ENHANCEMENT OF SECURITY AND RELIABILITY WITH MIMO COMMUNICATION FOR THE SMART GRID

by

AMIT ABHIMANYU DEOKAR

Presented to the Faculty of the Graduate School of
The University of Texas at Arlington in Partial Fulfillment
of the Requirements
for the Degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

THE UNIVERSITY OF TEXAS AT ARLINGTON
May 2013

Acknowledgements

I would like to express my greatest gratitude Dr. Qilian Liang for his continuous support for the thesis, from initial advice and contacts in the early stages of conceptual inception and through ongoing advice and encouragement to this day. I am thankful to him for guiding me to the wireless communication field.

I would like to thank Dr. Davis and Dr. Gibbs for serving on my thesis advisory committee.

I am thankful to Xin Wang and Dr. Ioannis Schizas, for their suggestions and patience in answering all my questions which helped me in successfully completing my work.

I would like to express my greatest gratitude to the people who have helped and supported me throughout my research.

I wish to thank my parents for their undivided support and special thanks to my sister Pradnya Deokar-Nagane who inspired me and encouraged me to go my own way, without her it would have been difficult to complete my thesis.

April 18, 2013

Abstract

ENCHANCMENT OF SECURITY AND RELIABILITY WITH MIMO COMMUNICATION FOR THE SMART GRID

Amit Deokar, M.S

The University of Texas at Arlington, 2013

Supervising Professor: Dr. Qilian Liang

In smart grid applications, developing appropriate wireless communication architecture is extremely important as wireless communication faces security and reliability challenges. To combat severe communication impairment induced by invader, it is proposed to implement space-time block coding over virtual MIMO. With an increment of diversity in virtual MIMO, BER performance has been improved by 18dB. Furthermore, with more redundant copies of transmitted signals at receiver, reliability of system has increased by 4 times in 4x1 V-MIMO and by 8 times in 8x1 V-MIMO than traditional SISO case.

Security challenges from malicious additive attack and data piracy have been examined. Simulations show that malicious attack could be effectively mitigated using space time block coding. It has been verified that more virtual sources will give more diversity gain and better performance. Simulation also shows that data piracy is a very severe problem and cannot be alleviated by space time block code only. Hence, concluded that if the attacked smart meter could be detected, performance could be improved. Finally, studies also showed that, in link failure scenario, the space-time block coding could provide satisfying performances with a low-complexity in design.

Extensive numerical studies with use of link adaptation technique and channel coding were also performed under similar attack scenarios which provide forward error correction. Simulations indicate that, even if attacks were very severe, bit-error-rate (BER) performance has been improved by 15 to 25 dB.

Table of Contents

List of Illustrations

List of Tables

List of Acronyms

Ant	Antenna
AWGN	Additive White Gaussian Noise
BCJR	Bahl-Cocke-Jelinek-Raviv algorithm
BER	Bit Error Rate
BPSK	Binary Phase Shift Key
CSI	channel state information
EPRI	Electric Power Research Institute
fd	Doppler Frequency
FEC	Forward Error Correction
LSB	Least significant bit
MAP	Maximum a posteriori probability
MIMO	Multiple Input Multiple Output
MISO	Single Input Multiple Output
ML	Maximum Likelihood
MRC	Maximum Ration Combining
MSB	Most significant bit
PSK	Phase Shift Key
SIMO	Multiple Input single Output
SISO	Single Input Single Output
SNR	Signal to Noise Ratio
STBC	Space Time Block Coding

Chapter 1

Introduction

1.1 Smart grid

Smart grid is an integration of information technology and advanced communications into the power system. It attempts to predict and intelligently respond to the behavior and actions of all electric power users in order to deliver efficient, reliable, economic, and sustainable electricity services. Like every complex system, smart grid also has vulnerabilities and security challenges.

Serious concerns have been raised regarding to whether or not smart grid can resist attacks and heal itself without causing infrastructure and equipment damages or large-scale blackouts [1]. As mentioned in smart grid cyber security report of Electric Power Research Institute (EPRI) [2], one of the most challenging tasks facing the smart grid development is the cyber security of systems. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software and alter load conditions to destabilize the grid in unpredictable ways. As a critical infrastructure element, smart grid requires the highest levels of security.

On the demand-side, old metering data recorded hourly or monthly is replaced by a smart meter that collects data every minute [3]. Smart meter, as a kind of sensor, could allow for real-time determination and information storage of energy consumption, and provide the possibility to read consumption both locally and remotely. Further, smart meters provide means to detect fluctuations, power outage at home, two-way low electricity and real-time information. They also permit the meters to be switched off. This results in important cost saving and enables utilities to prevent electricity theft.

Smart meters have unintended consequences for customer privacy. Energy utility information stored at the meter and distributed thereafter acts as an information-rich side channel, exposing customer habits and behaviors [4]. Hackers who maliciously attack a meter can immediately manipulate their energy meter reading, sabotage the real-time communication between the smart meter and local central system and finally turn it into profits. Even without malicious attacks, the link between smart meter and central system could fail unintentionally. Ensuring the secure and reliable communication between smart meter and the central system is of great importance.

The study on physical layer secure communications was pioneered by Shannon and Wyner. Shannon introduced the information-theoretic framework for studying secrecy in communications [5]. Wyner [6] developed the concept of secrecy on achievable information rate pairs. One cannot hope to ensure security without some cooperation between the transmitter and receiver [7]. One of the most common forms of cooperation is the use of a code [8] to encrypt each date stream transmitted which can only be decoded at the receiver using a private shared key. One can refer to this method as single-channel temporal data encryption. Channel coding, such as Turbo coding and LDPC coding fall into this category. Another common form of cooperation is to adopt information-hiding measures to prevent unauthorized detection of any signaling activity [9]. A well-known example is spread-spectrum modulation for wireless channels, which hides the spectral signature of the signal in the broad-band noise background.

1.2 Outline

This thesis takes a different point of view from previous works in which the security and reliability challenges are addressed in the specific context of smart grid. In this thesis the main focus is on the real-time communication between the smart meter and central system in smart grid. To combat severe communication impairment induced by additive malicious attacks, data piracy or link failures, implementing space-time coding at the transmitter and/or multiple antennas at the receiver has been proposed. First, the security challenge from malicious attacks has been investigated. The BER performance under different kinds of malicious attacks is evaluated. Then BER performance under Data piracy case is demonstrated. Reliability challenge from link failure is then considered. Later part of the thesis contains extensive numerical studies on the multiple-link attack, the multiple-link failure and the receiver with detection scenarios.

All scenarios mentioned above are also compared under various cases such as LOS and non-LOS, channel coding and Link adaptation techniques. Their respective effects on performance of the system are also studied.

Chapter 2

MIMO wireless communication

2.1 Introduction

A decade ago, a person has to sit on chair in front of a big personal computer with RJ-45 cable connected to it, to check emails or to access internet which has very limited mobility across the monitor. But now it can be done through less than 4.87 inches length, less than 2.31 inches width and which weighs less 3.95 ounces which can fit in your pocket. That device is called a cell phone. The mobility has now increased from few meters to infinite distance. All this was possible because of wireless technology. Although wired communication brings more stability, better performance, and higher reliability, it comes with the necessity of being restricted to a certain location or a bounded environment.

Recent advances in wireless communication systems have increased the throughput and reliability. Though various wireless applications have different specifications and technologies, most of them face similar challenges. Some of the challenges in wireless communications are[10]

- High data rate;
- Quality of service;
- Mobility;
- Connectivity in wireless networks;
- Interference from other users;
- Privacy or security.

The priorities of the different challenges in wireless communications are dependent on different applications. For example, mobile subscriber will have more priority to quality of service than high data rate and service provider to mobile customer will face more issues related to mobility as customer will be moving from 0.5 mph to 80mph.

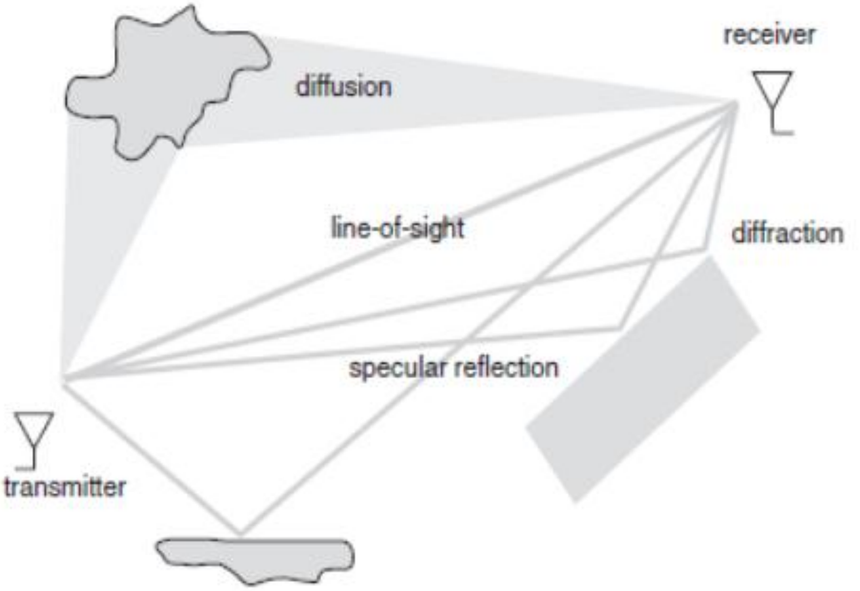

Figure 2-1 A multiple reception scenario [10]

As shown in Figure 2-1, at receiver, multiple paths can result in either different versions of transmitted signal at different time or combined together at the same time. Each path experiences different path loss and phases. Since AWGN model cannot be described as a wireless channel, it is very important to find other models that represent the channel.

2.2 Wireless channel

Wireless channels can be distinguished by their unique properties of propagation mechanisms and their combination. Received signal power can be reduced in different ways. There are two separate aspects of such a power reduction. One is the large-scale effect which corresponds to the characterization of the signal power over large distances or the time-average behaviors of the signal. Second aspect is the rapid change in the amplitude and power of the signal, this is called small-scale fading, or fading. It relates to the characterization of the signal over short distances or short intervals of time.

2.2.1 Path Loss Model

As the name indicates, this model demonstrates propagation losses caused by the natural expansion of radio waves in free space and losses caused by the signal when it passes through a medium. It is a deterministic propagation loss model and determined by empirical measurements in specific areas.

$$\frac{\Pr(d)}{\Pr(d0)} = \left(\frac{d}{do}\right)^{-\beta} .$$

Where,

Pr (d) is power received by receiver from distance d.

Pr(do) is power received by receiver from distance do.

β is path loss exponent.

From the equation, the power received is indirectly proportional to the distance from the transmitter. Also it decays with the power of β. β is equal to 2 in case of free space propagation and 4 in case of two ray propagation model. Typically it has a value from 3 to 5 for urban propagation environment model.

2.2.2 Large scale fading

Large scale fading is caused by variation of the signal strength for an arbitrary transmitter-receiver separation over a long distance, for example 10≈ 100λc. Shadowing is a propagation model which accounts for signal changes due to the peculiarities of the particular environment surrounding the transmitter or the receiver or both. Shadowing happens at a faster time-scale when compared to path loss, but slower compared to multi-path. Shadowing usually accounts for losses due to absorption by the local surrounding media such as trees and buildings for example. Shadowing model provides correction to deterministic path loss model. It is empirically determined by the field measurements and helps to translate rough cell plans into statistical measures of services.

2.2.3 Small scale fading

Small-scale fading is caused by the interference between more versions of the transmitted signal which arrive at the receiver at slightly different times. These signals, called multipath waves, combine at the receiver antenna. This resulting signal can vary widely in amplitude and phase.

Many factors influence small scale fading, such as

- ➢ Multipath propagation
- ➢ Relative velocity
- ➢ Transmission bandwidth of the signal

- Doppler shift

Apparent change in frequency due to the relative velocity between transmitter and receiver is called Doppler shift. Doppler spreading also consists of multipath components which arrive at receiver from different directions.

- Delay spread

Delay spread is a natural phenomenon caused by reflected and scattered propagation paths in radio channels. Delay spread can be derived in relation to coherence bandwidth. Coherence bandwidth is a statistical measure of the range of frequencies over which the channel can be considered as ‘flat’.

Depending on the relation between the signal parameters and channel parameters, different transmitted signals will undergo different types of fading.

1. Flat fading

When bandwidth of the signal is less than bandwidth of the channel or Delay spread of channel is less than transmitted symbol period, flat fading occurs.

2. Frequency selective fading

When bandwidth of the signal is greater than bandwidth of the channel or Delay spread of channel is greater than transmitted symbol period, frequency selective fading occurs.

3. Slow fading

When channel variations is slower than baseband signal variations i.e. coherence time is greater than transmitted symbol period, slow fading occurs.

4. Fast fading

When channel variations is faster than baseband signal variations i.e. coherence time is less than transmitted symbol period, fast fading occurs.

2.2.3.1 Rayleigh fading channel

To describe flat fading signal or multiple path component received from channel, Rayleigh distribution is commonly used. Envelope of the sum of two quadrature Gaussian noise signals obeys Rayleigh distribution. Let A and B be the “in phase” and “quadrature random variable” terms for the signal envelope you received. Rayleigh distribution probability density function can be given by

$$f_R(r) = \frac{r}{\sigma^2} \exp\left(\frac{-r^2}{2\sigma^2}\right), \quad r \geq 0,$$

where σ^2 is the variance of the random variables A and B. The received power, is an exponential random variable with a pdf:[10]

$$f(x) = \frac{1}{2\sigma^2} \exp\left(\frac{-x}{2\sigma^2}\right), \quad x \geq 0.$$

2.2.3.2 Ricean fading channel

In a flat fading channel, if in addition to random multiple paths, a dominant stationary component exists, the Gaussian random variables A and B are not zero mean anymore. This, for example, happens when a LOS path exists between the transmitter and the receiver. In this case, the distribution of the envelope random variable R is a Ricean distribution with the following pdf [10]:

$$f_R(r) = \frac{r}{\sigma^2} \exp\left(\frac{-(r^2 + D^2)}{2\sigma^2}\right) I_0\left(\frac{Dr}{\sigma^2}\right), \qquad r \geq 0,\ D \geq 0,$$

where D denotes the peak amplitude of the dominant signal and $I_0(.)$ is the modified Bessel function of the first kind and of zero-order. As expected, the Ricean distribution converges to a Rayleigh distribution when the dominant signal disappears, i.e. $D \rightarrow 0$.

2.3 Channel coding

Various channel impairments such as noise, interference and channel fading which affects transmitted signals can degrade the performance of the system. Signal processing technique such as channel coding which accommodates information with some compromises, can improve performance. BER versus bandwidth and Power versus bandwidth are some compromises. By accepting one these compromises, a design can be made to achieve the desired performance.

