RESEARCH ARTICLE OPEN ACCESS

Ksa Algorithm for Energy Efficient Wsn

Alka P. Sawlikar
Asst Prof. Electronics Engg. R.C.E.R.T. Chandrapur (India)

ABSTRACT: In OFDM systems Channel coding plays a very important role. Channel coding along with frequency and time interleaving, provides a link between bits which are transmitted on separate carriers of the signal spectrum, in such a manner that the message conveyed can be easily reconstructed by faded carriers. Security in the wireless network is a critical issue. By most wireless and wired communication standards Orthogonal Frequency Division Multiplexing (OFDM) is the most reliable modulation technique which has been adopted. In this paper the objective is to carry out an efficient implementation of the OFDM system using different combinations of Encryption and compression algorithm for the energy optimization on data transmission is carried out. The best combination for the encryption and compression of the data transmission and energy optimization is found out and implemented in NS2 for finding different parameters like delay, energy and throughput.

Keywords: OFDM, KSA, NS2, bit- quantization, SSL, AES, DES, RSA,ECC, Hill Climber

Date of Submission: 28-01-2020 Date Of Acceptance: 11-02-2020

I. INTRODUCTION

Some applications required to transmit same message or information which contains signal over channels. When there is a high percentage of unreliability of transmission of any information then at that time some special types of modes of transmission should be selected. So to overcome the effects of collision or interference multichannel signaling is introduced in wireless communication systems. By doing so one can transmit same message or information which contains signal over channels so that the information can be recovered. To reduce storage cost by eliminating redundancies which occurs in number of files, data compression techniques are used. As we know two types of data compression techniques are there: one is lossy and another is lossless and for reducing file size after decoding, lossy compression technique is used for video, audio and text compression[4]. For storage of dataand for transmission we have to pay money and this cost increases with the quantity of data available. But this cost can be reduced by processing the data so that it takes less transmission time and less memory and for this we have to find compression ration.

Various data types consist of many lumps of repeated data. Such "raw" or fresh data can be altered into a compressed data representation form which saves a lot of storage and transmission costs. Well- known data compression algorithms are available and this paper deals with various data compression and encryption algorithms. The analysis of these algorithms can be used for finding various parameters which is applied in this proposed system. As their classification is done on the basis of transformation and compression transformation algorithm should be rearranged or modify the data to optimize input. The new data compression technique has been proposed in this paper which is based on bit quantization level and is renamed as KSA algorithm[7].

In this paper, comparison of the variouscompression algorithms along with new compression technique is clearly discussed and is combined with various cryptographic techniques and then transferred over channels using OFDM transmitter and receiver. At the OFDM transmitter text file is randomly selected and compression is performed and then encryption is done. At the OFDM receiver encrypted data is first decrypted and then decompressed. MATLAB simulation for the best crypto system is shown in figure 1, figure2, figure 3 and the results were observed [6].This crypto system is then applied to wireless communication network using NS2 software. Observation shows that the new proposed compression technique when combined with cryptographic technique gives the best results in terms of various parameters like delay, throughput and energy.

As it is known cryptography is an art of hiding information and has been known

from a long time ,e.g. credit cards, debit cards, bank accounts, important documents and what not, everything needs protection. Without the identical crypto-compression key, the decompression process will be disabling and the cryptanalysis can't even be completed. The result shows that if KSA is combined with cryptographic algorithm through protocol or without protocol performance is improved as compared common algorithms. This can be improved by compression and encryption, such type of scheme is known as compression–crypto scheme. That means ciphering/encryption is indeed a secure coding technique and data compression So the data, which needs to be protected, is increasing at a rapid rate and can be handled a bit if we can remove the redundancy or can reduce its size and for this both encryption algorithm and compression technique have to be combined and made them work on data so that our valuable information or message or file will be of compressed and encrypted form and is easy to handle and secure because of its reduced size and encrypted form which extends many advantages like saves space, manageable, easily transferrable, practical, and feasible.

II. LITERATURE SURVEY

In the paper "A Comparative Study of Lossless Compression Algorithm on Text Data", Jain et al.,2013 shows the comparison of different lossless compression algorithm over text data which contain different text patterns and had drawn compression ratio of all the algorithm by considering the compression time, decompression time and from comparison they concluded that the Huffman Encoding is considered as the most efficient algorithm.[1]
The paper "Network Conscious Text Compression System" (NCTCSys) by N. Motgi & A.Mukherjee, 2001 proposes to tackle the problem of transmitting explosively increasing data on the internet.[2]

Franceschini et al., 1996 in "Data CompressionUsing Encrypted Text," presents an algorithm for text compression that exploits the properties of the words in a dictionary to produce an encryption of given text [3] .

