Quantum Cryptography Technique for Security of Wireless LAN

M.S.Vinu

Assistant Professor, Dept of CSE, Sri Eshwar College of Engineering, Coimbatore, TN, India.

Lavanya Krishnasamy

ME (CSE), Dept of CSE, Sri Eshwar College of Engineering, Coimbatore, TN, India.

Abstract:

Wireless LANs are formed to transfer data over radio frequencies. IEEE 802.11i protocol is used to handle the data transmission over the wireless LAN nodes. Key distribution is the problem of classical cryptography algorithm Key distribution requires safe channel to transfer key values. Quantum states of light concept are used to carry out the key transmission process. In the quantum cryptography technique two parties simultaneously generate shared secret key values. Quantum cryptography could distribute key in quantum channel. If a quantum channel is attacked Q Bit Error Rate (QBER) is increased so the attack can be easily detected. Several researches are carried out in the area of quantum cryptography and mobile networks. The quantum cryptography and 802.11i security mechanisms are integrated to provide security for wireless LANs. The Pairwise Transient Key (PTK) is established and used for the cryptography process. Key generation, key distribution, encryption and decryption operations are carried out in the wireless LAN nodes. The system implementation is done with the J2EE and Oracle back end.

Keywords – Wireless LAN, Quantum Cryptography, RSA algorithm, BB84 protocol.

INTRODUCTION

Quantum cryptography exploits the quantum mechanical property that a qubit cannot be copied or amplified without disturbing its original state. Alice and Bob use a quantum channel to exchange a random sequence of bits, which will then be used to create a key for the one-time pad used for

communication over an insecure channel. Any disturbance of the qubits, for example Eve trying to measure the qubits' state, can be detected with high probability [5]. In this section, we describe the BB84 protocol proposed by Charles Bennett and Gilles Brassard in 1984[2]. It was the first protocol that suggested the use of quantum mechanics for two parties to agree on a joint secret key.

In this protocol, Alice and Bob use a quantum channel by sending qubits. They are also connected by a classical channel, which is insecure
against an eavesdropper. We can use photons of different polarizations to represent quantum states: The polarization basis is the mapping that is decided to be used for a particular state.

EXISTING SYSTEM

A. Authentication

Authentication is the first thing to do when a mobile terminal wants to join a network. In order to rectify the flaw of the WEP (Wired Equivalent Privacy) based authentication mechanism specified in the 802.11 standard, 802.lIi defines the 802.lX authentication based on EAP (Extensible Authentication Protocol) [6] as illustrated in Figure 2.1.

Figure2.1 presents the architecture of 802.lX authentication with three elements: the supplicant, the authenticator, and the authentication server. The supplicant corresponds to the mobile terminal which wants to joint a network. The authenticator corresponds to the access point which realizes the 802.lX access control and only admits data traffic from supplicants who are authenticated by the authentication server. EAP is a flexible protocol allowing the running of different authentication methods between the mobile terminal and the authentication server. Depending on the EAP method used, we can have a strong or weak, simple or mutual authentication.

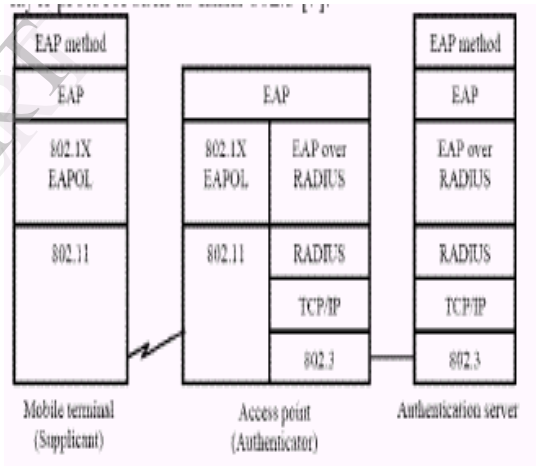

Figure 2.1 A protocol stack for 802.IX authentication

B. Key management

The process in which the mobile terminal and the access point authenticate each other and build the key hierarchy from the PMK is called the 4-way handshake [8] and presented in Figure 2.2.

The 4-way handshake is started by the Authenticator by

sending the value ANonce (Authenticator Nonce) to the Supplicant. Upon receiving the value ANonce, the Supplicant has all materials to build the key hierarchy. However, this hierarchy is not used until the Authenticator is authenticated and ready to use these keys. In the second message of the 4-way handshake, the Supplicant sends to the Authenticator the value Snonce (Supplicant Nonce) and a MIC calculated based on the content of the message and the KCK which has just derived. Upon receiving this message, the Authenticator has all materials to build the same key hierarchy. Then it uses the KCK to check the MIC. If the MIC is correct, that means that the Supplicant obtains the PMK, and thus the Supplicant is authenticated.

In the third message of the 4-way handshake, the Authenticator tells the Supplicant that it has finished the derivation of the key hierarchy. It also sends a MIC calculated based on the content of the message and the KCK which has just derived. Upon receiving this message, the Supplicant checks the MIC in order to verify that the Authenticator obtains the PMK, and thus authenticates the Authenticator. Then, the key hierarchy can be used without the doubt about the authenticity of the access point. This message can also be used as a means to distribute the GTK to the mobile terminal.

