INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Security Enhancement for Data Transmission in Mobile AD-HOC Networks

K. Jeyalakshmi
Assistant Professor, PG and Research Department of Computer Science
Hindusthan College of Arts and Science, Hindusthan Gardens, Coimbatore, India
C. Prabhu
Assistant Professor, Department of Computer Applications
Hindusthan Institute of Technology, Othakalmandapam, Coimbatore, India

Abstract:
Mobile Ad-hoc Networks is one of the most popular and widely usable wireless technologies. Among so many wireless standards, Ad-hoc technology won the favor of people because of its lower construction and operating costs, higher data rate, farther transmission distance and better extensibility, etc. But it can be less secure than wired connections because an intruder does not need a physical connection. So security is a key issue in data transmission through this network. In this research work an integrated cryptographic scheme has been proposed to overcome the security problems and to enhance the security of Mobile Ad-hoc Network. This scheme is based on DES, RSA and Rijndael algorithm. These three algorithms are used to generate the key to encrypt the data. Among the three algorithms, Rijndael algorithm has variable block and key length. Since the extension of blocks is possible in Rijndael algorithm, we can extend the block length and key length by multiples of 32bits in order to avoid the loss of data while transferring the biggest files.

Key words: *Ad-hoc, DES, RSA, Rijndael algorithm*

1. Introduction

An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of existing network infra-structure or centralized administration. Due to the limited transmission range of wireless network interfaces, multiple network hops may be needed for one node to exchange data with another across the network. In such a network, each mobile node operate not only as a host but also as a router, forwarding packets for other mobile nodes in the network, that may not be within the direct reach wireless transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multi hop paths through the network to any other node. The idea of an ad hoc network is sometimes also called an infrastructure-less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly. DES key generation is consists of two steps, The Feistel Function of four stage and Key Schedule. RSA algorithm involves public key and private key .public key knows everyone and used for encryption and private key knows receiver and used for decryption. RIJNDAEL algorithm is used for generating key and block size then encryption occurs in following steps initial, Nr-1 and final round and decryption is as same as but decryption key must loaded in key buffer before decryption begins. This research work proposed here is done to enhance the security in Ad Hoc Network by using DES, RSA and Rijndael algorithm. The main goal is to access the server with a physical drive and password in order to achieve the security.

2. Methodologies

Methodology is the systematic, theoretical analysis of the methods applied to a field of study, or the theoretical analysis of the body of methods and principles associated with a branch of knowledge. The algorithms used for the proposed work are DES Algorithm, RSA Algorithm, Rijndael Algorithm. The Data Encryption Standard is a block cipher algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bitstring of the same length. The key consists of 64 bits only 56 of these are actually used by the algorithm and remaining eight bits are used for checking parity. The key is stored or transmitted as 8 bytes, each with odd parity. Structure of DES,16 identical stages of processing, termed *rounds*. There is also an initial and final permutation, termed *IP* and *FP*, which are inverses. The F-function scrambles half a block together with some of the

key. The output from the F-function is then combined with the other half of the block, and the halves are swapped before the next round. After the final round, the halves are swapped; this is a feature of the Feistel structure which makes encryption and decryption similar processes.

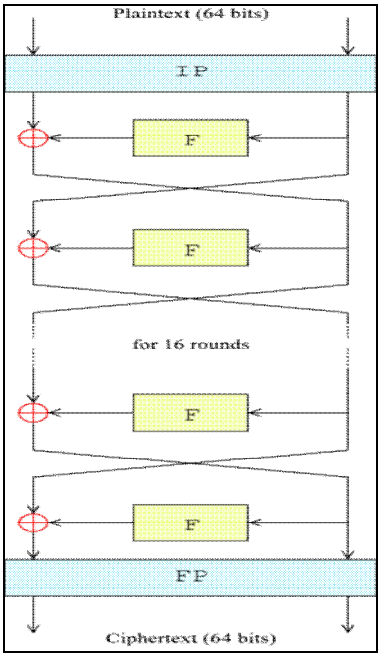

Figure 1: Structure of DES

RSA stands for Ron **R**ivest**,** Adi **S**hamir and Leonard **A**dleman. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message. The Rijndael encryption algorithm has been used for the Advanced Encryption Standard. Resistance against all known attacks; Speed and code compactness. Rijndael is an iterated block cipher. Rijndael defines a method to generate a series of subkeys from the original key. The generated subkeys are used as input with the round function. Rijndael accepts one-dimensional 8-bit byte arrays that create data blocks. The plaintext is input and then mapped onto state bytes. The cipher key is also a one-dimensional 8-bit byte array. With an iterated block cipher, the different transformations operate in sequence on intermediate cipher results (states).

