ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 10, October 2016

Comparative Analysis of Direct Sequence Spread Spectrum using Rabbit Stream Cipher

B. Sree Devi*

J.L.Jini Mary*

G.Monica Bell Aseer*

*Assistant professor, Department of Electronics and Communication, VV College of Engineering

***Abstract*- The main objective of the work is to design and develop a secure wireless system using direct sequence spread spectrum and Rabbit stream cipher which combats to hostile jamming and interference at very weak signals. To develop a PN code for the system to save it from external interference and reduce the error rate of the system in jamming environment. The performance analysis of DSSS under different jamming environments is analysed to securely transmit the data.**

***Index Terms* – Bit Error Rate, Direct sequence spread spectrum, Security, Wireless networks.**

I. INTRODUCTION

Spread spectrum is a means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information. The band spread is accomplished by means of a code which is independent of the data, and synchronized reception with the code at the receiver is used for de-spreading and subsequent data recovery.The use of these special pseudo noise codes in spread spectrum (SS) communications makes signals appear wide band and noise-like. It is this very characteristic that makes spread spectum signals possess the quality of Low Probability of Intercept. Spread spectrum signals are hard to detect on narrow band equipment because the signal's energy is spread over a bandwidth of maybe 100 times the information bandwidth.

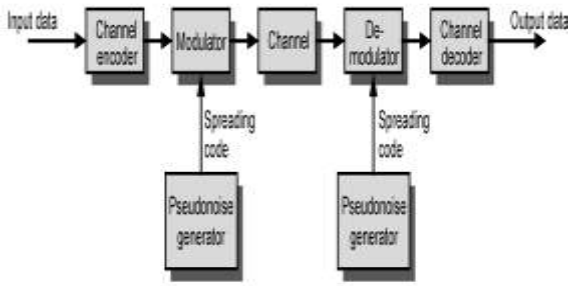

Figure 1: General Model of Spread Spectrum System

Spread Spectrum uses wide band, noise-like signals. Because Spread Spectrum signals are noise-like, they are hard to detect. Spread Spectrum signals are also hard to Intercept or demodulate. Further, Spread Spectrum signals are harder to jam (interfere with) than narrowband signals. These Low Probability of Intercept (LPI) and anti-jam (AJ) features are why the military has used Spread Spectrum for so many years. Spread signals are intentionally made to be much wider band than the information they are carrying to make them more noise-like.

The main objectives of spread spectrum modulation are

- To avoid being detected.
- To prevent eavesdropping.
- To prevent the jamming of signals.

II. DIRECT SEQUENCE SPREAD SPECTRUM

Conceptually, spread spectrum generators are rather simple devices, having been aptly referred to as "glorified shift registers." In short, they generate linear recursive sequences (LRS) using a linear-feedback shift register (LFSR).

These sequences are often referred to as pseudo noise, or PN, codes because of their noise-like properties. But, while the sequences do appear random for a while, they *will* eventually repeat in a periodic fashion.

In a direct-sequence spread spectrum transmitter, the digital data stream to be transmitted is multiplied by a PN sequence running at a much higher clock rate, or chip rate, than the baud rate of the data. This results in the frequency spectrum of the data being spread by a factor equivalent to the chip-rate/baud-rate ratio. This ratio is called the *processing gain*, and is a measure of the interference rejection provided by the system.

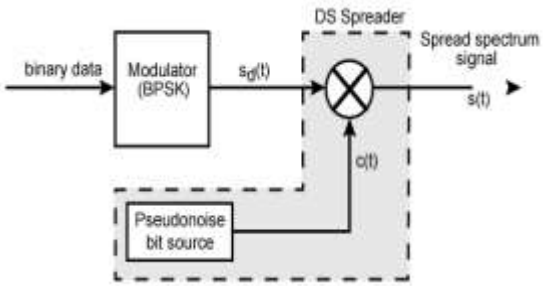

Figure 2: Direct Sequence Spread Spectrum

Transmitter

Direct-sequence spread-spectrum transmissions multiply the data being transmitted by a "noise" signal. This noise signal is a pseudorandom sequence of 1 and −1 values,

at a frequency much higher than that of the original signal, thereby spreading the energy of the original signal into a much wider band.

