Diyala Journal
of Engineering
Sciences

ISSN 1999-8716

Vol. 03, No. 02, pp.70-78, December 2010

Proposed System for Wireless Security

Ali N. Hamied, Saad Qassim Fleh, Hussain F. Mahdi

College of Engineering, University of Diyala, Iraq

(Received:25-11-2009; Accepted:23-6-2010)

ABSTRACT - Secured wireless computer networks are more important because signals are available through air and it’s easier to attacks from passive eavesdropping and active interfering. Now it was suffered from more problems, one from these problems is attach from the users and hackers. Therefore, wireless computer networks security is very important to solve or decrease this attach, a lot of researches were worked improved wireless security in this field but in different ways and different methods. This project had been represented how to prevent hackers’ accessing to the server, by using encryption to media access control “MAC address” from the two ends (server and user), using RSA public-key cryptosystem.

***Keywords*: -** Wireless security, MAC address, RSA Public-Key Cryptosystem.

1. INTRODUCTION

Data signals are transmitted from one device to another using one or more types of transmission media, including twisted-pair cable, coaxial cable and fibre-optic cable. A message to be transmitted is the basic unit of network communications. A message may consist of one or more cells, frames or packets which are the elemental units for network communications. Networking technology includes everything from local area networks (LANs) in a limited geographic area such as a single building, department or campus to wide area networks (WANs) over large geographical areas that may comprise a country, a continent or even the whole world (1).

According to Sumathy and Kumar, Active attacks involve actions performed by adversaries, for instance the replication, modification and deletion of exchanged data.

External attacks are typically active attacks that are targeted to cause congestion, propagate incorrect routing information, prevent services from working properly or shut down them completely. External attacks can typically be prevented by using standard security mechanisms such as firewalls and encryption techniques[2].

2. WIRELESS NETWORKING

The wide wireless networking is the various types of 2.4 GHz WiFi devices, is used to meet many needs. Perhaps the most common use is to connect laptop users who travel from location to location. Another common use is for mobile networks that connect via satellite. A wireless transmission method is a logical choice to network a LAN segment that must frequently change locations [3].

There are two ways to verify wireless networking through IP address (Internet Protocol) or MAC address.

3. MAC ADDRESS

The MAC address is a unique value associated with a network adapter. MAC addresses are also known as hardware addresses or physical addresses. They uniquely identify an adapter on a LAN.

MAC addresses are 12-digit hexadecimal numbers (48 bits in length). By convention, MAC addresses are usually written in one of the following formats [4,5].

MM:MM:MM: SS: SS: SS

MMMM-MMSS-SSSS

The first half (24 BITS) of a MAC address contains the ID number of the adapter manufacturer. These IDs are regulated by an Internet standards body (see sidebar). The second half (24 MORE BITS) of a MAC address represents the serial number assigned to the adapter by the manufacturer.

Recall that TCP/IP (Transmission Control Protocol/Internet Protocol) and other mainstream networking architectures generally adopt the OSI model (Open Systems Interconnection). In this model, network functionality is subdivided into layers. MAC addresses function at the data link layer (layer 2 in the OSI model). They allow computers to uniquely identify themselves on a network at this relatively low level as shown in Fig. (1).

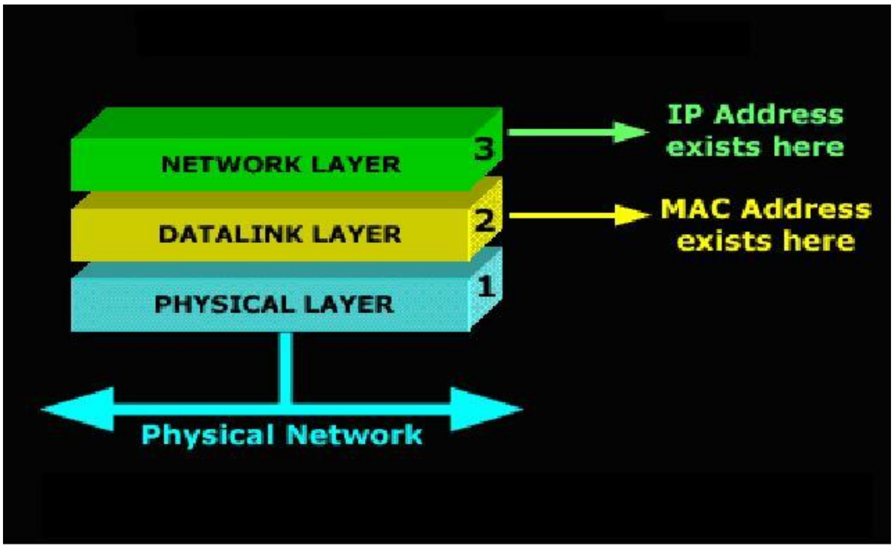

Fig. (1): First Three OSI Layers

4. WIRELESS SECURITY

There are many ways to protect the user or computers from hackers, like user name, password … etc, in this work are taken some options can hackers or hacker's program that enter to the network, this option is MAC address.

