Pseudo Random Generator Based Public Key Cryptography

Neha Saini[1], Kirti Bhatia[2]

[1]M. Tech (Student), SKITM, Ladrawan,Haryana, India
[2]HOD of CSE department, SKITM, Ladrawan, Haryana, India

Abstract*— *Advances in communication technology have seen strong interest in digital data transmission. However, illegal data access has become more easy and prevalent in wireless and general communication networks. In order to protect the valuable data from illegal access, different kinds of cryptographic systems have been proposed. In this paper, a new integrating channel coding and cryptography design communication systems is proposed. So we use cryptography as an error detection tool. In order to preserve the advantages of encryption and to improve its disadvantages, we place the encryptor before the encoder. The hamming encoder is used to select the generator matrix to be used as a block code to form the new system .In this the security of common cryptographic primitive i.e a key stream generator based on LFSR can be strengthened by using the properties of a physical layer.So, a passive eaves dropping will experience great difficulty in cracking the LFSR based cryptography system as the computational complexity of discovering the secret key increases to large extent. The analysis indicates that the proposed design possesses the following feature. Its security is higher than the conventional one with the channel encoder only. Privacy is more due to unknown random codes. As the applied codes are unknown to a hostile user, this means that it is hardly possible to detect the message of another user. Anti-jam performance is good. It overcomes the disadvantage of Chaos based cryptography system as input data is not extended and hence bandwidth is not wasted. Moreover, the computer simulation shows that the proposed system has a good ability in error detection especially when the SNR per bit is moderate high, and the detection ability is enhanced when the increased length of Hamming code is employed.

***Keywords*— Cryptography, LFSR, Pseudorandom codes, hamming codes.**

I. INTRODUCTION

Cryptography is the study of secret (crypto) writing (graph). Attempt to retrieve plain text or key is called Cryptanalysis. Cryptanalysis and Cryptography together are called Cryptology. Cryptanalysis to the science and art of breaking them with the knowledge of the sender; while cryptology, often shortened to just crypto, is the study of both. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries. The input an encryption process is commonly called the plaintext, and the output the cipher-text. Within the context of any application-to-application communication, there are some specific security requirements, including:

- Authentication: The process of proving one's identity.
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original

The communication services not only need to be provided but rather provided in a secure and reliable manner. For reliable transmission of data over the imperfect channel, channel coding is done. Linear block codes and convolutional codes are mainly used for channel coding. The basic linear block codes used are hamming codes. Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is system presented in this thesis is designed to merge channel coding with the cryptography to provide more security to the data signal to be transmitted over the channel. To reduce the computational and communication cost of two major cryptographic operations say channel coding and cryptography has been combined.

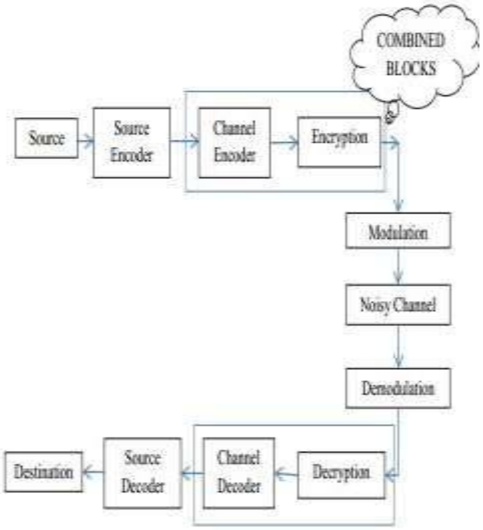

Fig.1: Block Diagram of Communication System

II. PROPOSED ANALYSIS OF CHANNEL CODING TECHNIQUE USING PUBLIC CRYPTOGRAPHY SYSTEM.

Various Steps Have Been Followed For Merging Channel Coding And Encryption Block In Communication System, So That More Secure Transmission Of Data Without The Increase In Bandwidth Can Be Achieved Than The Conventional One With Channel Encoder Only, and Are Explained Step By Step. Fig.2 Shows The Flowchart Of Proposed Channel Coding Using Public Cryptography.

