Eng. & Tech. Journal, Vol. 28, No.24, .2010

Proposed Hybrid-Encryption System for Multicast Network

Mohammad Natiq Fadhil Ibraheem*

Received on: 4/10/2010
Accepted on: 2/12/2010

Abstract

In this paper the proposed method based on two encrypted algorithms (Public key, and Block cipher) at the same time, it allowed a sender to encrypt the multicast packet and forward it into the packet network on the optimal distribution tree. The packet may be replicated at the optimal locations in the network and delivered to all the receivers. The receivers are capable of decrypting the packet and forwarding the packet in the secure network environment. The sender must encrypt packets using a shared key that all the legitimate receivers use to decrypt thepackets. The security of the system is based on the ability to control the distribution of the keys only to those legitimate receivers.

Keywords: Encryption, Decryption, RSA, DES, Broadcast, Multicast, ISP, Packet

نظام مقترح هجين لأنظمة التشفير لأغراض الأتصالات عن بعد

الخلاصة:

أن الطريقة المقترحة في هذاالبحث تعتمد على خوارزميتي التشفير(المفتاح المعلن، والمفتاح السري) في نفس الوقت،حيث انها تسمح للمرسل أن يشفر حزمة البيانات ويرسله الى كل المستلمين من خلال طريقة توزيع محددة، المستلمين لهم القدرة على تحليل حزمة البيانات المستلمة وبتحقيق مبدأ البث بطريقة التسليم لجهه واحدة الذي هوmulticast يتم تحديد الشخص المستلم عن طريق تشفير المفتاح المخصص للحزمة المستلمة . على الجهة المقصود الأرسال اليها إجراء العملية المعاكسة وهي فتح الشفرة حسب البروتوكول المتفق عليه في حالة التاكد من المفتاح المشترك المتفق عليه بين الجهة المرسلة والمستلمة.

أن أمنية النظام تعتمد على سيطرة توزيع المفاتيح للمستلمين المخولين ودمج كلا من الخوارزميات (المفتاح المعلن، والمفتاح السري) لهذا أدت الطريقة المقترحة الى زيادة التعقيد وهذا يؤدي الى صعوبة التحليل لمحللي الشفرة وهذا بدوره يزيد من قوة الطريقة المقترحة.

1. Introduction

Management in all business areas and organizational activities are the acts of getting people together to accomplish desired goals and objectives efficiently and effectively. Management comprises planning, organizing, Staffing, leading or directing, and controlling an organization (a group of one or more people or entities) or effort for the purpose of accomplishing

* Computer Science Department, University of Technology/ Baghdad.

a goal. Resourcing encompasses the deployment and manipulation of human resources, financial resources, technological resources, and natural resources [1].

Because organizations can be viewed as systems, management can also be defined as human action, including design, to facilitate the production of useful outcomes from a system. This view opens the opportunity to 'manage' oneself, a pre-requisite to attempting to manage others [2].

2. Cryptograph and Network Security

Cryptography is the science and study of methods of protecting data in computer and communication system from unauthorized disclosure and modification [1]. The cryptographic systems are classified into two cryptosystems, private-key cryptosystem and public-key cryptosystem. Both are based on complex mathematical algorithms and are controlled by keys [3]. In this paper produced new approach that used Multi-Encryption methods for Multicast Network

The proposed system allowed a sender to encrypt the multicast packet and forward it into the packet network on the optimal distribution tree**RSA** and **DES** algorithms used in proposed approach because they are most popular and successful cryptography algorithms. And implemented in many commercial applications.

2.1. Rivest, Shamir and Adleman(RSA) Algorithm

Is an algorithm for public-key cryptography, the RSA algorithm involves three steps: key generation, encryption and decryption

2.1.1. RSA keys generation

The first step in RSA encryption is to generate a key pair. Two keys are generated of which one is used as the public key and the other is used as the private key. The keys are generated with the help of two large prime numbers. The keys are generated as follows:

1. Generate two large random primes p and q.
2. Compute n which is equal to product of those two prime numbers, n = pq
3. Compute $\varphi(n) = (p-1)(q-1)$.
4. Choose an integer e, $1 < e < \varphi(n)$, such that $\gcd(e, \varphi(n)) = 1$.
5. Compute the secret exponent d, $1 < d < \varphi(n)$, such that $ed \equiv 1 \pmod{\varphi(n)}$.
6. The public key is (n, e) and the private key is (n, d). The values of p, q, and $\varphi(n)$ should also be kept secret.

