Safe and Secure Data Transfer in Mobile AD-HOC Networks using Multilevel Encryption Techniques

Mr. P. Daniel Sundarraj[1],Dr. K. Arulanandam[2]

[1]Department of Computer Science and Application, K.M.G. College of Arts and Science, Gudiyattam,Tamil Nadu, India

[2]Department of Computer Application, Government Thirumagal Mills College, Gudiyattam,Tamil Nadu, India

ABSTRACT

At the time of sending any secret information from a source node to a destination node over a wireless network, it is very critical to transmit it in a safe and secure manner. A set of wireless nodes constructs an Ad Hoc network and this network does not have any central control or centralized administration. In self-mode, wireless Ad-hoc networks are organized and configured. All nodes in this network are set up by using a wireless transmitter and a wireless receiver. The wireless Ad Hoc network transmits data with other nodes within its communication range only. Using a common physical media, the data are transmitted between one node and another node in this network. Every node sends and receives signals using the same frequency band and it follows the same hopping method during data transmission. If the destination node is not inside the transmission range, the source node will use the other nodes to transmit the messages hop by hop. In order to send a message from one node to another node that is out of its frequency range, it needs the help of other nodes in the network for the data transfer. This technique is technically known as multi-hop communication. In this network, each and every node acts both as a host and as a router at the same time. Wireless Mobile Ad Hoc networks are usually attacked the sources such as intruders, hackers and other physical attacks. Constructing and configuring the safest and secure wireless ad-hoc network is very difficult for the reasons such as: the poor quality of communication paths and communication nodes, low quality infrastructure, frequently updating topologies and technologies. Due to these main factors, the wireless communication path or channel can be easily accessed by all the network users and the attackers and it makes the network operations very insecure and unsafe. Any user can easily break the network system and its operations by not following any specific protocol. Hence, a safe and secure protocol or an algorithm is to be developed for the safest data transfer. Also, there is another issue and it is the complexity of finding the routing mechanism to transfer our data from one node to another node in a safe way. In this paper, we are suggesting a multi-level encryption technique which can send the data over a wireless network in a safe and secure way.

Keywords: Ad-hoc Network, Encryption, Decryption, Routing, Multi Hopping, Cryptography, Cipher Text

I. INTRODUCTION

A. Ad Hoc Network: Characteristics

1. It does not have any fixed architecture.
2. It has a dynamic topology.
3. It is a Multi-hopping Network.
4. Scalability: It may have thousands of nodes.
5. Security: It is limited

B. Issues in Ad Hoc Networks

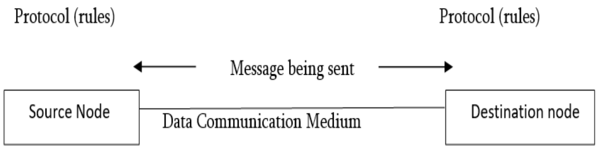
- Medium Access: Distributed, no time synchronization
- Routing: Route Acquisition Delay, Quick Reconfiguration, Loop Free
- Multicasting: The way of communication occurs between the nodes
- Transport Layer: Frequent path breaks
- Self-Organization: Neighbor discovery, Link failures
- Security: Jamming, Hackers and Intruders
- Energy Control: Transmission Power, Battery Monitoring, Processing Power.

C. Data Communication

Sharing our information with other people through a communication path or media is called data communication. This process can be local or remote. The local communication is done face to face. On the other hand, the data transfer in remote communication occurs over distance. The nodes or workstations in a network system are very useful devices to exchange information over a network. In the network system, each and every computer is known as a client machine or a node or workstation and it keeps a server machine to store the information in a central place. On request, the nodes will receive the required information from the server.

D. Computer Network

A group of computers form a computer network and the nodes in it are interconnected by using communication channels. Following are the important components of a network system.