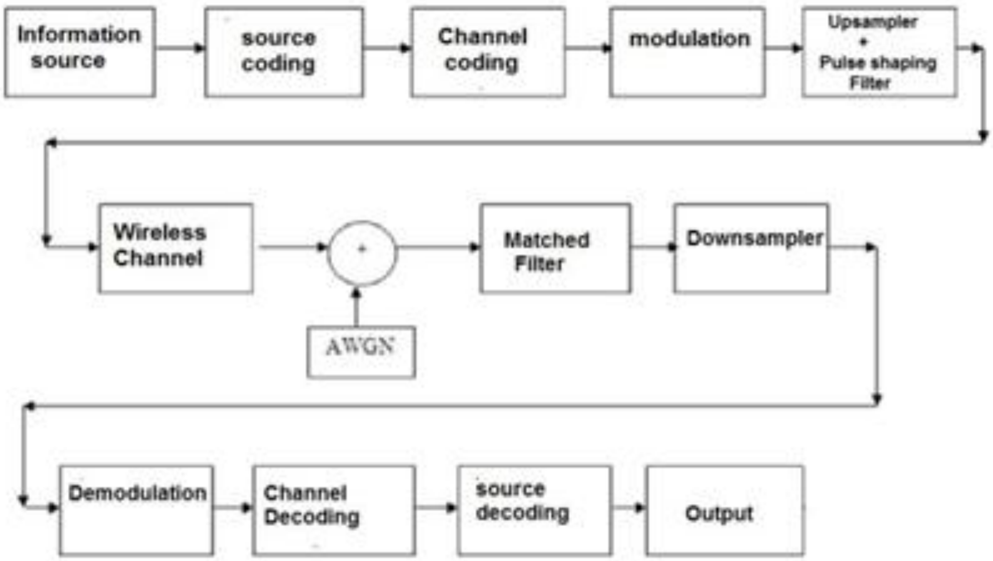

Figure 2-2 Block diagram of basic wireless communication system

There are different types of coding present to achieve these goals. For example, block coding, convolutional coding, turbo coding and etc. To secure a data for smart grid, convolutional and turbo coding are implemented.

2.3.1 Convolutional coding

Convolutional coding is a forward error control code. Because of its high process gain and better error controlling capabilities than block coding, it is used in speech coding or voice communication. Convolutional codes operate on serial data and few bits at a time. Convolutional encoding with Viterbi decoding is a FEC technique that is particularly suited to a channel in which the transmitted signal is corrupted mainly by channel fading and AWGN.

2.3.1.1 Convolutional encoder

Convolutional codes are usually described using two parameters: the code rate and the constraint length. The code rate (k/n) is a ratio of the number of information bits into the encoder (k) to the number of channel symbols output by the convolutional encoder (n). The m parameter is the memory length of the encoder.

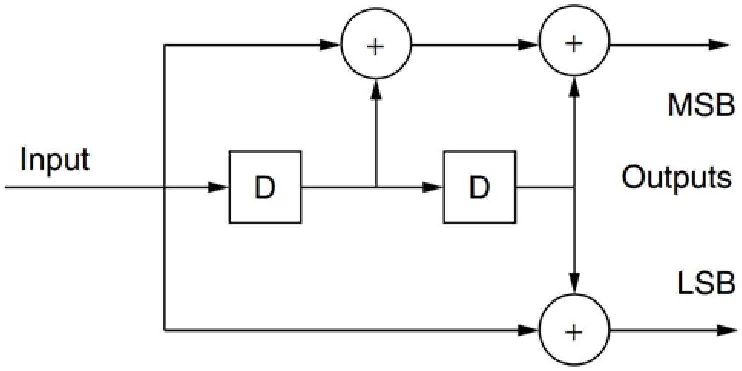

Figure 2-3 Convolutional Encoder [14]

In this thesis, k=1, n=2 and m =(7,5) are used. In this encoder, data bits are provided at a rate of k bits per second. Channel symbols output are at a rate of n = 2k symbols per second. The octal numbers 7 and 5 represent the code generator polynomials, which when read in binary are 1112 and 1012 that correspond to the shift register connections to the upper and lower modulo-two adders, respectively.

2.3.1.2 State table

State Table is a state transition table. Table 1 indicates data bit which indicates how input bits can change the memory states.

Table 1 State Table of convolutional code

	OUTPUT OF ENCODER	
Current State	When **Input = 0**	When **Input = 1**
00	00	01
01	10	11
10	00	01
11	10	11

2.3.1.3 State diagram

As convolutional codes are finite state machines, it can provide considerable insight into the behavior of codes. With presentational state diagram, quick insight of transition can be made. As shown in Figure 2-4, the states are labeled so that the least significant bit is the one residing in the leftmost memory element of the shift register. The branches are labeled with the 1-bit (single-bit) input and the 2-bit output are separated by a comma. The most significant bit (MSB) of the two-bit output is the bit labeled MSB.

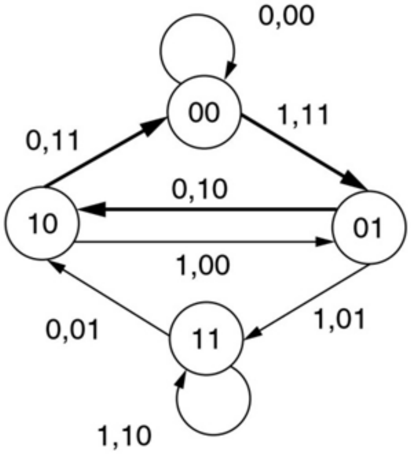

Figure 2-4 Sate diagram of convolutional code

Feed-forward convolutional codes are used. It has finite impulse response which results in high processing gain and easy to decode. Though performance with feedback convolutional coding is much better than feed-forward, it is more complex.

2.3.1.4 Trellis description of a convolutional code

Trellis diagram is one of the best ways to describe transition of encoder state at various inputs. The encoder in Figure 2-5 has four states (numbered in binary from 00 to 11), a one-bit input and a two-bit output. Each solid arrow shows how the encoder changes its state if the current input is zero and each dashed arrow shows how the encoder changes its state if the current input is one. The octal numbers above each arrow indicate the current output of the encoder.

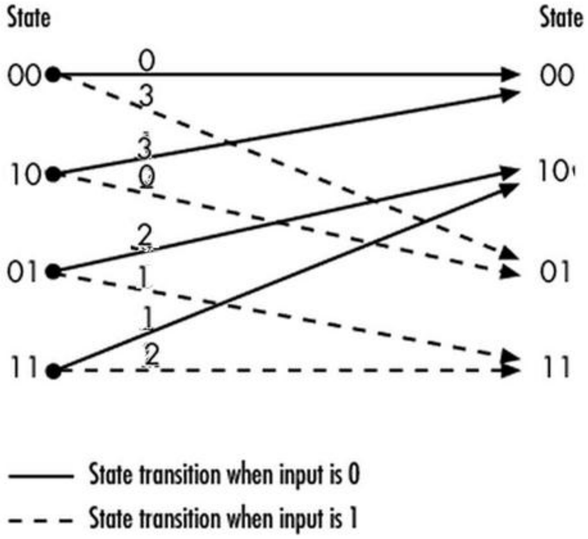
State
State
00
10
01
11
00
10
01
11
0
3
3
0
2
1
1
2
State transition when input is 0
State transition when input is 1

Figure 2-5 Trellis diagram of convolutional code

As an example of interpreting this trellis diagram, if the encoder is in the 10 state and receives an input of zero, it outputs the code symbol 3 and changes to the 00 state. If it is in the 10 state and receives an input of one, it outputs the code symbol 0 and changes to the 01 state.

2.3.1.5 Viterbi decoding

Viterbi originally described the decoding algorithm that bears his name in 1967 [13]. Forney's work [14,15] introduces the trellis structure and showing that Viterbi decoding is maximum-likelihood in the sense that it selects the sequence that makes the received sequence most likely.

The Viterbi algorithm is used for decoding convolutional codes. Basically it computes the path metrics from the received sequence to the possible transmitted sequences. The number of stages in the trellis will grow exponentially with the number of trellis paths. Viterbi algorithm takes advantage of the fact that the number of paths truly in contention to have the minimum distance is limited to the number of states in a single column of the trellis, assuming that ties may be arbitrarily resolved.

As an example of the Viterbi decoding algorithm, consider binary symmetric channel which has bit error probability less than 0.5 For this example, assume the encoder of shown in Figure 2-3 with the state diagram in Figure 2-4 and the trellis of Figure 2-5. It is assumed that encoder begins in state 00. Figure 2-6 illustrates the basic Viterbi algorithm for the received sequence is 01 01 10. At first, the only active state is 00. The circle representing this state contains a path metric of zero. Branch metrics label each branch, indicating the Hamming distance between the received symbol and the symbol transmitted by traversing that branch in the encoder. The path metric for each destination state is calculated by the sum of the branch metric for the incident branch and the path metric at the root of the incident branch.

Eventually only the path with the minimum path metric will survive . For example, state 00 (the top state) in the fourth column has a path incident from state 00 in the third column with a path metric of 2+1 = 3. It also has a path incident from state 10 in the third column with a path metric of 3+1 = 4. Only the path with the smaller path metric needs to survive. Figure 2-6 shows the incident branches of survivor paths with thicker arrows than non-survivor paths. Finally, each state in the last column will have exactly one survivor path and the values shown indicate the path metrics of the survivor paths.

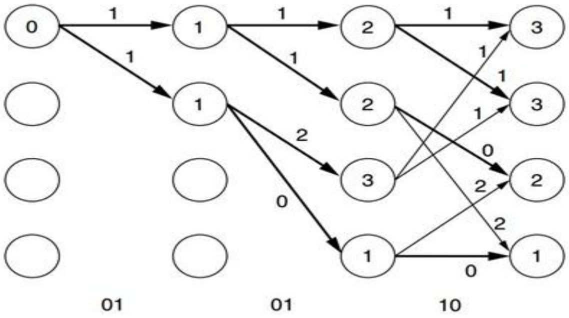

Figure 2-6 Viterbi Decoding for static channel

After all received symbols have been processed, the final step in decoding is to examine the last column and find the state containing the smallest path metric. Reference to Figure 2-6 reveals that the maximum likelihood path is the state trajectory 00 →01 → 11 →11, which differs in exactly one bit position from the received sequence as indicated by its path metric. The input information sequence is decoded to be 1 1 1.

2.3.1.6 Hard versus Soft Decoding

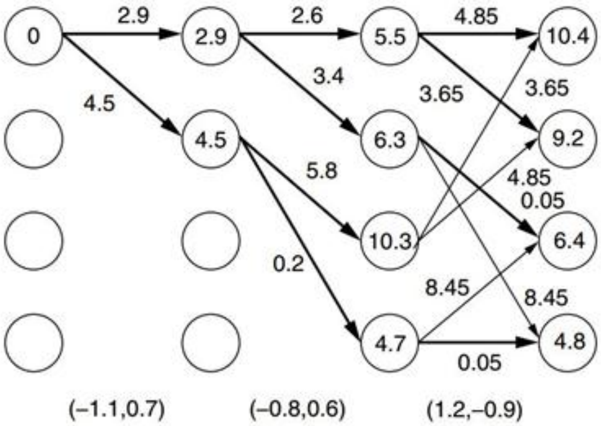

Figure 2-7 Soft Viterbi decoding

In previous section, binary symmetric channel is assumed. But for the AWGN channel, binary phase shift keying (BPSK) represents binary 1 with 1 and binary 0 with

−1. These two transmitted values are distorted by additive Gaussian noise, so that the received values will typically be neither 1 nor −1.

Each received values can be quantized to closest of 1 or -1 and assign the appropriate binary value. This method of decoding is called hard decoding, because the receiver makes a binary (hard) decision about each bit before Viterbi decoding. Hard decoding performs worse by about 2 dB than a more precise form of Viterbi decoding known as soft decoding. Soft decoding passes the actual received values to the Viterbi decoder. These actual values are called soft values because hard decisions (binary decisions) have not been made to Viterbi decoding. Soft Viterbi decoding is very similar to hard decoding, but branch and path metrics, as shown in Figure 2-7, use squared Euclidean distance rather than Hamming distance.

2.4 Diversity

Due to sudden declines in the power because of the destructive nature of propagation media, usually minimum received SNR is set for which the receiver can reliably detect and decode the transmitted signal. If the received SNR is lower than such a threshold, a reliable recovery of the transmitted signal is impossible. This is called “outage.” The probability of outage can be calculated based on the statistical model that models the channel or based on the actual measurements of the channel.

Diversity provides different replicas of the transmitted signal to the receiver by means of adding redundancy in transmitter or receiver side. Possibility of these different replicas fading independently will be very less. So receiver can decode the transmitted signal using these received signals.

Based on how replicas of the transmitted signal are provided at the receiver, types of diversity have been distinguished.

The following classes of diversity schemes can be identified:

- Time diversity: Multiple versions of the same signal are transmitted at different time instants.
- Frequency diversity: The signal is transmitted using several frequency channels or spread over a wide spectrum.
- Space diversity: The signal is transmitted over several different propagation paths for example via multiple wires or by using multiple transmitter antennas and/or multiple receiving antennas.
- Polarization diversity: Multiple versions of a signal are transmitted and received via antennas with different polarization.

2.4.1 *Impact to performance*

Let’s assume D is diversity order which is nothing but number of effectively independent replicas at the receiver. So the probability bit error for single path reception can be defined as [10]

$$P_b \overset{\text{def}}{=} K \left[\frac{E_b}{N_0}\right]^{-1} \tag{2-1}$$

With number reception, more independent paths will improve performance of system by diversity gain D.[10]

$$P_b \overset{\text{def}}{=} K \left[\frac{E_b}{N_0}\right]^{-D} \tag{2-2}$$

It can be concluded that with diversity (D) the performance will improve by order of D i.e. number of independent receptions at receiver. It can also be proven that with more number of copies of reception the channel can be made to seem like a static channel.

For example, let’s assume two independent paths[10]

$$r_1(u,t) = g_1(t) \,.\, s_1(t) + n_1(u,t)$$

$$r_2(u,t) \; = \; g_2(t) \,.\, s_1(t) \; + \; n_2(u,t)$$

(2-3)

After combining this two independent paths will get

$$= \left(\frac{g_1(t) + g_2(t)}{2}\right) s_1(t) \; + \; \left(\frac{n_1(t) + n_2(t)}{2}\right)$$

(2-4)

$\left(\frac{g_1(t)+g_2(t)}{2}\right)$ = addition of channel random variable

According to the above term, as the number of reception paths increase or diversity channel, random channels can act as a static channel or a deterministic channel.

Also,

$\left(\frac{n_1(t) + n_2(t)}{2}\right) = \mathit{Addition\ of\ two\ gaussian\ random\ variable}$

With addition of two or more Gaussian random variables at the reception of same mean value and variance , that value will act as deterministic value as the number of independent paths increase. So with term at (2.4) , that random process r(u,t)   will have lesser variance results and better performance after reception determination.

2.5 Combining methods

It very important to combine these copies efficiently which gives less variance results and better performance. Various methods of combining at receiver are as follows,

2.5.1 Selection combining

In this combining method only the path which has maximum signal energy or SNR value irrespective of considering other branches or independent paths is selected. Selection diversity is easy to implement. For this type combining method, a side monitoring station and an antenna switch at the receiver is needed. However, it’s not optimal diversity technique because it does not use all the possible branches simultaneously.