- n is known as the *modulus*.
- e is known as the *public exponent* or *encryption exponent*
- d is known as the *secret exponent* or *decryption exponent*

2.1.2. RSAEncryption

Encryption is done using the public key component e and the modulus n. To whomever we need to send the message, we encrypt the message with their public key (e, n). Encryption is done by taking an exponentiation of the message m with the public key e and then taking a modulus of it. The following steps are done in encryption.

1. Obtain the recipient's public key (n,e)

2. Represent the plaintext message as a positive integer m < n
3. Compute the ciphertext c = m^e mod n.
4. Send the ciphertext c to the recipient.

2.1.3. RSADecryption

Decryption is done using the Private key. The person who is receiving the encrypted message uses his own private key to decrypt the message. Decryption is similar to the encryption except that the keys used are different.

1. Recipient uses his private key (n, d) to compute m = c^d mod n.
2. Extract the plaintext from the integer representative m.

The RSA algorithm has been implemented in many applications and it is currently one of the most popularly used encryption algorithm. RSA algorithm is based fully on mathematics and in the next section we will see the mathematics behind RSA.

2.2. Data Encryption Standard (DES)

The Data Encryption Standard (DES) was developed to set a standard that everyone could use to securely communicate with each other. It operates on blocks of 64 bits using a secret key that is 56 bits long [4]. The original proposal used a secret key that was 64 bits long. It is widely believed that the removal of these 8 bits from the key was done to make it possible for U.S. government agencies to secretly crack messages [5]. The DES algorithm has been a successful effort in the early development of security mechanisms. It is the most widely analyzed, tested, and used crypto algorithm and it will continue to be for some time yet to come. But perhaps the most important contribution of the DES in proposed system is that it has led us to other security considerations, beyond the algorithm itself that must be made in order to have secure computer systems and networks [6].

2.2.1. Requirements for DES algorithm

Encryption of a block of the message takes place in 16 stages or rounds. From the input key, sixteen 48 bit keys are generated, one for each round. In each round, eight so-called S-boxes are used. These S-boxes are fixed in the specification of the standard. Using the S-boxes, groups of six bits are mapped to groups of four bits. The S-boxes appear to be randomly filled, but this is not the case [4].

The block of the message is divided into two halves. The right half is expanded from 32 to 48 bits using another fixed table. The result is combined with the sub key for that round using the XOR operation. Using the S-boxes the 48 resulting bits are then transformed again to 32 bits, which are subsequently permutated again using yet another fixed table. This by now thoroughly shuffled right half is now combined with the left half using the XOR operation. In the next round, this combination is used as the new left half [7].

3. Network Multicasting Technique

IP multicast is the delivery of a message or information to a group of destination computers simultaneously in a single transmission from the

source creating copies automatically in other network elements, such as routers, only when the topology of the network requires it.

In multicast, the security is required from sender to receiver which implies the sender must replicate the packet on each of the secure connections - one for each receiver. As the number of receivers grows, the sender must scale by replicating the packet to each of the receivers. The processing load placed on the sender can be high which limits the scalability of the sender. A new System was required to securely transmit multicast and this was referred to as Secure Multicast or Multicast Security [6], the (Fig .2) shows the structure of multicast mechanism.

Multicast channels provide a mechanism for broadcasting a stream of messages to a collection of threads. Threads receive multicast messages via an *output port*; each port receives its own copy of every message sent since the port was created. Multicast channels are particularly useful for communicating with a dynamically varying group of threads, since the sender does not need to know how many threads are listening [9].