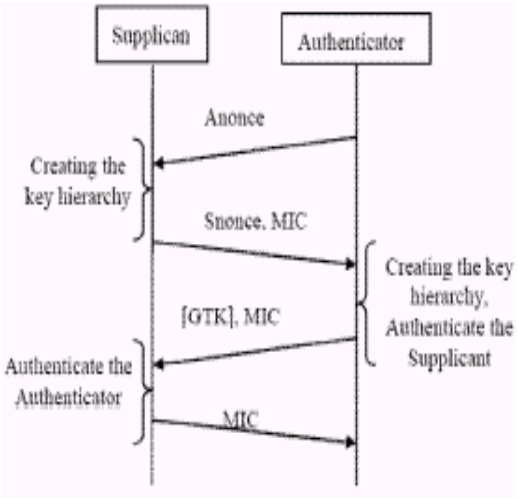

Figure 2.2. The 4-way handshake

In the last message of the 4-way handshake, the Supplicant tells the Authenticator that the 4-way handshake is now successfully completed. This message also includes a MIC to assure the Authenticator that this message is sent by the Supplicant and that it is not modified. After the 4-way handshake, the Temporal Key (TK) is used by the encryption algorithm to provide confidentiality of user data.

PROPOSED SYSTEM

The wireless LAN security system using quantum cryptography technique is designed as client server application. The system is designed using the Java language. The server application is designed to manage clients under the wireless LAN environment. The client nodes are designed to perform the message communication under the wireless LAN environment. The Oracle back

end is used to maintain the user and key information. The RMI technique is used for client server communication. The TCP is used for the message communication. Socket communication model is used in the system. The system uses the RSA and AES algorithm for security process. The quantum cryptography is used to perform the key distribution process.

A. Wireless LAN Server

The wireless LAN server application is designed to manage the users and key values. The user accounts are created under the wireless LAN server environment. All the user information are stored under the Oracle database in the wireless LAN server. The system uses the quantum channels for key distribution process only. The key values are maintained under the server environment. The system support symmetric and asymmetric key cryptography techniques. The client server communications are carried out using the Remote Method Invocation method. The socket communication model is used for the client to client communication.

B. Client Application

The wireless LAN client application is designed to perform the message communication under the wireless LAN environment. The user account details are stored and authenticated under the server. The server issues the key values. The quantum channels are used to transfer the message and key value. The session based key values are used in the message communication. The system uses the dual quantum channel for key exchange process.

The intra group and inter group communication security for grid nodes is provided by the global dominator and local group dominators. The nodes are assigned with a personal key. The asymmetric cryptography is used for the personal communication. The communication between the nodes and the dominators are secured by the personal key. The system uses two different group key values. They are local group key and global group key. The global group key is used for the communication between the dominators. The local group key is used for the message communication among the local group members. The Rivert, Samir and Adelman (RSA) algorithm is used for the personal key. The Advanced Encryption Standard (AES) algorithm is used for the group key.

C. RSA Algorithm

The Rivert, Shamir, Adelman (RSA) scheme is a block cipher in which the Plaintext and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits or 309 decimal digits.

Description of the Algorithm

Plaintext is encrypted in blocks, with each block having a binary value less than some number

n. That is, the block size must be less than or equal to $\log_2(n)$; in practice, the block size is k bits, where $2^k < n \leq 2^{k+1}$. Encryption and decryption are of the following form, for some Plaintext block M and cipher text block C

$C = M^e \bmod n$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Both sender and receiver must know the value of n. The sender should know the value of e, and the receiver should know the value of d. Thus, this is a public-key encryption algorithm with a public key of KU = { e,u} and a private key of KR ={d,n}.

Key Generation

Select p,q , p≠q	p and q both prime
Calculate n = p x q	
Calculate $\phi(n)=(p-1)(q-1)$	
Select integer e <e < $\phi(n)$	$\gcd(\phi(n),e) = 1$; 1
Calculate d	$d = e^{-1} \bmod \phi(n)$
Public key	KU = {e, n}
Private key	KR = {d, n}

Encryption

Plaintext	M <n
Cipher text	$C = M^e \pmod n$

Decryption

Cipher text	C
Plaintext	$M = C^d \pmod n$

CONCLUSION

In this paper, we propose a scheme integrating quantum key distribution in 802.11 networks. A modified version of the 4-way handshake, the Quantum handshake, is defined to integrate the BB84 protocol for the distribution of the cryptographic keys used by 802.1 Ii. The quantum handshake is our first step in the integration of quantum cryptography in mobile wireless networks. Open issues and future works have been discussed. When the research on the application of quantum cryptography in mobile wireless networks is still very premature, we hope that the work presented in this paper can contribute to the evolution of this research field.

REFERENCES

[1] Nicolas Gisin, Gr"egoire Ribordy, Wolfgang Tittel and Hugo Zbinden." Quantum cryptography" (April 1, 2007; submitted to Reviews of Modern Physics)

[2] C. Bennet, and G. Brassard, G. "Quantum cryptography: Public key distribution and coin tossing", IEEE International Conference on Computers, Systems, and Signal Processing, IEEE Press, LOS ALAMITOS, 1984.

[3] N. Namekata, S. Mori, and S. Inoue, "Quantum key distribution over an installed multimode optical fiber local area network", Optical Express, 2005.

[4] IEEE Standard 802.11i, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, July 2004.
[5] K. G. Paterson, F. Piper, and R. Schack, "Why quantum cryptography?", Quantum physics, quant ph/0406147,2004
[6] ANSI/IEEE Standard 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999 Edition, Reaffirmed June 2003.
[7] B. Aboba, L. Blunk, 1. Vollbrecht, 1. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)",RFC 3748, June 2004.
[8] 1. Edney, and W..A. Arbaugh, Real 802.11 Security - Wi-Fi Protected Access and 802.11i, Addison-Wesley, 2004.
[9] A.Falahati , Hadi Meshgi “Using Quantum Cryptography for securing Wireless LAN networks” 2009 International Conference on Signal Processing Systems,IEEE.