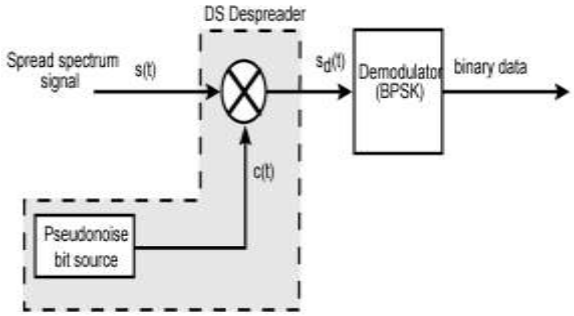

Figure 3: Direct Sequence Spread Spectrum

Receiver

III. USES OF DSSS

The United States GPS, European Galileo and Russian GLONASS satellite navigation systems .DS-CDMA (Direct-Sequence Code Division Multiple Access) is a multiple access scheme based on DSSS, by spreading the signals from/to different users with different codes. It is the most widely used type of CDMA.

Cordless phones operating in the 900 MHz, 2.4 GHz and 5.8 GHz bands ,IEEE 802.11b 2.4 GHz Wi-Fi, and its predecessor 802.11-1999. (Their successor 802.11g uses OFDM instead),Automatic meter reading,IEEE 802.15.4 (used e.g. as PHY and MAC layer for ZigBee)

IV. ADVANTAGES OF DSSS

DSSS has the advantage of providing higher capacities than FHSS, but it is a very sensitive technology, influenced by many environment factors (mainly reflections). The best way to minimize such influences is to use the technology in either (i) point to multipoint, short distances applications or (ii) long distance applications, but point to point topologies.

In both cases the systems can take advantage of the high capacity offered by DSSS technology. As so, typical DSSS applications include indoor wireless LAN in offices (i), building to building links (ii), Point of Presence (PoP) to Base Station links (in cellular deployment systems) etc.

V. PERFORMANCE OF DSSS

- Under AWGN
- Pulse noise jamming
- Synchronization between transmitter and receiver
- No synchronization
- BER for multiuser case

A. Pulse Noise Jamming

Consider a coherent binary phase-shift keyed (BPSK) communication system which is being used in the presence of a pulse –noise jammer. A pulse noise jammer transmits pulses of band limited white Gaussian noise having total average power J referred to the receiver front end. The jammer may choose the center frequency and width of the noise to be identical to the receiver's center frequency and bandwidth. In addition, the jammer chooses its pulse duty factor p to cause maximum degradation to the communication link while maintaining constant average transmitted power J.

The bit error probability of a coherent BPSK system is given by

$$P_e = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \qquad (1)$$

Where E_b represents the received energy per binary symbol and N_0 is the one-sided receiver front-end thermal noise power spectral density. when transmitting ,the noise jammer increases the receiver noise power spectral density from N_0 to $N_0 + \frac{N_j}{\rho}$,where $N_j = \frac{J}{W}$ is the one sided average jammer power spectral density and W is the one-side transmission bandwidth. The jammer transmits using duty factor ρ, the average bit error probability is

$$P_E = (1-\rho)\, Q\left(\sqrt{\frac{2E_b}{N_0}}\right) + \rho Q\left(\sqrt{\frac{2E_b}{N_{0+N_J/\rho}}}\right) \qquad (2)$$

The jammer given this formula chooses ρ to maximize P_E.

When a system is being designed to operate in a jamming environment, the maximum possible transmitter power is generally used and receiver front end thermal noise can be safely neglected. In this case, the first term in the above equation vanishes and P_E can be approximated by

$$P_E = \rho Q\left(\sqrt{\frac{2E_b\rho}{N_J}}\right) \qquad (3)$$

The Q function can be bounded by an exponential yielding

$$P_E \leq \frac{\rho}{\sqrt{4\pi E_b\rho/N_J}} e^{-\frac{E_b\rho}{N_J}} \qquad (4)$$

The maximum of this function over ρ can be found be taking the first derivative and setting it equal to zero.

The maximizing ρ is found to be $\rho = N_J/2E_b$ and $P_{E,\max}$ is

$$P_{E,max}=\frac{1}{\sqrt{2\pi e}} \quad (5)$$

Here the duty factor must be less than or equal to unity so that above equation applies only when $E_b/N_J \geq 0.5$. for E_b/N_J<0.5,P_E is given by equation (2) with ρ=1.0.observe that the exponential dependence of bit error probability on signal to noise ratio of 1 has been replaced by an inverse linear relationship in above equation.

