ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol3, Issue 5, May 2016

Encryption Protocol for Securing MANET-L to S

[1] P.N. Sharath sagar reddy, [2] Manasa.S, [3] Anitha A, [4] Jhansi Rani, [5] Sheela Devi, [6] Sowmya.A.M
[1][2] [3] [4] [6] UG Scholors, [5] Asst Professor
Dept of Computer Science and Engineering, SSCE, Anekal, Bangalore

***Abstract*— Mobile ad hoc network are a kind of wireless ad hoc network that usually has a routable networking environment on top of a link layer ad hoc network. The technological growth in the field of wireless technologies provides communication between mobile users. Any invention is to say success, only if it is useful in a meaningful manner. Wireless technology is the one that will help an emergency needy like in any natural disaster, emergency rescue operations, military battle-field etc. With the advent of Mobile Ad-Hoc Networks, an immediate self-configuring network can be created. Being an open network, security is the main concern for MANETs. In such situations to protect the confidentiality of the message to be transmitted, cryptography is the one of the solution. The process of converting the original data into a secret form is known as cryptography. It hides the actual information and sends the encrypted message. At the destination end, the message can be recovered by using decryption. Here we are proposing a new encryption technique named as Letter-Shape Encryption. This method exchanges different shapes for letters in a message to be transmitted. This approach is safe against man in middle attacks.**

***Keywords*— MANET, Encryption, Decryption, RSA algorithm, Key distribution, man-in-middle attacks.**

I. INTRODUCTION

The Present day information technology is mainly based on wireless technology [1],[2],[3]. With the advent of wireless networks we can exchange information between anybody located at any distance. Because of fixed infrastructure need of a conventional communication networks makes its use to be limited. If so, to help an emergency needy like natural disaster help, it is not possible to establish a communication network within hours. As a solution mobile ad hoc networks were invented. MANETs are the self-configuring networks, which forms a temporary network by requesting help from neighboring mobile nodes. MANETs plays a vital role in the field of wireless networks [4]. MANETs does not rely on any central control. Here communication can be initiated by any node in the network. i.e., any node can acts as source or destination. Node which wants to start communication will transmits a request of route to the next nearby nodes by mentioning the destination node address. If an intermediate node has a path to the receiver, a route reply will be sent back to the source node. Base on the short metric, source will selects the communication path towards receiver.

MANETs proposes many advantages like dynamic topology, self- configuring, self-organizing, and any node can initiate communication, no central administration, no need of infrastructure, can be set up anywhere. Since every invention has merits and demerits too. MANETs are basically wireless networks; there should be a prescribed security mechanism to protect the privacy of the data. Lack of central administration fails in detection and prevention attacks. MANETs also have few limitations. Energy constraints, limited security, topological changes, multiuser interference, limited bandwidth and power limitation become relevant issues.

Since in MANET, communication is achieved with the help of neighboring mobile nodes, the nodes have to cooperate with each other for the operation of the network. But sometimes nodes may refuse to cooperate in the form of dropping the packets. Ensuring security in MANET is a difficult issue. Moreover, in military environment preservation of security is a very serious issue. MANETs found its useful application military tactical communication. So far done researches proposed many algorithms rely on providing security for routing protocols, key management, and trust in MANETs; most of it is associated with cryptography, providing digital signature, certification etc.

Fig.1 shows the general principle of cryptography. The message to be encrypted is given as input and it is termed as plain text. Encryption algorithm converts plain text into a secret form using a key. This converted form of plain text is known as cipher text. Cipher text is allowed for transmission through the network. At the destination end cipher text is decrypted by using the decryption algorithm with the same key to get back the plain text

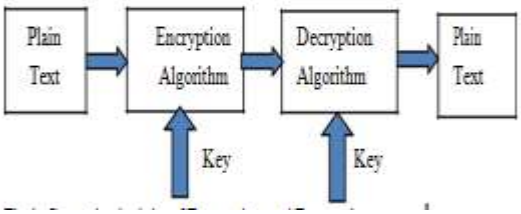

Fig 1. General principle of Encryption and Decryption process

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 4, May 2017

II PREVIOUS WORK

Providing security for a dynamic topology network like MANET is very difficult [5,6]. By taking the advantage of redundancies in the network, one can guess that what will be the next route, to steal the data. The main figure of merit of cryptography is the key distribution. One can say that the proper distribution of key will increases the chances of protecting data from the hands of unauthorized persons. Thus, designing an ad-hoc network with a secure key is a challenging problem to the designer. One of the solutions proposed by Diffie–Hellman key exchange method, which builds a temporary security, fails avoiding man –in- the-middle attack. Zhang and Lee [7] proposed an approach of tracing the data to describe the legitimate updates of routing information at each and every node. Since the legitimate change also includes physical movement of a node and also changes in the participating node members, so author has to take a prior step of deciding to use the node movement changes stored in routing table as the trace data. Trace data also gives information about similarity in the node movements and also updates the routing table. An algorithm called classification algorithm is defined to calculate the proportion of altered paths and the proportion of sum of changes in the hops of all routes. A detection model is defined to calculate the eccentricity scores of irregular from regular updates of routing table. Unluckily, there is no clear data on experimental results to measure the performance.

