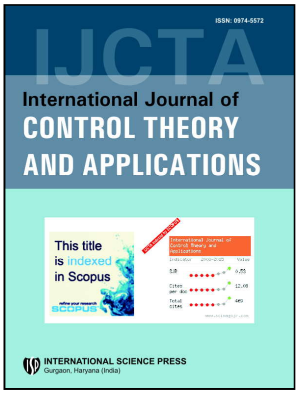

ISSN: 0974-5572
IJCTA
International Journal of
CONTROL THEORY
AND APPLICATIONS
INTERNATIONAL SCIENCE PRESS
Gurgaon, Haryana (India)

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 13 • 2017

Masonic Cipher for MANET

A. Maheswary[1] and S. Baskar[2]

[1] *Research Scholar, VELTECH University, Avadi, Chennai, India, Email: maheswaryswaroop@gmail.com*
[2] *Department of Electrical and Electronics Engineering VELTECH University, Avadi, Chennai, India,*
Email: drbaskar@veltechuniv.edu.in

Abstract: Mobile communication area has become very advanced with the technical advances in the field of wireless technology. The revolutionary changes of wireless technology made it possible for people to use mobile networks while on move. This has created demand for infrastructure less networks. Such networks are known as Mobile Ad Hoc Networks (MANET). MANETs are self-configuring temporary networks created with the help of neighbouring nodes. An intermediate mobile node can acts as router to forward packet to its next node and this process will repeat until the destination has reach. MANETs are well suited for use in rescue operations and disaster monitoring situations where an immediate communication network was needed. As the MANET is created with the available nodes and these nodes are mobile nodes which has a continuous movement causes frequent changes in network topology. Sometimes these nodes are not trusted nodes too. So there is no security to the data to be transmitted. In this research work, we are defining security as protecting the data from the hands unauthorized persons. Being an open networks appropriate security measures must be applied such as cryptography to ensure the security of data. The latest survey conducted in 2014 the Open Web Applications Security Project (OWASP) placed the lack of encryption in data transmissions as number four among the top ten security issues [1]. To solve this problem we are proposing a new encryption algorithm for security. This work focuses on securing data by exchanging letters of the data by masonic cipher algorithm. To reduce the encryption time further we are using data compression technic. By using the RSA algorithm further enhancement in security is possible. The performance of the solution is measured by timing the security process takes to encrypt and decrypt the data. Heavier security mechanisms were applied for data communication to the final destination. Deep packet inspection was used to verify data was secured at both stages of transfer.

Keywords: MANET, Encryption, Decryption, Network Security, DES, Data Compression, Huffman Code.

I. INTRODUCTION

Many individual advantages made MANETs to be stand as one of the best over wired networks, to say its self-organizing characteristics and ease of deployment finds wide spectrum of applications. Historically, Mobile Ad Hoc Networks (MANETs) have been primarily used in military battle field communications [2]. Since the ease deployment of MANETs and its support for more advanced functions makes them to be useful in many serious applications. In MANET mobile node itself works as source, destination and also as a router. MANETs are self-organizing and a collection of mobile nodes were connected with wireless links to form a temporary network for a specific application, hence they are named as mobile (nodes are mobile) ad hoc (for the particular purpose) networks. MANETs are normally a decentralized network. MANETs are named as ad hoc because network is created temporarily for specific purpose by the mobile nodes. These networks are dynamic since nodes which are formed network are not permanent. MANETs are self–forming, they forms the network with the available nodes. MANETs supports two types of architectures namely: flat and hierarchical [3, 4]. Every node of MANET is equipped with an antenna, a power source and a transceiver. The nodes are characterised by their size, battery power, transmission range and processing ability. Some nodes have the ability to acts as servers, others as clients and some of them have the ability to acts as both. Some other nodes can also acts as router to carry the information from one node to another [5]. Some applications cannot rely on the centralised management, for those applications MANETs are well suited. Ad hoc networks can also incorporate with the existing wired network which increases the scope of their applications [4, 6]. Besides of useful advantages there are many issues in MANET. Since the nodes of MANET are mobile, there will be frequent changes in network topology and these nodes has the freedom to move anywhere it is not possible to predict the changes of network topology. The available bandwidth of MANET is limited and it is less than that of wired networks. The operation of network nodes depends on power and those are restricted by battery size. The communication of MANET uses the intermediate available nodes and those nodes are may or may not be trusted nodes, so security of the data is the considerable factor.

