IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 6, Ver. I (Nov - Dec 2018), PP 01-05
www.iosrjournals.org

Implementation of Network Security in Mobile AD-HOC Networks using Multilevel Encryption Techniques

Mr. P. Daniel Sundar Raj& Dr. K. Arulanandam
Department of Computer Science and Application K.M.G. College of Arts and Science, Gudiyattam
Department of Computer Application Government Thirumagal Mills College, Gudiyattam
Corresponding Author: Mr. P. Daniel Sundar Raj

Abstract: *When we are sending a secret information fromsource to destination over a wireless network, safe and secure transmission is a critical issue. An ad-hoc network is a set of wireless nodes and any type of central control or centralized administrationis not in this network. Wireless Ad-hoc networks are organized and configured in self mode. Each and every node in this network is set up using a wireless transmitter and a wireless receiver. The networktransmits data with other nodes in its communication range only. When the data are transmitted, the nodes communicate with each other usinga common physical media. The nodes send and receive signals using the same frequency band and by doing so, it follows the same hopping method. If the receiving node is not inside the transmission range, the source node uses the other nodes to transmit the messages hop by hop. For sending a message from one node to another node that is out of its frequency range, it gets the help of other nodes in the network for an effective data transfer. This technique is called as multi-hop communication. Hence, every node acts both as a host and as a router at the same time. Wireless Mobile networks are usually attacked by many sources, such as hackers, intruders and other physical attacks. Creating and configuring a safe and secure wireless ad-hoc network isvery difficult for the reasons such as: the poor quality of communication channels and nodes, poor infrastructure, frequently changing topology and technology.Due to this factors, the wireless channel can be very well and easily accessible by all the network users and the attackers. An attackercan easily break network operations by not following the specifications of network protocol. Hence, a secure protocol is to be created for safe data transfer. Because of frequently varying techniques in the network topology, there is a complexity to routing among the various mobile nodes in a safe way. In this paper, a multi-level encryption methodis suggested for sending the data over a wireless network and this form of methodhelps us to send our secret message in a more secured way over a wireless network.*

Keyword: *Network Security, Plaintext, Cipher Text, Cryptology, Multi-level Encryption, Decryption*

Date of Submission: 22-10-2018 Date of acceptance: 05-11-2018

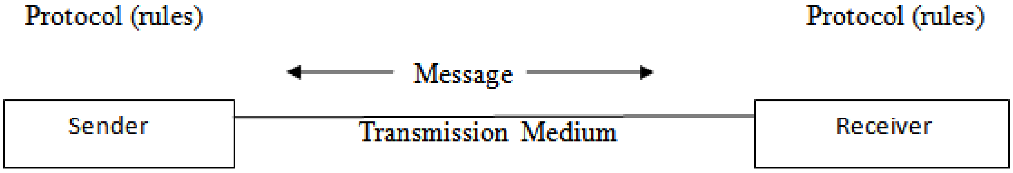
I. Introduction:

1.1 Data Communication

Sharing of our information with others through a communication channel is called data communication. This process of sharing the information can be local or remote. The local communication occurs face to face, where as in the remote communication, the data transmission occurs over distance. Computers which are connected with a network system are very useful devices to exchange information over a network. In the network system, every individual computer machine is known as a client machine or a node and there will be a server machine to store the information in a central place. The nodes can get the required information from the server on request.

1.2 Computer Network

A computer network is a set of computers which are interconnected using a common communication channels. A fine data communication system consists of the following main components.



Message : The sender transmits the message to the receiver.
Sender: Sender is a device at the source which sends the data to the receiver.
Receiver : Receiver is a device at the destination which receives the data sent by the sender.
Transmission Medium : It is the channel or a physical path by which the data travel from a sender to a receiver.
Protocol : It is a set of rules to be followed for transmitting data bits from the sender to the receiver through a Transmission Medium.

1.3 Network Security

When we are transmitting an important message from a sender to a receiver over a network, the message should not be accessed and damaged by any unauthorized users in the middle. Hence proper principles and methods are required in order to protect the messagethat we are sending over a network.

1.4 Cryptography

Cryptography is a technique which is able to convert an intelligible message into an unintelligible message that should not be understood by others. This process of converting a message is very essential to send the data from a sender to a receiver and it provides help to protect our all our data being sent. Since the data travels in an unintelligible format over a network, any unauthorized person in the middle cannot understand it and hence he may not damage or corrupt the data. After the transmitted message is received at destination, the message is again converted into its original intelligible format.

