SECURITY ALGORITHMS IN MANET

Lipsa Ahuja, Kunal Gupta(Guide)

Abstract: Security is very important for every communication. Security principles like authentication are required to be maintained. Since there are threats in traditional wireless system as well, with addition of mobility to it i.e. in MANET there exist various point for attacks as in MANET there is no fixed topology and any node can send and receive message with any other different node so there are large number of privacy problems that results in attacks. Thus, security becomes an important issue in MANET. Our paper presents various techniques of cryptography to provide security to the information flowing through the mobile ad-hoc networks with the help of various information hiding algorithms for making MANET more secure.

Index Terms: Authentication, Audio Data Hiding, Cryptography, DSA, Encryption, LSB Algorithm, Steganography.

1 INTRODUCTION

In the previous approaches, the wireless network includes a base station, switching centers(MSC's, BSC's) for initiating exchange of information between a source and destination node(destination node can be within or outside the network)[1]. On the other hand with the introduction of MANET there is no such need. It allows communication between nodes present in an autonomous, infrastructure less network also not following any topology since the nodes are mobile in nature. All such additive features provide ways for attacks to get into the network and thus suspects the security [4]. So, there arises a great need to provide more secure solutions to MANET as compared to traditional wireless network [5]. We are proposing a system in which we provide security to MANET using three cryptographic algorithm schemes: Digital Signature, EDES [6] and LSB [7] for hiding encrypted information in audio signal. A Digital Signature is a technique of signing a document using hash code and then verifying the sender using secret key [1]. EDES is used to encrypt information [2] and LSB for hiding data [3]. Our paper is organized in the following manner. Section 2 describes the existing cryptographic techniques through which we can secure MANET Section 3 describes the proposed system of securing the MANET. Section 4 describes the conclusion of the proposed system.

2 USE OF CRYPTOGRAPHIC ALGORITHMS FOR SECURING INFORMATION IN MANET

A. Digital Signature:

Digital signature algorithms are primarily used in cryptographic techniques to give privacy services including various security principles such as authentication. [1]

Steps in Digital signature algorithm:

1. A hash code of the message is taken. Hash code will become the fingerprint of the message.
2. The hash code is signed with private key of the sender.
3. Signed hash code is then combined with the original message.

Verification of the hash code:

1. Verification of the hash code is done by using public key of the sender. New hash code is then compared with signed hash code; if it comes out to be same then the recipient conformed that the message is same as sent by the sender. Integrity of the message is preserved.

2. The receiver of the message is now aware that the sender is original sender of the message, because only sender is aware of the private key.

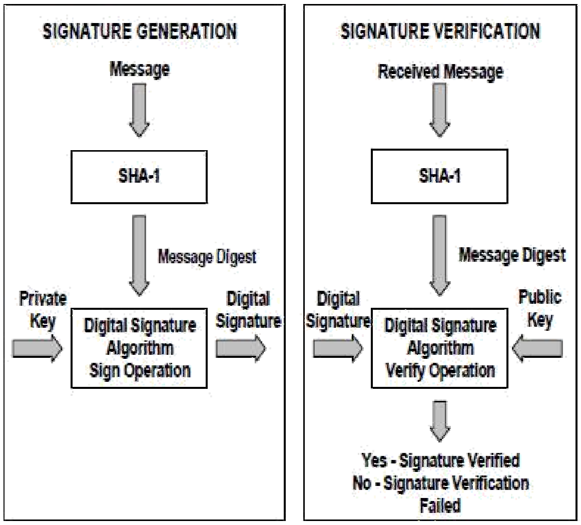

Fig1.Implementation of Digital Signature Algorithm.

