Effective User Authentication using Quantum Key Distribution for Wireless Mesh Network

G. Murali
Asst Professor
Dept of CSE
JNTUACEP

R. Sivaram Prasad
Research Director
Dept of CSE
Acharya Nagarjuna University

K.V. Bhaskar Rao
M-Tech
Dept of CSE
JNTUACEP

ABSTRACT

Quantum key distribution can provide sophisticated solution for efficient authentication in wireless mesh networks. In quantum cryptography, the key is created during the process of key distribution, where as in classical key distribution a predetermined key is transmitted to the legitimate user. The most important contribution of quantum key distribution is the detection of eavesdropping.

Keywords

Authentication, BB84 Protocol, Cryptography, eap-tls, eap-ttls, Quantum Key Distribution, WMN.

1. INTRODUCTION

In Wireless networks, there is high probability to violate authentication. Authentication refers to ensuring parties involved in the communication are genuine. cryptography mechanisms are introduced to ensure authentication. In cryptography, keys are used to encrypt and decrypt the message, when key is known to eavesdropper then authentication violates. classical cryptography is facing the threat of quantum computers. Since quantum cryptography does not depend on difficulty of mathematical problems for its security, quantum cryptography is introduced. Quantum key distribution (QKD) is used in quantum cryptographic systems to exchange secret key between parties who need to communicate secretly. The QKD protocol was first published by Bennett and Brassard in 1984 and is now well known as BB84 . In 1992, Bennett published another QKD scheme (B92) and proposed that it could be implemented using single photon interference with photons propagating for long distances.

2. WIRELESS MESH NETWORK

In WMNs[6], nodes are comprised of mesh routers and mesh clients. Each node operates not only as a host but also as a router, forwarding packets to other nodes that may not be within direct wireless transmission range of their destinations. A WMN is dynamically self-configured, with the nodes in the network maintaining mesh connectivity among themselves . This feature brings many advantages to WMNs such as low up-front cost, easy network maintenance, robustness, and reliable service coverage. Conventional nodes (e.g., desktops, laptops, PDAs, PocketPCs, phones, etc.) equipped with wireless network interface cards (NICs) can connect directly to wireless mesh routers. Customers without

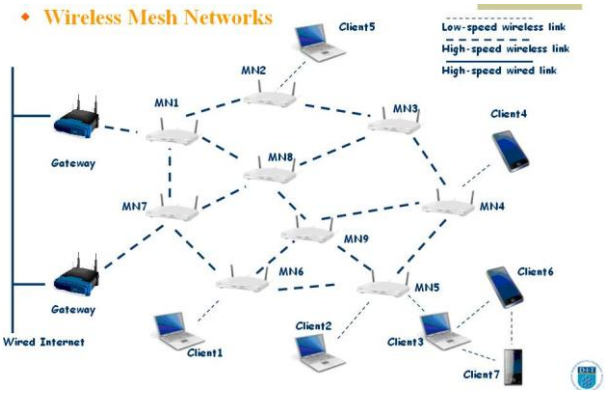

Figure 1 : An Overview of Wireless Mesh Network

wireless NICs can access WMN by connecting to wireless mesh routers through, for example, Ethernet. Thus, WMNs will greatly help the users to be always-on-line anywhere anytime. Moreover, the gateway/bridge functionalities in mesh routers enable the integration of WMNs with various existing wireless networks such as cellular, wireless sensor, wireless-fidelity (Wi-Fi), worldwide inter-operability for microwave access (WiMAX), WiMedia networks.

3. MAJOR ATTACKS OF WMN

There are many kinds of attacks in wireless mesh network. The main types of attack are given below

3.1 Denial of Service Attack

It can be occurred either by accident failure or from malicious activity. One way to create denial of service attack is to flood resource so that it stops working or no longer it works. An example of dos attack is synchronous flooding. A distributed denial of service is even more dangerous than dos, it causes network down. It is happened by group of nodes.

3.2 Impersonation Attack

If proper authentication is not supported, he may able to join the network, then unauthorized nodes may access the network management system, may change the configuration of system as legitimate user. It may send false routing information. It creates serious security to wireless mesh networks.

4. AUTHENTICATION PROTOCOL IN WIRELESS MESH NETWORK :

There are two types of authentication. They are

- User Authentication
- Message Authentications

A Good authentication procedure in wireless mesh network is that it best detects and exclude unauthorized access. But the difficulty here is to define the characteristics of authentication , it differs from application to application. IEEE 802.11 was the first wireless standard .The two authentication methods are given below

- Open System Authentication
- Shared Key Authentication

Open System Authentication provides global authentication which allows every clients to connect to network where as shared key authentication makes use of shared key to use WEP to encrypt communication. The following is the figure illustrates the authentication process.