From another end of security by means of cryptographic techniques, symmetric key algorithms experiences more insecurity as compared to asymmetric key algorithms because it uses single key for encryption and decryption, by carefully listening to the network one can easily guess the message by trying all the possible keys.

The immobile nodes, spontaneous and unpredictable interaction of nodes in MANET requires more careful and complex encryption algorithms. Comparing with symmetric key algorithm, public key cryptography suits this. So far developed different asymmetric algorithms, relies on different ways of using mathematical functions. Rivest et al. [8] proposed RSA algorithm, the main principle behind RSA is that, it strongly depends on the truth that factorization is more complex than multiplication. Getting the product of two prime numbers together is easy, but knowing those two numbers from the product is not an easy task. In RSA, the main drawback is that they depends lot on CPU, so it is not possible to encrypt the message through a mobile phone. One solution to overcome this situation is encrypts the data with a symmetric algorithm and its key generated by the network and sent to the handset using an asymmetric algorithm.

Sawlikar et al.[9] proposed an encryption technique along with data compression. This method provides a solution to protect the data from eavesdropping. Proposed approach provides better efficiency and security. To provide multilayer protection algorithm named as DNA-Genetic Encryption Technique (D-GET) is proposed in [10]. This is less predictable and more secure algorithm which uses multiple key sequences.

Samreen et al. [11] proposed a double layer encryption technique designed for image encryption. This technique will protects image transfer from breaching attacks. A hybrid image security has been proposed. It used a combination of image compression, steganography and cryptography techniques. A session based symmetric key cryptographic algorithm is proposed in [12], which is a Matrix Based Bit Permutation Technique (MBBPT) method. Here the ASCII code equivalent of plain text is converted into a binary bit stream. Then these bits are arranged in diagonally upward fashion in a left to right trajectory into a square matrix of suitable order n. For encryption, the bits are considered from right to left trajectory. The same process is performed in reverse to get the plain text. In [13] several network security issues, the role of cryptography, the status of network security were addressed and finally steps to be taken for implementing the efficient security policy is also proposed. In [14] by combining Advanced Encryption Standard algorithm with Diffie-Hellman key exchange protocol Nitin K proposed an improved strong secured communication algorithm. Increasing the key length to 256 bits the strength of security level of AES algorithm can be improvised. More number of bits increases the number of rounds and provides a good encryption method. Further by applying Automatic Variable Key in AES, RSA security level can be further increasable during transmission [15]. By using parallel computing and reliability, time complexity can be reduced. Variable data with variable key is the most secured mode of transmission. For securing data over internet transmission and to achieve electronic data confidentiality in internet genetic algorithms (GAs) are proposed.in [16]. To encrypt and decrypt data stream with genetic algorithms is nothing but generating pseudo random function. Here both text and multimedia data can be encrypted. In this paper the author [17] proposed Random Key cryptographic algorithm, where the performance of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 4, May 2017

encryption process completely depends on the size of the message and the key size. Results show that this algorithmic approach provides an efficient security mechanism. In this paper the author [18] presents a comparative study on various symmetric key encryption techniques, detailed about the attacks to which they are vulnerable. Along with the method encryption, encryption time also plays an important role in cryptography. This can be better explained as, Let us consider an emergency needy attacked in natural disaster, because of lack of time for establishing a network we are preferring MANET for this situation, But an encryption method with high encryption and decryption time is also not preferable. So an encryption algorithm must be designed such that it has to be deciphered with in short period of time along with more security. Such a solution is addressed in [19]. Deepti A. Chaudhari proposed Enhanced Adaptive ACKnowledgement (EAACK).Without knowledge of false misbehavior report, this method will detects malicious nodes.

III. PROPOSED APPROACH

As Mobile wireless networks are generally open and dynamic network there are more chances of network and data security attacks than infrastructure based networks. Hence adequate security is an essential issue. In general, military environments use cryptography to protect confidential information from the hands of unauthorized hands. Encryption can be performed in various methods, few of them are:

- Secret Key Cryptography,
- Public Key Cryptography,

Secret key cryptography is also known as symmetric key cryptography, in which encryption and decryption will be done based on single and same key. Here sender will decide the key and that will be communicated to the receiver in a secret manner. Then receiver uses this key for decryption.

Public key method is also known as asymmetric key cryptography. This method differs from secret key in terms of different keys for encryption and decryption. The two keys are known as public and private keys. Here sender will encrypt the message by using public key, which is known to the entire node in the network. By using private key receiver is able to decrypt the message.