A. Using Symmetric Secret Key

Each encryption system requires a key (or crypto variable) to function and all of the secrecy in the encryption process is maintained in the key. The keys may be identical or there may be a simple transformation to go between the two keys. The key represents a shared secret between two parties to communicate that can be used to maintain a private information link.

B. Generating Pseudo Random Sequence Using LFSR

A linear feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state. The most commonly used linear function of single bit is XOR. Thus, an LFSR is most often a shift register whose input bit is driven by the exclusive-or (XOR) of some bits of the overall shift register value.

For a 4-bit key, tapping is defined by the polynomial, Polynomial: x4+x3+1

The initial value of the LFSR is called the seed, and because the operation of the register is deterministic, the stream of values produced by the register is completely determined by its current (or previous) state. Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle. A 4 bit key is given as input to the filter then this will generate a long p-n sequence.

C. Encoding and Encrypting

Error control coding is a method to detect and possibly correct errors by introducing redundancy to the stream of bits to be sent to the channel. The Channel Encoder will add bits to the message bits to be transmitted systematically.

D. Decoding and Decrypting

Decoding Hamming codes is almost as simple as encoding. The parity check matrix is used to decode linear block codes with generator matrix G. The parity check matrix H corresponding to a generator matrix G = [Ik|P] is defined as:

H= [PT| In-k]

It is easily verified that GHT= 0k, n−k, where 0k,n−k, denotes an all zero k ×(n−k) matrix. A given code word C in the code is obtained by multiplication of the information bit sequence i by the generator matrix, G: C = i*G.

III. RESULTS

The proposed system is tested for BER at different SNR values using MATLAB software version 7.0. BER comparison is shown for the transmitted signal over the noisy channel with and without channel coding. Since a secret key is used to generate the p-n sequence which is further used to select the G-matrix, it is impossible for intruder to decrypt the data and crack the channel code.

CASE1: When the data is transmitted over a channel without any channel coding.

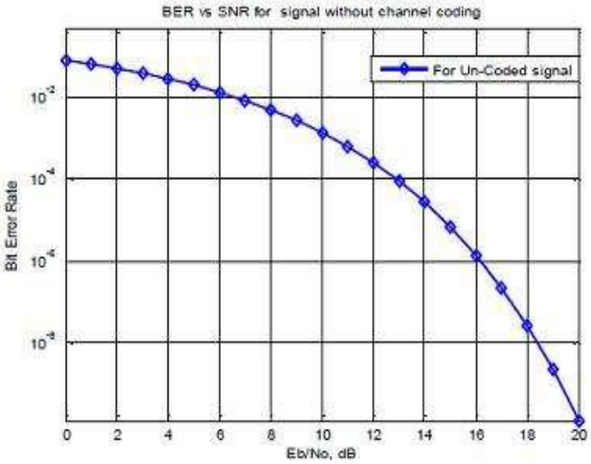

Fig. 2: SNR vs. BER Graph for Case

Table.1: SNR vs. BER Graph for Case 1

SNR value in dB	BER for data without channel coding
0	0.07865
1	0.06373
2	0.050219
3	0.038323
4	0.028184
5	0.019864
6	0.013328
7	0.00845
8	0.005017
9	0.002761
10	0.001392
11	0.000634
12	0.000256
13	9.05E-05

Figure and table for case1 above shows the results that BER is very high even for the moderate SNR i.e. above 13 db. So to reduce BER channel coding technique is used.

CASE 2: When data is transmitted over the channel without channel coding and with channel coding using cryptography. At the receiver side, the received word is decoded using the same key used at transmitter end. Fig. 3 shows the comparison for SNR and BER for data with and without channel coding.