3. Algorithms Used For Proposed Work

3.1. The Key Generation of the Des Algorithm Consists Of the Feistel Function and Key Schedule

i) The Feistel(F) functions operations on half a block (32 bit) at a time and consist of four stages:

- **Expansion** — the 32-bit half-block is expanded to 48 bits using the expansion permutation, denoted *E* in the diagram, by duplicating half of the bits. The output consists of eight 6-bit (8 * 6 = 48 bits) pieces, each containing a copy of 4 corresponding input bits, plus a copy of the immediately adjacent bit from each of the input pieces to either side.
- **Key Mixing** — the result is combined with a sub key using an XOR operation. 16 48-bit sub key, one for each round — are derived from the main key using the key schedule
- **Substitution** — after mixing in the sub key, the block is divided into eight 6-bit pieces before processing by the S-boxes, the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation.
- **Permutations** — finally, the 32 outputs from the S-boxes are rearranged according to a fixed permutation, after permutation, each S-box's output bits are spread across 4 different S boxes in the next round.

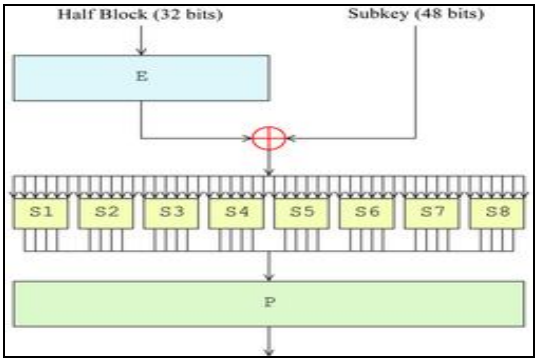

Figure 2

ii) Choice 1: Initially 56 bits of key are selected from 64 by permuted and remaining 8 bits are used for parity check. Then 56 bits are divided into two 28 bits, both rotated left by 1 or 2 bits. Choice 2: 48 subkey bits are selected and divided into two, 24bits left and 24 bits right side.

3.2. RSA Involves A Public Key For Encrypt Messages And Private Key For Decrypet Message

- Choose two distinct prime number p and q for security purpose.
- Compute n=pq, n is used as the modulus for both the public and private keys.
- Compute $\varphi(n) = \varphi(p)\,\varphi(q) = (p-1)(q-1)$, where φ is Euler's totient function.
- Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e. e and $\varphi(n)$ are coprime.
- Determine d as $d^{-1} \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).

Encrypting Message: Alice gives her public key (n & e) to Bob and keeps her private key secret. Bob wants to send message M to Alice. First he turns M into a number smaller than n by using an agreed-upon reversible protocol known as a padding scheme. Compute the cipher text $c$corresponding to:

$c \equiv m^e \bmod n$

Decrypting message: Alice can recover $m$from c by using private key d in the following procedure: Given$m$, can recover the original message M. The decryption procedure works because first

$$c^d \equiv (m^e)^d \equiv m^{ed} \pmod{n}$$

Now, since $$ed \equiv 1 \pmod{p-1} \text{ and } ed \equiv 1 \pmod{q-1}$$

Fermat's little theorem yields, $m^{ed} \equiv m \pmod{p}$ and $m^{ed} \equiv m \pmod{q}$.

