ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Issue 4, April 2017

TIC-TOC-TOE Encryption for MANET Routing Protocols

Maheswary A[1*], Baskar S[2]

Research Scholar, Veltech University, Avadi, Chennai, Tamilnadu, India[1]

Professor, Department of EEE, Veltech University, Avadi, Chennai, Tamilnadu, India[2]

Abstract: In the case of an emergency such as a disaster or any rescue operations during Military wars, a communication network is needed. But for an immediate communication, it is not possible to wait for a network to be created. In such cases, a Mobile Ad Hoc Network (MANET) is used to create a temporary network. MANET is a temporarily formed network, which is a self-forming and self-configuring network. This network automatically forms a communication network by requesting help form the neighbouring nodes. Since MANETs are taking help from neighbouring nodes, there is no guarantee that the responding node is a trusted node. To be precise, the intermediate node should not change the content of the message. Many researches have provided solutions to this problem in the form of assigning certificates to the trusted nodes, verifying signatures of the nodes, authenticating the message, encrypting(hiding the message) etc. Each method is best in its own right but the attackers are succeeding in guessing the message by trial and error methods. Our method proposes a new encryption technique named as TIC-TOC-TOE encryption, which encrypts the data to be sent with prescribed shapes. To reduce the time of encryption, data compression is used before encrypting the data. By reducing the redundant data before applying encryption algorithm, encryption time can be reduced. So by using encoding and encryption data can be protected from eavesdropping. Here we are presenting an optimized encoding technique along with the encryption technique. The experimental results show that our proposed method performs better than many existing techniques with respect to compression ratio, encryption and decryption times and the speed of compression. The analysis includes comparison of encryption time and decryption time. For this analysis, we used NS 2.35 in a laptop with 2.4GHz CPU, in which the performance data is collected. This algorithm takes less processing time and it will work faster for encryption and decryption. It is concluded that the proposed algorithm will produce better performance than the other common encrypted algorithms.

Keywords: MANET, Network security, TIC-TOC-TOE encryption, Decryption. Data compression.

I. INTRODUCTION

At present, the field of Telecommunication Networks is dominated by the use of wireless networks. The very special feature of that wireless networks is the possibility of accessing information without considering the geographical traits of user. The exploits of a wireless network can be observed in the speedy development of the Internet and mobile phones. As compared to wired networks, wireless network does not rely on infrastructure. This characteristic worked as an add-on to the emergence of wireless networks. In other words, in places such as the disaster areas or a military battlefield, communications require an immediate and fast communication network, which is not possible to establish within hours. Such situations are better handled by the mobile ad-hoc networks (MANETs) [1-4], a wireless ad hoc network mechanism.

The Latin term “ad-hoc” means “for the purpose”. The network was created for the specific cause by mobile (moving) nodes. Hence the name mobile ad hoc networks are justified. MANETs are formed with the surrounding nodes. Here, the communication network can be established with any node (source) to reach any other node (destination) through intermediate nodes (router) and any node can act as a source, a destination or a router. With the help of neighbour nodes, data packets are forwarded to the destination. MANETs are self-configurable and self-organizing networks. They are de-centralized networks; no central administration is required to complete the communication process. MANETs process real-time data without being concerned with topological changes of the network. Simply we can say that MANETs are stand-alone networks, which are very suitable for the military tactical communications operation [3] or a rescue mission in the disaster area.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Issue 4, April 2017

Many advantages: MANET is made to stand out from the wired networks. The advantages are [5,6]: mobility, flexibility, and no fixed infrastructure is required [4], dynamic topology, low bandwidth, no centralized administration, low cost, fast establishment of a network. However, apart from these advantages, there are various crucial issues to consider with regards to a MANET. There are two challenges that need special concentration; performance and security [7]. To evaluate the communication protocol of MANET, performance is the key aspect. The optimal performance of routing protocol improves the quality of the communication process. Quality includes maximum packet delivery rate, minimum delay in the communication process, minimum overhead and maximum throughput. Frequent changes in the network topology and external attacks are the causes for degradation of performance. The special feature which makes MANET the best also presents some serious challenges in the security domain. MANET's open peer-to-peer networks and shared wireless medium, infrastructure-less networks, no central administration, and different nodes in the network, unpredictable behaviour and highly dynamic network topology causes these security threats. Designing a solution to these security issues will clearly achieve the desirable network performance. Security solution to a MANET not only focuses on avoiding attacks, but also on the performance of the network and node's power. Before trusting the nodes of the networks, MANET has to rely on their own specific security concerns. Two categories of security mechanism have defined MANET routing protocols; cryptographic mechanism and trust based mechanism. Cryptographic mechanism hides the original data and transmits the converted form of data through the network. At the receiver end the original message can be retrieved back by performing the re-conversion process. These two consecutive processes are known as encryption and decryption respectively. Many types of cryptography algorithms have been applied to secure the packet. The trust mechanism calculates the trust relationship between nodes before performing the communication process, which is calculated from the network behaviour. We choose the cryptographic mechanism to improve the security aspect of the protocol.