In the paper "A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms", Nivedita Bisht & Sapna Singh,
2015suggested importance of data security in wireless network and for this proved that cryptography plays a crucial role which means "secret writing". This paper provides a comparative study between various encryption algorithms like AES, DES, RSA and DIFFIE-HELLMAN [4].

The principal goal of the paper "A performance comparison of data encryption algorithms", A. Nadeem, 2006 has given the design of encryption algorithm which must be secured against unauthorized attacks. Based on the experiments, it has been concluded that the Blowfish is the best performing algorithm among the algorithms chosen for implementation [9] .

III. PROPOSED COMPRESSION AND DECOMPRESSION ALGORITHM

The different steps of the proposed algorithm are:
(1) Take input data string of random length or specified length.
(2) Decimate the data length by 2
(3) Convert decimal data string to binary
(4) Find the polarity of consecutive input sample as if next_sample > current_sample
Make LSB bit of current output as '1'
Else make LSB bit of current output as '0' (5) Convert binary data string to decimal
(6) We will get compressed output data string For decompression:
(1) Take first compressed output bit as it is
(2)Consider two consecutive bits and check current _sample and next_sample
(3) Convert decimal data string to binary
(4) If current_sample has 1 in LSB position then current _sample is always equal to new_output. else add two consecutive samples and divide it by 2 that will be new_sample
unauthorized attacks. Based on the experiments, it has been concluded that the Blowfish is the best performing algorithm among the algorithms chosen for implementation [9].

III. PROPOSED COMPRESSION AND DECOMPRESSION ALGORITHM

The different steps of the proposed algorithm are:
(1) Take input data string of random length or specified length.
(2) Decimate the data length by 2
(3) Convert decimal data string to binary
(4) Find the polarity of consecutive input sample as if next_sample > current_sample
Make LSB bit of current output as '1'
Else make LSB bit of current output as '0' (5) Convert binary data string to decimal
(6) We will get compressed output data string For decompression:
(1) Take first compressed output bit as it is

(2)Consider two consecutive bits and check current _sample and next_sample
(3) Convert decimal data string to binary
(4) If current_sample has 1 in LSB position then current _sample is always equal to new_output. else add two consecutive samples and divide it by 2 that will be new_sample
(5) Convert binary data string to decimal.

Repeat the same process for complete data length; we will get decompressed output bits The length of input bits will always equal to length of decompressed data bits. This algorithm can apply to any number of data bits and this algorithm is named as KSA algorithm.

IV. SECURE DATA TRANSMISSION WITH KSA ALGORITHM

Combination of compression and encryption of large text data gives an efficient way of handling as this reduces the size first and then makes the reduced size secured, which is a less time consuming process. Such methods can be helpful in saving memory, cost and transfer of data.

In this paper to prove cryptanalysis we have taken the sample of text i.e. say 100bits,200bits, compressed it with common algorithms such as RLE,DCT,DWT,LZW. Also we have combined this technique with different encryption algorithm such as AES, Interleaver, Hill-Climbing, RSA, ECC. Then the parameters like normal data size ,compressed data size, time required for compression ,time required for encryption ,total time required for complete cryptanalysis and compression ratio has been found. We have found that our KSA technique gives better results as compared to the above techniques.

Following Table 1 shows the parametric evaluation and proposed method provided good results by combining with encryption algorithms and is found to be better in all terms. Experimental Analysis and Results
After the combination of compression and encryption techniques the best combination have been found out and energy optimization is carried out over channels using OFDM transmitter and receiver using security protocol SSL(Socket Secure Layer).