B. Encryption of Data Using EDES:

Encryption is a technique in which we convert plain text into cipher text and which can be decoded back to original message. This technique is used to hide the important information flowing through the network [8]. There are many different encryption algorithms for hiding the information. [8] EDES (enhanced data encryption standard) is one such algorithm that consumes less computation power. [5]

Steps in EDES:

1. Divide the text into blocks of 64 bit. Initial permutation function is applied on 64 bit text block.
2. On original text initial permutation is performed.
3. Two halves are produced with initial permutation function. left plain text (LPT) and right plain text.
4. 16 rounds will be performed on LPT and RPT for encryption.
5. In the end LPT and RPT are combined and a final permutation is performed on the combined block.
6. The result of this process produces 64 bit cipher text.

Initial Permutation (IP): In this the characters in the plain text are simply transpositioned. The rearrangement takes place using IP table. After performing IP, 64 bit text is divided into 32 bit each LPT and RPT.

Rounds: each of 16 rounds consists of the following: 1. Key Transformation: In this step 8 bit key is produced from56 bit key and it is partitioned into parts, which is 28 bit in length. These are circularly shifted to left by single or double positions. After appropriate Shifts 48 bits are selected from 56 bit.

Expanded Permutation: In this 32 bit RPT is expanded to form 48 bit. This is done as follows- 32 bit text is divided into 8 blocks of 4 bit. 4 bit of each block is expanded to 6 bit.

2. S-Box Substitution: In this step 8 bit key produced at

1st step and 48 bit RPT produced at 2nd step are XOR and 32 bit output is produced using substitution technique.

The substitution is performed by 8 S-boxes which accepts 6 inputs and produces 4 outputs:

1. P-Box Permutation: In this step simple permutation of the characters is performed using P-box table. Result of this step is 32 bit text.
2. XOR and swap.
3. Final Permutation (FP): At the end of 16 rounds FP is performed only once. This is a simple transposition using a FP table. The output of FP is 64 bit encrypted block.

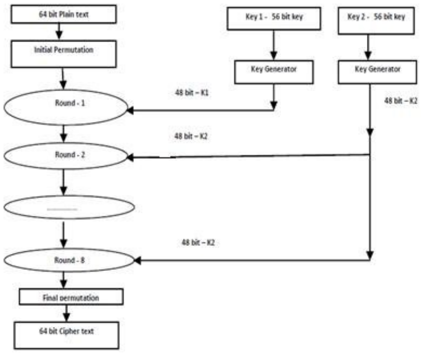

Fig 2. Implementation of EDES.

C. Hiding the Encrypted Data in using steganography:

It is a technique which is used to keep the encrypted message more secure using audio. Steganography is a technique of encrypting the message in a way which is difficult to understand. Steganography using audio is a technique of transmitting the message hidden in audio which is difficult to modify. This technique is mainly used for increasing the security. Steganography act as additional security to encrypted data.

Least Significant Bit (LSB) Coding: LSB is an algorithm which is used to hide the message in audio. In this technique binary equivalent of audio blocks is removed with binary equivalent of message. [9]

Steps in steganography:

1. In the first step audio file is selected for merging the original message.

2. Check the audio by playing it to see if it is clearly audible or not.

3. In the third step the file that contains the private message is selected.

4. Contents of the file are encoded.

5. Size of text file and audio file is compared.

If the size of text file size is greater than the audio file contents Error message will be displayed. Cannot merge the message.

Otherwise merge the message in the audio in the fourth and fifth Least Significant Bit of audio blocks. 6. The message of the new audio file is displayed after merging the message.

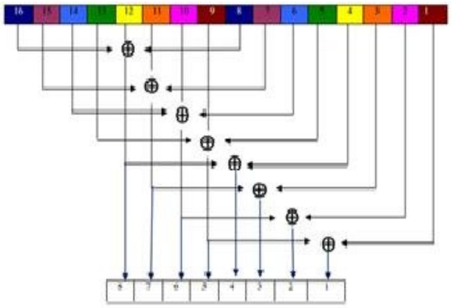

Fig 3. LSB algorithm

3 PROPOSED WORK

MANET is unsecure because of following features:

- Unreliability between wireless link because they have limited energy supply for wireless nodes.
- Constantly changing topology as nodes are moving continuously.
- Lack of secure boundaries.