Equations (1) and (5) are plotted in figure 6,where it can be seen that the optimized pulse noise jammer causes a degradation of approximately 31.5dB relative to continuous jamming at a bit error probability of 10^{-5}.

The severe degradation in system performance caused by the pulse noise jammer can be largely eliminated by using a combination of spread spectrum technique and forward error correction coding with appropriate interleaving. The effect of the spectrum spreading will be to change the abscissa of fig 6.

B. Synchronization of Spread Spectrum

All digital communication systems must perform synchronization. Synchronization is the process of aligning any locally generated reference signals with the incoming waveform. Synchronization must be accomplished for symbol timing, frame timing, carrier frequency and possibly carrier phase. In spread spectrum systems, we have the additional burden of synchronizing the spreading waveform. Recall that in order for despreading to take place at the receiver, the locally generated spreading waveform must be aligned with the incoming spreading waveform.

Due to the low SNR prior to despreading this synchronization is a priority in the overall process and includes synchronization at the chip level and at the sequence level. The impact of timing error on the despreading process can be seen by examining the decision statistic for a DS/SS BPSK system. Recall that the received signal can be written in complex baseband notation as

$$r(t) = \tilde{s}(t) + \tilde{n}(t) = \sqrt{P}b(t)a(t) + \tilde{n}(t) \quad (6)$$

where P is the received signal power, b(t) is the data waveform, a(t) is the spreading waveform, and $\tilde{n}(t)$ is a complex Gaussian random process representing AWGN.

The simulation results for the bit error rate performance of direct sequence spread spectrum is plotted below.