II. LITERATURE REVIEW

Many solutions were proposed by the researchers to provide better security for MANET, particularly on each communication layer. Angelos M [2] believes that direct attacks are prevented starting from the lower layers. The proposed approach uses a lightweight security infrastructure which considers the flaws that occur in higher years**.** In contrast, Saltzer et al. [8] suggested the application of end-to-end (before and after data is sent) security without interfering with the actual routing protocol will lead to a better security. It is a cryptographic mechanism proposed to secure the data in routing packet while in data exchange, in route creation and in route maintenance. Some of the cryptographic algorithms use common techniques like assigning certificates to the nodes for trusted participation or digitally signing the packets to enable the destination node to ensure the source node or any secret keys at both ends like symmetric and asymmetric key mechanisms etc. Zapata et al. [9] proposed Secure Ad-hoc On-Demand Distance Vector (SAODV). A hash chain technique is used to authenticate the hop count of RREQ and RREP messages. Every node after receiving the RREQ and RREP messages immediately verifies the hop count. So that hop count has not been decremented by an attacker. Digital signatures are also used; the signature has been verified every time after the reception of RREQ and RREP messages. The route will be created for the host only if the signature has been verified and the signature will be stored for further processing. Additionally, a new host also includes its signature as the second signature. Of course, this double signature idea enhances the security but also consumes time and network resources. Pirzada et al. [10] proposed a secure mechanism where all the nodes of the network must register themselves once with a Certification Authority before joining the network. Nodes are distributed with session keys and these keys are subsequently used in route discovery. Application of session keys and multi-layer encryption mechanisms protects passive or active attacks against the network. Akhlaq et al. proposed a secure scheme named as Classified AODV (CAODV) [11]. In this approach a trusted certification authority issues digital certificates after ensuring a trusted relationship between CA and all nodes of the network. This method uses asymmetric cryptography where two separate keys are used for encryption and decryption known as public and private keys respectively. It uses a double encryption method and also session keys for enhanced security. Symmetric key encryption, such as AES algorithm, is used to ensure confidentiality and integrity of data. Source node starts communication by sending RREQ along with its certificate and sends it to all the neighbouring nodes. At the same time source node requests the destination node for session key. Route discovery mechanisms start as per its definition, i.e., the intermediate nodes rebroadcast the RREQ packet. After reaching the destination node RREQ, destination node generates a session key after verifying the source node certificate. The session key is in its encrypted form, which was encrypted by using the source node's public key. Now destination node broadcasts RREP along with an encrypted session key to the source node. After receiving a RREP, the source node will decrypt the encrypted session key by its private key and then obtain the session key. This session key will be used for secure data exchange. The double encryption mechanism at the source and destination

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Issue 4, April 2017

nodes became inefficient in terms of delay. The new idea of securing all possible facets of the route discovery mechanism was proposed by Eichler et al. [12] and it is named as AODV-SEC. The mandatory requirement of this algorithm is that every node has to own a valid certificate issued by the certificate authority (CA) to participate in the network. To trust a node, it has own a certificate and a public key infrastructure (PKI). This algorithm also uses digital signature to ensure the authenticity and the integrity of the data, hash algorithms to count the hop of messages respectively. The routing packet header contains the certificate and hash details. Inclusion of the certificate and hop count in the routing packet increases the size of routing packets. The larger the packet consumes longer time to broadcast. Therefore packets size is also an important design criterion. To address this issue AODV-SEC used mCert, which contains only the relevant data of the certificate. The network operator will control and manages all the communication. Hence, one single public key infrastructure (PKI) is employed to introduce trust on a node level. Identifiable problem with this method is the distribution of certificates. In large networks, it is not feasible to exchange the certificates of all nodes beforehand. On the other hand, packet routing becomes big due to the hash and certificate extensions. It can increase the bandwidth consumption.

III. PROPOSED METHOD

3.1. Data Compression Algorithm

A data compression algorithm is a technique, which reduces the size of the data by avoiding redundancies in the data. The proposed compression technique works as follows:
Step1- Consider the data as an example **"SUCCESS"**.

By the standard ASCII encoding, this 7 character string involves 7*8=56 bits total. The table below displays the relevant subset of the standard ASCII Table 1.

Character	ASCII Number	Binary Number
S	83	01010011
U	85	01010101
C	67	01000011
E	69	01000101

Table 1: The string "SUCCESS" would be encoded in ASCII as 83, 85, 67, 67, 69, 83, 83.

Step 2- In the example string only four distinct characters are there and here we defined a special coding table using three bit of each characters.

Character	ASCII Number	Binary Number
S	0	000
U	1	001
C	2	010
E	3	011

Table 2: The string "SUCCESS" would be encoded in ASCII as 0, 1, 2, 3.

Step 3- Using the three bits table the string **"SUCCESS" is encoded as 0 1 2 2 3 0 0.** Represented as binary numbers: 000 001 010 010 011 000 000 (Table 2).

Using this special coding technique 56 bits string is encoded into 21 bits, so compressing ratio is 62.5% to its original size [13].