2.5.2 Maximum ratio combining

In maximal ratio combining, the path r_i from each of the independent path are co-phased to provide coherent addition and individually weighed to provide optimal SNR. Maximal ratio combining can produce a result or decision output SNR equal to individual SNRs. Thus this combining method has the ability to produce an acceptable SNR even when no other individual signals are acceptable. This method uses maximum likelihood decision method for an output.

Let's assume 3 independent paths at receiver. i.e. $r = [r_1 , r_2 , r_3]$

Combined PDF of this received signals can be stated as follows

$$P(r_1, r_2, r_3) = \prod_{i=1}^{N} \aleph \left(m_i, \frac{N_0}{2}\right)$$

Where $m_i = g_i . s_i$

Mean value m_i can be determined by the channel gain of each individual reception.

So final decision can be made as follows

$$\max_{i=1,2,3} P(r_1, r_2, r_3 \;/\; S_i) = \prod_{i=1}^{N} \aleph \left(m_i, \frac{N_0}{2}\right)$$

Where Si indicates number of possible symbols for given modulation techniques.

At different values of S maximum probability for a particular received vector which is also called maximum likelihood decision method is found. This method gives the best statistical reduction of fading known as linear diversity combiner.

2.5.3. Equal gain combining

In most cases, it is not convenient to provide for weighting variable capabilities required for true maximal ratio combining. In such cases, the path weights are all set to unity and signals from each branch are co-phased to provide equal gain combining diversity.

2.6 MIMO

Wireless communication using multiple-input multiple-output (MIMO) systems enables increased spectral efficiency for a given total transmit power. Increase in capacity is achieved by introducing additional spatial channels that are exploited by using space-time coding.

A typical MIMO system can be described as shown in the Figure 2-8below.

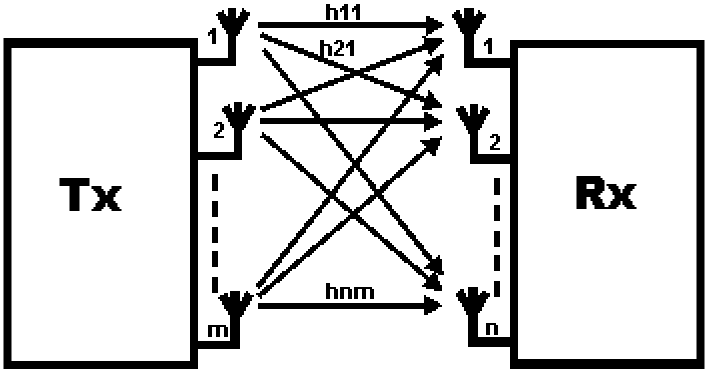

Figure 2-8 MIMO communication [17]

Implementation of MIMO can be sub-divided into three main categories, pre-coding, spatial multiplexing or SM and diversity coding.

1. Pre-coding:

It is basically spatial processing that occurs at the transmitter. The same signal is emitted from each of the transmitting antennas with appropriate phase weighting such that the signal power is maximized at the receiver input. The benefits of pre-coding is to increase the received signal gain, by making signals emitted from different antennas add up constructively and reduce the multipath fading effect. Pre-coding requires knowledge of channel state information (CSI) at the transmitter.

2. Spatial multiplexing:

In spatial multiplexing, a high rate signal is split into multiple lower rate streams and each stream is transmitted from a different transmitting antenna in the same frequency channel. If these signals arrive at the receiver antenna array with sufficiently different spatial signatures, the receiver can separate these streams into parallel channels. Spatial multiplexing is a very powerful technique for increasing channel capacity at higher signal-to-noise ratios (SNR). Spatial multiplexing can be used with or without transmit channel knowledge.

3. Diversity decoding:

In diversity methods, a single stream is transmitted, but the signal is coded using technique called space-time coding. The signal is emitted from each of the transmit antennas with full or near orthogonal coding. Diversity coding exploits the independent fading in the multiple antenna links to enhance signal diversity.

2.7 Spatial multiplexing gain and its trade-off with diversity

In MIMO, diversity gain can be achieved by using both the transmitted and receive antennas. However, multiple transmitted antennas can be used to increase higher capacity. Instead of sending same information through all transmitter antennas, each antenna can send different information which results in increase in capacity by number of transmitter antennas. Therefore, the advantage of a MIMO channel can be utilized in two ways:

(i) To increase the diversity of the system.

(ii) To increase the number of transmitted symbols.

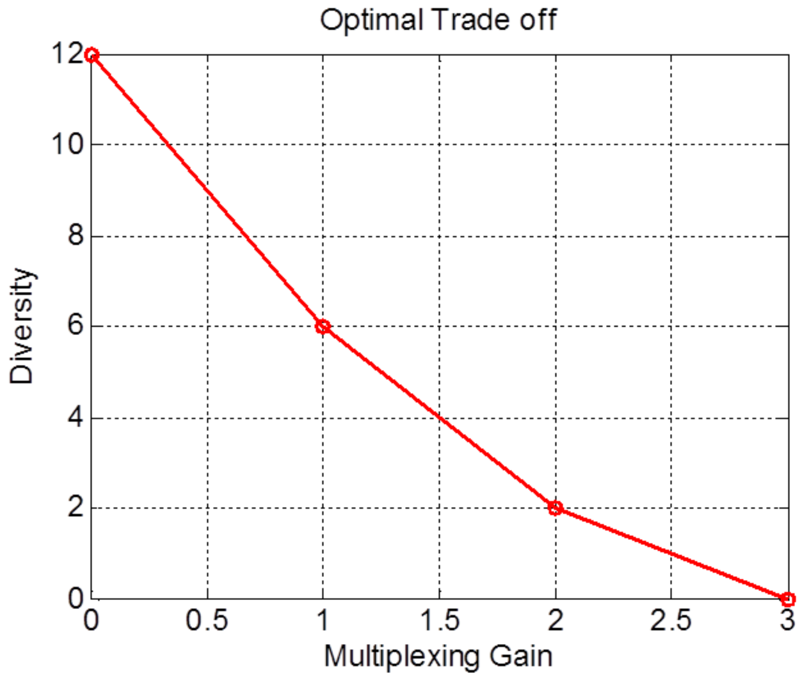

Figure 2-9 Optimal trade off in MIMO [10]

As shown in Figure 2-9, there is a clear tradeoff between diversity and multiplexing gain or capacity. Depending on the application, an optimal point can be chosen to satisfy requirements of customers.

So to analyze overall data rate for MIMO system, MIMO should decompose into parallel fashion.

$$Y = H.X + N$$

$$\begin{bmatrix} y1 \\ y2 \\ \vdots \\ \vdots \\ yr \end{bmatrix} = \begin{bmatrix} h11 & \cdots & \cdots & h1t \\ h21 & \cdots & \cdots & h2t \\ \vdots & & & \vdots \\ \vdots & \cdots & \cdots & \vdots \\ hr1 & & & hrt \end{bmatrix} \begin{bmatrix} x1 \\ x2 \\ \vdots \\ \vdots \\ xt \end{bmatrix} + \begin{bmatrix} n1 \\ n2 \\ \vdots \\ \vdots \\ nr \end{bmatrix}$$

. (2-5)

$$y_i = \sum_{n=1}^{Mt} (h_{ij} . x_j) + n_i \quad \Longrightarrow \quad y_i = h_i . x_i + n_i$$

Where Y is receiver matrix , X is transmitter matrix and H is channel matrix of MIMO. Where column indicates the number of transmitter and rows indicates the number of receiver.

After decomposition of the above equation (2.5) by converting H matrix into diagonal form using matrix factorization. After factorization, the new gain of MIMO will be (rXR).

Where r is rank of matrix H and R is number of receivers. If H is a full rank matrix, which is possible in rich scattering environment, then

$$\text{Rank of (H)} = \min(\text{Mt}, \text{Mr})$$

So it is very crucial to design matrix to make sure to achieve desired diversity gain and multiplexing gain. This can be achieved using space time block coding.

Chapter 3

Space Time Block Coding

3.1 Introduction

For simplicity, let's consider a communication system, where *N* signals are transmitted from *N* transmitters simultaneously. The signals are the inputs of a multiple-input multiple-output (MIMO) channel with *M* outputs i.e. *M* receivers. The coefficient $\alpha_{n,m}$ is the path gain from transmit antenna *n* to receive antenna *m*. Based on this model, the signal $r_{t,m}$, which is received at the time *t* at antenna *m*, is given by[10]

$$r_{\ t,m} = \sum_{n=1}^{N} \alpha_{n,m} \mathbf{c}_{t,n} + \eta_{t,m}, \qquad \text{(3-1)}$$

Where $\eta_{t,m}$ is the noise received by the receive antenna *m* at time *t*. Each of these replicas of the transmitted signals from the transmit antennas are added to the signals of each of the receive antennas.

To form a more compact input-output relationship, let's form a matrix of signals that are transmitted from *N* transmit antennas during *T* time slots in a *T* × *N* matrix, **C**, as follows:

$$C = \begin{bmatrix} \mathbf{C}_{1,1} & \cdots & \mathbf{C}_{1,N} \\ \vdots & \ddots & \vdots \\ \mathbf{C}_{T,1} & \cdots & \mathbf{C}_{T,N} \end{bmatrix}$$

Similarly, construct a *T* × *M* received matrix **r** that includes all received signals during *T* time slots:

$$r = \begin{bmatrix} \mathbf{r}_{1,1} & \cdots & \mathbf{r}_{1,M} \\ \vdots & \ddots & \vdots \\ \mathbf{r}_{T,1} & \cdots & \mathbf{r}_{T,M} \end{bmatrix}$$

And similarly channel matrix **H**

$$H = \begin{bmatrix} \alpha_{1,1} & \cdots & \alpha_{1,M} \\ \vdots & \ddots & \vdots \\ \alpha_{N,1} & \cdots & \alpha_{N,M} \end{bmatrix}$$

Where N *is* the $T \times M$ noise matrix defined by

$$\mathbf{r} = \mathbf{C} \cdot \mathbf{H} + N,$$

Where N is the $T \times M$ noise matrix defined by

$$N = \begin{bmatrix} \eta_{1,1} & \cdots & \eta_{1,M} \\ \vdots & \ddots & \vdots \\ \eta_{1,T} & \cdots & \eta_{T,M} \end{bmatrix}$$

In the spatial domain, each different path gain can be considered independent from each other i.e. $\boldsymbol{\alpha}_{n.m}$ is independent from $\boldsymbol{\alpha}_{n'.m'}$ for $n \neq n'$ or $m \neq m'$. Size of the codeword matrix depends on the channel fading as it is assumed that the channel remains same during that time.

Codebook is a set of all code words which contains C_1 and C_2, then denote the pairwise error probability of transmitting C_1 and detecting it as C_2 by P ($C_1 \rightarrow C_2$). Then the probability of error when transmit C_1 is upper bounded by [10]

$$[\![P(C^1 \rightarrow C^2]\!]) = E\,[\![P(C^1 \rightarrow C^2/H]\!]) \leq \frac{1}{\prod_{n=1}^{N}\left[1+(\frac{\gamma\lambda n}{4})\right]^{M}}$$

The average symbol transmission power from each antenna is, Es = 1/N and the variance of the noise sample is E[|ηt,m|2] = N0 = 1/γ . λn is the Eigen values of matrix (r.C.H).

From above equation, for lower BER, large number of N and M is needed.

Unfortunately for a system, it is fixed. So to improve the performance, two factors need to be increased.

1. Increase r which is the rank of a matrix H.
    - This is possible when matrix A is full rank.
    - It will help to improve the diversity gain of a MIMO communication system.
2. Increase $\prod_{n=1}^{r}\lambda$
    - This is possible when det(A) is maximum.
    - It will help to improve coding gain MIMO communication.

STBC can also be considered as modulation schemes for multiple transmit antennas that provide full diversity and very low complexity encoding and decoding.

3.2 Orthogonal space-time block codes

Let us assume a system with N = 2 transmit antennas and one receive antenna, employing Alamouti code as show in Figure 3-1

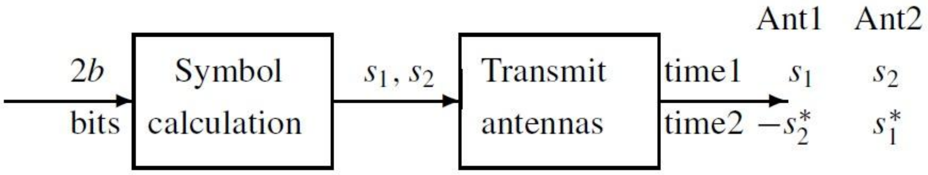

Figure 3-1Transmitter block of Alamouti code [10]

First, the transmitter picks two symbols from the constellation using a block of 2*b* bits. If s_1 and s_2 are the selected symbols for a block of 2*b* bits, the transmitter then sends s_1 from antenna one and s_2 from antenna two at time t_1. Then at t_2, it transmits $–s_2^*$ and s_1^* from antennas one and two, respectively. Therefore, the transmitted codeword is

$$C = \begin{pmatrix} S_1 & S_2 \\ -S_2^* & S_1^* \end{pmatrix}$$

To check if the code provides full diversity, the rank of all the possible difference matrices *D*(**C**,**C**') and show that it is equal to two for every **C**' ≠ **C**. Let us consider a different pair of symbols (s'_1, s'_2) and the corresponding codeword

$$C' = \begin{pmatrix} S'_1 & S'_2 \\ -S'^*_2 & S'^*_1 \end{pmatrix}$$

The difference matrix *D*(**C**,**C**') is given by

$$D(C, C') = \begin{pmatrix} S'_1 - S_1 & S'_2 - S_2 \\ S_2^* - S'^*_2 & S'^*_1 - S_1^* \end{pmatrix}$$

The determinant of the difference matrix det [*D*(**C**,**C**')] = $|S'_1 - S_1|^2 + |S'_2 - S_2|^2$ is zero if and only if S'_1= s_1 and S'_2= s_2. Therefore, *D*(**C**,**C**') is always full rank when **C**' ≠ **C** and the Alamouti code satisfies the determinant criterion. It provides a diversity of 2*M* for *M* receive antennas and therefore is a full diversity code

Let us assume that the path gains from the transmit antennas are α_1 and α_2, respectively. Then, based on our model in (3.1) the decoder receives signals r_1 and r_2 at times one and two, respectively, such as

$$r_1 = \alpha_1.s_1 + \alpha_2.s_2 + n_1$$

$$r_2 = -\alpha_1.s_2^* + \alpha_2.s_1^* + n_2$$

The receiver knows the channel path gains α_1 and α_2 is assumed, maximum-likelihood detection aggregates in minimizing the decision metric as shown below .

$$|r_1 - \alpha_1.s_1 - \alpha_2.s_2|^2 + |r_2 + \alpha_1.s^*{}_2 - \alpha_2.s_1^*|^2 \qquad (3\text{-}2)$$

Expanding the above equation (3.2), ignore the common term $|r_1^2| + |r_2^2|$. Then, it can be decomposed into two parts, one of which,

$$|s_1|^2 \sum_{n=1}^{2} |\alpha_n|^2 - \left[r1\alpha_1^* s_1^* + r_1^* \alpha 1 s 1 + r2\alpha_2^* s_1 + r_2^* \alpha_2 s_1^*\right] \qquad (3\text{-}3)$$

is only a function of s_1, and the other one

$$|s_2|^2 \sum_{n=1}^{2} |\alpha_n|^2 - \left[r1\alpha_2^* s_2^* + r_1^* \alpha_2 s_2 - r_2 \alpha_1^* s_2 - r_2^* \alpha_1 s_2^*\right] \qquad (3\text{-}4)$$

From above equation (3.3) and (3.4) it can be concluded that the decoding complexity of the code increases linearly, instead of exponentially, by the number of transmit antennas. Also , as in case of PSK, all the constellation symbols have equal energies. The terms $\sum_{n=1}^{2} |\alpha_n|^2$ and $\sum_{n=1}^{2} |\alpha_n|^2$ can be ignored. As a result, the maximum-likelihood decoding can be further simplified as to minimize

$$|s_1 - r_1\alpha_1^* - r_2^*\, \alpha_2|^2$$

to decode s_1 and minimizing

$$|s_2 - r_1\alpha_2^* + r_2^*\, \alpha_1|^2$$

to decode s_2. Therefore, the decoding consists of first calculating

$$\tilde{s_1} = r_1\alpha_1^* + r_2^*\, \alpha_2$$

$$\tilde{s_2} = r_1\alpha_2^* - r_2^*\, \alpha_1$$

Then, to decode *s*1, the receiver finds the closest symbol to $\tilde{s_1}$ in the constellation.