VI SIMULATION RESULTS

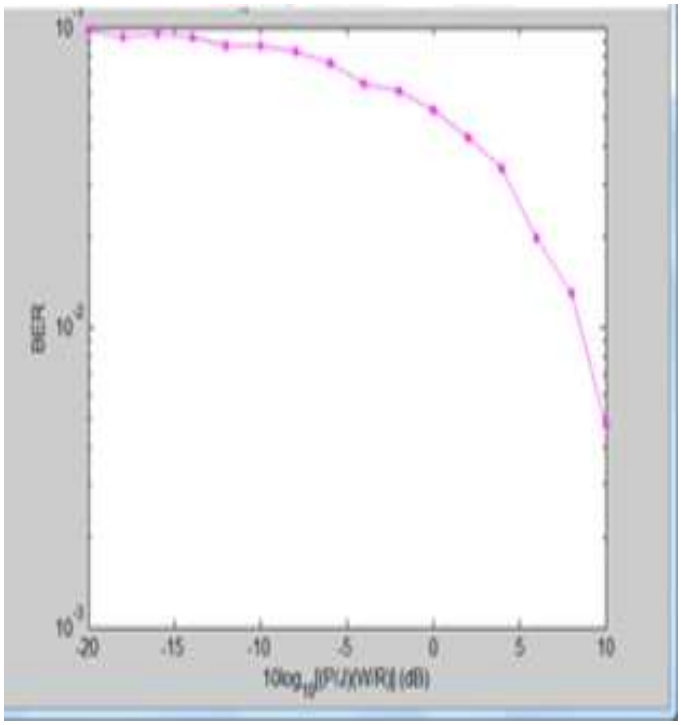

Figure 4: Performance of DSSS Under the Influence of AWGN

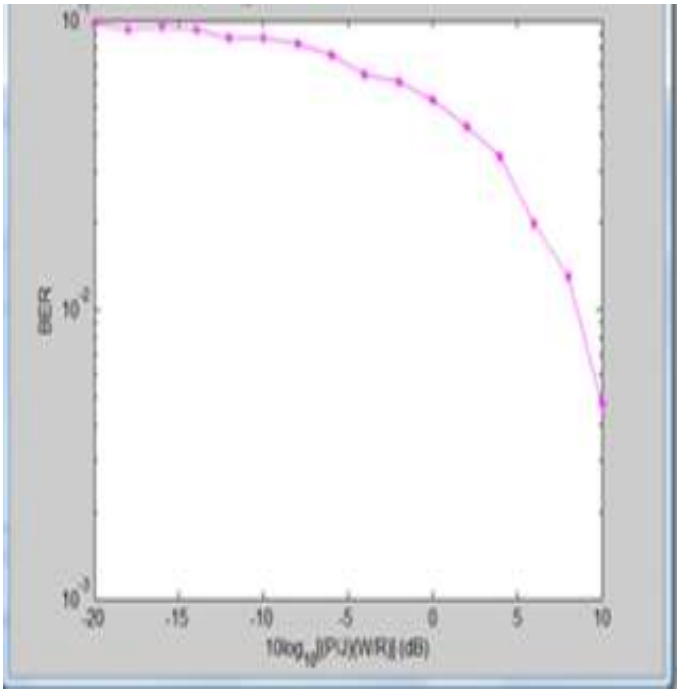

Figure 5: Performance of DSSS Under Pulse Noise Jamming

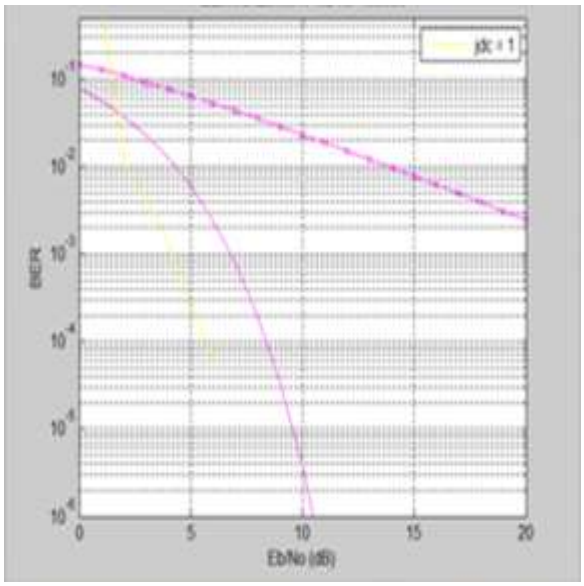

Figure 6: BER Probability under Worst Case and Continuous Noise Jammer

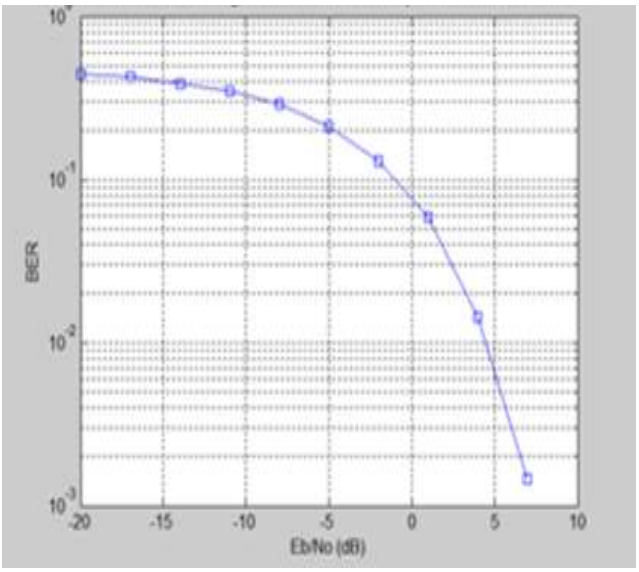

Figure 8: Eb/No Vs Pe for Random Asynchronization between Transmitter and Receiver

