layer security has been introduced to strengthen the secure transmission of wireless communications. The key idea behind physical layer security is to exploit different characteristics between the main channel and the eavesdropper's channel. The author first introduced the concept of the wiretap channel and demonstrated that perfect security can be achieved when the quality of the eavesdropper's channel is inferior to that of the main channel. Key are used to encrypt and decrypt the data. Key distribution are divided into two categories 1. Secret key 2. Public key. In this proposed system, we use secret key for diffie-Hellman algorithm. To thoroughly assess the secrecy performance by the proposed scheme, we drive new closed form expression for the exact secrecy outage probability and probability of non-zero outage probability for arbitrary. The rest of the paper is organized as follows. Section I, STNCspace time network coding). Section II,TAS(transmit antenna selection). Section III, CSI(channel state information). Section IV, MRC(maximal ratio combining). Section V, Data Encryption and Decryption. Section VI, Simulation Results, Section VII, Conclusion.

***SECTION I*: (SPACE TIME NETWORK CODING)**

The concept of our proposed STNCs is very general. The space-time network coding (STNC) scheme was proposed in this method, which uses time-division multiple access(TDMA) to deal with the imperfect synchronization issues. Importantly, this scheme achieves the full diversity order. STNC combines information from different sources at each relay node and transmits the combined signal in dedicated time slots, which jointly exploit the benefits of both networking coding and space-time coding. In other major techniques are time division multiple access (TDMA), frequency division multiple access (FDMA) and code division multiple access (CDMA).This techniques are occur the imperfect synchronization of the network.

***SECTION II*: TRANSMIT ANTENNA SELECTION (TAS)**

The application of TAS may pose a challenge. In practice, the signal-to-noise ratios (SNRs) of all branches need to be known for optimal antenna selection. This leads to the fact that the CSI associated with the selected transmit antenna during the antenna selection process may not be the same as the CSI during the subsequent data transmission. It is a new secure transmission scheme to avoid the occurrence of the connection outage in the presence of outdated antenna selection.

***SECTION II*: CHANNEL STATE INFORMATION(CSI)**

In MIMO systems, channel state information (CSI) refers to instantaneous information of the channel for data transmission or interference channels. CSI is useful for adapting transmission waveforms at transmitters, detecting data or interference cancelation at receivers, or scheduling at base stations. First, transmit CSI allows a data symbol to be mapped to transmit antennas after being multiplied with weights, which are selected for maximizing the power of the received symbol. This transmission strategy and the weight vector are called beam forming and a beam forming vector, respectively. Beam forming effectively reverses the adverse effect of fading and increases the propagation distance over which wireless signals can be reliably received, called the transmission range. Second, the former supports a single data stream with maximum reliability and hence achieves the full diversity gain; preceding enables multiple data streams in space and attains spatial multiplexing gain. Third, transmit CSI allows adaptive modulation and power control for attaining the capacity of a time-varying channel. Finally, in ad hoc networks, transmit CSI of both data and interference channels enables a transmitter to avoid interference to unintended receivers.

In many MIMO systems, transmit CSI must be acquired by feedback from receivers to transmitters. In systems using time-division multiplexing, transmit CSI can be obtained by estimating the reverse-link channel from the receiver to the transmitter, since its realization is very close to that of the forward-link channelgiven hardware calibration. In practice, CSI inaccuracy exists due to finite-rate CSI feedback and imperfect CSI estimation. Moreover, due to multiuser and the multiplicity of MIMO channel coefficients, acquiring CSI can incur overwhelming training or feedback overhead.

Addressing these issues, the theme of this dissertation is to design efficient algorithms for CSI acquisition and characterize the fundamental effects of CSI inaccuracy on the throughput of different types of MIMO systems including the point-to-point link, the cellular downlink and uplink, and the mobile ad hoc network. Considering MIMO systems with different complexity allows us to focus on different subsets of issues related to CSI inaccuracy and thereby maintain mathematical tractability. For the cellular downlink and uplink, this dissertation focuses on combining scheduling and CSI feedback for coping with CSI inaccuracy. For the mobile ad hoc network, the research focus shifts towards spatial interference cancelation using imperfect CSI and the effects of CSI inaccuracy on the network spatial reuse efficiency. This dissertation provides methods and guidelines for transforming MIMO technologies from theory into practical applications.

***SECTIONIV*: MAXIMAL RATIO COMBINING (MRC)**

The antenna receiver and the antenna eavesdropper adopt maximal ratio combining (MRC) to combine the received signals. The TAS was examine in MIMO channels, together with maximal ratio combining (MRC) and generalized selection combining at the legitimate receiver.