One of the solutions to the problem of MANET security is encrypting the information into secret form or unreadable form before transmission. At the destination end the encrypted information can get back by doing the reverse process of encryption known as decryption. There are two types encryption namely symmetric and asymmetric key encryptions. Symmetric key encryption uses same key for both encryption and decryption and asymmetric key encryption uses two different keys known as public and private keys separately for encryption and decryption. Because of single key for encryption and decryption the delay in the process of symmetric-key encryption is very less. In symmetric-key encryption secret key is shared to the only trusted nodes so more security can possible. Authentication is also possible in symmetric as only one key is used and cannot be decrypted with any other key. Thus, high security is possible in symmetric key encryption as long as the symmetric key is kept secret by the two parties using it to encrypt communications. Asymmetric key encryption is also called as Public Key algorithms and it uses two keys separately for encryption and decryption. Key used for Encryption is known as public key and it is shared to all the nodes in the network. Private Key is used by the destination alone and it is to decrypt the message. Asymmetric cryptography wires authentication so it can be used for providing digital signature. Two separate keys for used for encryption and decryption. Ciphered information can be deciphered with a key that is differing from ciphered key. Moreover, there will be no clue provided to calculate the decryption key from the encryption key.

As today we are dealing with large amount of data, so for any further step proceeding requires that the data has to be compressed by reducing the redundancy in the data. Compression has two steps namely encoding and decoding. Encoding generates a compressed form of data and decoding reconstructs the original message. There are two forms of compression namely lossy and lossless algorithms. A lossless algorithm decodes the data exactly and a lossy algorithm generates an approximated form of the data. Text messages are compressed by lossless algorithm as original message cannot be predictable from approximate text message whereas images and sounds can be compressed by lossy algorithm because it is possible to reconstruct the original image from the approximated version. Better compression is possible by reducing the redundancy of the data or by replacing the words by its synonyms. Compression is therefore all about probability. For better understanding of compression first it is better to distinct between model and coder. Model component models the probability distribution of the message by observing the chances of occurrence of the message. Then *coder* component assigns codes to the message based on their probability of occurrence. Coder works on assigning short length codes to high probability message and high length codes to low probability messages. For example high probability message like "sun rises in the east" is coded with less number of bits and low probability messages like "natural disaster" are coded with the more number of bits. Coder uses Huffman coding and Shanon- Fano coding technics. One can characterise this compression by amount of time required for compression and reconstruction, Size of message to be compressed, the amount of compression, the runtime, and the quality of the reconstruction.. In the case of lossy compression the judgment is further complicated since we also have to worry about how good the lossy approximation is. The Archive Comparison Test (ACT) given by Jeff Gilchrist is a systematic method used to compare lossless compression algorithms. It compares compression times and compression ratios of compression algorithms. It gives the output as in the form of a score based on average of amount of time taken for compression and the compression ratio.