Table.2: Comparison of data transmission with and without channel coding for 1-20 SNR

SNR value in dB	BER for data without channel	BER for data with channel
	coding	coding
0	0.07865	0.119545
1	0.06373	0.084665
2	0.050219	0.055140
3	0.038323	0.031610
4	0.028184	0.016035
5	0.019864	0.006425
6	0.013328	0.002385
7	0.00845	0.000620
8	0.005017	0.000140
9	0.002761	3.50E-05
10	0.001392	0
11	0.000634	0
12	0.000256	0
13	9.05 E-05	0
14	2.73 E-05	0
15	6.83 E-06	0
16	1.38 E-06	0

Table.3: SNR vs. BER Graph for case3

SNR value in dB	*BER for data without channel coding*	*BER for data with channel coding*	*BER for data with channel coding using wrong key*
0	*0.078650*	*0.12058*	*0.50000*
1	*0.063730*	*0.08313*	*0.50000*
2	*0.050219*	*0.05480*	*0.37500*
3	*0.038323*	*0.03170*	*0.50000*
4	*0.028184*	*0.01589*	*0.40625*
5	*0.019864*	*0.00667*	*0.53125*
6	*0.013328*	*0.00229*	*0.59375*
7	*0.008450*	*0.00055*	*0.46875*
8	*0.005017*	*0.00018*	*0.43750*
9	*0.002761*	*0*	*0.50000*
10	*0.001392*	*0*	*0.53125*
11	*0.000634*	*0*	*0.46875*

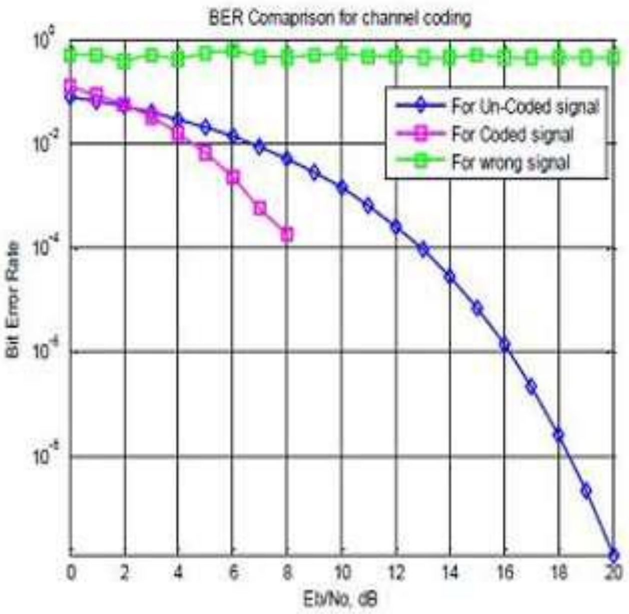

Fig.3: Shows SNR vs BER graph for the various signals

In above case shows that when data is intercepted by wrong receiver and tries to crack it using wrong key the BER will increase drastically to large value for SNR values more than 9.

CASE 4: Considering the worst case if intruder knows the key length and is able to calculate the LFSR sequence but still not knowing the number of bits of LFSR sequence used to select G-matrix. Fig.4 shows SNR vs BER graph for the various signals.