Since $p$and $q$are distinct prime numbers, applying the Chinese remainder theorem to these two congruence's yields

$$m^{ed} \equiv m \pmod{pq}. \qquad \text{Thus, } c^d \equiv m \pmod{n}.$$

3.3. Rijndael Key Generation Key and Block Size Operate On Varying Sizes of Keys and Data Blocks

- **The Sub key and the Key Schedule**: The sub keys are derived from the cipher key. This is expanded to create an expanded key and the sub key is created by deriving a 'round key'.
- **Encrypting with Rijndael:** The Rijndael cipher is an iterative block cipher. It therefore consists of a sequence of transformations to encipher or decipher the data. Rijndael encryption and decryption begin and end with a step to mix subkeys with the data block. This extra step is done as a protection against cryptanalysis. To encipher a block of data in Rijndael, you must first perform an Add Round Key step (XORing a subkey with the block) by itself, then the regular transformation rounds, and then a final round with the Mix Column step omitted. The cipher itself is defined by the following steps: an initial Round Key addition, Nr-1 Rounds, a final round. Where Nr is the number of rounds, Nr is length of the data block (Nb) and the length of the key (Nk).
- **Decrypting with Rijndael:** The appropriate basic decryption key must be loaded in the key buffer before the decryption Beginning.

4. Simulation and Result

- **Setup And Implementation**
  We used NS2 tool for node creation and transmission of packets. Initially we check with the single – hop transmission after the successful of the setup, it is expanded to multi-hop transmission. The packets are made available in the queue until any neighbour node is reached.
- **Data Conversion And Transmission**
  We apply these algorithms DES, RSA and RIJNDAEL the data is encrypted in the source node and choose appropriate destination node then the packets are transmitted.

5. Experimental Results

Experimental results are obtained from the implementation of the proposed work

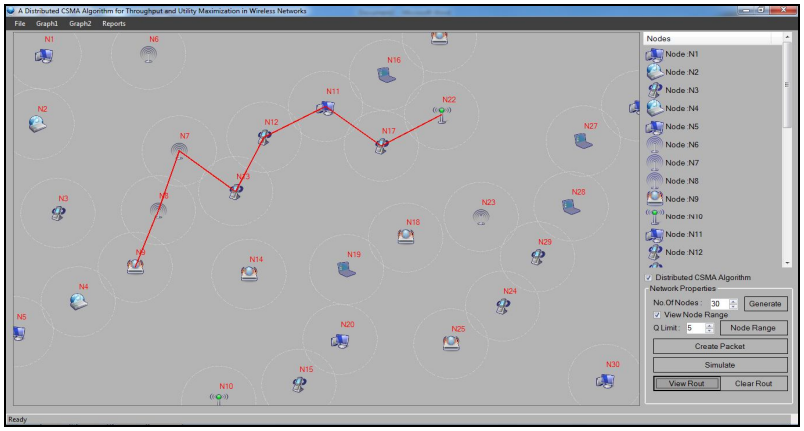

Figure 3: Data Transmission Path from Source Node (N9) to Destination Node (N22)

Using DES algorithm the data is encrypted and send source to destination with the parameters, the processing time taken for encryption procedure, block size and travelling time. Again the same data is encrypted using RSA algorithm and Retransmitted from same source to destination the above process is repeated by applying RIJNDAEL algorithm by comparing above three algorithms based on parameter taken from the transmission process. The RIJNDAEL algorithm is greatly out performance the other two algorithms.

6. Comparison of Popular Block Cipher Algorithms

Algorithm	Key Size	Block Size	Algorithm Structure	Rounds
Rijndael	128 bits, 192 bits, 256 bits	128 Bits	Substitution-Permutation Network	10, 12 or 14
Twofish	128 bits, 192 bits or 256 bits	128 Bits	Feistel Network	16
Blowfish	32-448bit in steps of 8 bits. 128 bits by default	64 Bits	Feistel Network	16
RC4	Variable	Variable	Stream	Unknown
RC2	8-128 bits in steps of 8 bits. 64 bits by default	64 bits	Source-Heavy Feistel Network	16 Mixing 2 Mashing

Table 1

7. Conclusion

In this paper it is stated that the wireless Ad hoc network is hardly vulnerable to attacks. We try to inspect the security issues in the mobile ad hoc networks, which may be a main disturbance to the operation of it. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks. First we briefly introduce the basic characteristics of the mobile ad hoc network. Because of the emergence of the concept pervasive computing, there is an increasing need for the network users to get connection with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network. However, with the convenience that the mobile ad hoc networks have brought to us, there are also increasing security threats for the mobile ad hoc network, which need to gain enough attention.