The operation of connection between the server like "Mikrotik server" (that's wide used in our country) and user by IP address as shown in figure (2), this connection happen when the user send message to access point and through access point to the server, server are register the new user by (user name and password), after this operation the connection are continue, and many packets of data are translated between server and user, one of properties of Mikrotik server, is the server deals with MAC address of user not with IP address after connection because the MAC address are represent the physical address, when the user are stooped or separate from the server in few minutes, the hacker is connect with the server by taken the user's MAC address (through some of program).

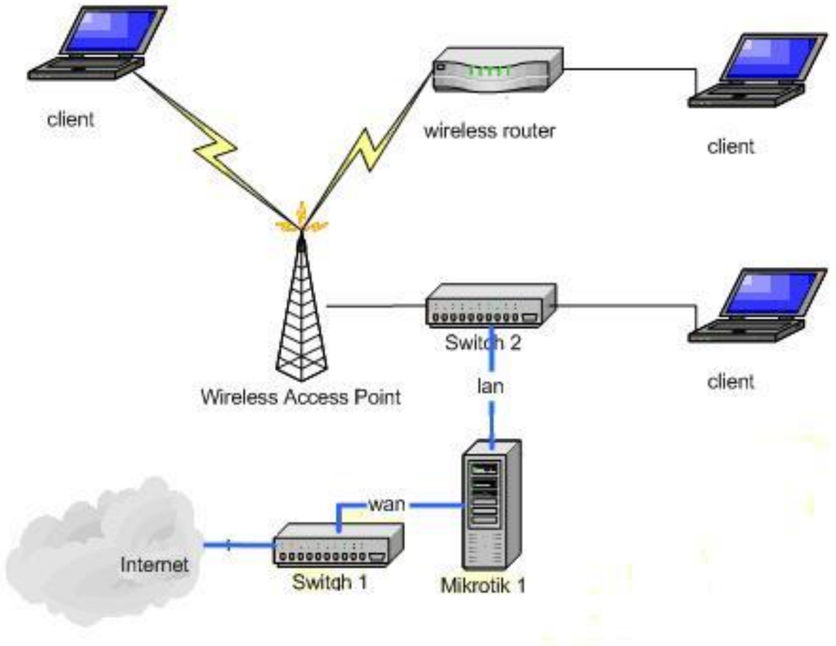

Fig. (2): Basic network topologies

5. PROPOSED SYSTEM

5.1. STEPS OF PROPOSAL SYSTEM

The steps of proposal system for wireless networking by the RSA public-key cryptosystem are: -

1- Register user's MAC address in Mikrotik server.

2- Encryptions MAC address.

3- Send crypto MAC address through access point.

4- Receive Crypto Mac address from server.

5- Decryption MAC address in user's computer.

6- Encryptions MAC address.

7- Send crypto MAC address through access point.

8- Receive Crypto Mac address from user.

9- Decryption MAC address in Mikrotik server.

Figure (3) shows the flowchart of the steps of proposal system.