4. Proposed Hybrid-Encryption System

The proposed system depends on multicast method by sending secret message to all receiving stations, but only one recipient is the intended. The packet is divided into three encrypted sections: the identification section, the secret key and the secret message sections. Action Steps of the proposed system could be clarified as follows:

4.1. The Identification Section

- Select an **Id** for each recipient and reserve it in message provider table as identification of each recipient.
- The recipient generate public and private keys for RSA, then the user publish the ($e_1,e_2,e_3,\ldots,e_j,n_1,n_2,n_{3,\ldots},n_j$) and keep the secret keys ($d_1,d_2,d_3,\ldots,d_i$), where j is the number of users. Then
- Choose the symmetric key (Y_{DES}) used the key to encryption and decryption message in DES algorithm.

4.2. The algorithms of the proposed system

Two Algorithms below can be summarized the work of the proposed system, as illustrate in the (Fig. 3)

The proposed algorithm for encryption process

Input: m, n, Y_{DES} as string; j as integer variable

Output: X, Y, Z, XYZ as String; "X is first section, Y is second section, Z is Third section"

Process:

Step-1: Encrypt the plain text by using DES algorithm and used the key (Y_{DES})

$Z = DES(m, Y_{DES})$

Step-2: Encryption Y_{DES} by using RSA algorithm depends on special user $Y = Y_{DES}^{E_j} \bmod n_j$ When **j** is the number of specific user

Step-3: Encryption the identification user part **Id** by using RSA depend on special user

$X = Id^{E_1} \bmod n_1$

Step-4: Merge all parts to get cipher message and send it using multicast method (XYZ)

End. "End of proposed encryption algorithm"

The proposed algorithm for decryption process

Input: Id as integer variable, XYZ as string

Output: M as string

Process:

Step-1: Divided the received XYZ message into three sections (**X** ,**Y** , **Z**)

Step-2: Decrypt the identification part (**Id**)

Step-3: **If Id** equal to ***Id of user*** then go to step 4

Else

go to End

Step-4: Decrypt the symmetric of DES **Y = RSA (Y_{DES}, e_1)**

Step-5: Decrypt the cipher message by using DES and Encryption key(**Y**) then we get Plain Text**M = DES (Z, Y)**

End. "End of proposed decryption algorithms"

5. The applications of proposed system

The proposed system has been applied to two case studies, as follows:

Case study 1:

In this section, we explain the problem of organizing and directing the work of taxis by sending a secure message by the taxis service provider through the network, as it is known that the message sent will be received by all taxis in the network. The proposed system encrypts and sends the multicast packet by using two encryption algorithms (public key, Block cipher)

Here the taxi service system (the sending) will send a multicast message to taxi cars (the recipients); all taxis have card information registered with the Central Station as shown in (Fig. 4).

Strategy protocol of Taxi Service System Case study are:

1- Service provider read the **Id** of **Taxi (1)** from Taxi card information Table.

2- Encrypt (**M**) message by symmetric key $\mathbf{Y_{DES}}$ to get cipher message**(Z)**.

3- Encrypt Symmetric key by public key of **Taxi (1)**, depending on information stored in Taxi card Information Table ($\mathbf{e_1}$,$\mathbf{n_1}$) to get **YZ**

4- Encrypt **Id** for **Taxi (1)** by public key of **Taxi (1)** to get **XYZ**

5- Send the encrypted **XYZ** packet through Transport channel using multicast technique.

6- Then, the message **XYZ** received by all Taxi cars, all Taxi cars encrypt the first section of received packet to select the **Id** by secret **key(di)**, if **Id** match with the **Id Taxi** then continue else discard the message.

7- Decrypt the symmetric key by secret **key(Id)** to get $\mathbf{Y_{DES}}$

8- Decrypt the **M** by DES and $\mathbf{Y_{DES}}$

Case study 2:

As shown in (Fig. 5), Internet service provider (ISP) sends a message to every customer asking them to transfer balances for each client separately from the other, as we know that the process of transferring funds utmost confidentiality therefore possible to use the proposed system to keep the message sent secret to each client and denied the other.

Benefit of implementing the proposed system in this case study is to be able to Internet service provider to maintain the amount of money exchanged between him and the agents through the multiple encryptions of messages and reduce the time of the transmission using the multicast technique.