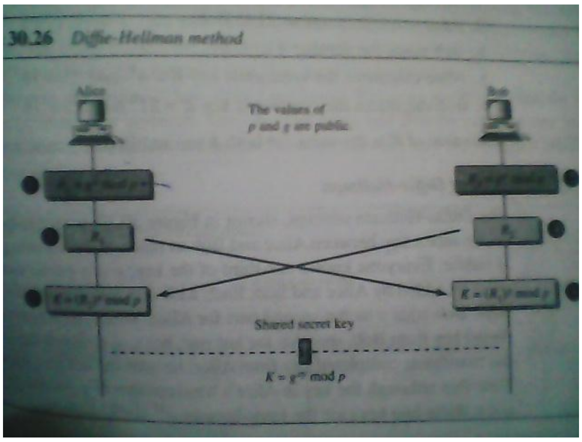
Diversity combining is a well-known technique to mitigate the performance degradation of multipath fading and co channel interference (CCI) in wireless systems. In flat fading channels, maximal ratio combining (MRC) diversity is well known to be optimum in the sense of maximizing the output signal-to-noise ratio (SNR). If the desired signal s affected by both co channel interference (CCI) and flat fading, the diversity combining technique that maximizes the output signal-to-interference pulse noise ratio (SINR) is the so called optimum combining (OC). However, OC is much more complex than MRC and typically requires information about the CCI that may not be available at the receiver. Thus, in practice many wireless systems will use MRC even in the presence of CCI .The transmit antenna array can also be used to provide diversity gain, and the optimum technique under background noise is Maximal Ratio Transmission (MRT), equivalent to MRC. MIMO systems employing both MRT and MRC are usually referred to as MIMO MRC. Various transmit diversity techniques have been proposed in the open literature, delay transmit diversity scheme [3] and transmit diversity is a simple but effective scheme proposed by Alamouti.However, these transmit diversity techniques were built on objectives other than to maximize the SNR. That is, they are suboptimum in terms of SNR performance. Accordingly, the frame work of maximum ratio Combining (MRC) will be established here in terms of concept and principles[5]. It is well known that maximal-ratio combining (MRC) [6] is the optimal linear combining technique. However, with receiver MRC, most of the system complexity concentrates at the receiver side. To decrease the receiver complexity in terms of the number of RF chains, a simple suboptimal combining scheme, referred to as selection combining (SC), was proposed, in which only one receive antenna with the largest signal-tonoise ratio (SNR) is selected for demodulation. The SC scheme has been extended to the cases where the signals on more than one receive antenna with the largest instantaneous SNRs are combined [8]. This scheme is referred to as maximal-ratio combining .MRC is a powerful technique. It is most common in SIMO channels. This paper presents the concept, principles, and analysis of maximum ratio transmission for wireless communications, where multiple antennas are used for both transmission and reception. The principles and analysis are applicable to general cases, including maximum-ratio combining. Simulation results agree with the analysis. Analysis includes simulated result for the no of receiving channel VsEb/N0, BER of different modulation schemes for MRT-MRC, providing a performance comparison of systems.

***SECTION V*: DATA ENCRYPTION AND DECRYPTION**

In a simplest form, encryption is to convert the data in some unreadable form. This helps in protecting the privacy while sending the data from sender to receiver. On the receiver side, the data can be decrypted and can be brought back to its original form. The reverse of encryption is called as decryption. The concept of encryption and decryption requires some extra information for encrypting and decrypting the data. This information is known as key. There may be cases when same key can be used for both encryption and decryption while in certain cases, encryption and decryption may require different keys.

Generally, cryptography method are used encrypt and decrypt the data for secured transmission. This method are used secret key and public key for encrypt and decrypt the data. In our system, we use secret key of deffie-hellman algorithm for secured data transmission.

Diffie-hellman was originally designed for key exchange. deffie-Hellman cryptosystem, two parties create asymmetric session key to exchange data without having to remember or store the key for future use. They do not have to meet to agree on the key ; it can be dome through the internet. Let us see how the protocol works when alice and bob need a symmetric key to communicate. Before establishing a symmetric key, the two parties need to choose tow number p and g. the first number, p, is a large prime number on the order of 300 decimal digits(1024 bits). The second number is a random number. These two numbers need not be confidential. They can be sent through the internet; they can be public. The diagrammatic representation are,



Steps are:

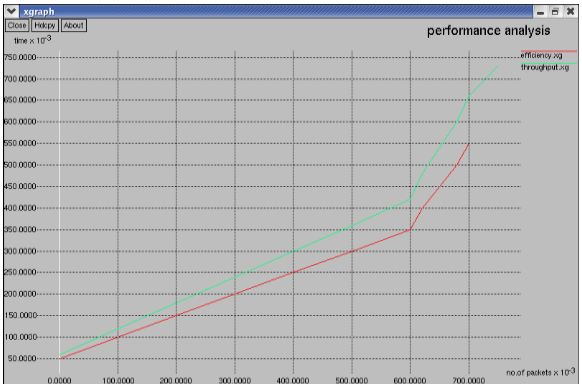
1. Alice chooses a large random number x and calculate $R_1=g^x \bmod p$.
2. Bob chooses a large random number y and calculates $R_2=g^y \bmod p$.
3. Alice sends R_1 to bob. Note that alice does not send the values of x; she sends only R_1.
4. Bob sends R_2 to alice. Note that alice does not send the values of y; she sends only R_2.
5. Alice calculate $K=(R_2)^x \bmod p$.
6. Bob also calculates $K=(R_1)^y \bmod p$.

The symmetric key for the session is K. $(g^x \bmod p)^y \bmod p=(g^y \bmod p)^x \bmod p=g^{xy} \bmod p$

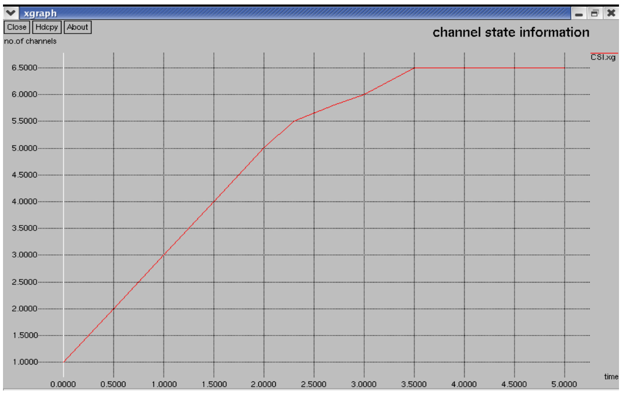
These are process of key distribution from sender to receiver. This providesecure transmission of data from sender to receiver.

***SECTION VI*: SIMULATION RESULT**

This picture represent the throughput and efficiency of the proposed system.



This picture represent the channel state information of the proposed system.



***SECTION VII*: CONCLUSION**

In proposed system the transmit antenna selection with maximal-ratio combining (TAS/MRC) is adopted in user-destination and relay-destination links where a single transmit antenna that maximizes the instantaneous received signal-to-noise ratio is selected and fed back to transmitter by receiver and all the receive antennas are combined with MRC. In practice, the signal-to-noise ratios (SNRs) of all branches need to be known for optimal antenna selection. However, it is indeed challenging to know these SNRs when there is only one radio frequency (RF) chain at the transmitter.To thoroughly assess the secrecy performance achieved by the proposed scheme, we derive new closed-form expressions for the exact secrecy outage probability and the probability of non-zero secrecy capacity for arbitrary SNRs.

REFERENCES

[1]. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 74–80, Oct. 2004.

[2]. M. Xiao and M. Skoglund, "Multiple-user cooperative communications based on linear network coding," *IEEE Trans. Commun.*, vol. 58, no. 12, pp. 3345–3351, Dec. 2010.

[3]. Zhang, N. B. Mehta, A. F. Molisch, J. Zhang, and H. Dai, "Asynchronous interference mitigation in cooperative base station systems," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 155–165, Jan. 2008.

[4]. X. Li, T. Jiang, S. Cui, J. An, and Q. Zhang, "Cooperative communications based on rateless network coding in distributed MIMO systems,"*IEEEWireless Commun.*, vol. 17, no. 3, pp. 60–67, Jun. 2010.

[5]. H.-Q. Lai and K. J. R. Liu, "Space-time network coding,"*IEEETrans.SignProcess.*, vol. 59, no. 4, pp. 1706–1718, Apr. 2011.

[6]. K. Xiong, P. Fan, T. Li, and K. B. Letaief, "Outage probability of spacetime network coding over Rayleigh fading channels," *IEEE Trans. Veh.Technol.*, vol. 63, no. 4, pp. 1965–1970, May 2014.

[7]. Z. Chen, J. Yuan, and B. Vucetic, "Analysis of transmit antenna selection/maximal-ratio combining in Rayleigh fading channels," *IEEETrans. Veh. Technol.*, vol. 54, no. 4, pp. 1312–1321, Jul. 2005.

[8]. M. Jankiraman, *Space-Time Codes and MIMO Systems*. Boston, MA, USA: Artech House, 2004.

[9]. N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Multiuser MIMO relay networks in Nakagami-*m* fading channels," *IEEE Trans. Commun.*,vol. 60, no. 11, pp. 3298–3310, Nov. 2012.

[10]. Kai Yang, Nan Yang, Jinsong Wu," space time network coding with transmit antenna selection and maximal ratio combing"IEEE Tans. On Wireless Communication, vol 14.no 4, April 2015.