A NOVEL CRYPTOGRAPHIC APPROACH TO SECURE DATA IN MANET

Dr. V. Harsha Shastri[1] & V. Sreeprada[2]
[1]Lecturer, Dept. of CSE, Loyola Academy Degree and P.G College, Alwal, TS, India
[2]Lecturer, Dept. of Computer Science, Vasundara Degree and P.G College, ECIL, TS, India

Received: May 09, 2018 Accepted: June 24, 2018

ABSTRACT *A communication network is needed in case of emergency such as disaster or any rescue operations such as Military wars. We need an immediate communication network. In such cases a temporary network such as Mobile Ad hoc Network is created. MANET is a temporarily formed network, which is a self-forming and self-configuring network. Since MANETs are taking help from neighboring nodes, there is no guarantee that the responding node is a trusted node. 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. We propose a new encryption technique named as TIC-TOC-TOE encryption, which encrypts the data to be sent with prescribed shapes. So by using encoding and encryption data can be protected from eavesdropping.*

Keywords: *MANET; TIC-TAC-TOE; Encryption; Decryption;, Data Compression*

Introduction

We can access information using wireless network irrespective of the geographical traits. Wireless network can be observed in the speedy development of Internet and mobile phones. These networks do not rely on the infrastructure. In places where military fields or disaster areas, communications require an immediate and fast communication network which cannot be established within hours, we need a Mobile Ad hoc Network (MANET). The term "ad-hoc" means "temporary". The network was created for the specific cause by mobile (moving) nodes. 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 neighbor nodes, data packets are forwarded to the destination. MANETs are de-centralized networks; no central administration is required to complete the communication process. Frequent changes in the network topology and external attacks are the causes for degradation of performance.
The figure 1 shows an ad-hoc network in which nodes are participating connected to each other via wireless links [5]. Each device in a MANET independently moves from one point to another without restrictions in each and every direction, and it reconfigures its links to the other devices frequently.

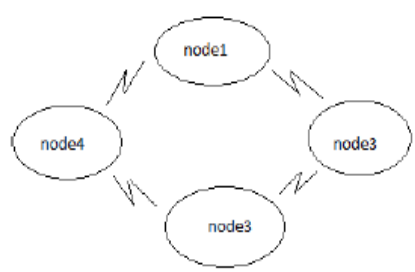

Figure 1: A wireless mobile ad-hoc network

Because of the de-centralized network, MANETs are prone to security threats. Security solution to a MANET not only focuses on avoiding attacks, but also on the performance of the network and node's power.
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 behavior. We choose the cryptographic mechanism to improve the security aspect of the protocol.

A. Advantages of MANET

The advantages of Mobile Ad-Hoc networks are huge because they deliver access to information as well as services indifferent to the geographical location. One of the typical advantages of MANETs is that they are free from central network administration due to self-configuration. Each of the system connected to a MANET are termed as Nodes. Nodes also act as routers and are cheaper than wired network. Scalability feature provides conformism for addition of more nodes. They are robust due to decentralized administration. MANETs can be best recognized for their following self-assured characteristics:

- Data Integrity: It ensures the node from being altering the data.
- Data update: It maintains data in the correct order and up-to-date
- Non-repudiation: It ensures a node cannot deny sending a message.
- Data Confidentiality: The data is hidden and disclosed to outsiders.
- Data Availability: Whenever the data is being requested, it is always available.

B. Applications of MANET

The application of MANETs with other network or operating systems gives it superior accessibility in wider domains such as

- Defense services: The setup of a fast and reliable MANET can provide quality communication through a highly secure medium. A challenging domain could be a military area.
- Collaborative computing: Computing based on collaborative methods give an edge to business meetings and information sharing outside the office environment when there are two different parties working on a same project.
- Bluetooth and Personal Area Networks: Short range MANETs can be used for the information exchange among cross platforms using Bluetooth involving various nodes.
- Educational Services: MANETs efficiently provide an interactive medium in the educational environment; MANETs can be used to provide rapid and firm multimedia or data sharing within an enclosed environment.