Similarly, decoding of *s*2 consists of finding the closest symbol to $\tilde{s_2}$ in the constellation.

$$\tilde{s_1} = \sum_{m=1}^{M} [r_1 \alpha_{1,m}^{*} + r_{2,m}^{*} \alpha_{2,m}]$$

$$\tilde{s_2} = \sum_{m=1}^{M} [r_{1,m} \alpha_{2,m}^{*} - r_{2,m}^{*} \alpha_{1,m}]$$

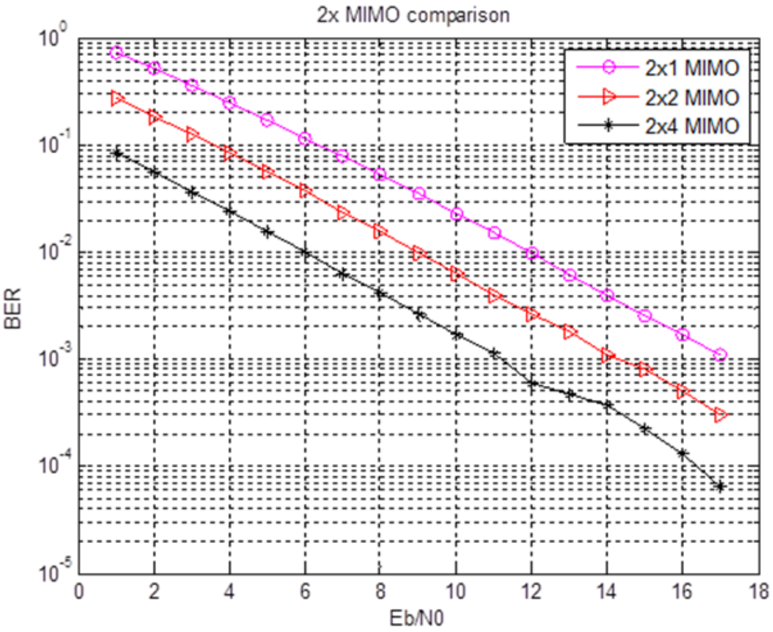

Figure 3-2 Performance comparison of MIMO for 2 transmitter antenna

The performance of the Alamouti code over Rayleigh fading channel using a BPSK constellation and one receive antenna is provided in Figure 3-2. As it can be seen, the performance of the Alamouti code with two receive antennas is much better than that of the system with one receive antenna. At a symbol error probability of 10^{-3}, the Alamouti code provides more than 11 dB improvement for 4 receive antennas.

3.3 Orthogonal design for more than two transmit antennas

Similar to Alamouti code for two transmit antennas, to design space-time codes that provides simple decoding and maximum diversity properties for more than two transmit antennas, the code should satisfy two main criteria. It should have simple ML decoding and should satisfy the orthogonal property. With orthogonal properties, full diversity can be achieved which results in higher path gain. For example $|\alpha_1|^2 + |\alpha_2|^2$ path gain is possible in case of Alamouti code. Similarly, with more than one transmit antenna, path gain equals to N times $|\alpha|^2$.[10]

$$\Omega.\Omega^H = (|\alpha_1|^2 + |\alpha_2|^2)I_2$$

Where Ω is

$$\Omega = \Omega(\alpha_1, \alpha_2) = \begin{pmatrix} \alpha_1 & \alpha^{\bullet}{}_2 \\ \alpha_2{}^{\bullet} & -\alpha^{*}{}_1{}^{\bullet} \end{pmatrix}$$

Also, I_2 is a 2 × 2 identity matrix. The structure of the Alamouti code by the following generator matrix

$$G = \begin{pmatrix} x_1 & x_2 \\ -x_2{}^{\bullet} & x_1{}^{\bullet} \end{pmatrix}$$

is a result of the orthogonally of the columns of *G* and the following

$$G^H G = (|x_1|^2 + |x_2|^2)\, I_2$$

To generate similar generator matrices for more than two transmit antennas, a complete study of real orthogonal designs was provided by Radon and Hurwitz family of matrices. According to its properties

I. A real orthogonal design exists if and only if N = 2, 4, 8.

II. Each member of matrix is orthogonal to each other

Generator matrix for N =2,4 or 8 can be obtained. As according to the properties of orthogonal matrix, matrix can have orthogonal property even with complete removal of a column. So, if required, G for odd number of transmit antennas is generated, which can be done by column removal process called ‘shortening’. For example, let’s assume G_4 as follows

$$G_4 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & -x_1 & x_4 & -x_3 \\ x_3 & -x_4 & -x_1 & x_2 \\ x_4 & x_3 & -x_2 & -x_1 \end{pmatrix}$$

Generator matrix for 3 transmit antennasby removing any column from G_4 is obtained. For example

$$G_3 = \begin{pmatrix} x_2 & x_3 & x_4 \\ -x_1 & x_4 & -x_3 \\ -x_4 & -x_1 & x_2 \\ x_3 & -x_2 & -x_1 \end{pmatrix} or \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & -x_1 & x_4 \\ x_3 & -x_4 & -x_1 \\ x_4 & x_3 & -x_2 \end{pmatrix}$$

Chapter 4

System Model

4.1 Smart meter

A smart meter is an electrical meter that records consumption of electric energy in a certain interval of time and communicates the information, both ways, with the ability for monitoring and billing purposes. The system model is shown below in Figure 4-1.

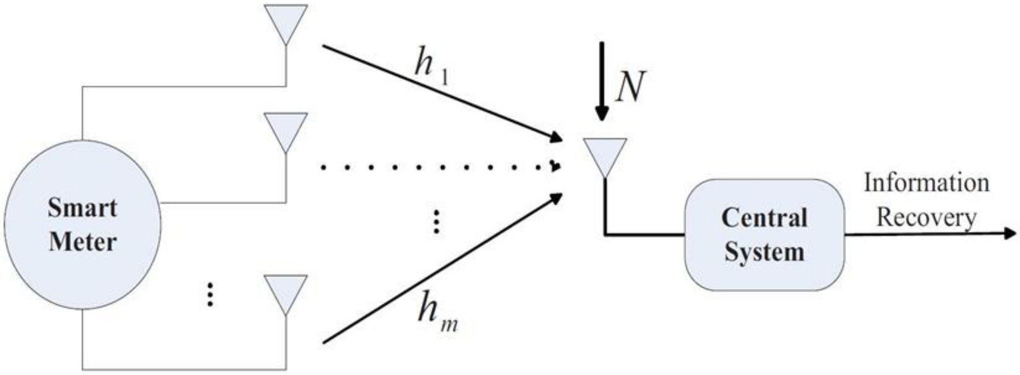

Figure 4-1 System model of smart grid

In the thesis proposal, Assuming that several smart meters are connected to one power line. Each smart meter must be aware of how much energy other smart meters are consuming. To analyze performance of system under various attacks and link failure cases , I have also assumed that the smart meter which are connected to common power line are synchronized to each other.

4.2 Block Diagram

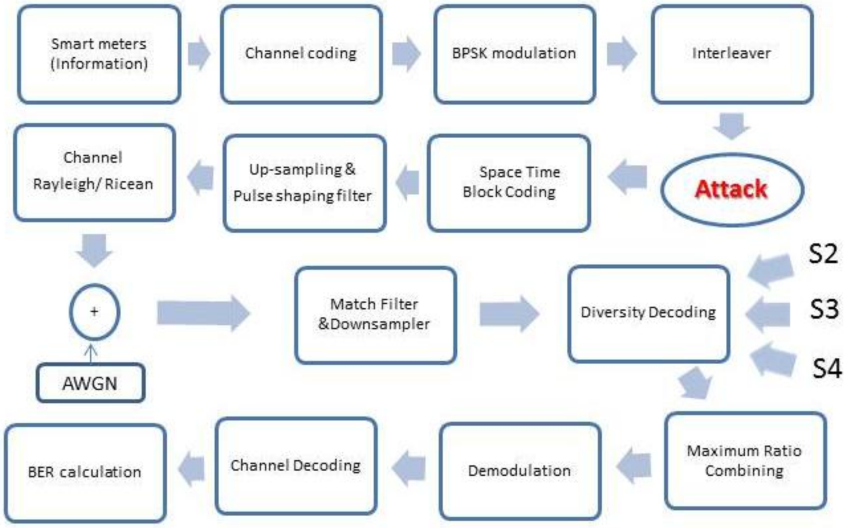

Figure 4-2 Block Diagram of system model

4.3 Virtual MIMO

Virtual MIMO is a technique of implementing multiuser transmitter as analogous to a transmitter with more than one antenna using STBC. For example, in the case of a 4x1 MISO, there will be 4 smart meter/users that are sharing or are aware of each other's information in a timely manner. For example, consider a BPSK modulation system.X_1, X_2, X_3, X_4 is the information transmitted by smart meters - S1, S2, S3 and S4 respectively. Since the first smart meter S1 is also aware of X_2, X_3 and X_4 and all smart meters are synchronized with each other, S1 will transmit X_1, X_2, X_3, X_4 one block at a time. Similarly, S2 will transmit X2,-X1,-X4, X3. So when the control center or utility receives this information, it will try to combine these results constructively to decide which information has been transmitted correctly.

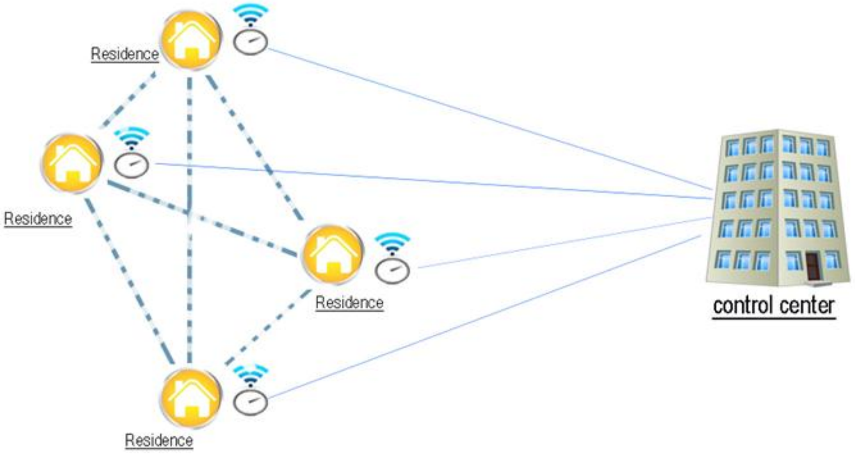

Figure 4-3 Virtual MIMO in smart grid

As shown in Figure 4-3, this thesis proposal implements a 4x1 virtual MIMO with Maximum Ratio Combining method at the receiver. Consider that four smart meters are connected to the control center with smart meters smart meter-1, smart meter-2, smart meter-3, smart meter-4. These four smart meters send information X_1, X_2, X_3 and X_4 respectively through channels h_1, h_2, h_3 and h_4.

4.4 Channels

If the receiver is closer to the transmitter the possibility of having an accurate LOS path is much more than when the receiver is placed remotely. In the smart grid, the control point or aggregator are situated very close to residences. So a smart meter will have a LOS path. Receiver experiences Rician channel fading when it has a LOS path and Rayleigh fading when multipath components are present. This concept has been simulated with a model as shown below.

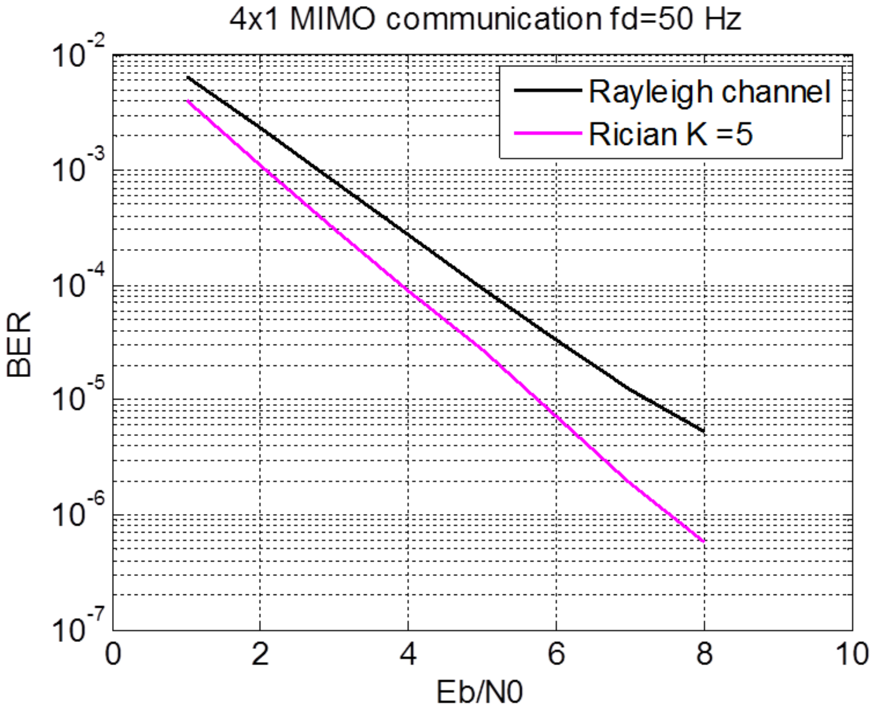

Figure 4-4 Performance comparison of 4x1 VMIMO over fading channels

Jake's model [12] has been used here to randomly generate the independent Rayleigh and Rician channel model. A Doppler shift frequency of fd = 50Hz is chosen for the mobile receiver and 5Hz for a fixed receiver. For a scenario where LOS path a Rician fading factor of K= 5 has been used for modeling. The simulation results (as in figure above) clearly show that the Rician channel has better performance than Rayleigh and thus LOS path seems to have more dominance over multipath signals.

