International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 11, November 2014 **ISSN 2319 - 4847**

Design and Performance Analysis of new Cryptographic Algorithm for Wireless Sensor Networks & Broadcasting Applications Security

Arun Singh Chouhan[1], Bipin Pandey[2]

[1]Associate Professor ,Vyas Institute of Engineering & Technology, Jodhpur

[2]Assistant Professor ,Vyas Institute of Engineering & Technology, Jodhpur

[2]Second Author Affiliation with address

ABSTRACT

The prerequisite of data security in Wireless sensor networks and broadcasting applications has undergone major make over in the earlier time and contemporary era. In the prior times physical means is used to provide security to networks and its devices. Wireless sensor networks should broadcast for operations such as software updates, network queries, and command propagation. To maintaining the confidentiality and authenticity of the source and data, keeping the broadcast data secret is essential in convinced relevance such as battleground control, crisis reaction, and natural resource administration. Critical wireless sensor networks deployed in defense and resource management applications require confidentiality of broadcast traffic in addition to protection against attacks.

Keywords:- Cryptography, private key, Wireless Sensor Network, Broadcasting Applications.

1. INTRODUCTION

The prerequisite of data security in Wireless sensor networks and broadcasting applications has undergone major make over in the earlier time and contemporary era. In the prior times physical means is used to provide security to networks and its devices. Wireless sensor networks should broadcast for operations such as software updates, network queries, and command propagation. To maintaining the confidentiality and authenticity of the source and data, keeping the broadcast data secret is essential in convinced relevance such as battleground control, crisis reaction, and natural resource administration. Critical wireless sensor networks deployed in defence and resource management applications require confidentiality of broadcast traffic in addition to protection against attacks. With the beginning of computers in every field, the need for software tools for defensive files and other information stored and broadcast on the networks became important. Security mechanisms usually engage more than a particular algorithm or protocol for encryption & decryption purpose and as well as for generation of sub keys to be mapped to plain text to generate cipher text. It means that participants be in possession of some secret information (Key), which can be used for protecting data from unauthorized users. Thus a model has to be developed within which security services and mechanisms can be viewed.

2. PROPOSED METHODOLOGY & ALGORITHM

We propose a computationally lightweight block cipher based algorithm allows sensor nodes to authenticate broadcast messages from a base station in a wireless sensor network. In this algorithm uses a matrix key which on multiplication with a ternary vector and applying a sign function on the product generates a sequence. This sequence will be used to generate a perfect model of substitution technique. Thus the algorithm is considered to be a substitution algorithm which uses a single key to be shared by both the sender and receiver, and the cipher processes the input element continuously, producing output one element at a time. The type of operations used for transforming plain text to cipher text. All encryption algorithms are based on two general principles. Substitution in which each element in the plain text is mapped to another element and transposition in which the elements in the plain text are re-arranged. Most systems involve multiple stages of substitution and transpositions. The number of keys used. If the sender and receiver use the same key, the system is referred as symmetric, single key, secret key or conventional encryption. If the sender and the receiver each uses a different key, the system is referred to as asymmetric, two key or public key encryption. The way in which plain text is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input element continuously, producing output one element at

a time, as it goes along. In this cryptographic algorithm for keys generating we used a very strong and lightweight block cipher algorithm that given as:
The steps that are involved in the proposed block cipher algorithm is as follows.
Step #1. The decimal values and letters of the plain text are given numerical values starting from 0.
Step #2. A random matrix is used as a key. Let it be X.
Step #3. A "Ternary Vector" for 3^3 values i.e. from 0 to 26 is generated.
Step #4. Let this be "Y".
Step #5. 1 is subtracted from all the values of ternary vector.
Step #6. The modified ternary vector is multiplied with the matrix key.
Step #7. A sign function is applied on the product of ternary vector & matrix key.
Step #8. 1 is added to all values of Step #7.
Step #9. A sequence is generated which is used as sub key
Step #10. The sub key is added to the individual numerical values of the message to generate cipher text.
It can be seen that to extract the original information from the coded text is highly impossible for the third person who is not aware of encryption keys and the method of coding. Even if the algorithm is known it is very difficult to break the code and generate key, given the strength of the algorithm .Thus given a short response time through Wireless Sensor Network and broadcasting communication, the algorithm is supposed to be safe.

3.COMPUTING POWER ANALYSIS

Total number of computations considered in the given model for converting plain text to cipher text.
Computation 1: Converting N=0 to 26 to ternary vector. Let it be TVM.
Computation 2: Calculating TVM-1 and storing it in TVM.
Computation 3: Multiplying TVM with the key considered.
Computation 4: Applying sign function on the product. Store it in TVM.
Computation 5: Calculating TVM +1.
Computation 6: Converting output ternary vector to integer form. Let this be S, the sequence generated.
Computation 7: Converting plain text to alphanumerical value.
Computation 8: Adding alphanumerical value of plain text to sequence generated.
Computation 9: Applying mod 32 function on the output.
Computation10: Converting the output to characters of the alphabet to get cipher text. Thus the total number of computations in the proposed model is 10.