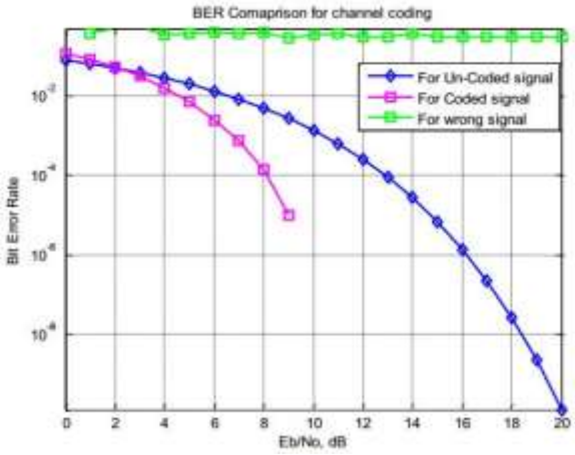

Fig.4: SNR vs. BER Graph for Case 4

In this case even if the intruder knows the key and its length then even he can‟t crack the data because pseudorandom codes generated using LFSR i.e which pn sequence we are using for channel coding .So again the BER will be high for moderate SNR The output of the system is in decimal notation and powers of 10 are represented in scientific „E‟ notation. When data is transmitted using L‟ bit key and it is intercepted unauthenticated receiver who tries to crack the channel coding using random key. Fig.4.3 shows SNR vs BER graph for the various values of SNR i.e 0 to 20 db. If intruder knows the key length and is able to calculate the LFSR sequence but still not knowing the number of bits of LFSR sequence used to select G-matrix So, for the coded data, the probability of error is nearly 0 for moderate SNR but BER for the signal decoded by the intruder using unknown key is quite high.

IV. CONCLUSION

Channel Coding using pseudo random generator using public key Cryptography is an efficient system for correction of channel decoding results of messages which are protected by security mechanisms. It would be very hard for intruder to guess the right G matrix and to interpret the right information as different G-matrix is used for each data block. Analysis shows that the bir error rate has been reduced to zero value as signal is increased to large value by using the proposed system. Hence, this system provides better security than the conventional one with the channel encoder only. Anti-jam performance is also good. It overcomes the disadvantage of cryptography system as no additional redundancy, in the form of additional bits that are added to data, is used and hence bit rate reduces and lower bandwidth is needed for transmission. Thus, the system becomes more efficient. Moreover, the computer simulation shows that the proposed system has a good ability in error detection and correction especially when the SNR per bit is moderately high.

V. FUTURE SCOPE

Future work should include analysis of the influence of Channel Coding using Cryptography to different channel encoders with implementation, proof and comparison. For the intruder, the probability of error should be increased to maximum. Also, the improvement in the current security level, fast speed and reliable message recovery at receiver end with respect to key generation, encryption, decryption, signing and verification with small key length for data

REFERENCES

[1] Shannon, C.; (1953), "General treatment of the problem of coding," Information Theory, IRE Professional Group, vol.1, no.1, pp.102-104.

[2] Wax, N.;(1959), "On upper bounds for error detecting and error correcting codes of finite length," Information Theory, IRE Transactions on , vol.5, no.4, pp.168-174.

[3] Marquart, R. G.; Hancock, J. C.; (1963), "Performance of Hamming Codes," Space Electronics and Telemetry, IEEE Transactions, vol.9, no.4, pp.115-126.

[4] Simon Haykin,(1988), " Digital Communications", John Wiley & Sons, New York.

[5] Agnew, G.B.(1990), "Cryptographic systems using redundancy," Information Theory, IEEE Transactions on , vol.36, no.1, pp.31-39.

[6] Rivest, Ronald L. (1990), "Cryptology", Handbook of Theoretical Computer Science vol. 1, pp. 717-755.

[7] Ranjan Bose (2002), "Information theory, Coding & Cryptography", Tata McGraw-Hill, New Delhi.

[8] Ziviae, N.; Ruland, C.; Rehman, O.U.; (2009), "Error correction over wireless channels using symmetric cryptography," Wireless Communication, Vehicular Technology, 1st International Conference on , vol., no., pp.752-756.

[9] Zivic, N.; Rehman, O.U.; Ruland, C.; (2009), "Using HMAC for Error Correction over a Wireless Channel," Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC '09. Symposia and Workshops, vol., no., pp.252-256.

[10] Chan Chen; Jensen, M.A.; (2010), "Improved channel quantization for secret key establishment in wireless systems," Wireless Information Technology and Systems (ICWITS), IEEE International Conference on, vol.,