4.4 Modulation Techniques

The modulation technique - Binary phase-shift keying (BPSK) has been implemented for optimized analysis of security concerns in smart grid applications, irrespective of hamming distance.

4.5 Link Adaptation Techniques

Link adaptation technique has been used to combat channel fading and attacks using random block interleaver.

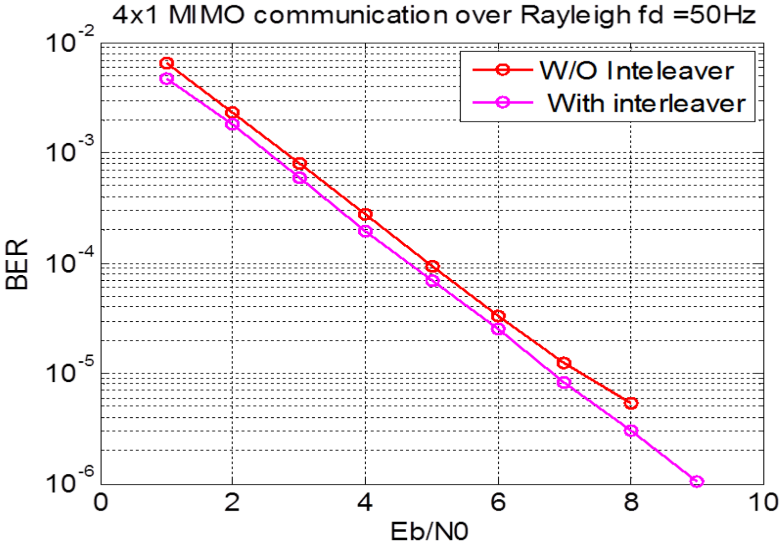

Figure 4-5 Performance of virtual 4x1 MIMO over Rayleigh

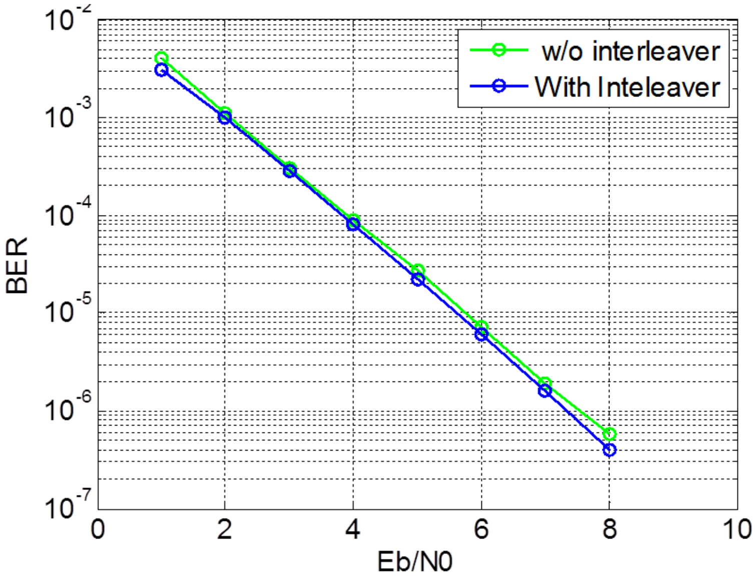

Figure 4-6 Performance of virtual 4x1 MIMO over Rician

The above diagrams show, that interleaver implementation has improved the performance by a small margin. The important point to be considered here is that the improvement of BER over Rician (around 10%) is less than the improvement of BER over Rayleigh channel fading (around 15 to 20%). This is because of the fact that the LOS path has more dominance over multipath.

4.6 Channel Coding

Channel coding adds redundancy in the source code and is an efficient decoding algorithm which can be dealt with error control techniques. If the data at the output of a communication system has errors that are too frequent for the desired use, the errors can often be reduced by the use of a number of techniques of channel coding. Though coding permits a decreased information rate, it increases information transfer at a fixed error rate, or reduces error rate for a fixed transfer rate.

Following diagram compares the performance of Convolution coding and Turbo coding.

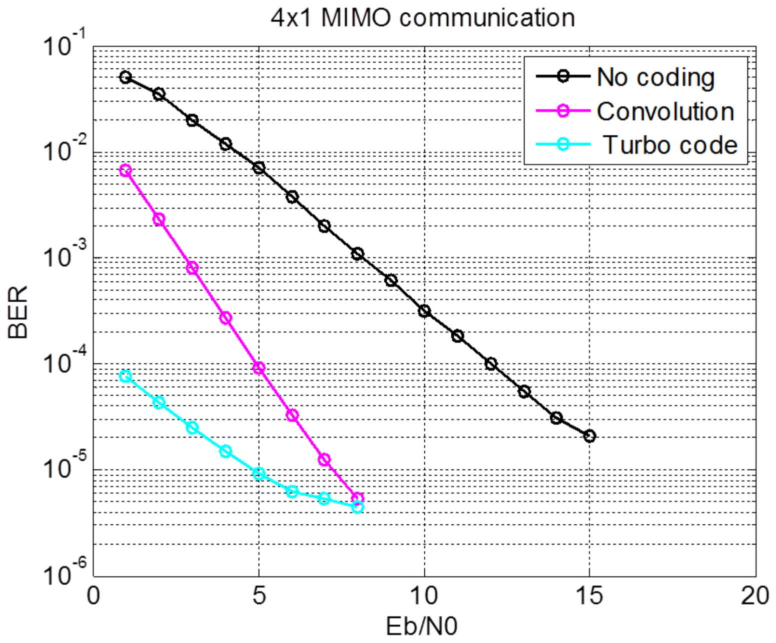

Figure 4-7 Comparison channel coding for MIMO

Generally, turbo codes have better performance than convolutional coding. The complexity of turbo code is much higher than convolutional coding. Turbo codes are nonlinear and require iterative decoding at receiver. On the other hand, convolutional codes are linear and do not require feedback to achieve effective performance. The decoding algorithms considered for turbo decoding is Max-log-MAP/BCJR which is used iteratively. To get better BER performances with turbo coding, iterations of upto 18 have to be performed. This shoots up the processing time, in other words decreases the processing gain. On the other hand, Viterbi algorithm which is used in convolutional decoding uses maximum likelihood decoding technique. It is faster than iterative decoding techniques as convolutional codes are linear and do not have any feedback.

Thus the high processing gain factor in convolution decoding makes it more appropriate to be used in smart grid applications.

4.7 Diversity decoding

A utility receives multiple versions of each smart meter reading created by the pre-coding schemes. Here, the assumption is that the receiver has received channel information already. So when a utility receives multiple copies of readings from different channels, the receiver antennas combine these copies together. Since the channel matrix is orthogonal to the received signal matrix, a receiver multiplies the channel matrix with the transpose version of the combined signal. The product of that matrix is then compared with the alpha value of the MIMO channel. Finally, using the MRC scheme the final decision will be taken by the receiver. To analyze the effect of malicious attack and data piracy on smart grid , plotted on a logarithmic axis below is the BER vs. SNR graph.

Chapter 5

Results and Conclusion

Security is the main concern when using a smart grid communication system. It is very important to make it more immune to attack and jamming to avoid an imbalance between generation and demand/consumption. First, consider the scenario where the communication between the smart meter and central system is under malicious attack.

5.1 Additive Malicious Attack Scenario

The malicious attack term signifies that that addition of garbage elements into data is being sent over the channel and which are not easily distinguishable with the original data set. Communication with single input and single output is highly vulnerable to such kind of an attack without the assistance of some effective security measurements. With MIMO, even when one link is attacked one or more good links are left with which the receiver can recover data. Space time block coding, as discussed before, has better process gain and better performance than other block codes. So, space time block coding technique has been implemented over multiple antennas at transmitter and /or multiple antennas at receiver to combat severe communication impairments induced by malicious attacks.

Consider 4 residential smart meters, where each smart meter is transmitting information independently to control center. Each smart meter is aware of the information regarding other smart meters.

$$\begin{array}{cc}
\begin{array}{cccc}\text{Smart Meter 1} & \text{Smart Meter 2} & \text{Smart Meter 3} & \text{Smart Meter 4}\\ \downarrow & \downarrow & \downarrow & \downarrow\end{array} & \\
\left(\begin{array}{cccc} x_1 & x_2 & < x_3 > & x_4\\ -x_2 & x_1 & < -x_4 > & x_3\\ -x_3 & x_4 & < x_1 > & -x_2\\ -x_4 & -x_3 & < x_2 > & x_1\end{array}\right) & \begin{array}{l}\leftarrow \text{Ts}\\ \leftarrow \text{2Ts}\\ \leftarrow \text{3Ts}\\ \leftarrow \text{4Ts}\end{array}
\end{array}$$

Figure 5-1 Symbol matrix

As shown in fig 5-1, the columns indicate the smart meters and the rows indicate the symbol time. For example, at the first symbol time S-1 smart meter will send X1 , S-2 will send X2 and so on. Similarly, S-4 will send X4 in first symbol time, X3 in second so on. So a 4 X 4 space time orthogonal design is derived as follows

$$G = \sum_{k=0}^{4} X_n B_n \tag{5-1}$$

Where B_1 equals the identity matrix I_4 , and matrix B_2, B_3 , B_4 are chosen from Hurtwitz-Randon family. Generation matrix, $G_{1,}$ will provide the following orthogonal property without attack

$$G_4^T\, G_4 = (\sum_{k=0}^{4} X_n^2\ )I_4$$

The notation, ‘ <>’ in Figure 5-1 implies that the communication link between the third transmit antenna and the receiver is under malicious attack. The attack pattern could be numerous and diverse. The additive malicious attack is mainly addressed here, which is a very practical attack pattern for analysis. The coding rate R is defined as R = (K symbols/T timeslots). In the above 4 × 4 orthogonal design, K = T = 4 and therefore R

= 1. An orthogonal design with rate R = 1 is called the full code-rate orthogonal design. Even though the receiver cannot detect which communication link (or links) is under attack, space-time block coding could still recover the original transmitted signal to certain accuracy, in virtue of the transmit and/or receiver diversity. According to the system model and generation matrix, the received y can be represented as:

$$y^T = H^T . G_4^T + N^T$$

$$= H^T . \sum_{k=0}^{4} X_n \; B_n^T + N^T$$

$$= (x_1, x_2, x_3, x_4) . \Omega + N^T \qquad (5\text{-}2)$$

Here H is the corresponding 4 × 1 channel vector. The Ω matrix in (5-2) , whose nth row Ωn equals to $H^T B^T_n$, has been proved to be orthogonal in [10]. The orthogonal property of the Ω matrix will play a key role in parallel decoding at the receiver.

To decode the received information, the receiver will multiply both sides of equation (5-2) by the Ω^T. The orthogonal properties of Ω help us reach the following parallel decoding. Parallel decoding, a low-complexity design, will significantly simplify the receiver's physical design and prolong the battery life. After parallel decoding, the Maximum-Likelihood (ML) detection can make the proper decision. The Maximum Ratio Combining (MRC) could be used for more than one receiver antenna. To construct the Ω matrix for parallel decoding, the receiver needs the information of the channel because Ωn = H^T B^T . Consider the scenario in which the fading coefficients are known, i.e., accurately estimated by the receiver, but not fully known to, or not exploited by the transmitter.

Due to the randomness of the channel gain matrix, Monte Carlo simulations were employed to analyze the BER performance in terms of different kinds of attack.

Rayleigh and Ricean fading channel is chosen for simulation . $|h_n|^2$ is the chi-square distributed with two degrees of freedom. As it is known, a chi-square random variable with two degrees of freedom is the same as an exponential random variable with unit mean.

5.1.1 Additive attack without channel coding

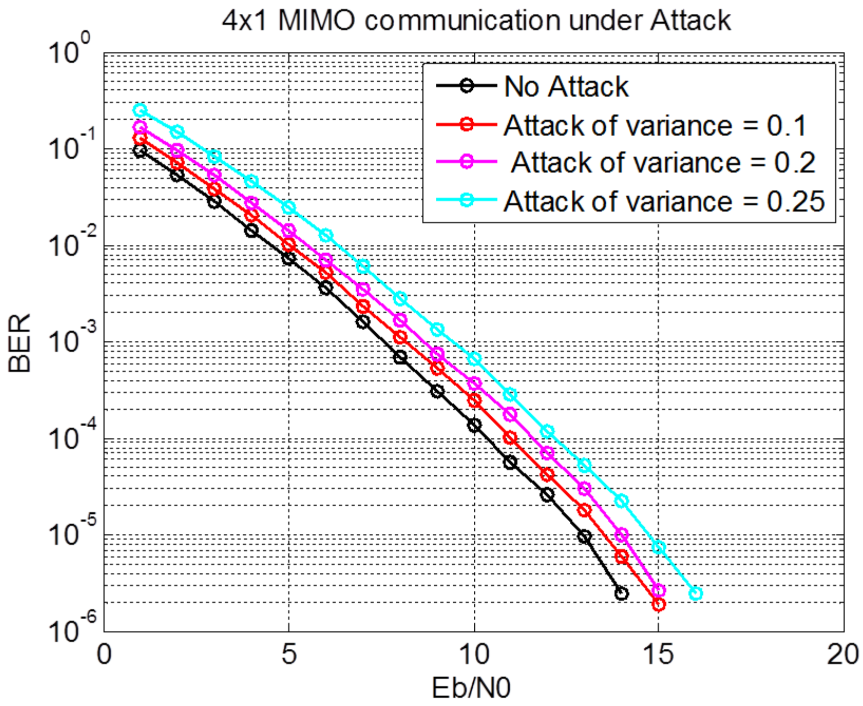

Figure 5-2 Additive malicious attack w/o channel codinng

Figure 5-2 verifies the validity of space-time block coding in combating a malicious attack without using any channel coding or any link improvement techniques. The plot in Fig 5-2 I compares d ifferent kind of malicious attacks, the power of which are σ^2 = 0.1, σ^2 = 0.2 and σ^2 = 0.25, respectively. If the attack is very severe (σ^2 = 0.25), space-time block coding can still recover the information effectively.