2. LITERATURE REVIEW

A system which deals with all possible plain texts, cipher texts and keys is known as a crypto system [7,8,9]. Rapid change in the digital world increases the importance of security of information. Recently a new cryptographic algorithm is proposed [10]. It is based on generating multiple keys randomly for each block of data. This method guarantees security by using separate keys for each block. Another type of cryptographic technic based on permutations in matrix is proposed in [11]. Here the data is first converted into binary bit form, and then finite numbers of bits are considered as blocks. These bits are further fit diagonally in a matrix from left to right. The proposed encryption scheme is considering the bits from the matrix from right to left. Data transmission by selecting optimum path is proposed in [12]. Here the path selection is based on some distribution models. For a session a secret key is shared. To solve the problem of key distribution quantum channel solution is used. The DES algorithm is enhanced further by including some random bits in the particular places of the plain text. This method is called homophonic DES [12]. Adding of random bits to the plain text increases the probability between a pair of texts and also increases the complexity of guessing of the message. As compared to DES in Decryption of homophonic the added random bits are removed. Homophonic DES adds probabilistic features to DES algorithm to make it more secure than linear and differential crypto systems. Dynamic substitution mechanism was proposed in [13]. It is also similar to simple substitution; additionally it has one more input that will re-arrange the contents of substitution table. Dynamic substitution combines two data to produce a complex result; later a reverse mechanism will be performed to extract the actual data. This method will replace the exclusive-OR combiner used in Vernam stream ciphers. All the techniques used in Vernam ciphers can also be supported by dynamic substitution; A nonce [14] is a bit string that satisfies Uniqueness, that it has not occurred before in a given run of a protocol. Nonces use pseudo randomness so that next nonce cannot be predictable. There are several common sources of nonces like counters, time slots and so on. Another security method by encryption mechanism is proposed was one time pad [15] encryption. In this method a random number k will be chosen randomly. Then the data was exclusive ORed with k. So that security is provided. It has several limitations. As every time a new key is used for encryption, this new key has to be shared to participating parties every time. Stream ciphers [16] use a pseudorandom sequence of bits which are combined with the message to form an encrypted message. The combining operation is nothing but the XOR and implementations of these schemes are prone to bit-flipping attacks. There are two types of stream ciphers namely: synchronous and self-synchronizing. In the former, separate encryption algorithm is used but it is not correlated with the plaintext or cipher text and in the self-synchronizing, a part of information is used to inform the operation of encryption. A probabilistic encryption algorithms [17,18], uses multiple cipher texts were developed for single plain text, even a crypto analyst decrypts the message he is unable the exact sequence of the message correctly. In this scheme multiple encrypted message are formed for single message and the length of the encrypted message is larger than the plain text. This concept makes crypto analysis difficult to apply on plain text and cipher text pairs.

3. PROPOSED METHOD

Here is the proposed data compression algorithm which compresses the message:

Step 1: For every letter of the given data prepare a table with its range of probability of occurrence.

For ex: probability of occurrence of letter ‘a’ is 40% and its range is (0.00, 0.40). Similarly probability of occurrence of letter ‘p’ is 20% and its range is (0.40, 0.60).

Step 2: For every letter define two levels as higher limit and lower limit and assign initially values as 1 and 0 respectively.

Step 3: Find new values for current range, upper limit and lower limit with the following formulas:

Current range = Higher limit - lower limit

Higher limit = lower limit + (current range * Higher limit of new symbol)

Lower limit = lower limit + (current range * lower limit of new symbol)

Step 4: Now encode the string with any value within the range of probability and convert the output decimal number into its binary format.

Step 5: The number of bits can be reduced by using the formula.

No of bits=log [2/Higher limit of last encoded symbol - lower limit of last encoded symbol]

Step 6: Now for encryption proposed TIC-TOC-TOE encryption discussed below can be used.

First letters in the grid is encrypted with shape of lines around the letter. Second letter in the grid is encrypted with shape of the lines around the letter followed with a dot. For ex: letter **A** is encrypted as _| and the letter **B** is encrypted as **.**_| as shown in fig.2.

Step 7: Change the positions of letters in the shapes and try other combination by left and right shifts, Horizontal and vertical shifts and diagonal shifts. Approximately 146 combinations were possible. For each combination assign prime number combination and apply RSA algorithm to calculate public and private keys.

Step 8: For decompression and decryption the above steps in reverse order.