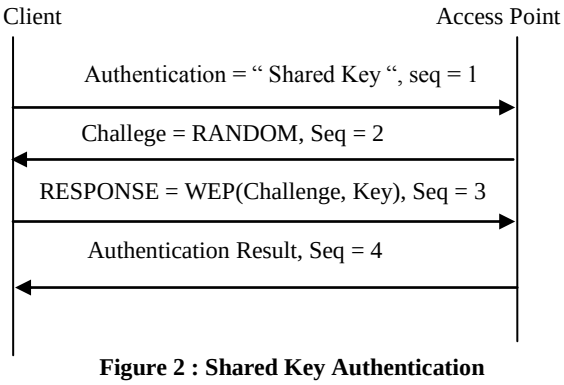

Figure 2 : Shared Key Authentication

In the above figure :2 access point sends 128 byte challenge message to the client. The client then generates 24 bit initial vector(IV) , encrypts the challenge using shared key and send both back to access point. The access point decrypts the message using shared key and compare the resultant with the sent challenge. If the resultant is equal to sent challenge, the client is authenticated.

The problems associated with design are :

1. No mutual authentication, a user does not have knowledge about " whether he connects to the right Access Point or not"
2. No individual identification, all clients share the same key
3. No key separation, the authentication procedure makes uses of same key as the encryption.

4.1 Extensive Authentication Protocol in Wireless Mesh Network

It was designed originally for dial up (PPP) authentication. To bring this work in wireless infrastructure, few modifications are required. The two methods that provide authentication are given below.

- EAP-TLS
- EAP-TTLS

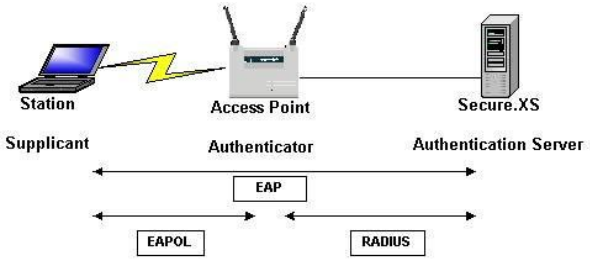

Figure 3 : EAP Authentication

The following is the figure 3 that shows EAP authentication architecture. Essential elements present in the architecture is given below.

- Supplicant
- Authenticator
- Authentication Server

Supplicant Supplicant is a client who wants to connect to wireless network .He sends authentication data to authenticator.

Authenticator The authenticator who is typically an Access Point which will forwards the information from the supplicant to the authentication server. Upon decision of the authentication server which allows or denies the access to the network.

Authentication Server It is typicall radious or Diameter server. It checks the identity of supplicant based on data provided by authenticator.

4.1.1 Eap-tls

One of the most famous EAP methods is EAP-TLS[2]. Developed by Microsoft in 1999 and is the only method which was standardized by the IETF. It provides mutual authentication. It is an extension of the Secure Socket Layer (SSL) protocol . Like SSL, TLS uses X.5096 Client/Server certificates, this includes the use of a Public Key Infrastructure .It may be difficult for the smaller companies to create such infrastructure so that they can prefer another method. One of the main disadvantages using EAP-TLS, is the big overhead caused by the authentication procedure. Both certificates need to be transferred to the other party. Additionally due to the use of asymmetric cryptography, the encryption and decryption process consumes time and performance.

The procedure is shown in below figure. The supplicant sends the ”Client Hello” message to the authentication server to establish the session. The server replies with a ”Server Hello” message contains the server certificate. This certificate is checked by the supplicant using a higher authority called RootCA. If the server side authentication was successful, the supplicant sends the client certificate which is checked by authentication server. Mutual authentication is accomplished successfully.