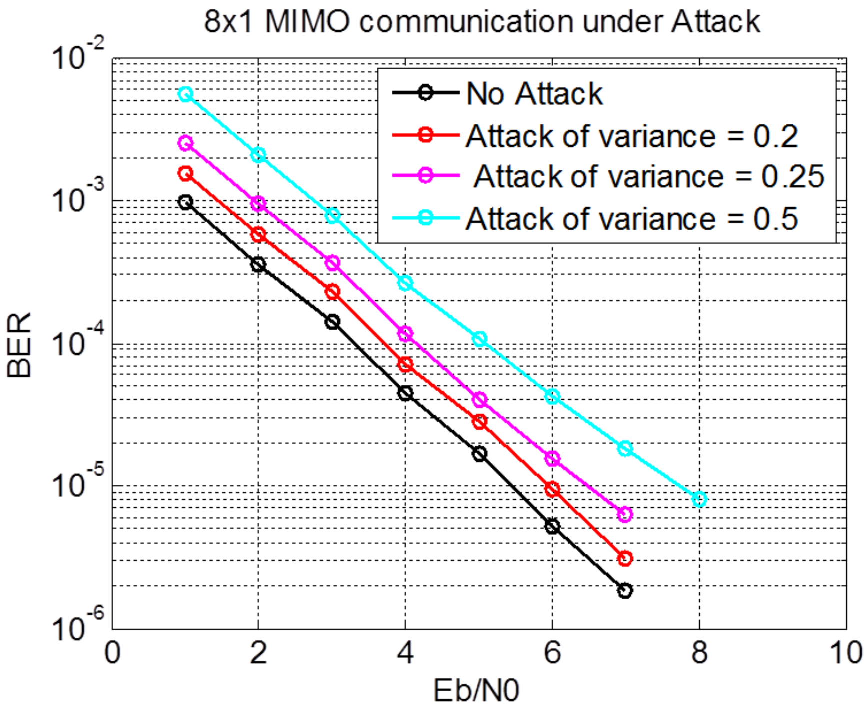

Figure 5-3 Additive malicious attack over virtual 8x1

The severe the malicious attack, the worse is the performance. This conclusion can be further verified in the 8x1 virtual MIMO. Figure 5-3 indicates that the BER performance of 8x1 virtual MIMO is much better than 4x1 virtual MIMO . This is because more virtual paths will give more diversity gain and better performance. However, the improved performance comes with the price of computation cost and synchronization complexity.

5.1.2 Additive attack with Convolutional coding

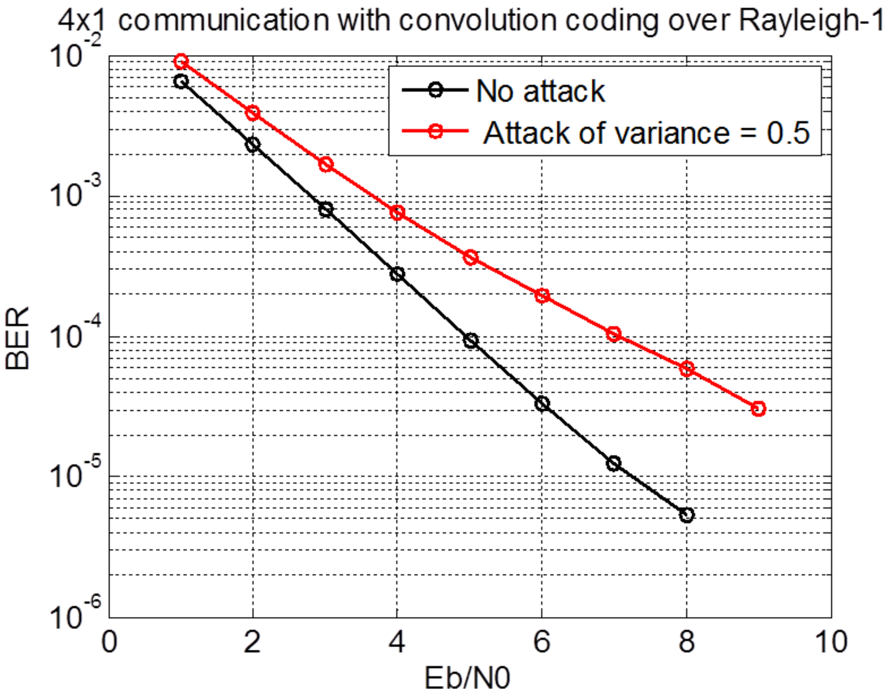

Figure 5-4 Additive attack over Rayleigh channels with Convolutional coding

As shown above in Figure 5-4, an additive attack has been introduced on data with a variance of 0.5 over a Rayleigh channel. In comparison, the performance of system under convolutional code is much better than the performance without any channel coding. Since convolutional coding uses the maximum likelihood decoding algorithm, it can be used in real time applications also.

Figure 5-5 depicts the analyses of the performance of the system over Hybrid (Rayleigh and Ricean) channels.

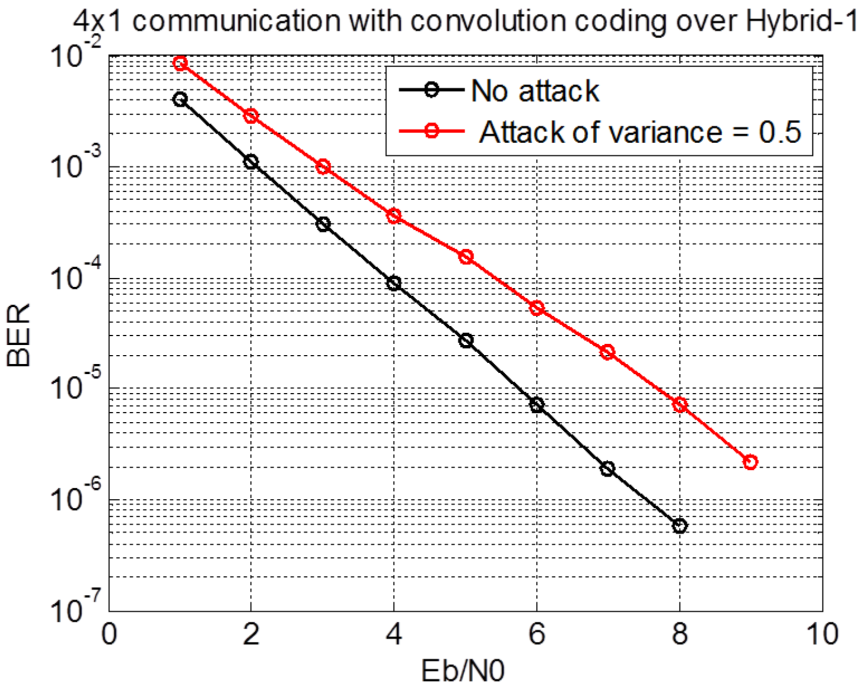

Figure 5-5 Additive attack over Hybrid channels with Convolutional coding

5.1.3 Additive attack with Convolutional coding and interleaver

Interleaver is one of the effective link adaptation techniques which helps in increasing performance of the system under scenario of burst error occurred because of channel fading.

Performance of the system with the deployment of interleaver in an additive attack scenario is then analyzed as shown in Figure 5-6 and Figure 5-7.

From Figure 5-4, Figure 5-6,Figure 5-7 and Figure 5-5 a conclusion can be derived that in both Rayleigh and Hybrid channel cases the performance of system has improved by 10 dB. It is greater than the performance under non-attack case as discussed in section 4.2.1. Basically, deployment of an interleaver helps to improve the performance under additive attack.

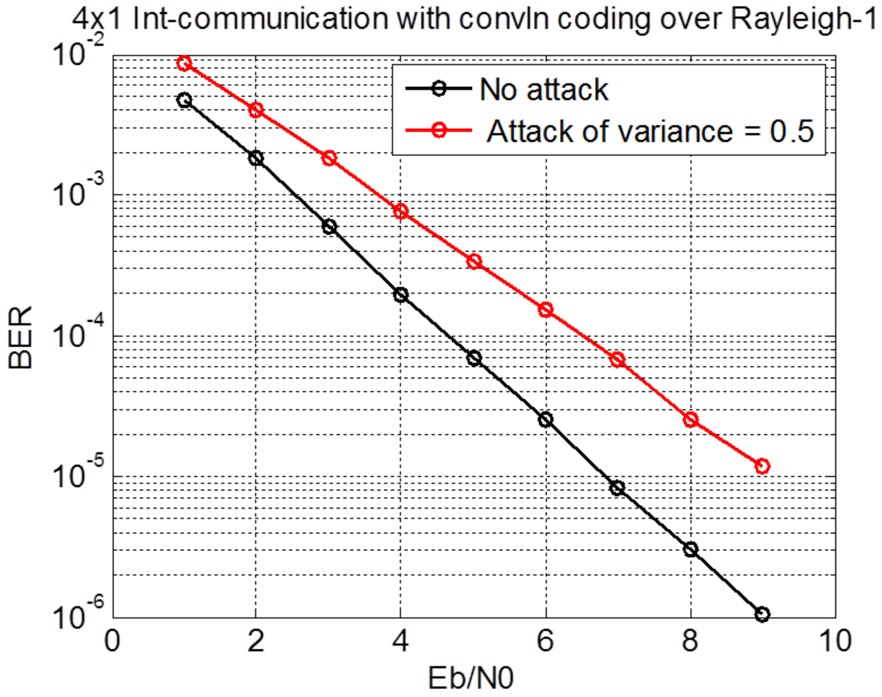

Figure 5-6 Additive attack over Rayleigh with Convolutional coding and interleaver

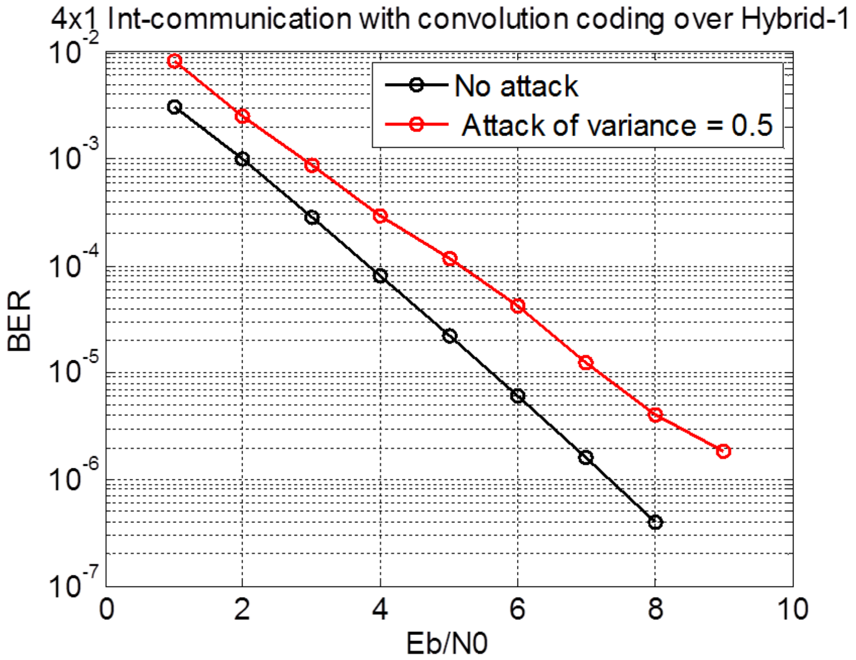

Figure 5-7 Additive attack over Hybrid channels with Convolutional coding and interleaver

5.2 Data piracy Scenario

5.2.1 Data piracy over without interleaver

Data piracy is a special type of attack where the data which is intended to be sent over a channel is corrupted by an intruder. In this scenario assumption is made that the intruder is aware and has full access to the data which is being transmitted through the smart meter.

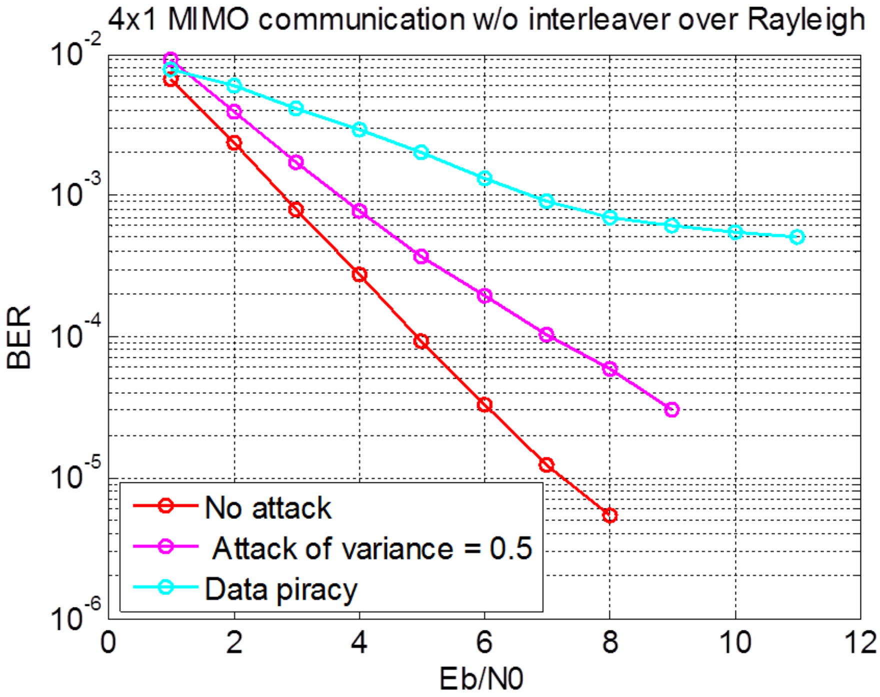

Figure 5-8 Performance comparison under Data piracy and Malicious attack over Rayleigh

As you can see from Figure 5-8, the performance of a system under data piracy case is more severe than the additive malicious attack. Even the presence of redundant data copies from anoother smart meter, STBC or MIMO will not be able to recover affective data. As shown below in Figure 5-9, a hybrid channel does not show any improvement.

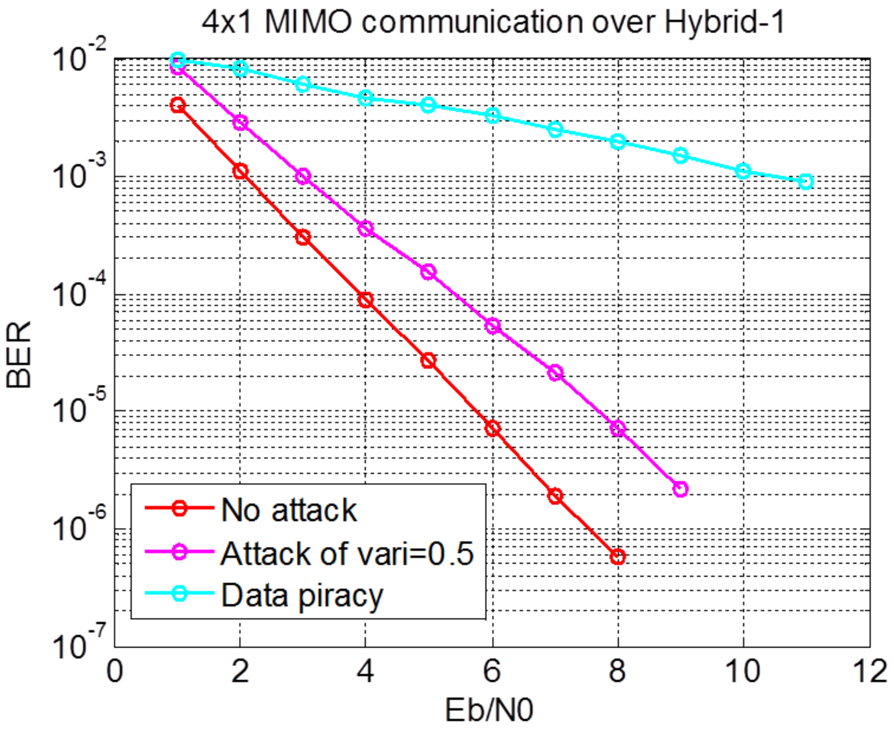

Figure 5-9 Performance comparison under Data piracy and Malicious attack over Hybrid channel

For example a smart meter wants to send data 101110, but an intruder interrupts and sends 010011

5.2.2 Data piracy over with interleaver

As shown in Figure 5-10 and Figure 5-11, deployment of an interleaver under a malicious attack has shown a significant improvement in performance. But in the case of data piracy, it fails to show an improvement.