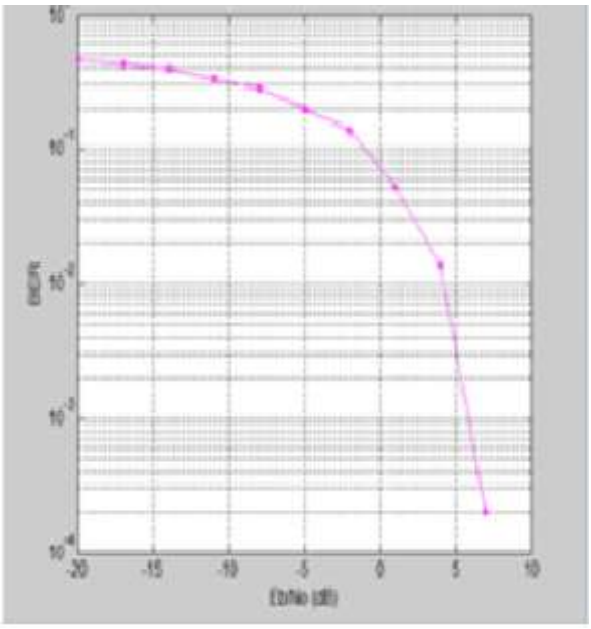

Figure 7: Synchronisation between Transmitter and Reciever

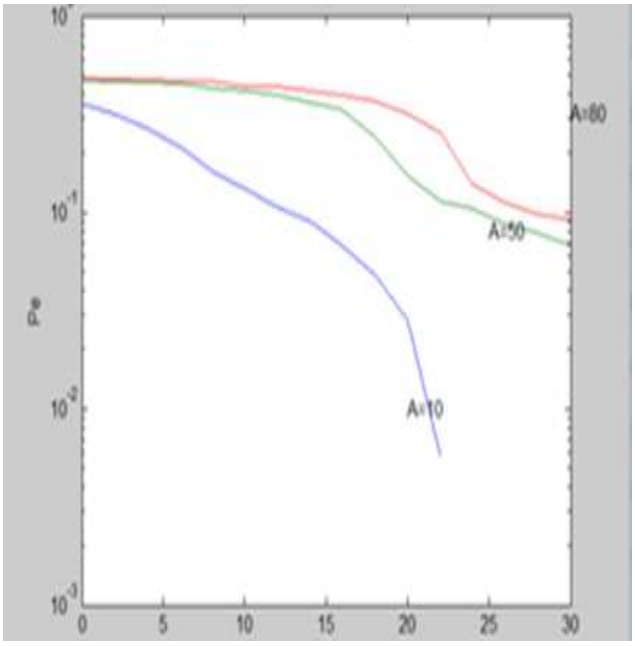

Figure 9: BER plot for multiuser BPSK system

Figure 9 shows the BER plot for multiuser BPSK system, where the number of users are taken to be A=10,A=50,A=80.. when the number of users are less the bit error rate goes low.

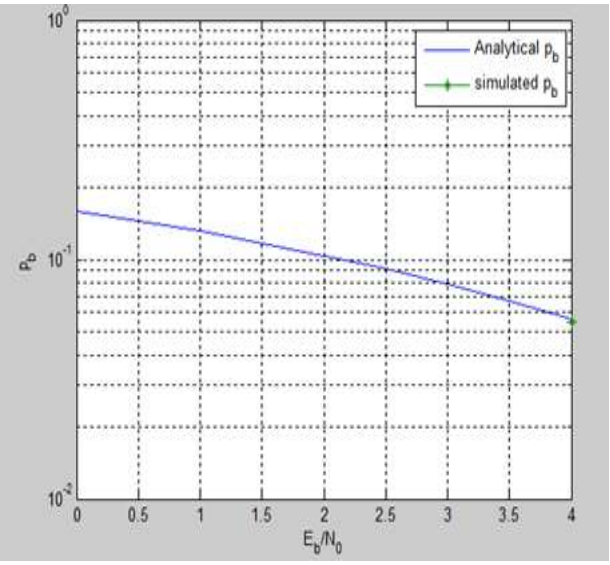

Figure 10: BER Plot for Multiuser DSSS BFSK

VII INFERENCE

Equations (1) and (5) are plotted in Figure 6, where it can be seen that the optimized pulse noise jammer causes a degradation of approximately 31.5dB relative to continuous jamming at a bit error probability of 10^{-5}.

VIII. INTRODUCTION TO" RABBIT" STREAM CIPHER

Rabbit was first presented at the Fast Software Encryption workshop in 2003. Since then, an IV-setup function has been designed and additional security analysis has been completed, but no cryptographical weaknesses have been revealed. The cipher is currently being submitted to the Ecrypt call for stream cipher primitives, negotiating further evaluation by cryptographic experts.

A. Algorithm Description

The Rabbit algorithm can briey be described as follows. It takes a 128-bit secret key and a 64- bit IV (if desired) as input and generates for each iteration an output block of 128 pseudo-random bits from a combination of the internal state bits. Encryption/decryption is done by XOR'ing the pseudo-random data with the plaintext/ciphertext.

The size of the internal state is 513 bits divided between eight 32-bit state variables, eight 32-bit counters and one counter carry bit. The eight state variables are updated by eight coupled non-linear functions. The counters ensure a lower bound on the period length for the state variables. Rabbit was designed to be faster than commonly used ciphers and to justify a key size of 128 bits for encrypting up to 264 blocks of plaintext. This means that for an attacker who does not know the key, it should not be possible to distinguish up to 264 blocks of cipher output from the output of a truly random generator, using less steps than would be required for an exhaustive key search over 2^{128} keys.