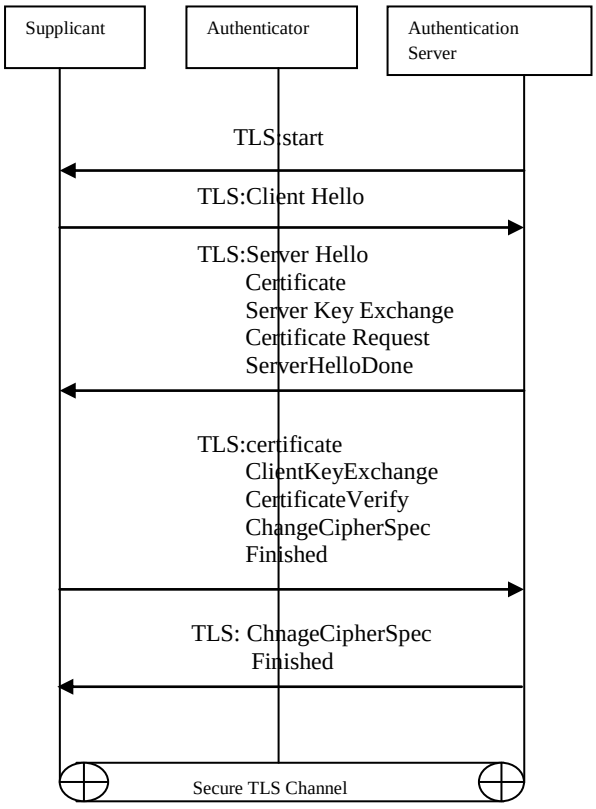

Figure 4 : Tls Authentication

4.1.2 Eap-ttls

EAP-TTLS is developed by Funk and Certicom in 2001, EAP-TTLS is an extension of EAP-TLS. Mutual authentication is optional in TTLS and generally not used because it would remove the key strength of TTLS. Additionally, it is not required to set up a public key infrastructure (PKI) This method uses two authentication layers

- Internal Authentication
- External Authentication

The external authentication makes use of TLS[3] handshake to establish a secure communication. During this step, it validates server certificate. The internal authentication which is used to identify the user, can be accomplished by any EAP method , usually done through password authentication procedure like PAP, CHAP, MS-CHAP or MS-CHAP-v2. It enables the use of existing databases, e.g. using a third party server. The following is the Figure 4 illustrates the tunneled authentication procedure.

It still provides a good level of security and is therefore a very popular solution which does not need a great effort to be set up.

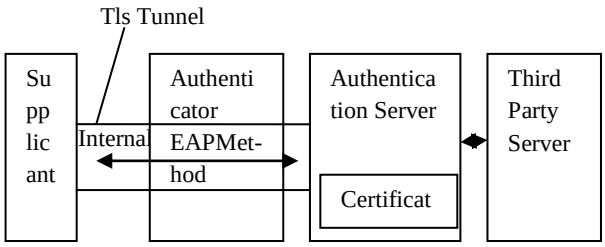

Figure 5 : TTLS Authentication

5. CRYPTOGRAPHY

Cryptography ensures authentication. Cryptography is a process of converting plaintext into cipher text (a process called encryption), then back again (known as decryption). There are several ways to classify the various algorithms. The most common types are

1. Secret Key Cryptography which is also known as Symmetric Key Cryptography and
2. Public Key Cryptography which is also known as Asymmetric Key Cryptography.

5.1 Secret Key Cryptography

In secret key cryptography[4], a single key is used for both encryption and decryption. the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver uses the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

Dis Advantage

- When key is known to attacker, he can decrypt the message.

5.2 Public Key Cryptography

Public or asymmetric key cryptography[5] involves the use of key pairs: one private key and one public key. Both are required to encrypt and decrypt a message or transmission. In public key cryptography, public key is known to all. Any one can send message by encrypting using public key but the correct receiver can only decrypt the message.

Dis Advantage

- It is easy to break pubic key cryptography on quantum computers

6. QUANTUM KEY DISTRIBUTION

Quantum Key Distribution[1], invented in 1984 by Charles Bennett and Gilles Brassard. The key is created during the process of key distribution in quantum cryptography, where a predetermined key is transmitted to the legitimate user in classical key distribution. The basic theme inside quantum key distribution is the detection of eavesdropper.

6.1 Quantum Properties

Quantum has some properties [7] which are so complex such that no one can understands quantum mechanisms. The strange properties of quantum superposition and quantum entanglement have direct consequences for the field of cryptography. These are presented below.

6.1.1 Quantum Superposition

A quantum is described by a probabilistic wave function (the Schrodinger equation) which gives the likelihood of finding the quantum at any particular position, but not its actual position. A quantum can have many possible states, but it exists in all of them simultaneously in the absence of an observer: this is quantum superposition. Once an observer measures the quantum, the wave function collapses and one of the previously superposed states is chosen according to the probability inherent in the wave function. This property is usually illustrated by the "Schrodinger's Cat" thought experiment shown in Figure 6.