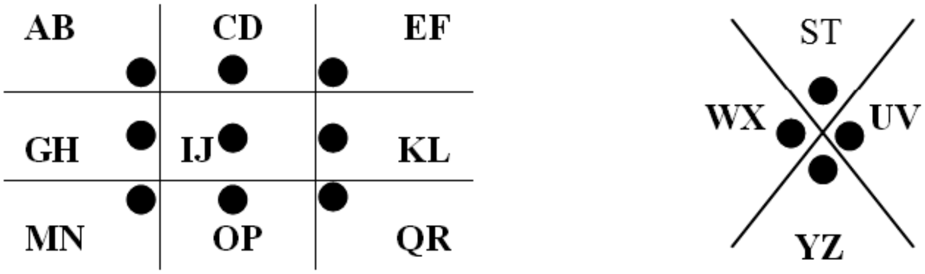

Figure 1: Letter-Shape Encryption

4. SIMULATION SETUP AND NETWORK SCENARIO

Of course various tools are available for simulating the mobile ad-hoc networks, our study have simulated the network in NS-2.35. Initial parameters were considered as follows: For simulation IEEE 802.11 protocol is used at the MAC layer. Node mobility is represented by Random waypoint model.

5. EXPERIMENT AND RESULT

Table 2 shows a clear cut analysis of comparison of encryption and decryption times required for various standard cryptography methods DES, AES, RSA and proposed technique for different packet sizes up to 868KB. Table 2 shows that proposed technique takes less time for encryption and decryption than RSA.

Table 1
Simulation parameters

Parameter	*Value*
set val(chan)	Channel/ Wireless Channel
set val(prop)	Propagation / Two Ray Ground
set val(netif)	Phy / Wireless Phy
set val(mac)	Mac/802_11
set val(ifq)	Queue/ Drop Tail / Pri Queue
set val(ll)	LL
set val(ant)	Antenna/Omni Antenna
set val(ifqlen)	50
set val(nn)	30
set val(rp)	DSDV
set val(x)	500
set val(y)	500

Table 2
Results Comparison Table

	Encryption Time(sec)				*Decryption Time (sec)*			
Packet Size (KB)	*DES*	*AES*	*RSA*	*PROPOSED*	*DES*	*AES*	*RSA*	*PROPOSED*
153	3.0	1.6	7.3	6.4	1.1	1	4.9	3.8
196	2.0	1.7	8.5	7.1	1.24	1.4	5.9	4.7
312	3.0	1.8	7.8	7.6	1.3	1.6	5.1	4.6
868	4.0	2.0	8.2	8.0	1.2	1.8	5.1	4.9

6. CONCLUSION

Our work concentrates on representing the significance of Encoding and Encryption of data for secure transmission over wireless networks like MANETs. As technology is improving in positive direction hacking is also improving in the same proportion so there is a serious need of encoding and encryption algorithms for securing the tactical communication from the hands of hackers. The advantage of encrypting data provides security and confidentiality in real time applications like email, mobile banking transactions where high security is necessary. The conclusions confirm that the encoding and encryption improves the efficiency of transmitting data. The methodology proposes new encryption algorithm in terms of multiple patterns foe letters of the data being transmitted. Further, the quantitative data compression reduces the encryption time further. The strength and security of the algorithms is very high. The security of the proposed models has more flexibility regarding computing power because it is free from key length. One more conclusion made from that the above study is free from public key attacks. With symbol encryption algorithm, a crypto analyst can no longer encrypt the plain text. Since key selection follows RSA algorithm guessing the prime numbers from the product is a complex process, so decryption is difficult. Thus the proposed work guarantees more security. In our study analysis has been done to introduce a new encryption technic called Letter to Shape Encryption suggested for secure communication through MANET. Some existing approaches in this regards have been compared with the proposed technic. In the future work for this paper includes reducing the encryption time with data compression technics. Proposed Letter to Shape encryption uses asymmetric keys for encryption and decryption. The encrypted keys are shared between the parties by including within the cipher text. This algorithm uses simple operations. Comparing with other encrypted algorithms, this method will reduce man in middle attacks. Since the proposed approach uses different shapes, it guarantees secure data transmission.