B. Key Setup Scheme

The algorithm is initialized by expanding the 128-bit key into both the eight state variables and the eight counters such that there is a one-to-one correspondence between the key and the initial state variables and the initial counters. The key is divided into eight sub keys and the state and counter variables are initialized from the sub keys. The system is iterated four times, according to the next-state function defined in section 6.4,to diminish correlations between bits in the key and bits in the internal state variables. Finally, the counter variables are modified to prevent recovery of the key by inversion of the counter system.

C. Initialization Vector Scheme

The IV setup scheme works by modifying the counter state as function of the IV. The system is iterated four times according to the next-state function, to make all state bits non-linearly dependent on all IV bits. The modification of the counter by the IV guarantees that all 264 different IVs will lead to unique keystreams.

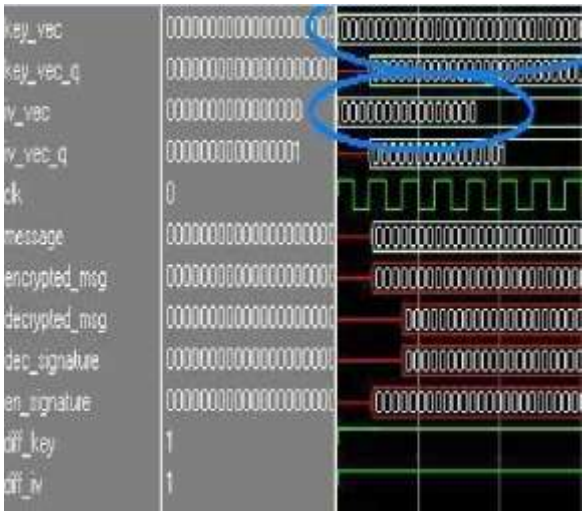

Figure 11: Key_IV to encryptor

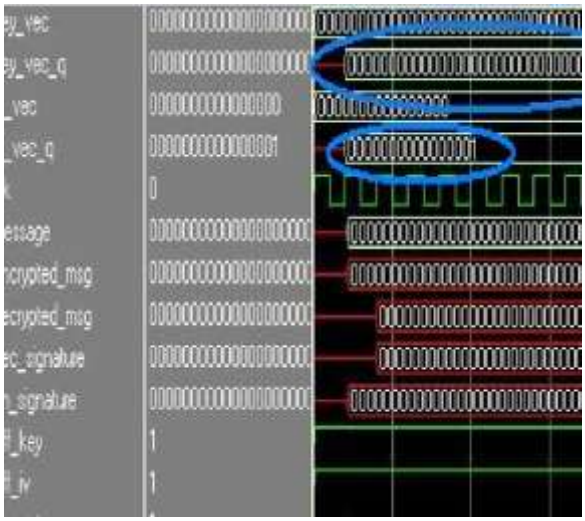

Figure 12: Key_IV to decryptor

The same key or different key can be used for encryption as well as for decryption. In the above figure the key which is used for encryption and decryption is different and the simulation result for this is shown in the Fig (11) and Fig (12).

D. Counter System

Before each execution of the next-state function , the counter system has to be updated. This system uses constants A1,...,A7, as follows:

A0 = 0x4D34D34D A1 = 0xD34D34D3
A2 = 0x34D34D34 A3 = 0x4D34D34D
A4 = 0xD34D34D3 A5 = 0x34D34D34
A6 = 0x4D34D34D A7 = 0xD34D34D3

E. Next-state Function

The core of the Rabbit is the Next-state function . Next state function is involved in both key setup and key stream generation.

It takes eight counter variables as input and produces a 128 bit key stream block after going through system iteration, counter modification and iteration of the g-function. The good diffusion and nonlinearity properties of next-state function prevent against all known attacks.

IX RESULTS AND DISCUSSION

Figure (13) shows the simulation result of the first message transmitted for encryption using the rabbit .