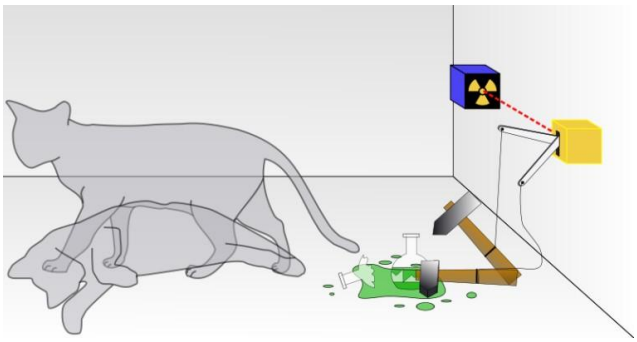

Figure 6 : Schrodinger's cat Experiment

A (quantum!) cat is locked in a box with a phial of cyanide which can be broken by some random mechanism – maybe a particle emitted from a radioactive source sets off a trigger– which will have predictably appalling consequences, if it is activated. There is no way of telling whether the cyanide has been released until the box is opened. A classical interpretation of this experiment is that the cat is alive OR dead in the box irrespective of when it is opened. However, the quantum interpretation is that the cat is both alive AND dead at the same time, and it is only the act of opening the box (i.e. measurement) which collapses the cat wave function into one or other of its possible states.

6.1.2 Heisenberg's Uncertainty Principle

There is a further complication to quantum observations: when you measure the position of a quantum, be it a photon, electron or whatever, you cannot know its velocity exactly, and vice versa: measure the velocity, and the position is unclear. This is the Heisenberg Uncertainty Principle, and it exists to protect quantum theory. Too accurate measurements would destroy the wave-like properties of quanta, and instantly quantum interference and superposition would disappear. The Uncertainty Principle is not confined to position and momentum: it affects any conjugate pair of states. These are states where measurements are not commutative, measuring A then B does not give the same answer as measuring B then A. The Uncertainty Principle is therefore the basis of many effects of the quantum world.

6.1.3 Quantum Entanglement

A quantum property relevance to QKD is that of quantum entanglement. Pairs of quanta can be produced which behave as if they are a single entity, so called EPR pairs. Quanta possess a property called "spin": one quantum could have spin up, one spin down, so that the total spin is zero but until a measurement is made it is not clear which is which of the pair. If the pair is separated, measuring one causes the other's wave function to collapse into the opposite state. It appears to know instantaneously that its partner has been measured, apparently contradicting Einstein's finding that nothing can travel faster than light. This is known as the EPR paradox.

6.1.4 Bell's Theorem

Bell investigated the properties of an entangled system in the case of 'strict locality' i.e. what happens to one particle depends only on events at its location and a different particle should only be affected by events at its (different) location. He showed that in this case, there are measurable effects which quantum physics showed would be violated when certain conditions were met. These are called Bell's inequalities, and experimental results demonstrated that 'strict locality' was not correct and quantum
entanglements hold even when the two component particles are separated physically.

6.2 General Methodology for Qkd

Quantum mechanics effects can be used to transfer information from Alice to Bob, and any attempted eavesdropping by Eve will always be detectable. Three distinct phases are present: raw key exchange, key sifting and key distillation, with the option to discard the secret key at any of the stages if it is appeared that not enough security could be obtained from it. General methodology for Qkd is shown in figure 7.

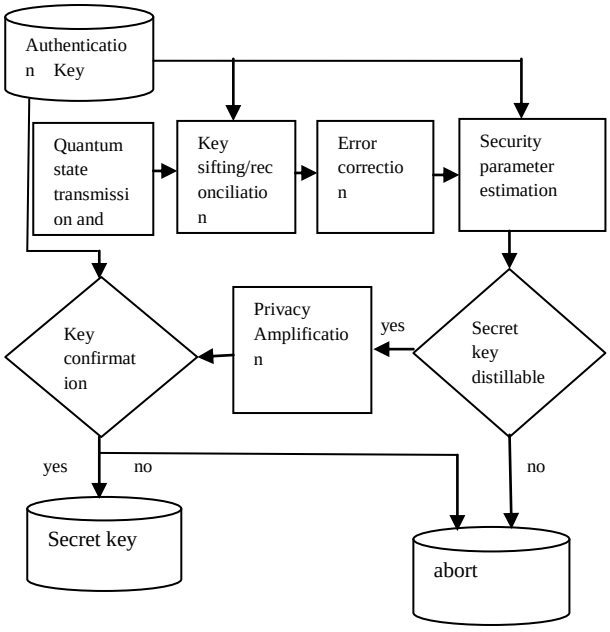

Figure 7 :General Methodology for QKD

6.2.1 Raw Key Exchange

This is the only quantum part of Quantum Key Distribution! Alice and Bob exchange 'some quantum states'. It actually doesn't matter what type of quantum state or technology is used – so quantum information is passed along a quantum

channel from Alice to be measured by Bob, with or without the presence of Eve, the eavesdropper. In all subsequent exchanges in a protocol, only a secure classical channel will be used. This is known as 'classical post-processing'.

