ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 9, September 2016

Design and Comparison of Security Enhanced Communication System

Rajan Kumar, Sandeep Kaur

***Abstract* — In communication system, occurrence of errors is one of the concerning factor which reduces security as well as effectiveness of system. To develop a minimal error affected system, various error controlling and detecting codes are adopted to provide a secured and effective throughput. Convolution and trellis coding is such an approach for detection and correction of errors in long distance communication. A system should be designed to detect, prevent and correct the errors.**

***Index Terms* — Convolutional, Trellis, BER, QPSK.**

I. INTRODUCTION

In open networked systems, information is being received and misused by adversaries by means of facilitating attacks at various levels in the communication. The encryption standards such as DES (Data Encryption Standard), AES (Advanced Encryption Standard), and EES (Escrowed Encryption Standard) are used in Government and public domains. With today's advanced technologies these standards seem not to be as secure and fast as one would like. High throughput encryption and decryption are becoming increasingly important in the area of high speed networking. With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and encryption is one the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, and military communication. There already exist several image encryption methods. They include SCAN-based methods, chaos-based methods, tree structure-based methods, and other miscellaneous methods. However, each of them has its strength and weakness in terms of security level, speed, and resulting stream size metrics. We hence proposed the new encryption method to overcome these problems.

Communication is a major impact in today's business. The communication devices transmit large amount of data with high security. In business, the amount approximately worth over $1 trillion is being transacted every week on the Net. But, unfortunately, the cyber-crimes are nearly 97% and such crimes are undetected. The security is still remains a risky one. At present, various types of cryptographic the algorithms provide high security in information, computer and network-related activities. These algorithms are required to protect the data, integrity and authenticity from various attacks [1]. This paper discusses a new technique of encryption algorithm which combines a convolution method and trellis generator.

Figure 1 shows the Convolutional encoder/decoder position in a digital communication system. Convolutional encoding is the way of channel encoding. Here, redundant bits are used for error determination. QPSK is most effectively used as modulation scheme [10].

In telecommunication, a convolutional code is a type of error-correcting code that generates parity symbols via the sliding application of a boolean polynomial function to a data stream. The sliding application represents the 'convolution' of the encoder over the data, which gives rise to the term 'convolutional coding.' The sliding nature of the convolutional codes facilitates trellis decoding using a time-invariant trellis. Time invariant trellis decoding allows convolutional codes to be maximum-likelihood soft-decision decoded with reasonable complexity. The operation of a convolution encoder can be explained in several but equivalent ways such as, by

a) State diagram representation
b) Tree diagram representation and
c) Trellis diagram representation.

a) State Diagram Representation

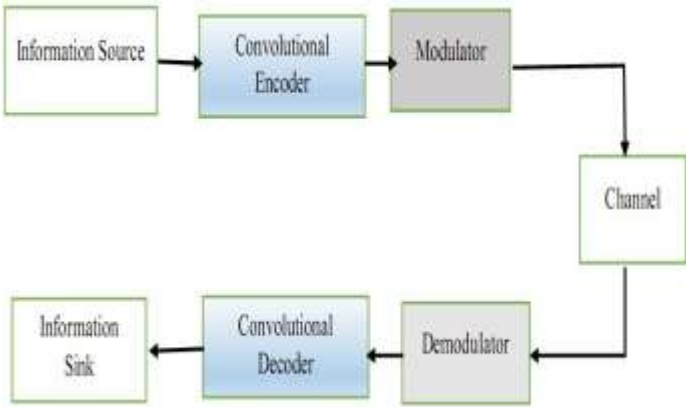

Figure1. Convolutional encoder/decoder position in a digital communication system

Manuscript received Sep, 2016.

***Rajan Kumar**, Department of Electronics & Communication Engineering, Punjab Technical University Jalandhar / GVIET/ Ramnagar, Banur, Punjab, India, Chandigarh, India, 7508680085.*

***Sandeep Kaur**, Department of Electronics & Communication Engineering, Punjab Technical University Jalandhar / GVIET / Ramnagar, Banur,Punajb, India, 9815206662,*

II. LITERATURE REVIEW

Salehe I. Mrutu et al.[2] discussed that for more than half a century, Forward Error Correction Convolutional Codes (FEC-CC) have been in use to provide reliable data communication over various communication networks. The recent high increase of mobile communication services that require both bandwidth intensive and interactive Real Time Applications (RTAs) impose an increased demand for fast and reliable wireless communication networks. Transmission burst errors; data decoding complexity and jitter are identified as key factors influencing the quality of service of RTAs implementation over wireless transmission media. This paper reviews FEC-CC as one of the most commonly used algorithm in Forward Error Correction for the purpose of improving its operational performance. Under this category, we have analyzed various previous works for their strengths and weaknesses in decoding FEC-CC. A comparison of various decoding algorithms is made based on their decoding computational complexity.