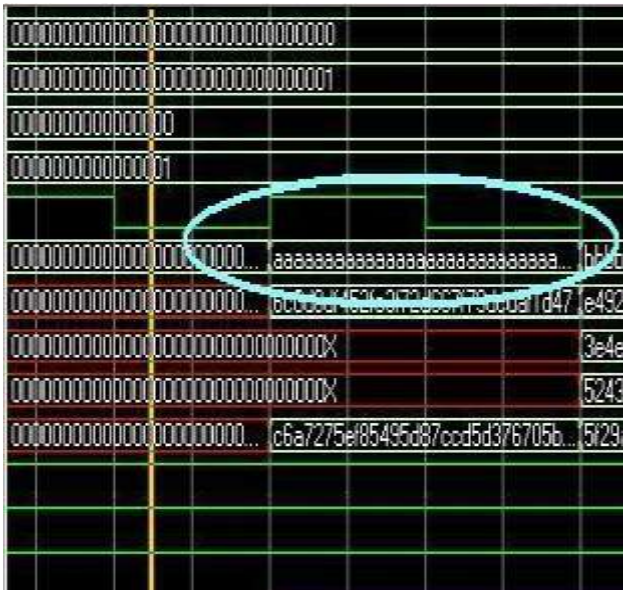

Figure 13: The message transmitted for encryption

Figure 14 shows the simulation result of encryption of message when using the different key.

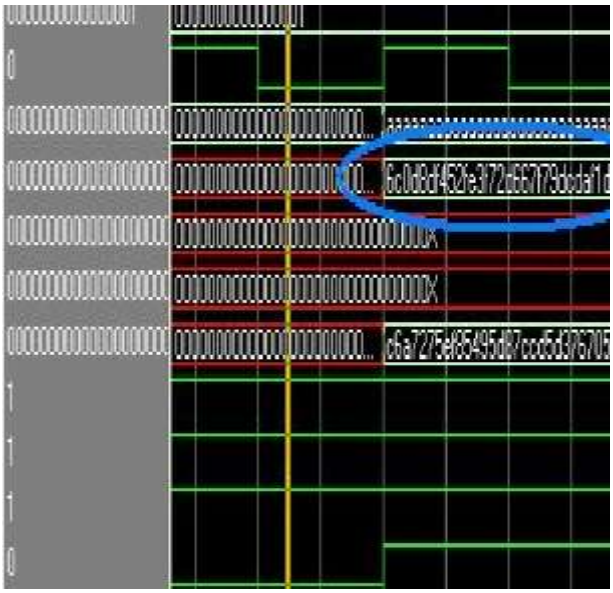

Figure 14: The encryption of the message transmitted

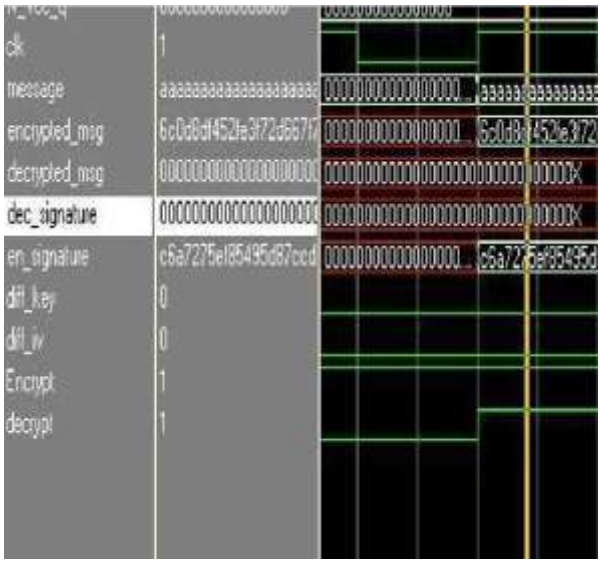

Figure 15: The same key for encryption and decryption

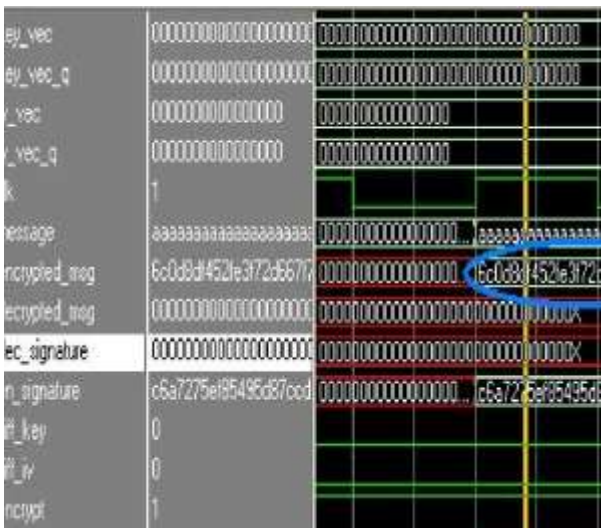

Figure 16: The encrypted message using same key

Figure (4) computes the average BER of a DS-SS/BPSK communication system in the AWGN channel. Figure (5) computes communication system in the presence of pulsed noise jamming and AWGN. The synchronisation and synchronisation between transmitter and receiver is being plotted in figure (7) and (8).when implementing rabbit stream cipher the message transmitted is put in the new folder. After simulating the folder contains the encrypted and the retrieved message.