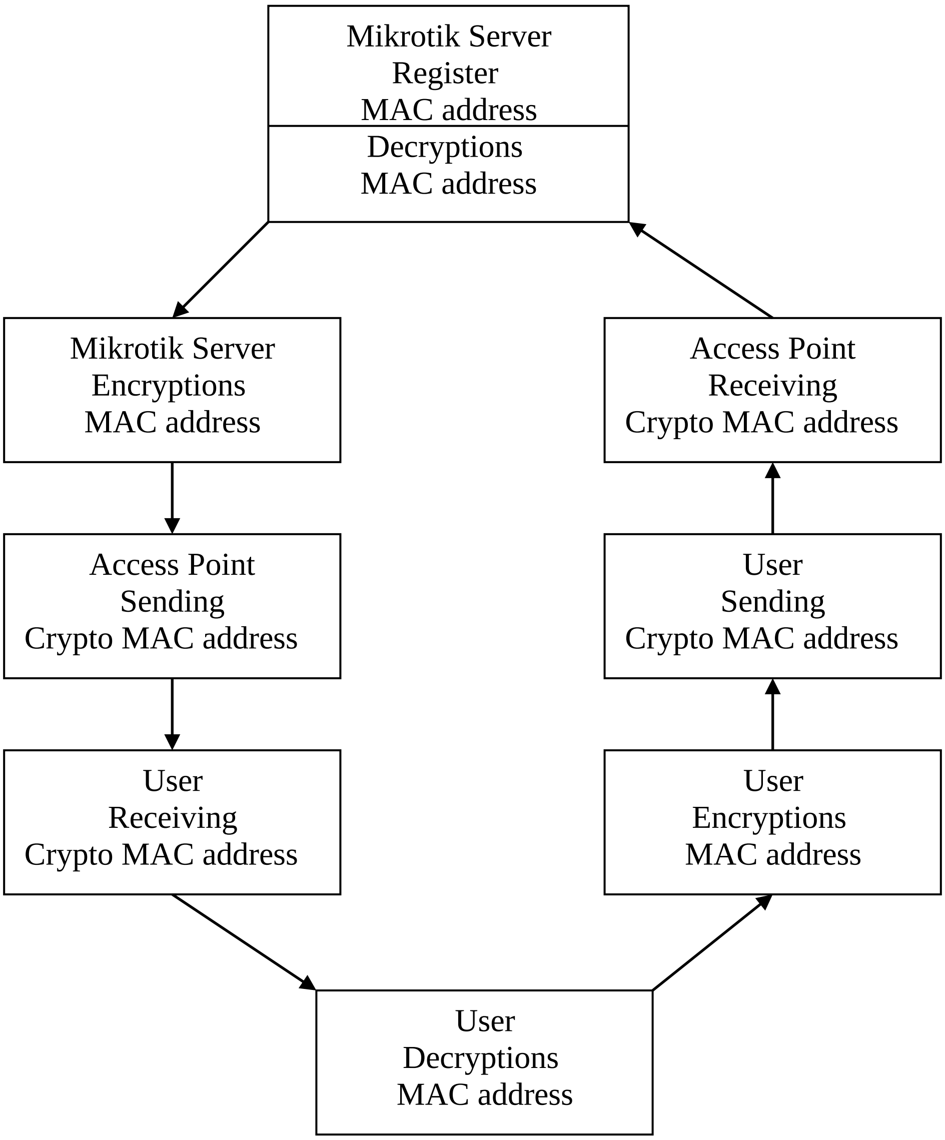

Fig. (3): Flowchart of proposal system

5.2. STEPS OF RSA PUBLIC KEY CRYPTOSYSTEM

The steps of RSA public key cryptosystem are [7,8].

1- Generate two keys (public key (e, n) and secret key (d, n)).

   a- each reserve generates three numbers:

   p , q (large primary numbers) and lets 3, 17 respectively

   and e (large number), lets 5.

   b- Then calculate public key (e, n):

   n = p *q = 51, the public key (5, 51)

   c- Then calculate secret key (d, n):

   $d = e^{-1} \bmod \Phi(n)$

Where Φ (n) = (p -1)(q -1), Φ (n) =32

$d = \frac{GCD(\Phi(n))\times\Phi(n)+1}{e}$, where GCD (2, 16) = 2

(Greatest Common Divisor)

d = 13, the secret key (13, 51).

2- Encryption MAC address, the proposal MAC address are :

11-22-33-AA-BB-FF

In this work are the numbers from (0 to 9) and the characters (A to F) are (10 to 15), each of MAC address are encryption as (m1, m2, …, m12) to (c1, c2, …, c12) by:

$C_1 = M_1^d(\text{mod}\,n)$, $C_1 = 1^{13}(\text{mod}\,51)$ = 01.

$C_3 \,\&\, C_4 = 2^{13}(\text{mod}\,51)$ = 32.

$C_5C_6 = 3^{13}(\text{mod}\,51)$ = 12.

$C_7 \,\&\, C_8 = 10^{13}(\text{mod}\,51)$ = 28.

$C_9 \,\&\, C_{10} = 11^{13}(\text{mod}\,51)$ = 41.

$C_{11} \,\&\, C_{12} = 15^{13}(\text{mod}\,51)$ = 36.

Now have encryption MAC address is represented by:

0101-3232-1212-2828-4141-3636

3- Decryption MAC address, after encryption MAC address the user are received it and decrypt MAC address by using:

$M_1 = C_1^e(\text{mod}\,n)$, $M_1 = 1^5(\text{mod}\,51)$ = 01.

$C_3 \,\&\, C_4 = 32^5(\text{mod}\,51)$ = 02.

$C_5C_6 = 12^5(\text{mod}\,51)$ = 03.

$C_7 \,\&\, C_8 = 28^5(\text{mod}\,51)$ = 10.

$C_9 \,\&\, C_{10} = 41^5(\text{mod}\,51)$ = 11.

$C_{11} \,\&\, C_{12} = 36^5(\text{mod}\,51)$ = 15.

Now get original MAC address (11-22-33-AA-BB-FF), figure (4) illustrated Steps of RSA public key cryptosystem.