5. The Computational Complexity of the Methods

Most cipher algorithms essentially depends on the complexity computational, therefore in this section we will compute the complexity degree of RSA and DES after computer the original encryption algorithms as follow [3]

5.1. RSA Complexity

The encryption scheme of RSA is

$C=M^e \mod n$

Then:

$T(C) = O(\log n)^3$ bit operation.

The Decryption Scheme of RSA is:

$M=C^d \mod n$

Then:

$T(M)=O(\log n)^3$ bit operation.

5.2. DES complexity

In the DES, the length is appropriate key 56 bits so we need $(2^{56})^{16}$ trials to find the correct key for brute force attack.

5.3. Proposed System

As mentioned previously in figure (3), the message sent is divided into three sections. In what follows we calculate the level of complexity of the proposed method

- $T(X) = O(\log_n)^3$
- $T(Y) = O(\log_n)^3$
- T(Z) = Complexity is (equal 256^{16})

Therefore,

$O(\log n)^3 + O(\log n)^3 + O(256)^{16}$

6. Conclusion

Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security.

The proposed method based on two encrypted algorithms (Public key, and Block cipher) at the same time. After we apply the system on two case studies has proven successful in the protection of data sent through the proposed protocol authorization data. The system is designed to be success on the multicast networks. The system could be developed to run on the broadcast networks to provide high security authorization.

References

[1] Wenbo Mao, "Modern Cryptography: Theory and Practice", Prentice Hall PTR, 2003

[2] Douglas Stinson, "*Cryptography: Theory and Practice*", Chapman & Hall/CRC, 2005

[3] Dr.Alaa K.Farhan ,"Security protocol for mobile data", Ph.D.Thesis, University of Technology at computer science, 2009

[4] William Stanlings, **"**Cryptography and Network Security: Principles and Practice (5th Edition)", Tata McGraw Hill, 2010

[5] Man Young Rhee, "*Internet Security (Cryptographic Principles, Algorithms and Protocols)*", Wiley, 2003

[6] Robert Rummler, Alexander Gluhak, "Multicast in Third-Generation Mobile Networks ", Wiley, 2009

[7] S. C. Coutinho ,"*The Mathematics of Ciphers: Number Theory and RSA Cryptography*", Department of Computer Science Federal university of Rio de janeiro,1999

[8] David Ireland Management Co., http://www.di-mgt.com.au/rsa_alg.html, DI Management Group, Sydney,Australia, 2010

[9] William R. Parkhurst , "Cisco Multicast Routing and Switching", Cisco Networking Academy, 1999