4.COMPLEXITY ANALYSIS BY CONSTRUCTION

1st Computation: Converting N=0 to 26 to ternary vector. Let it be TVM. The complexity is in multiples of N.
2nd Computation: Calculating TVM-1. The complexity is in multiples of N.
3rd Computation: Multiplying TVM with the key considered. The complexity is in multiples of N.
4th Computation: Applying sign function on the product. Store it in TVM. The complexity is in multiples of N.
5th Computation: Calculating TVM+1. The complexity is in multiples of N.
6th Computation: Converting output ternary vector to integer form.
Let this be S, the sequence generated. The complexity is in multiples of N.
7th Computation: Converting plain text to alphanumerical value. The complexity is in multiples of N.
8th Computation: Adding alphanumerical value of plain text to sequence generated. The complexity is in multiples of N.
9th Computation: Applying mod function on the output. The complexity is in multiples of N.
10th Computation: Converting the output to characters of the alphabet to get cipher text. The complexity is in multiples of N.
Thus we can say that the complexity of model1 is O (N).

5.COMPLEXITY OF THE ALGORITHM BY ITS STRENGTH:

Complexities can also be expressed as orders of magnitude. If the length of the key is k, then the processing complexity is given by 2k. It means that 2 k operations are required to break the algorithm. In the given algorithm a matrix key is used. This matrix key is multiplied with ternary vector. On the generated values a sign function is used to convert all positive values to 1, negative values to –1 and zero to 0. This provides the necessary strength to the algorithm. Thus known the algorithm, known the cipher text it is quite difficult to generate the matrix key. Thus in the present algorithm, there is no means by which the key can be retrieved, other than trying all the combinations of key, the complexity of the algorithm is said to be exponential in nature.

6.SECURITY ANALYSIS

The model uses a sign function on the product of ternary vector and a matrix key to generate the sequence. The sign function converts all positive values to 1, negative values to -1, and zero with 0.This sequence is substituted for plain text to generate cipher text. Thus it is impossible to generate the matrix key from the known plain text and cipher texts. Thus this model is free from differential crypto analysis. But this model uses a simple substitution technique to generate cipher text; it is some what susceptible to linear crypto analysis. The Key can not be gained and not a whole of information can be gained, but part of information may be gained in this model. This algorithm is completely free from cipher text only, type of attack. By the other attacks, the key may not be retrieved but a part of plain text may be retrieved.

7.EXAMPLE

Table 1: Encryption & Decryption process by Cryptographic Model

Plain Text	C	O	M	P	U	T	E	R
Alpha Numeric equivalent	12	24	22	25	30	29	14	27
Secret Key	2	0	0	18	0	3	3	6
Add	14	24	22	43	30	32	17	33
Mod 32	14	24	22	11	30	00	17	01
Cipher Text	E	O	M	B	U	00	H	01

Plain Text	E	O	M	B	U	00	H	01
Alpha Numeric equivalent	14	24	22	11	30	00	17	01
Secret Key	2	0	0	18	0	3	3	6
Subtract	12	24	22	43	30	32	14	05
ADD 32	14	24	22	11	30	29	14	27
Plain Text	C	O	M	P	U	T	E	R

8 ADVANTAGES

1. It is almost impossible to extract the original information.
2. Even if the algorithm is known, it is difficult to extract the matrix key.
3. Versatile to users. Different users of internet can use different modified versions of the new algorithm.
4. As per basin values, the same character is substituted by different alpha numerical value which provides more security for the message.

9 CONCLUSION

We conclude our cryptographic Algorithm for Wireless Sensor network and in this work a ternary system with a 3 digit number is used. So the sub key generated is a 33 i.e. a 27 digit number. By considering a ternary vector with a four digit number or five digit number, the length of the sub key can be increased by 34, 35 which increase the length of sub key generated. Similarly by considering n –array vector the length of the sub-key generated can still be increased. Thus by increasing the length of sub-key, security of cipher system can be increased still further. This Algorithm is very useful for providing security in broadcasting in battleground and short distance message communication.

REFERENCES

[1] Krishna A.V.N., S.N.N.Pandit: A new Algorithm in Network Security for data transmission, Acharya Nagarjuna International Journal of Mathematics and Information Technology, Vol: 1, No. 2, 2004 pp97-108
[2] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.
[3] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E., "Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002, pp. 393-422.
[4] J.William stalling ,"Cryptography and network security" Pearson Education,ASIA,1998.
[5] Chan, H, Perrig, A., and Song, D., "Random key redistribution schemes for sensor networks", In IEEE Symposium on Security and Privacy, Berkeley, California, May 11-14 2003, pp. 197–213.
[6] X. Du, H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications,2008.
[7] J. Granjal, R. Silva, J. Silva, "Security in Wireless Sensor Networks", CISUC UC, 2008.
[8] Al-Sakib Khan Pathan ,Security in Wireless Sensor Networks: Issues and Challenges Feb. 20-22, 2006 ICACT2006.
[9] Krishna A.V.N Phd. Thesis, performance evaluation of new Encryption algorithms with Emphasis on probabilistic Encryption & time stamp in network Security.

AUTHOR

Arun Singh Chouhan received the B.E in Computer Science & Engineering from University of Rajasthan ,Jaipur(Rajasthan) and M.Tech from Devi Ahilya University ,Indore(MP) and currently pursuing PhD in Computer Science and Engineering from Jodhpur National University, Jodhpur(Rajasthan).He is more interested in Cloud Computing, Computer Networks and Distributed system with challenges and application in computer science. He is member of various international bodies like IAENG, Hong-Kong, CSTA, New-York, USA, UACEE, USA and ISTQB, Germany.

Bipin Pandey received the B.Tech in Computer Science & Engineering from Gautam Budha Techincal University, Lucknow (UP) and currently pursuing M.Tech in Computer Science and Engineering from Jodhpur National University, Jodhpur(Rajasthan).He have wide knowledge of Java Programming and Database Management Systems and Internet Programming. He is also Oracle Certified Java Professional(OCJP) Certified professional.