To make MANET secure we need to use some techniques through which we can achieve security principles. We will use combination of three technologies to make the information secure in MANET.

1. AUTHENTICATION: Authentication helps in establishing proof of identities. It is defined as the assurance that the communicating entity is one that it claims to be. Authentication can be achieved by using DSA.

2. ENCRYPTION OF DATA: To secure the data we need to encrypt our data. For encryption there are various algorithm and we will use EDES algorithm with less power consumption to get a signed document.

3. HIDING INFORMATION IN AUDIO SIGNAL: Encryption is a technique which is used to convert the readable form of text into non readable format this protects the information and keep it secure but there are still some chances of attack to this information so, to make it more secure a new technique is used in which the information is hidden inside the audio signal and this reduces the transparency.

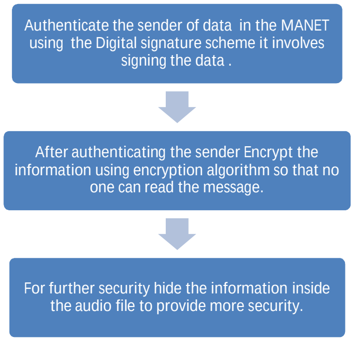
Authenticate the sender of data in the MANET using the Digital signature scheme it involves signing the data .
After authenticating the sender Encrypt the information using encryption algorithm so that no one can read the message.
For further security hide the information inside the audio file to provide more security.

Fig 4. Proposed System.

4 CONCLUSION

The proposed system is an effective method for hiding text and providing additional security in audio files such that data can securely reach the destination without being modified. Using the different techniques of cryptography with different kinds of data using encryption and decryption to make data more secure and transparency is reduced.

ACKNOWLEDGEMENT

I would like to express my gratitude to Mr.kunal Gupta and Mr. Abhishek Singhal faculty computer science and engineering department Amity University for their guidance and help in completing this work successfully.

REFERENCES

[1] P.Kitsos, N. Sklavos and O. Koufopavlou,"*an efficient implementation of digital signature* "VLSI Design Laboratory Electrical and Computer Engineering Department University of Patras. Patras, GREECE 2010.

[2]S.Sudha, V.Madhu Viswanatham, K.Brindha, L. Agilandeeswari , G.Ramya," *Implementation of Enhanced Data Encryption Standard on MANET with less energy consumption through limited computation*" International Journal of Engineering Research and Development eISSN : 2278-067X, pISSN : 2278-800X, www.ijerd.com Volume 2, Issue 4 (July 2012).

[3]Padmashree G, Venugopala P *S* ", *Audio Stegnography and Cryptography: Using LSB algorithm at 4th and 5th LSB layers*" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4, October 2012.

[4]Mihir Bellare and Sara K. Miner," *A Forward-Secure Digital Signature Scheme*" Dept. of Computer Science, & Engineering University of California at San Diego, 9500 Gilman Drive La Jolla, CA 92093, USA.

[5] Poulami Dutta, Debnath Bhattacharyya1, and Tai-hoon Kim, "*Data Hiding in Audio Signal: A Review*" International Journal of Database Theory and Application Vol. 2, No. 2, June 2009.

[6] Wenjia Li and Anupam Joshi," *Security Issues in Mobile Ad Hoc Networks*" Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County.

[7]M.Umaparvathi, Dr.Dharmishtan K Varughese, "*Evaluation of Symmetric Encryption Algorithms for MANETs*", 2010 IEEE.

[8] Coppersmith D, *"The Data Encryption Standard (DES) and Its Strength against Attacks.*" IBM Journal of Research 1994.

[9] K.P.Adhiya Swati A. Patil," *Hiding Text in Audio Using LSB Based Steganography*" Information and Knowledge Management 2224-5758 (Paper) ISSN 2224-896X, 2012.