Sandhu & paulraj in [3] presented Space-time block codes as remarkable modulation scheme discovered recently for multiple antenna wireless channels. They have well-designed mathematical solution for providing the full diversity over coherent, the flat-fading channel. In addition, they necessitate very simple encoding & decoding at transmit antenna & receive antenna respectively. They showed that even though scheme provided the full diversity at the low computational costs scheme incur a loss in its capacity.

Lai et al. [4] simulate the concatenated convolutional or the turbo codes with 2 temporally & spatially correlated antennas in the framework of WCDMA, but do not provide any analysis. Another class of space-time codes is trellis based spacetime codes (e.g. spacetime trellis codes [5], superorthogonal space-time trellis codes [6] etc.). These codes incorporate coding and diversity into a single design. Much of the analysis of these systems concentrates on uncorrelated antennas, e.g., the analysis of spacetimecodes in [7] and the analysis of super-orthogonal codes in [8]. In a few isolated cases, attempts have been made to explore the performance of MIMO systems when antennas are correlated.

Baraka W. Nyamtiga et al. [9] discussed that in mobile banking schemes; financial services are availed and banking services are provided using mobile devices. GSM services are greatly utilized for data transmission by the technologies used in conducting mobile transactions. In their operations; these technologies send data in plaintext. Financial service providers tend to rely on the security services provided by the GSM which has been proved to be susceptible to cryptanalytic attacks. The used algorithms for crypto mechanisms are flawed leaving data carried through the network vulnerable upon interception. Operators need to take precaution by enforcing some protective measures on the information to be transmitted. This paper describes an SMS based model designed with security features to enhance data protection across mobile networks. Features for data encryption, integrity, secure entry of security details on the phone, and improved security policies in the application server are incorporated. They address issues of data confidentiality, user authentication and message integrity in order to provide end-to-end security of data carried on GSM networks.

III. EXPERIMENT AND RESULT

In telecommunication, a convolutional code is a type of error-correcting code that generates parity symbols via the sliding application of a boolean polynomial function to a data stream. The sliding application represents the 'convolution' of the encoder over the data, which gives rise to the term 'convolutional coding.' The sliding nature of the convolutional codes facilitates trellis decoding using a time-invariant trellis. Time invariant trellis decoding allows convolutional codes to be maximum-likelihood soft-decision decoded with reasonable complexity. In thesis we give the comparison between modulation using convolutional and trellis code and modulation without convolutional and trellis code. Figure 2 shows the input data stream before encoding.

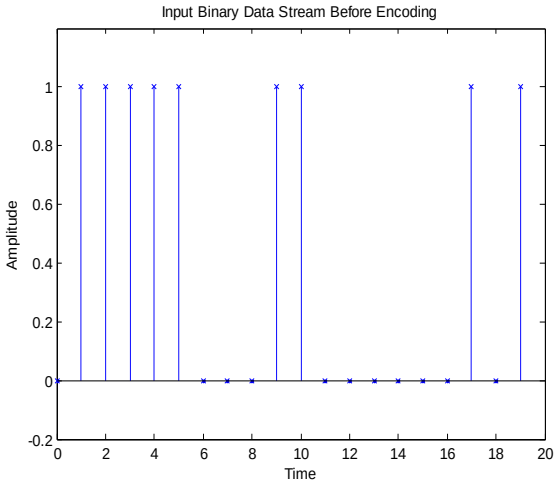

Figure 2 Input Binary Data stream before encoding

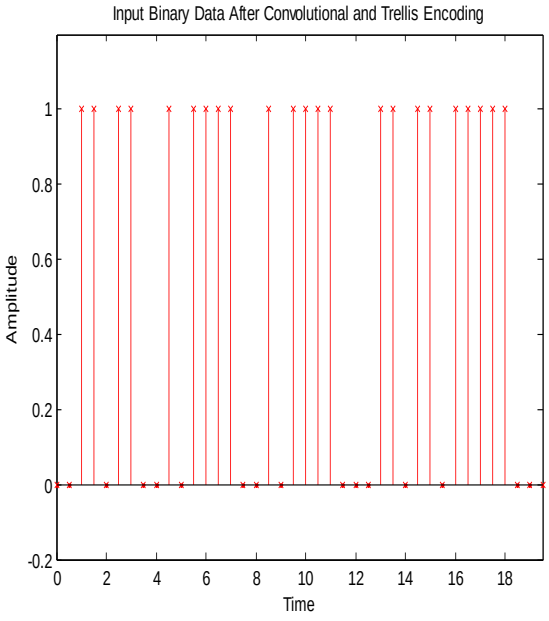

Figure 3 Input binary data after Convolutional and Trellis encoding

Figure 3 shows the binary data after convolutional and trellis encoding. The information bearing message stream is encoded in a continuous fashion by continuously interleaving information bits and error control bits.