The technical terms being used in cryptography technique are as follows.
Plaintext: A original intelligible message being sent from a source to a destination.
Ciphertext: The message after being converted into unintelligible format.
Cipher: It is an algorithm being used to transform an intelligible message into an unintelligible format.
Key: A specific key being used by the algorithm (Cipher) which is only known to the sender or receiver.
Encipher (Encoding): The process of converting a plaintext to cipher text with the help of a cipher (algorithm) and a key.
Decipher (Decoding): The process of converting a cipher text back to its original intelligible format (plaintext format).
Cryptanalysis: The study of principles and methods of converting a cipher text into a plaintext without knowledge of the key. It is known as "code breaking" and it is used by the intruders to read the protected data without the knowledge of sender and receiver.
Cryptology: It is the combination of cryptography and cryptanalysis.

II. Literature Review:

2.1 The initiative measures for the proposed

1) For the exchange of session key the concept of asymmetric cryptography (public key and private key cryptography) will be used.
2) Certificates will be used to attach asymmetric keys (public and private keys) to the nodes.
3) Certificates of source and destination are attached with RREQ and RREP messages.
4) Our proposal scheme uses the concept of asymmetric cryptography for exchange of session key only as it is resource intensive and could be considered as unsuitable choice for MANETs..
5) We propose use of a symmetric cryptographic technique such as Triple Data Encryption Standard (3DES) for data encryption providing more reliable and secure data transmission.
6) Certificates can be issued to all participating nodes in relation to unique identity of respective users.
Following symbols will be used in the proposed scheme, source (S), destination (D), session key (Ks), encrypted session key (Ke). Kax public key of x, Kbx private key of x, where X is either source or destination. Ek encryption using key K, Dk decryption using key K.

2.2 Issuing of certificates

Let U = {U1, U2, U3, … Un} are different users and ID = {ID1, ID2, ID3, …. IDn} be the identity (which is unique) of respective users in the mobile ad hoc network. Each user Ui has a unique identity IDi, which is well known to all the other users.
User Ui take his identification number IDi to the CA to obtain the signature Gi for IDi along with its public and private keys. If the center confirms the correctness and the relationship between Ui and IDi , then center calculates gi using:
Gi=(IDi ^Kbs)mod n and hands Gi along with its public and private keys to Ui as shown in fig 5.
Figure 5: Issuing of certificates by Certification When all the users have registered and got their Gi (i =1...n), public and private keys the centre does not need to exist in ad hoc network to any further extent.

2.3 Working

Source generates RREQ message, attaches its certificate, along with a request for the session key and sends it for route discovery of destination. The intermediate nodes rebroadcast the RREQ message according the operation of AODV protocol. On receipt of RREQ message, the destination node verifies the certificate of source and on authorization generates a session key. The destination encrypts the session key first through its private key and then encrypts Ke1 with the public key of the source as

Ke1= Ekbd (Ks))

Ke = Ekas (Ke1).

Destination act in response with RREP message attach its certificate and encrypted session key Ke. On receiving, the source confirms the authenticity of destination from its certificate, decrypts the session key first through its private key and then through public key of destination as Ke1= Dkbs (Ke)

Ks= Dkad (Ke1) respectively.

Finally session key is achieved that will subsequently be used for secure data exchange.

III. Data Security Design And Implementation:

Data Security Is Implemented Into Two Methods,

i) Message Encryption

ii) Message Decryption

3.1 Data Security Using RSA

- Source sends the encrypted data packet to the destination through the route discovered.
- Destination decrypts the data packet received from the source and sends theacknowledgement.

3.2 Input and Output Parameters

Input Parameters:

- At source, encrypted data packets are sent with destination address and route request..

Output Parameters:

- Receiving positive acknowledgement with efficient and reliable packet transmission.

Algorithm for Key Generation:

Step 1: Select two prime numbers p and q such that p
Not equal to q.

Step 2: Calculate n=p x q

Step 3: Calculate ø (n) = (p-1) (q-1)

Step 4: Select integer e such that
gcd (ø(n),e)=1;1<e< ø (n)

Step 5: Calculate d such that d=e^{1}mod ø(n)

Step 6: Public key KU= {e,n}

Step 7: Private key KR= {d,n}

Encryption:

- The plain text M (M<n) is encrypted to cipher text using public key e.
- C=M pow e (mod n)

Decryption:

- The cipher text C is decrypted to plain text using private key d.
- M=C pow d (mod n)

Algorithm Step By Step Description:

If the user wants to send data:

1. Get the Destination identifier and the encrypted data to be transferred.

2 .Initialize the buffer with the encrypted data to be transferred.