The number of sensor nodes can be varied 30,40,50 and accordingly energy, delay and throughput have been observed. KSA_energy, KSA_delay and KSA_throughput are energy, delay and throughput respectively when KSA combination is to be best found

Table 1: Parametric Evaluation of compression and encryption techniques along with new compression KSA algorithm

Input Bits=200					
Compression Tech	Encryption Tech	Time	Normal Data Size	Compressed Data Siz	Compression Ration
RLE	AES	6.85 sec	1719	208	87.91%
	INTERLEAVING	4.82	1299	208	84%
	HILL	3.1	1219	208	83%
	RSA	2.11	1191	208	83%
	ECC	2.97	1283	208	84%
DWT	AES	8.9556	208	104	50.00%
	INTERLEAVING	2.55	208	104	50.00%
	HILL	2.61	208	104	50.00%
	RSA	2.34	208	104	50.00%
	ECC	2.51	208	104	50.00%
DCT	AES	7.85	208	208	0.00%
	INTERLEAVING	3.28	208	208	0.00%
	HILL	2.05	208	208	0.00%
	RSA	2.15	208	208	0.00%
	ECC	2.44	208	208	0.00%
HUFFMAN	AES	5.77	208	208	0.00%
	INTERLEAVING	3.52	208	208	0.00%
	HILL	3.38	208	208	0.00%
	RSA	2.2	208	208	0.00%
	ECC	2.03	208	208	0.00%
LZ	AES	5.51	208	208	0.00%
	INTERLEAVING	2.56	208	190	9%
	HILL	2.991	208	187	10%
	RSA	3.6	208	191	8%
	ECC	2.73	208	187	10.10%
KSA	AES	7.28sec	208	104	50%
	INTERLEAVING	2.27sec	208	104	50%
	HILL	3.10sec	208	104	50%
	RSA	2.92sec	208	104	50%
	ECC	2.86sec	208	104	50%

Table 2: Energy Comparison table when protocol is not applied and using KSA for nodes=30

Simulation Time	O-Energy	Energy	KSA_ Energy
0	110	82	50
5	200	142	92
10	210	170	99
15	220	178	99
20	230	180	100
25	220	182	100
30	210	180	100

Figure 1: Comparative energy graph with number of nodes = 50 and stop time = 0.1sec

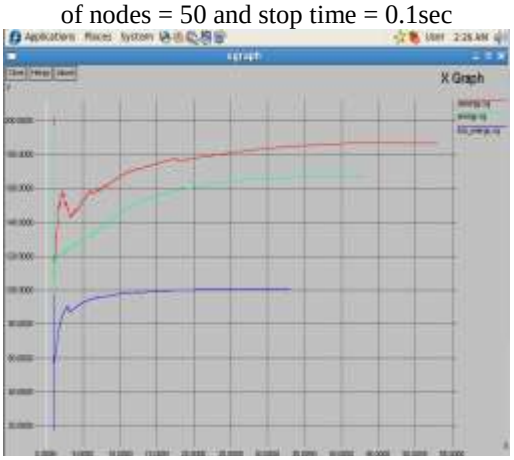


Figure 2: Comparative delay graph with number of nodes = 50 and stop time = 0.1sec

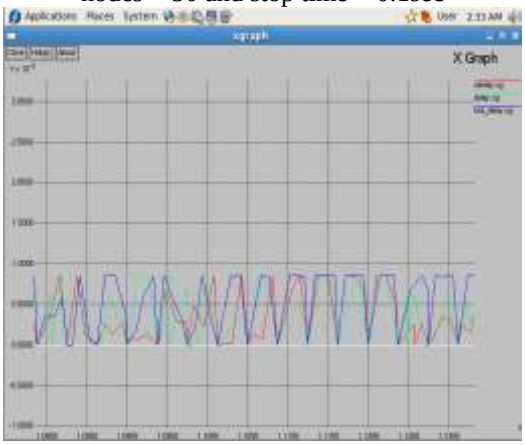
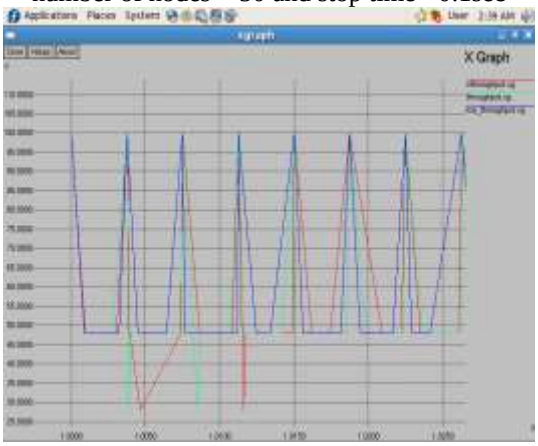


Figure 3: Comparative throughput graph with number of nodes = 50 and stop time =0.1sec