REFERENCES

[1] D Miessler, C Smith, and J Haddix, "OWASP Internet of Things Top Ten Project," Open Web Application Security Project, Informational 2014.

[2] N. Abramson, "The ALOHA - another alternative for computer communications", Proceedings of the fall joint conference", NJ, Vol. 37, pp. 281•285, 1970.

[3] S. Chakravarti, A. Mishra, "QoS issues in adhoc wireless networks", IEEE Communication Magazine, Vol. 39, pp. 142"148, February 2001.

[4] C. K. Toh, Adhoc Mobile Wireless Networks: Protocols and Systems, Prentice-Hall PTR, NJ, 2002.

[5] E.M. Royer, C. K Toh, "A review of current routing protocols for adhoc mobile wireless networks", IEEE Personal Communications, Vol.6, pp. 46"55, April 1999.

[6] Charles E. Perkins, Adhoc Networking, Addition Wesley, Reading, MA 2001.

[7] Amjay Kumar, Ajay Kumar: Development of New Cryptographic Construct using Palmprint Based Fuzzyvoult, EURASIP Journal on Adv. In Signal Processing, Vol 21, pp 234-238, 2009

[8] Brassard G.: Modern Cryptology , a tutorial lecture Notes on computer science , (325) (spring-verlas) .

[9] Bruce Scheneier: Applied cryptography (John Wiley & sons (ASIA) Pvt. Ltd.

[10] K. Vijaya Kumar, K.Somasundaram, " A Symmetric Multiple Random Keys (SMRK) Model Cryptographic Algorithm", Imternational Journal of Innovative rsearch in Computer and Communication Engineeringg, Vol 3, Issue 11, Nov.2015, pp 10896-10903.

[11] Manas Paul and Jyotsna Kumar Mandal, "A General Session Based Bit Level BlockEncoding Technique Using Symmetric Key Cryptography to Enhance the Security of NetworkBased Transmission", International Journal of Computer Science, Engineering and Information Technology Vol.2, No.3, June 2012, pp 31-42.

[12] P. Chakrabarti, B Bhuyan, A.Chowdhuri, C.T.Bhunia, "A novel approach towards realizing optimum data transfer and Automatic Variable Key(AVK) in cryptography",International Journal of Computer Science and Network Security, VOL.8 No.5, May 2008, pp 241-250.

[13] Amjay Kumar, Ajay Kumar: Development of New Cryptographic Construct using Palmprint Based Fuzzyvoult, EURASIP Journal on Adv. In Signal Processing, Vol 21, pp234-238, 2009

[14] Baocang Wang, Qianhong Wu, Yupu Hu: A Knapsack Based Probabilistic Encryption Scheme, On Line March 2007, www.citeseer.ist.psu.edu.

[15] Bluekrypt 2009: Cryptographic Key length Recommendations, http://www.keylength.com

[16] Blum L., Blum M , Shub M. : A simple unpredictable pseudo random number generator , SIAM J. compute , 1986, 15, (2), pp 364-383.

[17] Brics: Universally comparable notions of key exchange and secure channels, Lecture Notes in Computer Science, Springer, Berlin, March 2004.

[18] Sage.math.Washington.edu/home/jetchev/Public.html/docs/jetchev-talk.ppt- Broadcast encryption schemes.

[19] Brassard G.: Modern Cryptology , a tutorial lecture Notes on computer science , (325) (spring-verlas) .

[20] Bruce Scheneier: Applied cryptography (John Wiley & sons (ASIA) Pvt. Ltd.

[21] Carlone Fontaine & Fabien Galand: A Survey of Homomorphic Encryption for non specialists, EURASIP Journal,Vol 07, Article 10.

[22] Donavan G.Govan, Nathen Lewis: Using Trust for Key Distribution & Route Selection in Wireless Sensor Networks, International Conference on Network Operations & Management, IEEE Symposium 2008, PP 787-790.

[23] Dorothy E. Denning et al.: Time Stamps in Key Distribution Protocol,Communication of ACM, Vol 24, Issue 8, Aug 1981, pp 533-536.