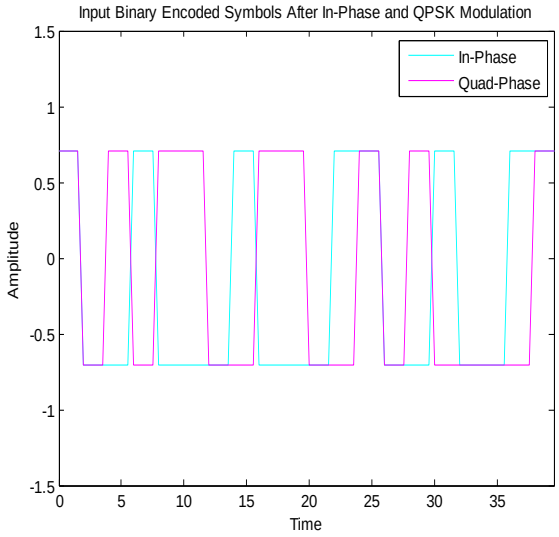

Figure 4 Input Binary encoded symbols after in-phase and QPSK Modulation

Figure 4 shows the input binary encoded symbols after in-phase and QPSK modulation.

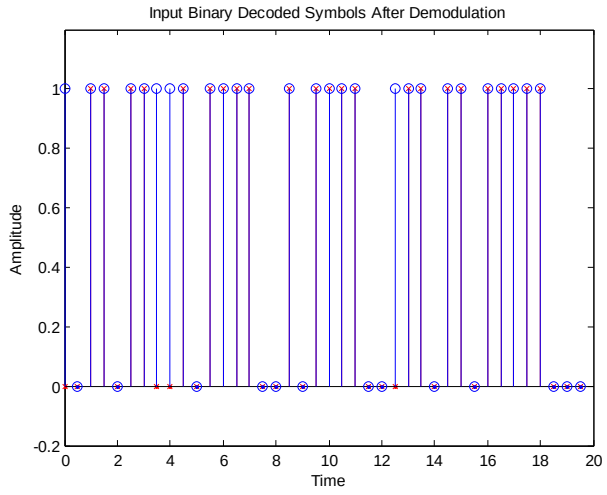

Figure 5. Input binary decoded symbols after demodulation

Figure 5 shows the input binary decoded symbols after demodulation.

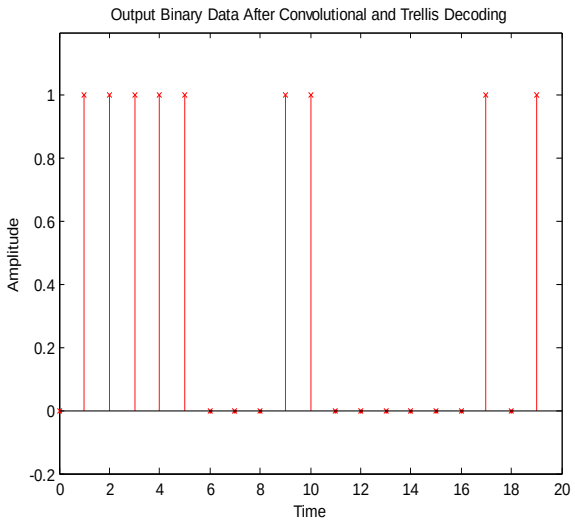

Figure 6. Output Binary data after convolutional and trellis decoding

Figure 6 shows the output binary data after convolutional and trellis decoding.

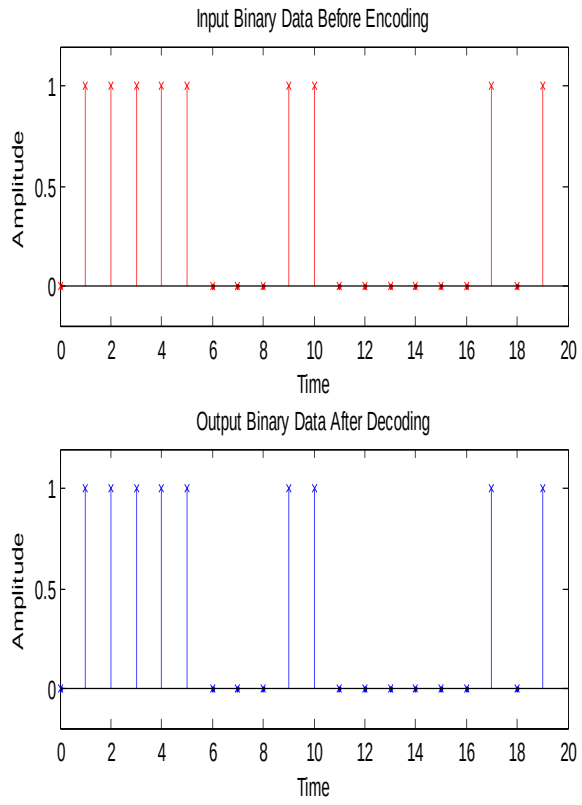

Figure 7. Input Binary data before encoding and Output binary data after decoding