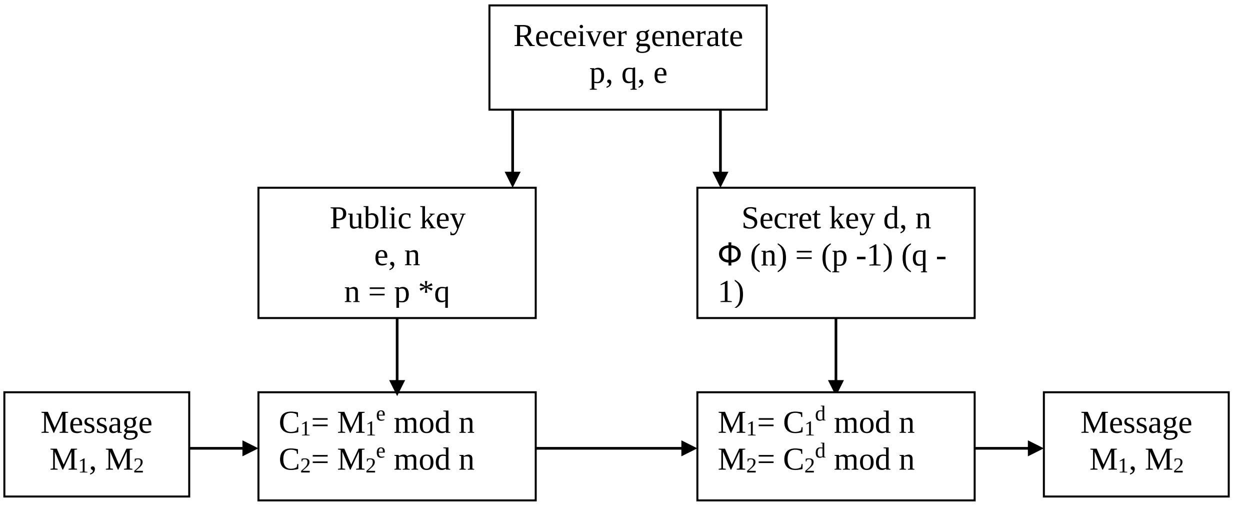

Fig (4): Steps of RSA public key cryptosystem.

6. CONCLUSIONS

From the dealing with wireless technology, and knowing how hackers are attempt to access to this connection (server) especially what was presented by this proposal system, it can be concluded that:

1- The proposal system is providing one of complex way that prevents the hackers to attach wireless connection.

2- Proposal system is used RSA public key cryptosystem that very difficult when use large primary numbers to make it very complex to solve from hackers.

3- Proposal system give to server more reliability and capability to the users, for using wireless service without any disconnection from the hackers.

4- Many researches development wireless networks in different ways and different methods.

REFERENCES

1. B. Pioper, "Internetworking Technology Overview", June 1999.

2. S. Sumathy and B. Kumar "Secure Key Exchange and Encryption Mechanism for Group Communication Wireless AD Hoc Networks" March 2010

3. http://en.wikipedia.org/wiki/Wireless.

4. http://www.firewall.cx/index.php .

5. http://www.dmasoftlab.com/cont/radman.

6. http://wiki.mikrotik.com/wiki/Initial_MAC_Winbox_Connection .

7.بروس بوزورث , الرموز والشفرات والحاسبات مقدمة الى امن المعلومات, ترجمة د. ميثم محمد زكري,
. د. اديب حمدون سليمان, د. ستار بدر سدخان, بغداد ١٩٨٩

8. Hellman, Martin E. “The Mathematics of Public-Key Cryptography ”, Scientific American, vol. 241, no. 16 (August 1979).

9. Rivest R., Shamir A., and Adelman L. “A Method for Obtaining Digital Signatures and Public-Key Cryptography” Laboratory for Computer Science, MIT Technical Memo LCS/TM 82 (April 1977).

نظام مقترح لأمنية اللاسلكي

حسين فالح مهدي	سعد قاسم فليح	علي نصر حميد
مدرس مساعد	مدرس مساعد	مدرس مساعد

كلية الهندسة –جامعة ديالى

الخلاصة

أمنية الشبكات اللاسلكية مهم جدا لان الإشارات تكون متوفرة في الفضاء وتكون سهلة للهجوم من التنصت السلبي و التدخل النشط. حاليا هذه الشبكات تعاني الكثير من المشاكل, احد هذه المشاكل هي الاعتداء او الهجوم من المستخدمين او الأعداء (القراصنة). لذلك فأن أمنية الشبكات اللاسلكية مهمة جدا لحل او تقليل هذا الاعتداء, وأكثر البحوث عملت وطورت هذا المجال باتجاهات وطرق مختلفة. هذا البحث يمثل كيف يمكن ان نمنع الأعداء من الوصول او الدخول إلى جهاز الخادم, وذلك عن طريق تشفير عنوان MAC من خلال النهايتين (طرف الخادم وطرف المستخدم او المخدوم) باستخدام طريقة نظام الشفير المفتاح العام RAS .