[24] E.C.Park, I.F.Blake: Reducing communication overhead of Key Distribution Schemes for Wireless Sensor Networks: Computer Communications & Networks, ICCCN 2007, pp 1345-1350.

[25] Georg J.Fuchsbauer: An Introduction to Probabilistic Encryption, 'Osjecki Matematicki List 6(2006), pp37-44.

[26] Guo D, Cheng L.M., Cheng L.L: A New Symmetric Probabilistic Encryption Scheme Based on Chaotic Attractors of Neural Networks, Applied Intelligence, Vol 10, No.1, Jan 99, pp 71-84.

[27] Hamid Mirvazri, Kashmiran Jumari Mahamod Ismail, Zurina Mohd. Hanapi: Message based Random Variable Length Key Encryption Algorithm, Journal of Computer Science, pp 573-578, 2009.

[28] Hianyi Hu, Gufen Znu, Guanning Xu: Secret Scheme for Online Banking based on Secret key Encryption, Second International Workshop on Knowledge Discovery & Data Mining, Jan 23-25 2009.

[29] Henry Baker and Fred Piper: Cipher systems(North wood books, London 1982).

[30] J.William stalling **:**Cryptography and network security (Pearson Education,ASIA1998).

[31] Kaiping Xue: Study of improved key Distribution Mechanisms based on two length structure for wireless sensor networks, International conference on adv. Information Technology, 2008.

[32] Krishna A.V.N.: A new algorithm in network security, International Conference Proc. Of CISTM-05, 24-26 July 2005, Gurgoan, India.

[33] Krishna A.V.N., Vishnu Vardhan.B.: Utility and Analysis of some Encryption algorithms in E learning environment, International Convention Proc. Of CALIBER 2006, 02-04 Feb. 2006, Gulbarga, India.

[34] Krishna A.V.N., S.N.N.Pandit: A new Algorithm in Network Security for data transmission, Acharya Nagarjuna International Journal of Mathematics and InformationTechnology, Vol: 1, No. 2, 2004 pp97-108

[35] Krishna A.V.N, S.N.N.Pandit, A.Vinaya Babu: A generalized scheme for data encryption technique using a randomized matrix key, Journal of Discrete Mathematical Sciences & Cryptography, Vol 10, No. 1, Feb 2007, pp73-81

[36] Krishna A.V.N., A.Vinaya Babu: Web and Network Communication security Algorithms, Journal on Software Engineering, Vol 1,No.1, July 06, pp12-14

[37] Krishna A.V.N, A.Vinaya Babu: Pipeline Data Compression & Encryption Techniques in e-learning environment, Journal of Theoretical and Applied Information Technology, Vol 3, No.1, Jan 2007, pp37-43.

[38] Krishna A.V.N, A.Vinaya Babu: A Modified Hill Cipher Algorithm for Encryption of Data in Data Transmission, Georgian Electronic Scientific Journal: Computer Science and Telecommunications 2007 !N0. 3(14) pp 78-83.

[39] Lester S. Hill, Cryptography in an Algebraic Alphabet, The American Mathematical Monthly 36, June-July 1929, pp306–312.

[40] Lester S. Hill, Concerning Certain Linear Transformation Apparatus of Cryptography, The American Mathematical Monthly 38, 1931, pp135–154.

[41] Maybec.J.S. (1981), Sign Solvability, Proceedings of first symposium on computer assisted analysis and model simplification, Academic Press, NY.

[42] M.Steiner, M.Waidner: Tutorial on Secure Electronic Commerce, 1999.

[43] Pandit S.N.N (1963): Some quantitative combinatorial search problems. (Ph.D.Thesis).

[44] Pandit S.N.N (1961): A New matrix Calculus, J Soc., Ind. And Appl. Math. Pp 632-637.

[45] Pci Yihting: A Temporal order Resolution algorithm in the multi server time stamp service frame work, International Conference on Advanced Information Networking & Applications, AINA 2005, Vol 2m 28-30 March, pp 445-448.