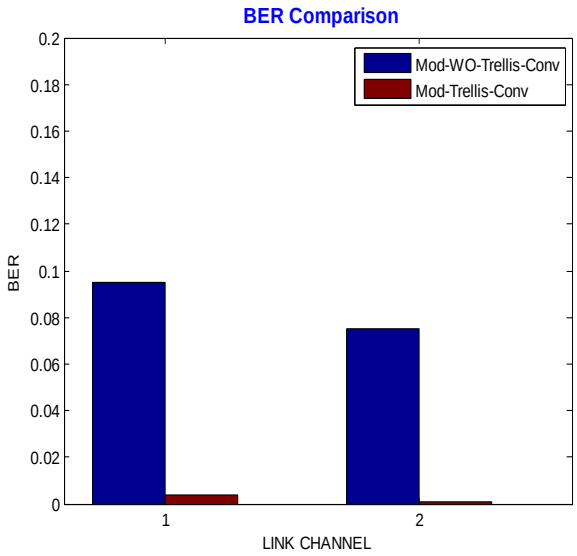

Figure 8. BER comparison of modulation without trellis convolution code and with trellis convolutional code

Figure 8 shows the Bit Error Rate comparison for two channels without trellis convolution code and with trellis convolutional code. This shows that the bit error rate decreases in both channels as we use the convolution and trellis code for encoding. But it increases without convolution and trellis encoding.

REFERENCES

[1] Shaik Rasool, G. Sridhar, K. Hemanth Kumar and P. Ravi Kumar(2011), "Enhanced Secure Algorithm For Message Communication", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5.

[2] Salehe I. Mrutu, Anael Sam and Nerey H. Mvungi(2014), "Forward Error Correction Convolutional Codes for RTAs' Networks: An Overview", I.J. Computer Network and Information Security, 2014, 7, 19-27.

[3] S. Sandhu, and A. Paulraj, "Space-time block codes: a capacity perspective," IEEE Communications Letters, vol. 4, no. 12, pp. 384- 386, 2000.

[4] J. Lai and N. B. Mandayam, "Performance of turbo coded WCDMA with downlink space-time block coding in correlated fading channels," accepted for publication in IEEE transaction on wireless communications, 2002.

[5] V. Tarokh, N. Seshardi, and A. Calderbank, "Space-time codes for high data rate wireless communication: Performance criteria and code construction," IEEE Trans. Inform. Theory, vol. 44, no. 2, pp. 744-765, March 1998.

[6] H. Jafarkhani and N. Seshadri, "Super-orthogonal space-time trellis codes," IEEE Transactions on Information Theory, vol. 49, no. 4, April 2003.

[7] M. K. Simon, "Evaluation of average bit error probabilities for space time coding based on a simpler exact evaluation of pairwise error probability," Journal of Communications and Networks, vol. 3, no. 3, pp. 257-264, September 2001.

[8] M. K. Simon and H. Jafarkhani, "Performance evaluation of superorthogonal space-time trellis codes using a moment generating function based approach," accepted, IEEE Transaction on Signal Processing, 2003.

[9] Baraka W. Nyamtiga, Anael Sam, Loserian S. Laizer(2013), "Enhanced Security Model for Mobile Banking Systems In Tanzania", International Journal of Technology Enhancements and Emerging Engineering Research, Vol 1, Issue 4.

[10] Neha, Gh.Mohammad Rather(2015), "Convolution Error Control Coding -A Review", Proceedings of 18th IRF International Conference, Pune, India.

BIOGRAPHY

Mr. Rajan Kumar is currently pursuing M.TECH (final year) in department of Electronics and communication Engineering GurukulVidyapeeth Institute of Engineering and Technology,Ram Nagar, Banur, Punjab,India.

Miss Sandeep Kaur is currently assistant professor at Gurukul Vidyapeeth Institute of Engineering and Technology,Ram Nagar, Banur (Punjab). She has completed her M.tech from University College of Engineering (UCoE) Punjabi University Patiala,India and B.tech from Yadavindra College of Engineering & Technology, Guru kashi campus Talwandi Sabo Bathinda , university, Patiala, India. She has 3 Years 8 months of academic experience. She has authored 8 research papers in reputed international journals and 6 papers and national conferences. Her areas of interest are wireless communication and signal processing & MATLAB.