V. CONCLUSION

In this paper, the new compression algorithm, KSA, which is a lossy compression, have been introduced which offers compression with less compression time. To strengthen the security of the communication network this technique has been suggested and with the experimental results it has been proved that it leads to increase not only security but is also energy efficient. The complete suggested design makes the cryptanalysis difficult for the intruder which is achieved effectively through a module which is a perfect blend of new compression technique with cryptography principles. This design is really instrumental in providing very big challenge to the intruders who attempt to break the algorithms by any means. Thus it can be concluded that the secret data can be transmitted securely in an insecure media using this module. Proposed algorithm is viewed best in terms of speed, cost, throughput, security and power consumption.

REFERENCES

[1]. A. Jain, K. I. Lakhtaria, P. Srivastav (2013) A Comparative Study of Lossless Compression Algorithm on Text Data. International Conference on Advances in Computer Science, AETACS-, Elsevier Digital Library, p 536.

[2]. N. Motgi and A. Mukherjee(2001) Network Conscious Text Compression Systems (NCTCSys). Proceedings of International Conference on Information and Theory: Coding and Computing, IEEE Computer Society.

[3]. Franceschini, Robert and A. Mukherjee(1996) Data Compression Using Encrypted Text.Proceedings of the Third Forum on Research and Technology,Advances on Digital Libraries.

[4]. Nivedita Bisht, Sapna Singh(2015)A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms.International Journal of Innovative Research in Science, ISSN (Print) : 2347 – 6710, Vol. 4, Issue 3, p 10281.

[5]. Idrizi, Florim,Dalipi, Fisnik & Rustemi , Ejup(2013).Analyzing the speed of combined cryptographyic algorithms with secret and public Key.International Journal of Engineering Research and Development,eISSN:2278067X,ISSN:2278 -800X, Volume 8,Issue 2 ,p.45.

[6]. Prashanti.G, Deepthi .S & Sandhya Rai.K(2013).A Novel Approach for Data Encryption Standard Algorithm . International Journal of Engineering and Advanced Technology (IJEAT) ISS: 2249-8958, Volume -2 Issue-5, p.264.

[7]. Vishwa Gupta, Gajendra Singh, RavindraGupta(2012).Advance Cryptography algorithm for improving data

security. International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X Volume 2, Issue 1..

[8]. Behrouz A. Forouzan Debdeep M ukhopadhyay ,cryptography and network security,2e, Mc Graw Hill Education (India) Private Limited.

[9]. [9].A.Nadeem,(2006)A performance comparison of data encryption algorithms. IEEE information and communication technologies.

[10]. Abdul D S, Eliminaam ,Kadar H M A and Hadhoud M M (2008) Performance Evaluation of symmetric Encryption Algorithms.IJCSNS International Journal of Computer Science and Network Security , VOL.8 No. 12.

[11]. Gurjeevan singh, Ashwani single, K Ssandha(2011)Cryptography algorithmcomparison for security enhancement in wireless intusion detection system.Internationaljournalofmultidisciplinary research, vol .1, issues 4.

[12]. William Stallings(2005) Cryptography and Network Security: Principles and Practices. International 4th Edition, Prentice Hall, vol 8,, p 28..

[13]. Y. K. Jain and P. B. Gosavi(2008) Email Security using Encryption and Compression.IEEEInternational Conference of Computational Intellegence Model Control Automation., CIMA, p 136.

[14]. M. Savari, M. Montazerolzohour and Y. E.Thiam(2012) Combining Encryption Methods in Multipurpose Smart Card. IEEE Int. Conf. CyberSec, ,p. 43.

[15]. E. Celikel and M. E. Dalkilic(2004) Experiments on A Secure Compression Algorithm. IEEE Proc. Int. Conf. Inform. Techno. Cod. Comput., ITCC, vol. 2, p 150.

[16]. N. Khanna, J. Nath, J. James, A.Chakrabarti, S. Chakraborty A. Nath (2011)New symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm. NJJSAA symmetric key algorithm. International Conference on Communication Systems and Network Technologies, p 126.

[17]. Nasreen Mev, Brig. R.M.Khaire (2013) Implementation of OFDM Transmitter and Receiver Using FPGA. International Journal of Soft Computing and Engineering (IJSCE), ISSN 2231-2307, Volume-3, Issue-3, p 199.