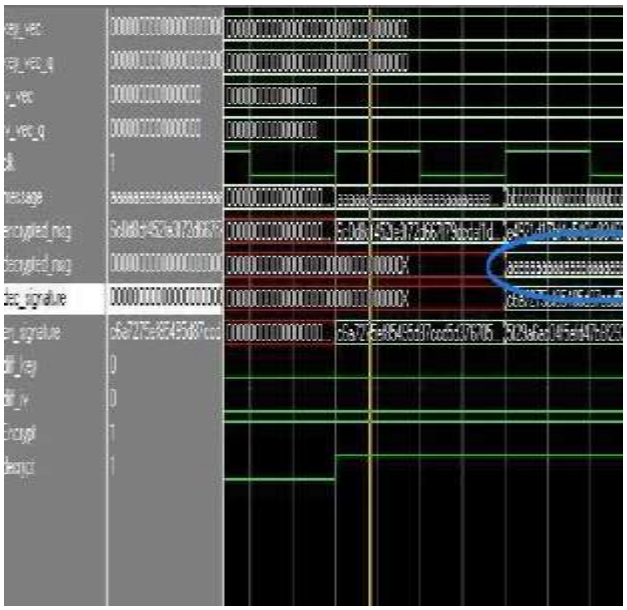

Fig 17 The decrypted message using same key

X CONCLUSION

The theoretical analysis of direct sequence spread spectrum under different jamming environment is done and the results are plotted. The BER for multiuser case is given.from this performance analysis DSSS is used for secure applications.The rabbit stream cipher is being simulated in Modelsim and the results are plotted. In future a stream cipher will be introduced with the DSSS to make it more secure for high data rate applications. The progress of the work is also extended to the hardware implementation using VHDL.

REFERENCES

[1] Nguyen Xuan Quyen, Vu Van Yem, and ThangManh Hoang , "A Chaos-Based Secure Direct-Sequence/Spread-Spectrum Communication System", *Hindawi Publishing Corporation ,Volume 2013, Article ID 764341*

[2] Md.Alamgir Hossain, Md. Shariful Islam, Md. Sadek Ali, "performance analysis of barker code based on their correlation property in Multiuser environment", *International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.1, January 2012*

[3] Heena Malik, Sandeep Singh Kang ," Designing and Evaluation of Performance of a Spread Spectrum Technique for Audio Steganography ",*International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013.*

[4] Yuan Wang, Zhoumo Zeng, Yibo Li,Wen Zhang, Hao Feng, and Shijiu Jin," Research on Improvement of Spectrum Efficiency of Spread Spectrum OFDM Communication Scheme for Cruising Sensor Network", *International Journal of Distributed Sensor Networks Volume 2014.*

[5] Nilesh Shirude , Manoj Gofane , M.S.Panse ," Design and Simulation of RADAR Transmitter and Receiver using Direct Sequence Spread Spectrum", IOSR Journal of Electronics and Communication Engineering *(IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 3, Ver. VI (May - Jun. 2014)*

[6] D. K. Kim, H. S. Lee, "Phase-Silence-Shift-Keying for Power Efficient Modulator," *IEICE Trans. Commun., Vol. E92-B, No. 6, June. 2009*

[7] Jung-Yeol Oh , Jae-Hwan Kim , Hyung-Soo Lee , Jae-Young Kim, *New modulation scheme for high data rate implantable medical devices* IEEE ISCIT ,2009

[8] H-G Ryu et.al., "Performance of DS/SFHSSMA System With Overlapping BFSK in the presence of Both MTJ and MAI," *IEEE Trans. Veh. Tech., vol. 52, pp267-273, Jan. 2003.*

[9] Arafat J.AL-Dweik," Exact performance analysis of synchronous FH-MFSK Wirelessneworks,"*IEEE Trans.commun. vol.58, No.7, September 2009*

[10] Padmavathy,M.Chitra," performance evaluation of energy efficient modulation scheme and hop distance estimation for WSN,"*IJCNIS,Vol.2,No.1,April 2010*