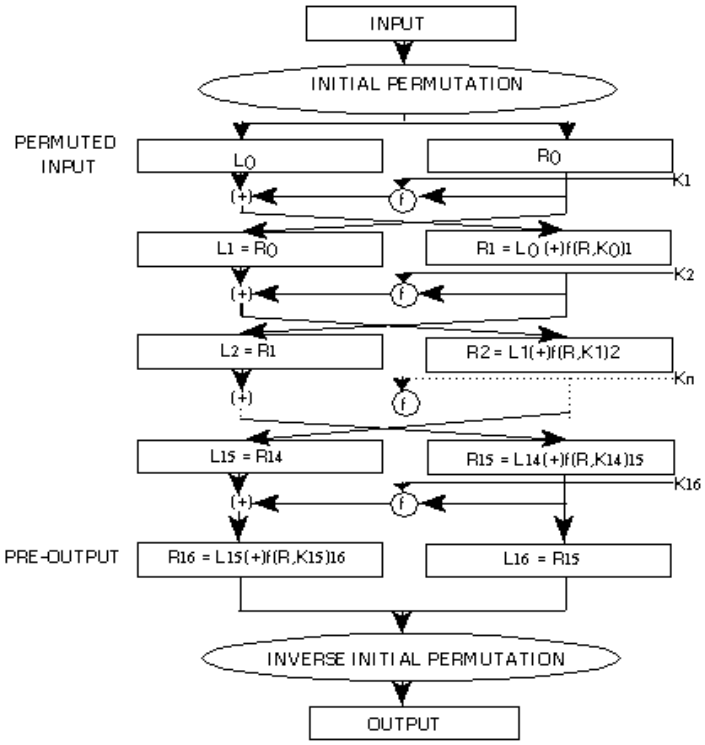

Figure.1. DES structure

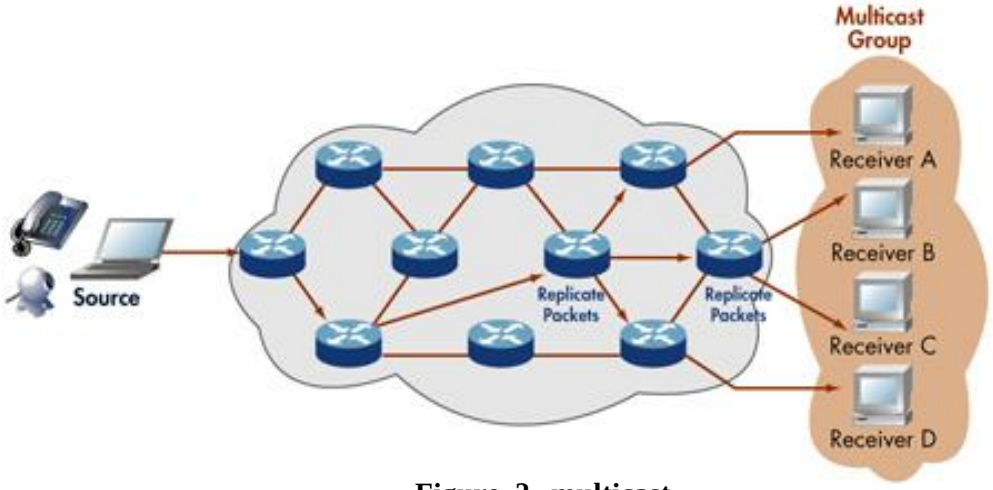

Figure. 2. multicast structure

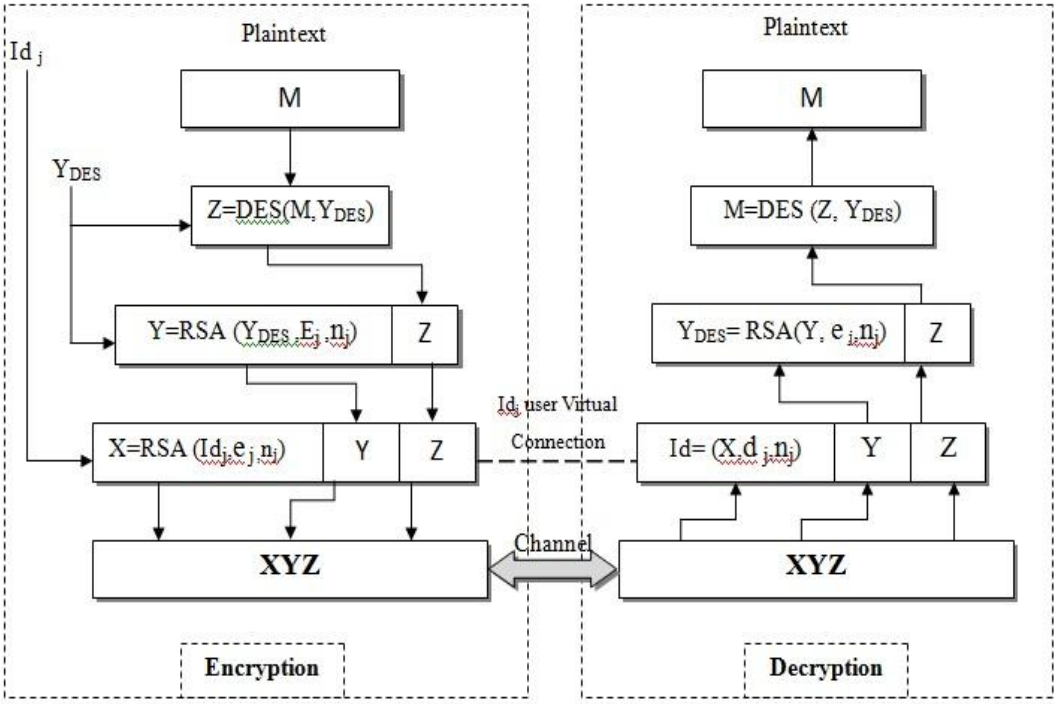

Figure. 3. The protocol of proposed system