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.

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 (Route Request) and RREP (Route Reply) 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 neighboring 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 nodes became inefficient in terms of delay.

CRYPTOGRAPHY IN NETWORK SECURITY

Network security issues are making a tremendous increase in the various dynamic, static or ad-hoc networks. These issues can be very well contained and handled by employing many cryptography based algorithm schemes into the key generation, encryption and decryption of various sensitive data that need to be provided with efficient security. Broadly these cryptographic algorithms are classified into Symmetric and Asymmetric.

In Symmetric algorithm, we have only one key called single key that is used for encryption and decryption purpose. Example: DES, AES

In Asymmetric algorithm, we have two keys namely public and private key for encryption and decryption purpose. Example: RSA, ECC.

Secret Key Cryptography- It uses single key for encryption and decryption. Eg: DES and AES.

Hash Function- It is based on the mathematical transformation to encrypt information which is irreversible. MD (Message Digest) Algorithm is an example.

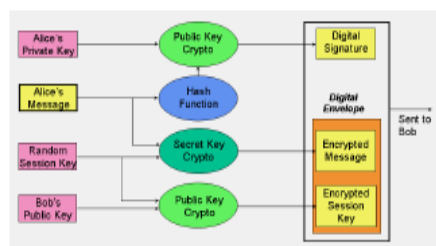

Figure 2: Types of Cryptographic Algorithms

PROPOSED METHOD

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 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.

Asymmetric key encryption uses two keys- private and public key. The public key is known to all the nodes in the network where as private key is known to only the receiver.

Symmetric key encryption uses single key. It is less secure as it relies on single key only but it takes less time for encryption and decryption.

Here we propose a TIC-TAC-TOE encryption algorithm to encrypt the data. This algorithm makes use of shapes to encrypt data. The pigpen cipher is a geometric substitution cipher which exchanges letters for symbols which are fragments of a grid.

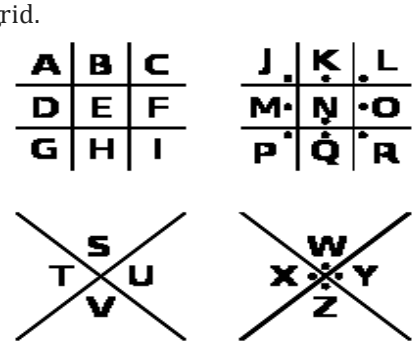

Figure 3: Letter Shape Encryption

The core elements of the proposed method is in TIC-TAC-TOE shape, X and dots. A letter is encrypted with the shape of lines around the letter. Also we can encrypt by using the shape of the line with dot around the letter. For example consider the message "X MARKS THE SPOT" is encrypted as:

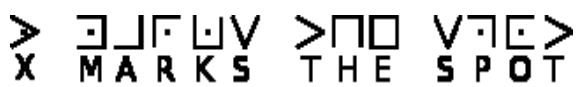

Figure 4: Message Encryption

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.

CONCLUSION AND FUTURE SCOPE

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. 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. In our future scope, we aim to reduce the encryption time with data compression techniques.

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. Shalini Saini, Asst. Professor Abhishek Shukla, Dr. Manish Verma "A Survey of Security in Mobile Ad-Hoc Networks using Cryptography" IJARCSE, Vol. 4, Issue 10, Oct 2014
4. Xuan Y, A Defense System on DDos Attacks in Mobile Ad Hoc Networks. Thesis Auburn University Alabama 2007.
5. Sarvesh Tanwar et al " Threats & Security Issues in Ad hoc network: A Survey Report" IJSCE, Vol.2, Issue-6, Jan 2013.
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. Vishwa gupta "Advance cryptography algorithm for improving data security" Int. J of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 1, January 2012
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 AODVSEC, Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on 2006; 481-484.
13. Menezes .A.et al "Hand book of Applied Cryptography,"CRC Press 1996.