While transmitting an secret message from a sender node to a receiver node over a network, the message should be protected from the unauthorized users. Hence proper techniques and methods are required to protect our secret message that we send from the source.

E. Cryptography

We can convert an intelligible message into an unintelligible message by using cryptographic techniques. This unintelligent format of message cannot be read by others.

In Cryptography, the following technical terms are used.

Plaintext: It is the message to be sent from a source node to a destination node in the network.

Ciphertext: After the message is converted into unintelligible format, this encrypted form of message is called Ciphertext.

Cipher: An algorithm which is used to convert an intelligible message into an unintelligible message is technically called as Cipher.

Key:A secret key is used by an algorithm (Cipher) for safe data transfer and this key is only known to the sender or receiver.

Encipher (Encoding): This is the process of converting a plaintext into a cipher text by using the cipher (algorithm) and the secret key is known as Encipher (Encoding)

Decipher (Decoding): This is the process of reconverting the cipher text into its original format (plaintext format) and it is technically called as Decipher (Decoding).

Cryptanalysis: The study of methods and principles to transform a cipher text (unintelligible form of message) into a plaintext (intelligible form of message) without using a secret key is called as Cryptanalysis or Code Breaking.

Cryptology: It combines both the cryptography and cryptanalysis.

II. OUR BASIC AND PROPOSED IDEA FOR THE IMPLEMENTATION OF SAFE AND SECURE DATA TRANSFER

1) To exchange our information between a source node and a destination node, the asymmetric cryptography method is used (public key and private key cryptography). A modified RSA algorithm is preferred here. The public key is known to all and the private key is kept secret in this technique.

2) The encryption is implemented in two stages by using a modified RSA algorithm which ensures security in data transferring.

III. RSA Algorithm in Cryptography (Modified Algorithm)

A. Steps to be used for converting data from plain text to cipher text format

1. The client node sends its public key to the server node and requests for its response.
2. The server encrypts the data asked by the client using the technique in RSA algorithm.
3. The Client node receives the requested data in its original form after decrypting the cipher text.

B. The Technique

1) The public key combines two numbers. In which, one number is the multiplication of two large prime numbers.
2) The private key is created with the help of the same two prime numbers.

C. Illustrating an example showing the Cryptographic Technique

Creating the Public Key

- Assume two prime numbers. (**M = 31 and N = 37**).
- The first part of the Public key will be now **n = M*N = 1147**.
- Calculate the exponent **e** with the following conditions :

e should be an integer value

e should not be a factor of n

Also, 1 < e <Φ(n)

Assume that e is equal to 3.

- Finally the Public Key is made of n and e

Generating Private Key

- Compute Φ(n) :

Φ(n) = (M-1)(N-1)

Hence, Φ(n) = 1086

- Compute to create the Private Key, **p** :
- **s = (r*Φ(n) + 1) / e** for some integer r
- For example if r = 2, the value of s is 724

Finally, we get the calculated Public Key is (n = 1147 and e = 3) and our Private Key is (s = 724)

D. Encryption

Suppose the message to be encrypted is **"BC"**:

- Convert the above characters into its sequence numbers (B = 2 and C = 3)
- Now the Encrypted Data will be **g = 23^e mod n**.
- Hence our Encrypted Data will be 697

E. Decryption

We need to decrypt **697** again into its original form:

- **The Calculation for Decrypting the Data is = g^s mod n**.
- Hence our Encrypted Data will be 23.

Finally we receive our original message "BC", since 2 = B and 3 = C.