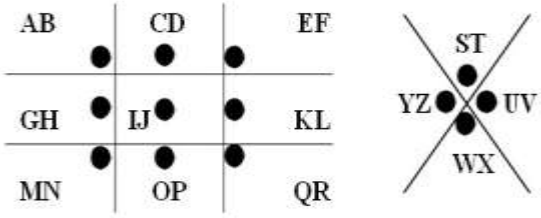

Fig..2 Letter-Shape Encryption

The core elements of the proposed method is TIC-TOC-TOE shape, X and dots. 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 example letter A is encrypted as _| and the letter B is encrypted as ._ | as shown in fig.2.Depending on sender freedom and by exchanging the same combinations with the receiver, attacker is unable to predict the message. By using this method sender can encrypt the message by using the shape around the letter, then receiver can decrypt the message.

IV. 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:

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

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 4, May 2017

V. RESULTS ANALYSIS

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 2 RESULTS COMPARISON TABLE

Packet Size (KB)	Encryption Time(sec)				Decryption Time (sec)			
	DES	*AES*	*RSA*	*L-S*	*DES*	*AES*	*RSA*	*L-S*
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

VI. CONCLUSION

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] NFS Wireless Information Technology and Networks Program Announcement, NSF 99-68, 1999.

[2] Report to the President, Information Technology: Transforming our Society, PITAC Report,February 1999.

[3] NFS Wireless and Mobile Communications Workshop, Northern Virginia, March, 1997.

[4] Kamal Kumar Chauhan, Amit Kumar Singh Sanger, Virendra Singh Kushwah, "Securing On-Demand Source Routing in MANETs ",IEEE Explore Digital library, 2010, pp:294-297.

[5] C. Pfleeger and D. Cooper, Security and privacy: Promising advances, IEEE Software, 1997.

[6] C. Perkins, Ad Hoc Networking, Reading, MA: Addison Wesley, 2001.

[7] B. R. Smith, S. Murphy, and J. J. Garcia-Luna-Aceves, Securing distance-vector routing protocol,in Proceedings Symposium Networking and Distribution Systems Security, 1997, pp. 85–92.

[8] Y. Zhang and W. Lee, Intrusion detection in wireless ad hoc networks, IEEE/ACM MobiCom Proc., 2000, pp. 275–283.

[9] Alka.p.Sawlikar, Dr.Z.J.Khan, Dr. S.G.Akojwar, "A new approach of compression and encryption algorithm", International journal of Advanced Research in computer science and software engineering, Vol 6, Issue 4, April-2016, pp-394-397.

[10] Hamdy M.Mousa, "International journal of computer network and Information Security", July 2016, 7, 1-9.

[11] Samrees Sekhon Brar, Ajitpal Brar, " Double layer image security system using encryption and steganography", Internation Journal of Computer Network and Information Security, March 2016, 3, 27-33.

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

[13] Dayanand Sharma , Abhijit Kulshreshtha, Shrawan Ram, "Network Security Challenges and Cryptography in Network Security", J. Comp. & Math. Sci. Vol.2 (1), 25-30 (2011)

[14] Nitin K. Jharbade,Rajesh Shrivastava, "Network based Security model using Symmetric Key Cryptography (AES 256– Rijndael Algorithm) with Public Key Exchange Protocol (Diffie-Hellman Key Exchange Protocol)", IJCSNS International Journal of Computer

Science and Network Security, vol.12 No.8, pp 69-74, August 2012

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

[16] Suvajit Dutta, Tanumay Das, Sharad Jash, Debasish Patra, Dr.Pranam Paul," A Cryptography Algorithm Using the Operations of Genetic Algorithm &Pseudo Random Sequence Generating Functions", International Journal of Advances in Computer Science and Technology, Volume 3, No.5, pp 325-331, ISSN 2320 – 2602,May 2014.

[17] Aruna Tomar, Sunita Malik, " A Random Key Based Visual Cryptography Approach for Information Security ", International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 6, pg.432 – 437, ISSN 2320–088X, June 2014.

[18] Saranya K, Mohanapriya R, Udhayan J, "A Review on Symmetric Key Encryption Techniques in Cryptography", International Journal of Science, Engineering and Technology Research

(IJSETR), Volume 3, Issue 3 pp 539-544, ISSN: 2278 – 7798,March 2014

[19] Deepti A. Chaudhari, Prof. S. B. Javheri, "An Intrusion Detection System for MANET using Hybrid Cryptography", International Journal of Advance Researn in Computer Science and Management Science, Volume 3, Issue 1, pp 347-352, ISSN 2321

– 7782,January 2015.

[20] R. Rivest, The MDS message-digest algorithm, RFC286, Internet Engineering Task Force,Symbolic, Inc., 1982.