3. Setup a Request Zone.

4. Build a Route Request packet having the information about the source and the

6. Destination identifiers, and the Request Zone information.

6. Broadcast the Route Request to its neighbors.

7. Setup a timer for receiving Route Reply.

8. . If the node receives a packet

9. Find the type of the packet received.

10. Depending on the type of packet received do one of the following processes.

11. Process Route Request.

12. Process Route Reply.

13. Process Data Packet.

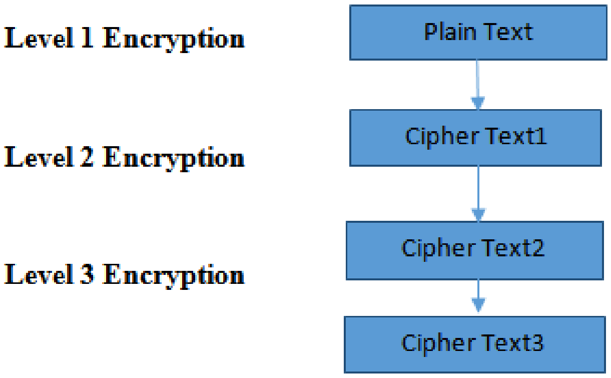
14. Process Decryption.

15. Process Acknowledgement.

16. Process Route Disconnect.
17. Process Route Disconnect reply.
18. Process Timer Run Out.

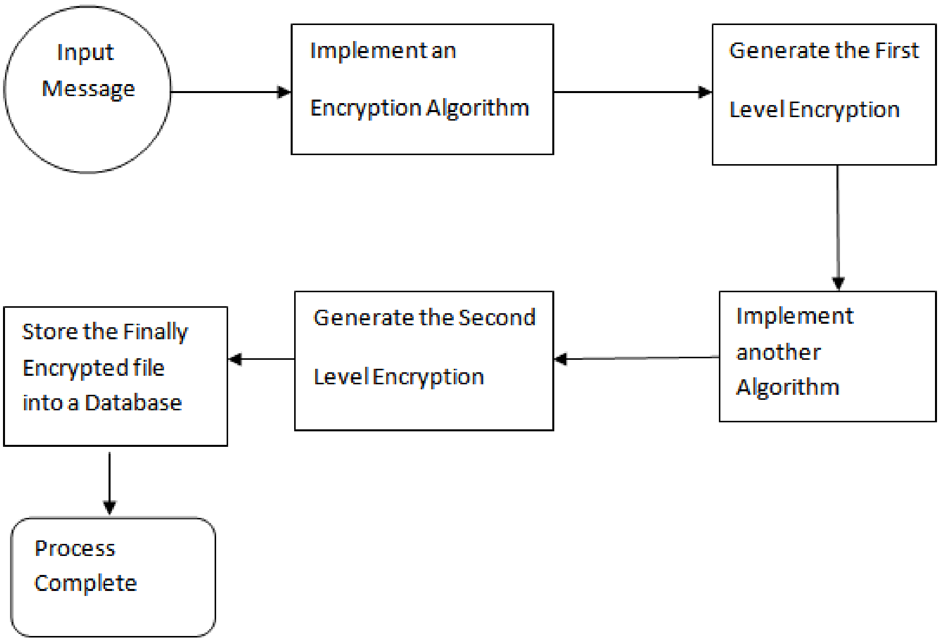
3.3 Multi-Level Encryption

It is the technique of encrypting an intelligent plain text more than once using various keys. Below is a Multi-Level encryption technique and it is implemented in three levels.



Level 1 Encryption:
In this level, the Plain Text is encrypted and converted into Cipher Text1.
Level 2 Encryption:
In this level, the Cipher Text1 is again encrypted and converted into Cipher Text2.

Level 3 Encryption:
In this level, the Cipher Text2 is encrypted and it is converted into Cipher Text3.
3.4 Steps to carry out the encryption technique in two levels
(The inverse algorithms are used for decrypting the message and to get the original message)


Input Message
Implement an Encryption Algorithm
Generate the First Level Encryption
Implement another Algorithm
Generate the Second Level Encryption
Store the Finally Encrypted file into a Database
Process Complete

IV. Conclusion:

After the original message in the form of plain text is encrypted in different levels as above, it is decrypted by using decryption algorithms to get back the original message. If the secret message is encrypted in multiple levels like as above, anyunauthorized persons in the middle cannot easily read the message. While doing so, time synchronization is a must one. For time synchronization, we should create encryption algorithms in such a way that it should not take more time for encryption process.

References:

[1]. Here we have mentioned various references from which we actually collected our problem and Also found the solution for our problem.

[2]. Kejun Liu, Jing Deng, Member, IEEE, Pramod K. Varshney, Fellow, IEEE, and Kashyap Balakrishnan, Member, IEEE

[3]. L. Buttyan and J.-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," ACM/Kluwer Mobile Networks and Applications, vol. 8, no. 5, 2003.

[4]. K. Balakrishnan is with the Security Services Group, Deloitte and Touche LLP, 1750 Tysons Boulevard, Suite 800, McLean, VA 22102. E-mail: kbalakrishnan@deloitte.com.

[5]. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom, Aug. 2000.

Mr. P. Daniel Sundar Raj. " Implementation of Network Security in Mobile AD-HOC Networks using Multilevel Encryption Techniques " IOSR Journal of Computer Engineering (IOSR-JCE) 20.6 (2018): 01-05.