Data Encryption Algorithm: Encryption is the process of hiding the original data by converting it into a secret form using a key. The key will be shared to the receiver in a secret manner; receiver can decrypt the data to get the original

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Issue 4, April 2017

data back. This encryption and decryption process together is known as ciphering process. Basically encryption may be performed in two ways known as symmetric key encryption and asymmetric key encryption.
Symmetric key encryption uses the same key for both encryption and decryption and asymmetric key encryption uses two different keys separately for encryption and decryption. The key used for encryption is known as public key and the key used for decryption is known as private key. Private key is known only to the receiver alone whereas public key is known to all the available nodes of the network. When compared to asymmetric encryption, symmetric encryption is less secure as it relies on single key only but it takes less time for encryption and decryption. Here we are proposing a new and different encryption algorithm shown in Figure 1 named as TIC-TOC-TOE encryption since TIC-TOC-TOE shape is used as the many tool of conversion(?). The proposed method exchanges letters of secret data with prescribed shapes.

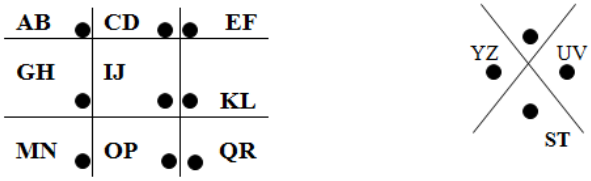

Figure 1: Letter-shape encryption.

The core elements of the proposed method is in TIC-TOC-TOE shape, X and dots. First letter in the grid is encrypted with shape of lines around the letter. Second letter in the grid is encrypted with the shape of the lines around the letter followed by a dot. For example, letter **A** is encrypted as **_|** and the letter **B** is encrypted as**._|** as shown in Figure 1. Depending on the freedom of the sender 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 and the receiver can decrypt the message later.

IV. SIMULATION SETUP AND NETWORK SCENARIO

Various tools are available for simulating the mobile ad-hoc networks; our study has simulated the network in NS-2.35. Initial parameters were considered as follows (Table 3):

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 3: Simulation parameters.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Issue 4, April 2017

V. RESULTS ANALYSIS

Table 4 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 the proposed technique takes less time for encryption and decryption than the RSA.

Packet Size (KB)	Encryption Time(sec)				Decryption Time (sec)			
	DES	*AES*	*RSA*	*TIC-TOC-TOE*	*DES*	*AES*	*RSA*	*TIC-TOC-TOE*
153	3.0	1.6	7.3	2.8	1.1	1	4.9	3.8
196	2.0	1.7	8.5	3.6	1.24	1.4	5.9	4.7
312	3.0	1.8	7.8	5.4	1.3	1.6	5.1	5.9
868	4.0	2.0	8.2	6.0	1.2	1.8	8.1	6.5

Table 4: Results comparison table.

VI. CONCLUSION

Based on our study, we introduced a new encryption technique called TIC-TOC-TOE Encryption for secure communication through MANET. Some existing approaches in this regards have been compared with the proposed technique. On the lines of this paper, we aim to reduce the encryption time with data compression techniques. Proposed TIC-TOC-TOE 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. When compared to 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. Abusalah L, Ashfaq K, et al. A Survey of Secure Mobile Ad hoc Routing Protocols. IEEE communications surveys & tutorials 2008; 10: 78-93.
2. Angelos M, Working with the Grid Kit Overlay Framework The Secure-AntHocNet Overlay. Thesis Lancaster University 2007.
3. David Gan CO, Ant Intelligence Routing Algorithm for Mobile Ad Hoc Networks. Thesis Malaysia University of Science and Technology 2004.
4. Xuan Y, A Defense System on DDos Attacks in Mobile Ad Hoc Networks. Thesis Auburn University Alabama 2007.
5. Toh C, Ad Hoc Mobile Wireless Networks: Protocols and Systems. Prentice- Hall New Jersey 2002; 34-37.
6. Murthy C, Manjo BS, Ad Hoc Wireless Networks: Architectures and Protocols. Prentice Hall communications engineering and emerging technologies series Upper Saddle River 2004.
7. Tarek Helmi Abd El-Nabi AA, Modeling And Simulation Of A Routing Protocol For Ad Hoc Networks Combining Queuing Network Analysis And Ant Colony Algorithms. Thesis Universität Duisburg-Essen 2005.
8. Saltzer J, Reed D, et al. End-To-End Arguments in System Design, M.I.T. Laboratory for Computer Science. MIT Boston Massachusets USA.
9. Guerrero Zapata M, Asokan N, Securing Ad hoc Routing Protocols. In Proceedings of the 1st ACM workshop on Wireless security, Atlanta, GA, USA, Sep 2002; 1–10.
10. Pirzada AA, McDonald C, Secure Routing with the AODV Protocol, Communications, 2005 Asia-Pacific Conference on 2005; 57-61.
11. Monis A, Noman Jafri M, et al. Addressing Security Concerns of Data Exchange in AODV. Transactions on Engineering, Computing and Technology 2006; 16: 29-33.
12. Stephan E, Christian R, Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC, Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on 2006; 481-484.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Issue 4, April 2017

13. Julie Z, Schwarz K, Huffman Encoding and Data compression. Hand outs, Spring May 23, 2012.