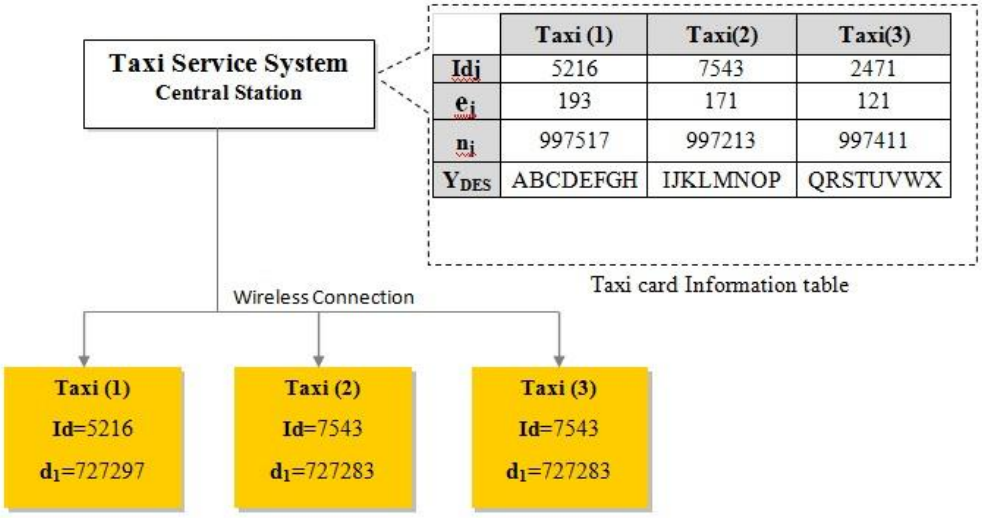

Figure. 4. The connections between Taxi Service System and Tax cars

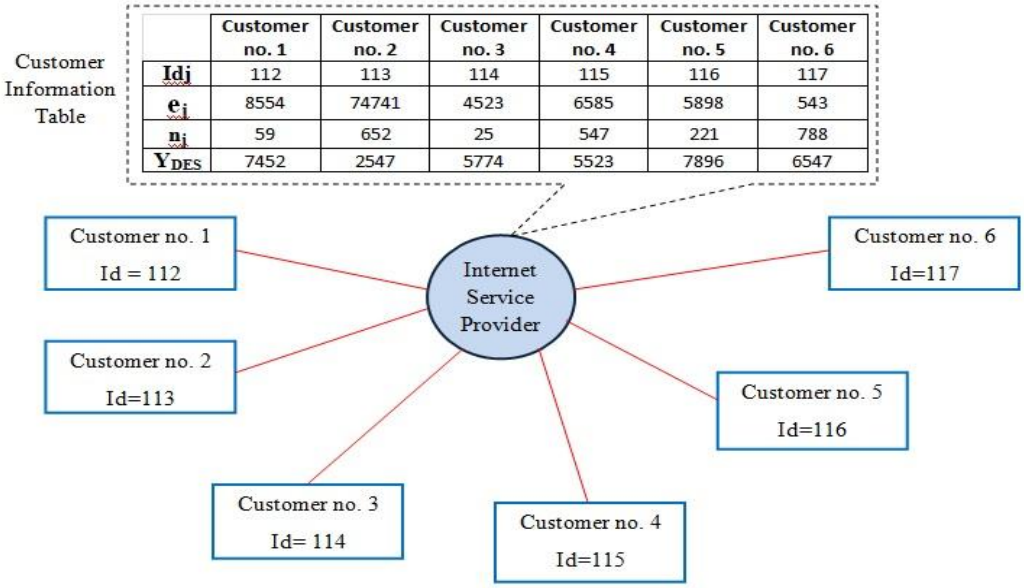

Figure. 5. Internet Service Provider