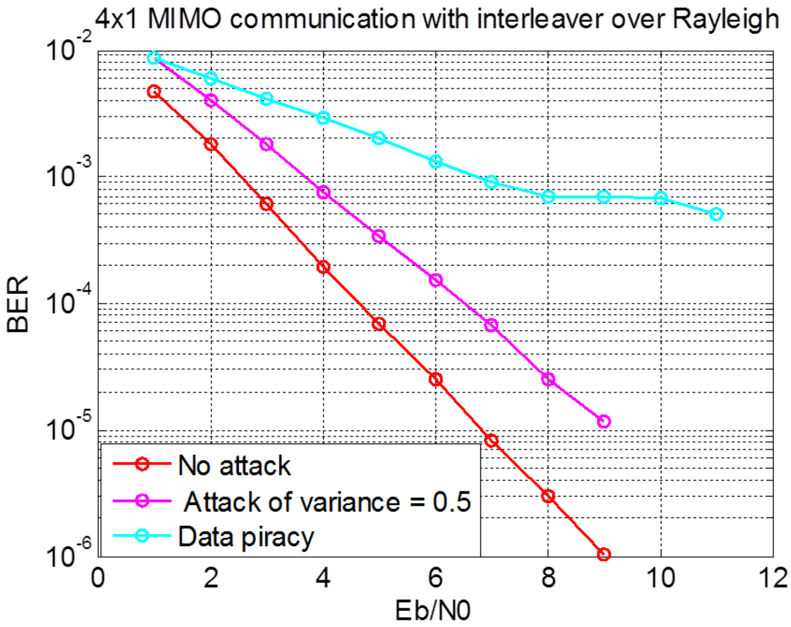

Figure 5-10 Comparison under Data piracy and Malicious attack over

Interleaver and Rayleigh channels

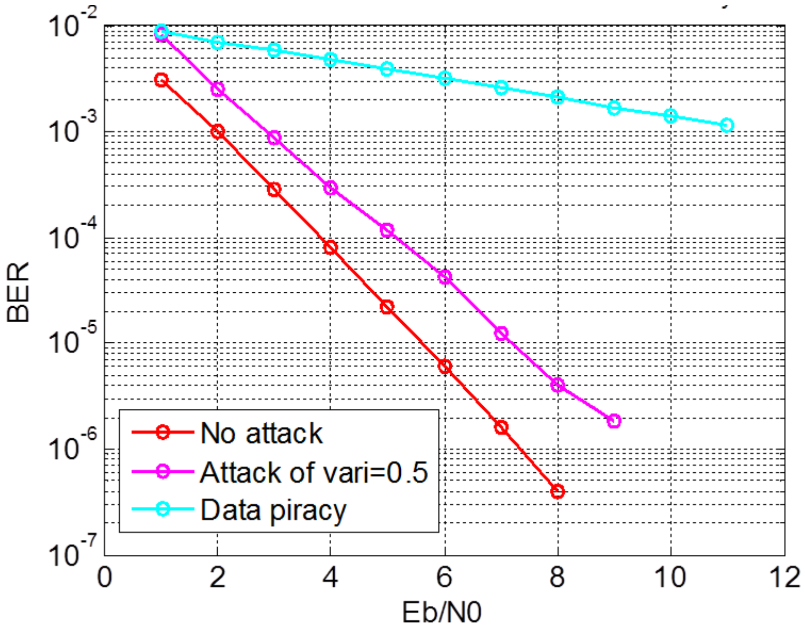

Figure 5-11 Comparison under Data piracy and Malicious attack over Interleaver over Hybrid

channels

5.3 Comparison of Malicious Attacks over channels

From Figure 5-12 and Figure 5-13, show the performance of the system in a LOS case i.e. Rician channel fading is better than nonLOS reception. When a receiver has LOS reception, received copies from direct path is dominant over the indirect path. Because of less fading or less attenuated using a direct path, better performance is achieved i.e. less Bit Error Rate.

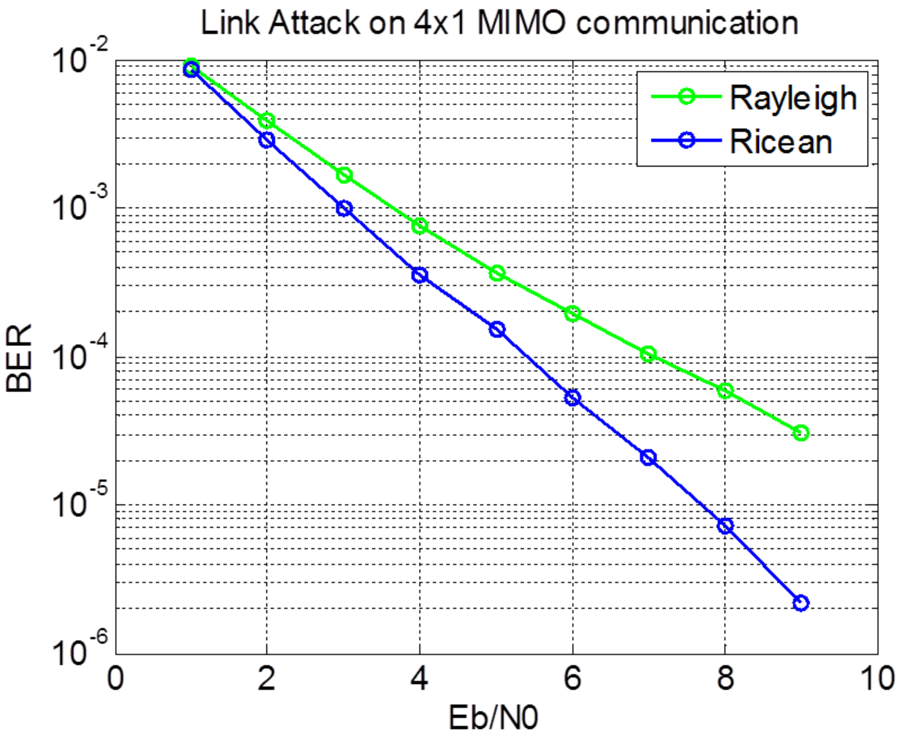

Figure 5-12 Performance comparison of Malicious attack channels

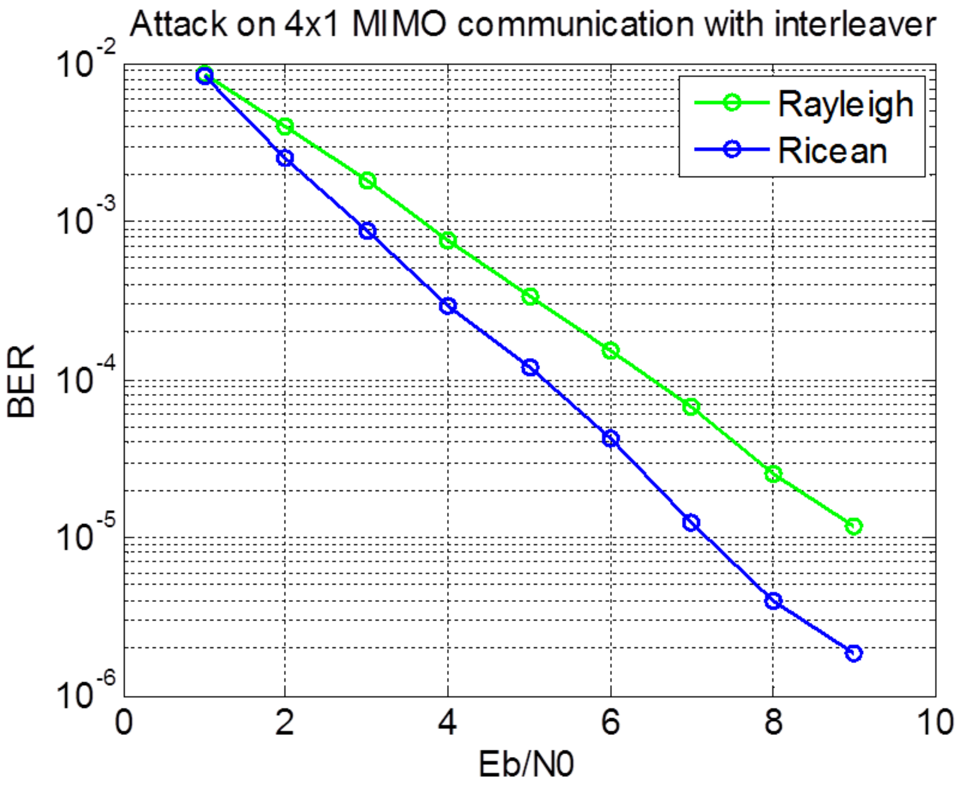

Figure 5-13 Performance Comparison of Malicious attack over Interleaver over channels

5.4 Performance comparison of Data Piracy over channels

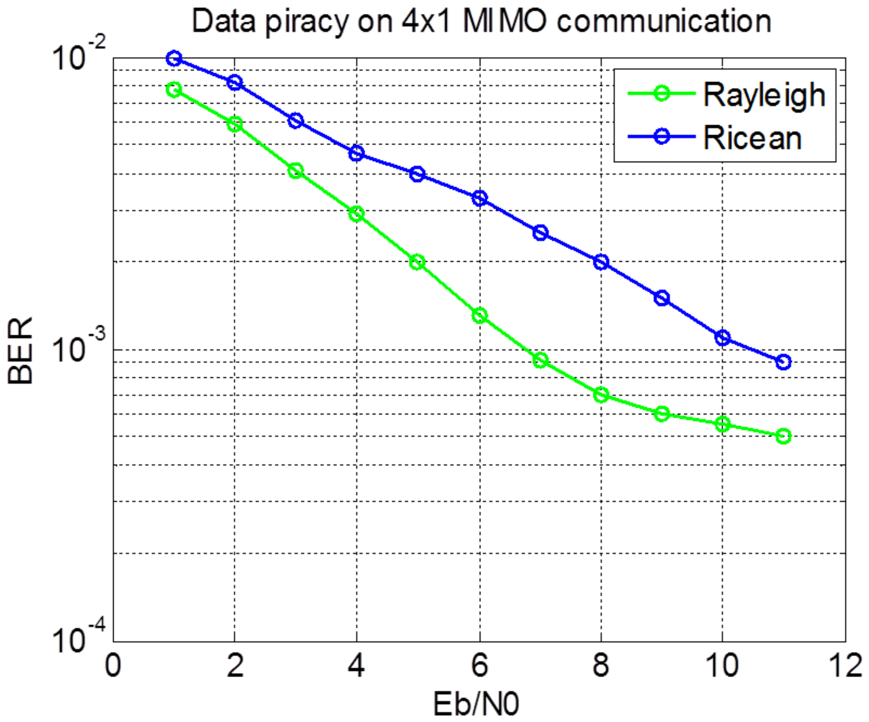

Figure 5-14 Performance comparison of Data Piracy over channels

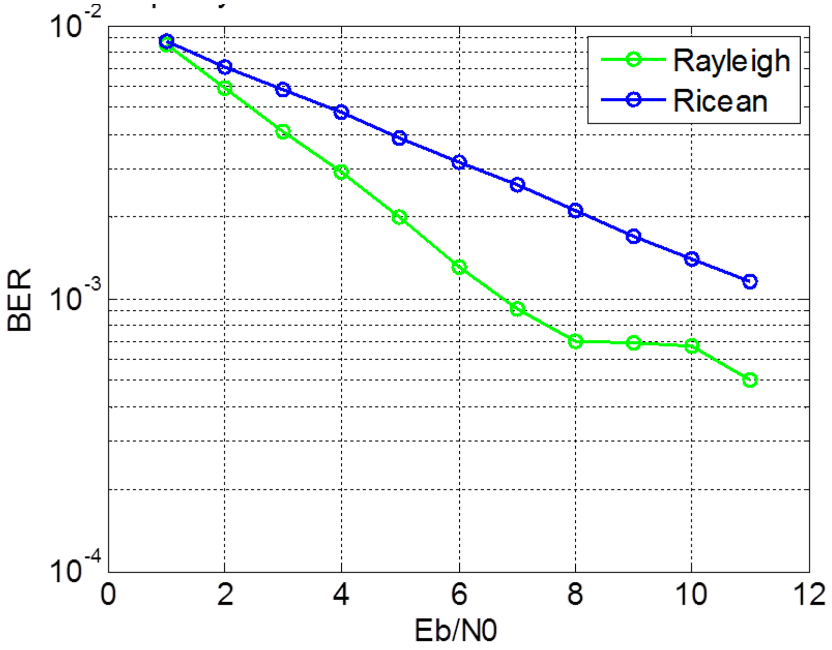

Figure 5-15 Performance comparison of Data Piracy over Interleaver and channels

Similarly, performance of the system is also evaluated under data piracy scenario. As discussed in section 5..2, data piracy is very severe attack on a smart meter. It degrades the performance of the system. Even link adaptation and channel immune techniques cannot recover data which is then stolen by an intruder.

Though the performance of the system is always better in the case of LOS path , direct paths has more dominance . Its an interesting to point out that from Figure 5-14 and Figure 5-15, that if a system is under attack, the performance of system will not improve but rather degrade in performance.

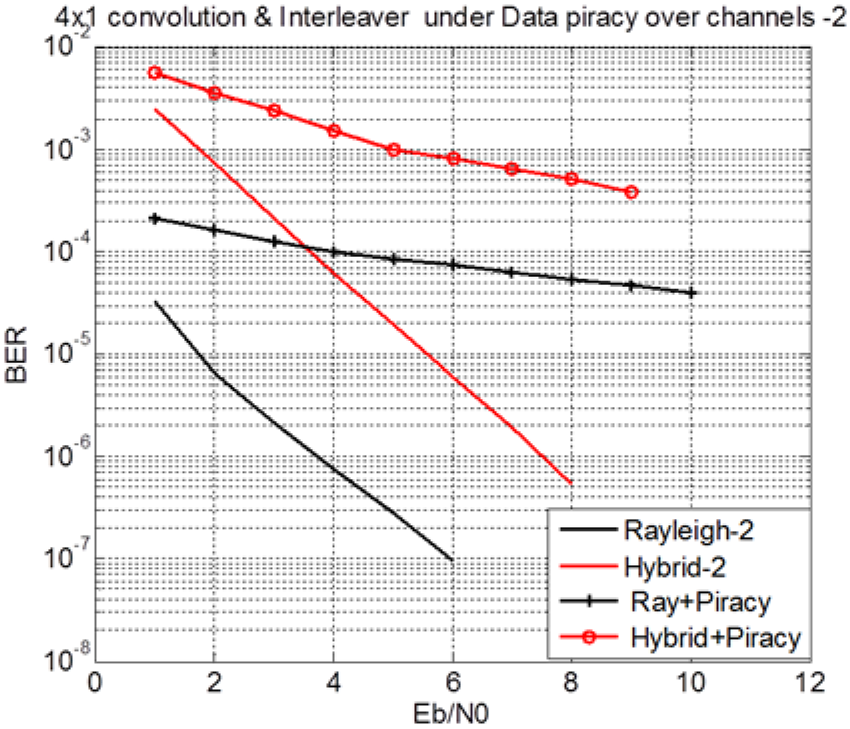

Figure 5-16 Performance comparison of Data Piracy

over less fading channels

When the receiver is stationary or there is very low relative velocity between the transmitter and the receiver ,the doppler spread wil be a few Hz. So here, a case where receiver is stationary and doppler spread is 5 Hz and K=5 Hz. Is considered.