Encryption / Decryption are recommended in situations where we want the original data back. The encryption standards must be used in order to provide security while transmitting the data. All type of data such as PDF (*.pdf), Text (*.txt), Audio (*.mp3), Video (*.avi) can be transferred through the network. Through this research work the security for the data transmission via Ad hoc network has been enhanced. According to file size, the blocks have been extended in order to avoid the missing files problem. It is more than likely secure enough for all applications in the real world and can be enhanced by simply adding more rounds in the algorithm.

8. Acknowledgment

I express my sincere thanks to all people who have contributed a lot for the successful implementation of this work. I take this opportunity to express my deep sense of gratitude to our Management Trustees, Hindusthan Educational and Charitable Trust, Coimbatore for providing abundant facilities to carry out my research work successfully on the campus.

I convey my sincere thanks to Dr. N. Balusamy, M.Cop, MBA, Ph.D, D.Ed, Principal, Hindusthan College of Arts and Science, Coimbatore, for his constant support and guidance. I express my deep sense of gratitude to Mr. R. Rangaraj, M.Sc, M.Phil, M.Sc(Psychology), (Ph.D), Head, PG and Research Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore, for his keen interest, support and suggestion.

I really deem this as a special privilege to convey my prodigious and everlasting thanks to my supervisor Mrs. K. Jeyalakshmi, MCA, M.Phil, (Ph.D), Assistant Professor**,** PG and Research Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore, for her valuable guidance and personal interest in my research work.

9. References

1. Trishna Panse, V. Kapoor, "An Integrated Scheme based on Triple DES, RSA and MD5 to Enhance the Security in Bluetooth Communication", International Journal of Computer Applications (0975 – 8887) Volume 50 – No.7, July 2012.
2. Bhoopendra Singh Rajput, Prashanna Gupta, Shweta Yadav, "An Integrated Encryption Scheme Used in Bluetooth Communication Mechanism", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 2
3. Vinayak P. Musale, S. S. Apte, "Security Risks in Bluetooth Devices" , International Journal of Computer Applications (0975 – 8887) Volume 51– No.1, August 2012
4. P S Patheja, Akhilesh A. Waoo, Sudhir Nagwanshi, "A Hybrid Encryption Technique to Secure Bluetooth Communication**",** Proceedings published by International Journal of Computer Applications (IJCA) International Conference on Computer Communication and Networks CSI- COMNET-2011
5. Mini Singh Ahuja, Sumit Chabbra, "A Review of Security Weaknesses in Bluetooth", International Journal of Computers and Distributed Systems, Vol. No.1, Issue 3, October 2012
6. D.Prabakar, Dr.M.Marikkannan, Dr.S.Karthik, **"**Various Security Threats and Issues in Wireless Networks: A Survey", International Journal of Advanced Research in Computer Engineering &Technology (IJARCET) Volume 1, Issue 10, December 2012
7. Gaurav Shrivastava, "An Integrated Encryption Scheme Used in Bluetooth Communication Mechanism", VSRD-International Journal of Computer Science and Information Technology, Vol. 1 (8), 2011, 567-572
8. Nateq Be-Nazir Ibn Minar, Mohammed Tarique, "A Secured Bluetooth Based Social Network"**,** International Journal of Computer Applications (0975 – 8887), Volume 26– No.1, July 2011.
9. Mardiana Mohamad Noor and Wan Haslina Hassan, "Wireless Networks: Developments, Threats and Countermeasures", International Journal of Digital Information and Wireless Communications (IJDIWC) 3(1): 119-134 the Society of Digital Information and Wireless Communications, 2013
10. Daniel Camps-Mur, Andres Garcia-Saavedra and Pablo Serrano, "Device to device communications with Wi-Fi Direct: overview and experimentation"
11. Sachin Upadhyay, Yashpal Singh, Amit Kumar Jain, "An Analysis of the Attack on RSA Cryptosystem Through Formal Methods", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012