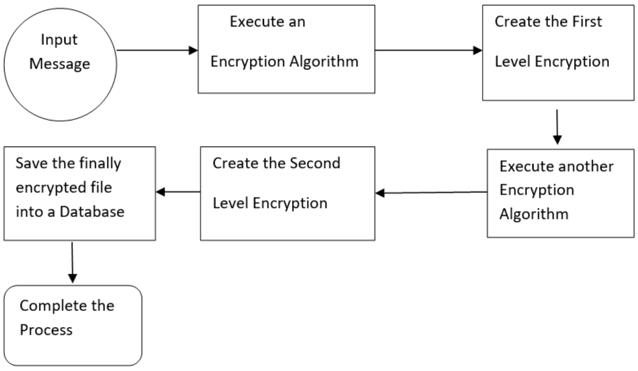
IV. FOLLOWING IS THE IMPLEMENTATION OF RSA ALGORITHM IN C PROGRAMMING LANGUAGE

```
// Our C program to implement the RSA
algorithm

#include<stdio.h>

#include<math.h>

// Finding the gcd of i and j

intgcd(inti, int j)

{

    int t;

    while (1)

    {

        t = i%j;

        if (t == 0)

          return j;

        i = j;

        j = t;

    }

}

 // RSA algorithm

int main()

{

    // Let us take any 2 random prime numbers

    double p = 3;

    double q = 7;

     // Computing the first part of public key:

    double n = p*q;

     // Computing the other part of public key.

    // e – Encryption

    double e = 2;

    double hi = (p-1)*(q-1);

    while (e < hi)

    {

        // e is co-prime to hi which is smaller than
hi.

        if (gcd(e, hi)==1)

            break;

        else

            e++;

    }

    // Creating the Private Key (d - Decryption)

    // selecting d such a way that it should satisfy

    // Calculating the d*e = 1 + k * totient

    int k = 2;  // A constant value

    double d = (1 + (k*hi))/e;

    // The Message to be encrypted is

    double mmesg = 20;

     printf("Our Message data is: = %lf", mmesg);

    // Calculating the message to be encrypted is :
s = (mmesg ^ e) % n

    double s = pow(mmesg, e);

    s = fmod(s, n);

    printf("\The encrypted data is: = %lf", s);
    // Calculating the message to be decrypted is :
f = (s ^ d) % n

   double f = pow(s, d);

   f = fmod(f, n);

   printf("\nThe Original Message in Plain Text
Format is: = %lf", f);

   return 0;

}
```

V. MULTI-LEVEL ENCRYPTION

Multi-Level encryption is a method or technique which encrypts the message more times in different levels.

(The inverse algorithms are to be used for decrypt the message and converting it into original message)



Input Message
Execute an Encryption Algorithm
Create the First Level Encryption
Execute another Encryption Algorithm
Create the Second Level Encryption
Save the finally encrypted file into a Database
Complete the Process

VI. CONCLUSION

After we encrypt the intelligible plain text message in multiple levels as stated above, the final encrypted message is decrypted by using the inverse algorithms in order to get the original message. If the message is transmitted like this, the hackers will find it very difficult in accessing our data and damage it and this type of technique is more secure and safe data transmission as well. While following this technique, the time synchronization process should be there to synchronize our data being sent and we need to also ensure that we get back the data in original format without any acquisition delay. For this time synchronization process, we need to create proper encryption and decryption algorithms so that it should not take much time for encryption and decryption process.

VII. REFERENCES

[1] Kejun Liu, Jing Deng, Member, IEEE, Pramod K. Varshney, Fellow, IEEE, and KashyapBalakrishnan, Member, IEEE

[2] 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.

[3] 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.

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

[5] V.-N. Padmanabhan and D.-R. Simon, “Secure Traceroute to Detect Faulty or Malicious Routing,” SIGCOMM Computer Comm. Rev., vol. 33, no. 1, Jan. 2003.

[6] Srinivasan, P. Nuggehalli, C.F. Chiasserini, and R.R. Rao, “Cooperation in Wireless Ad Hoc Networks,” Proc. INFOCOM, Mar.-Apr. 2003.

[7] D. Johnson, D. Maltz, Y.C. Hu, and J. Jetcheva, “The Dynamic Source Routing Protocolfor Mobile Ad Hoc Networks (DSR),” Internet draft, Feb. 2002.