From Figure 5-6 , two conclusions can be drawn. Even though the doppler spread is very low

1. The fading factor is highly dominant and plays a major role in degrading the performance in the case of data piracy
2. The BER is lower in the case of Rayleigh channel fading where there is no direct path signal transmitted to the receiver.

5.5 Solution over data piracy

This section, considers the receiver with detection. Sometimes, the receiver can detect the attacks when the attack is very strong. Meanwhile, if the link fails, then the receiver can not receive any noise. In this case it can still detect the link failure. (rate is different and diversity is different) Limited feedback from destination to source is exlpoited.

Detection of the attack link or failed link leads to shut down of the corresponding smart meter which is under data piracy attack. This will decrease the power consumption. Simulation to verify our proposed detection algorithm is as shown in Figure 5-17

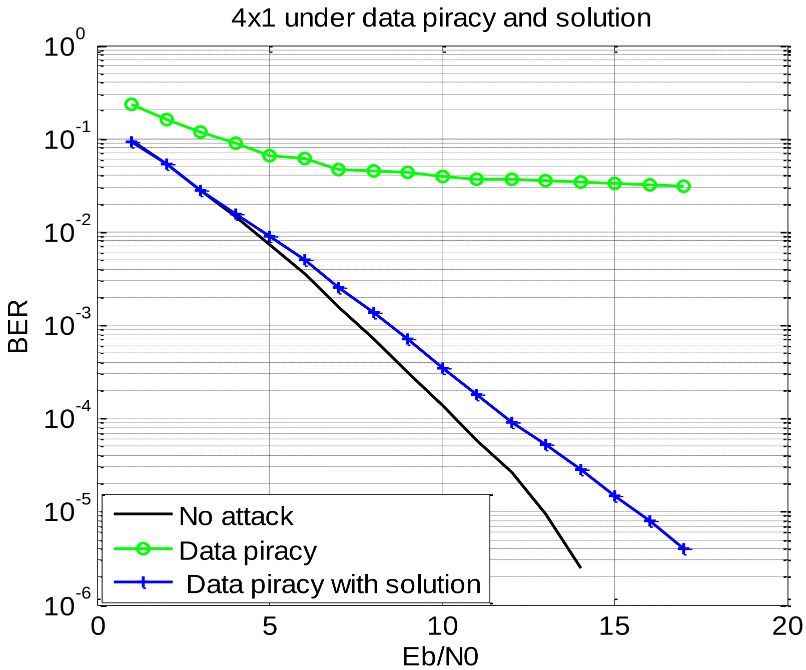

Figure 5-17 Performance of Data piracy with solution

5.6 Link failure scenario

The previous section investigated the security challenge under malicious attack. Another common scenario to take into consideration is link failure, which is related to the reliability challenge in the smart grid. Apparently,a SISO system is vulnerable to link failures for the reason that, if the only link between the transmitter and receiver failed, the communication is impossible. This section implements the space-time block coding to enhance the reliability of the communication between the smart meter and a central system.

Assuming that the link between the third transmit antenna and the receiver fails. Then what the receiver received from the third antenna is only noise, interference, and lacks any transmitted information. However, its required to reconstruct the Ω matrix, because the third link has failed implying $h_3 = 0$. In link failure scenario, the reconstructed Ω matrix is as follows

$$\Omega_r = \begin{pmatrix} h_1 & h_2 & 0 & h_4 \\ h_2 & -h_1 & -h_4 & 0 \\ 0 & h_4 & -h_1 & -h_2 \\ h_4 & 0 & h_2 & -h_1. \end{pmatrix}$$

where h3 = 0. The Ωr matrix help realize the parallel decoding at the receiver. After the parallel decoding, ML detection could make the proper decision. The Monte Carlo simulation for 4 transmit antennas with a link failure is shown in Figure 5-18.

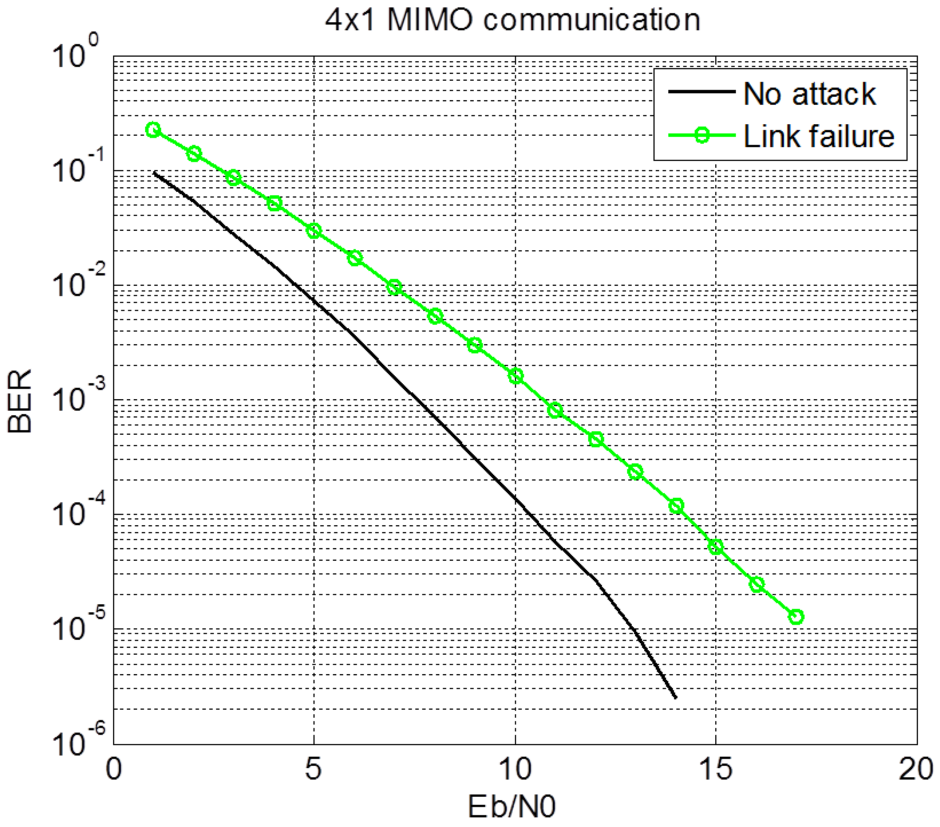

Figure 5-18 Performance of 4x1 system under link failure scenario

Space-time block coding provides satisfying BER performance in a link failure scenario can be concluded. It is known that for the SISO case, if a single link fails, the communication between the transmitter and receiver is impossible. Figure 5-18 indicates that even after one link fails, the receiver could still recover the received information effectively.

Another interesting conclusion is that the BER performance of a malicious attack scenario is better than link failure scenario, even if the attack is severe. One reasonable explanation is that in malicious attack scenario space-time block coding produces a larger diversity gain than the link failure scenario. Thus, even with malicious attack, the diversity order is Mt and diversity gain is $\Sigma\ |h_n|^2$; However, in the link failure case, the diversity order is Mt − 1 and the diversity gain is Σ $|h_n|^2$where n ≠j, wher j is the failed link.

The benefit of space-time block coding is further verified in the 8 transmit antennas case. Fig.5-19 indicates that an 8 transmit antenna design is more reliable than a 4 transmit antenna design when link failure occurs. This is due to the fact that 8 transmit antennas produces larger diversity gain. With better performance comes design complexity.

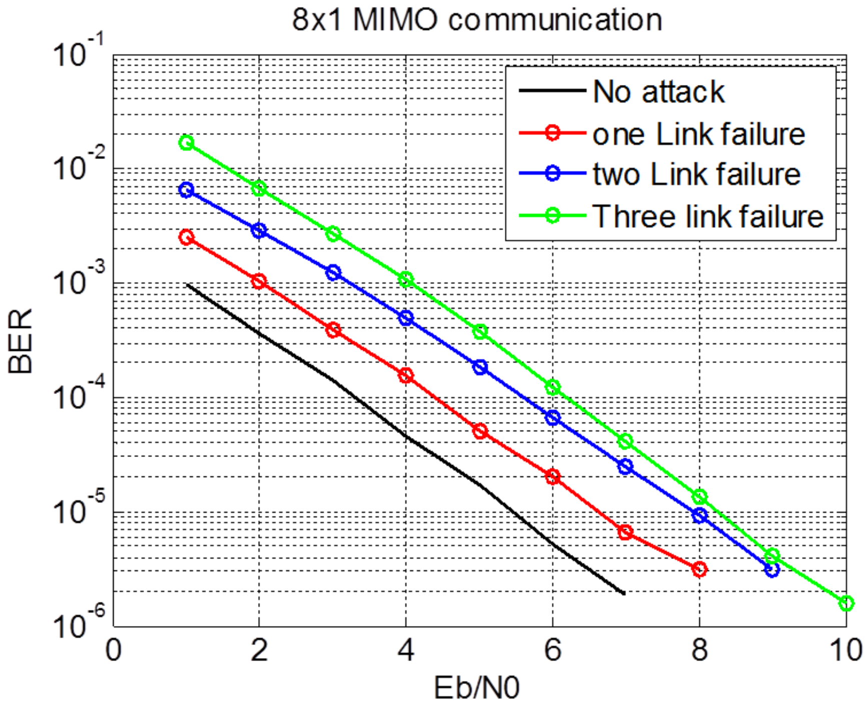

Figure 5-19Performance of 8x1 system under link failure scenario

5.7 Conclusion

This thesis has investigated the security and reliability challenges in smart grid applications. To combat severe communication impairments induced by malicious attacks or link failures, implementation of space-time block coding over multiple transmitter and/or multiple antennas at receiver has been proposed.

First, security challenges from malicious additive attacks have been analyzed. Furthermore, the BER performance under different kinds of additive attacks have been scrutinized. Simulation shows that additive attacks with different variance pattern could be effectively mitigated using space-time block coding. Also, it has been verified that more antennas will give more diversity gain and better performance. Link adaption technique also helped to improve performance in the case of malicious attack scenario.

Reliability challenges from link failures is then considered. It showed that space-time block coding could provide satisfying performances with lower complex design in a link failure scenario.

Data piracy by intruder is one of the most severe and dangerous attacks on smart meters. Even with link adaption techniques and higher order channels coding, we cannot recover correct data by just using space time block codes. Moreover, it has also been verified that LOS factor is as beneficial in malicious attack scenario as it is destructive in data piracy case.

Chapter 6 Future Work

After numerous simulations on various attacks and link failure cases, it can be concluded that STBC is effective except in the case of data piracy which looks very severe. Corrupted data cannot be recovered by the virtue of it. It may be recovered if corrupted data could be sensed from big bunch of data and process or neglect that data. With “Big Data” analytics, corrupted data can be segregated from big chunk of data and can be analyzed according to 3 V’s i.e. Volume, Velocity and Veracity.

Smart meter in smart grids requires a continuous real time communication between end to end nodes. It results in big data received in small interval of time. If this data is corrupted then it is very important to not only sense corrupted data but it should be done in a small interval of time to avoid further consequence in power distribution. With “Big Data Analytics” it may be possible.

References

1. Metke AR, Ekl RL. Security technology for smart grid networks. IEEE Transactions on Smart Grid Jun.2010; 1(1): 99–107
2. Perprot to NIST on Smart Grid Interoperability Standards Roadmap EPRI, Jun. 17, 2009.
3. H. Khurana, M. Hadley, N. Lu and D. A. Frinke ”Smart-grid security issues,” IEEE Security and Privacy, vol.8, no.1, pp. 81-85, Jan. 2009.
4. P. Mcdaniel and S. Mclaughlin ”Security and privacy challenges in the smart grid,” IEEE Security and Privacy, vol.7, no.3, pp. 75-77, Jun. 2009.
5. C. E. Shannon, ”Communication theory of secerecy systems,” Bell Syst. Techn. J., vol.28, pp. 656-715, Oct. 1949.
6. A. D. Wyner, ”The wire-tap channel,” Bell Syst. Techn. J., vol.54,no.8, pp. 1355-1387, Oct. 1975.
7. A. Hero, ”Secure space-time communication,” IEEE Transactions on Information Theory, vol.49, no.12, pp. 3235-3249, Dec. 2003.
8. C. E. Landwehr and D. M. Goldschlag, ”Securtiy issues in Networks with internet access” Proc. IEEE, vol.85, pp. 2034-051, Dec. 1997.
9. F. Petitcolas and R. Anderson, and M. Kuhn ”Information hiding-a survey,” Proc. IEEE, vol.87, pp. 1062-1078, Jul. 1999.
10. H. Jafarkhani, Space-time coding: theory and practice, Cambridge University. Press, 2005.
11. J. G. Proaksi, Digtial Communication, 4th ed. New York: McGrawHill, 2001.
12. J. N. Laneman, D. Tse and G. W. Wornell, ”Cooperative diversity in wireless networks: efficient protocols and outage behavior,”, IEEE Transactions on Information Theory, vol.50, no.12, pp. 3062-3080, Dec. 2004.
13. A. J. Viterbi, Error bounds for convolutional codes and an asymptotically optimal decoding algorithm, IEEE Trans.Inform. Theory 13: 260–269 (April 1967).
14. G. D. Forney, Jr., The Viterbi algorithm, Proce. IEEE 61:268–278 (March 1973).
15. G. D. Forney, Jr., Convolutional codes II: Maximum likelihood decoding, Inform. Control 25: 222–266 (July 1974).
16. S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, A softinput soft-output APP module for the iterative decoding of concatenated codes, IEEE Commun.Lett. 1(1): 22–24 (Jan.1997).

17. http://www.radio-electronics.com/

Biographical Information

Amit Abhimanyu Deokar completed his Bachelor degree in Electronics and Telecommunication Engineering from University of Pune, India in 2009. After bachelor degree, in 2010, he pursues his graduate studies in the Department of Electrical Engineering at The University of Texas at Arlington. During his graduate studies he worked under the guidance of Dr. Qilian Liang in the Wireless Communication and Networking Lab. He also interned at Ericsson .