6.2.2 Key Sifting

Alice and Bob decides which of the measurements will be used for the secret key. This decision making depends on which protocol is being used, and some measurements will be discarded e.g. if the settings used by Alice and Bob did not match.

6.2.3 Key Distillation

When reviewing experimental results (practical channels are lossy, and the presence of transmission errors) and in previous work on how the use of an authenticated public channel could repair the information losses from an imperfect private channel, three stages are suggested in Key Distillation. Error correction and privacy amplification , which are the first two steps in the key distillation phase of the classical post-processing of the remaining secret key bits. The third is authentication, which counteracts man-in-the-middle attacks.

6.2.3.1 Error Correction

Errors occur either through noise on the quantum channel, or the presence of an eavesdropper, but for security reasons, it is assumed that all errors are due to eavesdropping. A classical error-correction protocol estimates the actual error rate of the transmission, known as the Quantum Bit Error Rate (QBER). If the QBER is less than a pre-determined maximum value, then the secret key is passed on to the next step of key distillation. If the QBER is greater than this value, then the amount of information lost to an eavesdropper is too great to guarantee the secrecy of the key, and so the secret key is discarded.

6.2.3.2 Privacy Amplification

This is designed to counteract any knowledge Eve may have acquired on the raw key. Privacy amplification compresses the key material by an appropriate factor, determined by the previously calculated QBER: a high QBER needs more compression, as the purpose is to remove at least the same number of key bits that Eve may have gathered information about. There are provable privacy amplification processes, based on two-universal hash functions [JC79] [MW81] so the key material is still
unconditionally secure. (The output from error correction and privacy amplification is a known fraction of the original secret key, a 'gain'. Gain equations depend on the QBER and the efficiency of Alice and Bob's quantum creation and detection equipment.

6.2.3.3 Authentication

An adversary poses as Bob to Alice, and Alice to Bob and therefore all the traffic between Alice and bob is redirected through a third party, without them knowing. Hence authentication techniques are introduced to ensure the participants involved in the communication are genuine and are not subjected to man-in-the-middle (MITM) attack. Unfortunately, quantum processing itself is powerless against such an attack.

QKD have a property which can be used to strengthen classical authentication procedures. A secret key has to be pre-shared between Alice and Bob, for use in authentication of the very first quantum exchange. If authentication is unbroken during the first round of QKD, even if it is only computationally secure, subsequent rounds of QKD will be information theoretically secure.

6.3 BB84 Protocol

This BB84[8] protocol was proposed by Bennett et al. There are two different orthogonal bases of are there. They are

- Linear polarization basis +
- Diagonal polarization basis x.

The states $|0\rangle_+$and $|0\rangle_x$ represents the bit '0' and the other two $|1\rangle_+$ and $|1\rangle_x$ represents the bit '1'. Sender can choose at random one out of four states for polarized photons. Since the receiver does not know the basis on which sender send, receiver measures randomly.

In the next phase, sender and receiver discuss over a public channel and discard all the instances where they did not choose the same basis. The result is the sifted key, which may contain errors due to Eve's eavesdropping. Therefore to detect Eve, sender and receiver agreed publicly upon random subset of *n* bit locations in the raw key, and compare corresponding bits, making sure to discard from raw key each bit as it is revealed. An example of key exchange process is shown in below table 1.

Table 1 : BB84 Key Exchange

AliceRandomBit	0	1	1	0	1	0	0	1
AliceRandomSendingBasis	+	+	x	+	x	x	x	+
PhotonPolarizationAlice Sends	↑	→	\	↑	\	/	/	→
Bobs'sRandomMeasuringBasis	+	X	x	x	+	x	+	+
PhotonPolorizationBob Measures	↑	/	\	/	→	/	→	→
PublicDiscussionofBasis								
SharedSecretKey	0		1			0		1

7. CONCLUSION

In wireless Mesh Network there is a high probability to violate authentication and to encounter Man in the Middle attacks. To overcome those problems we have seen eap-tls and eap-ttls procedures. However there are some problems associated with both the models. A Quantum Key Distribution works effectively for authenticating the user. The effectiveness of the QKD will be understood by considering it's complex quantum properties. Thus Authentication in wireless mesh networks can be achieved through quantum key distribution. A key of arbitrary length can be generated using quantum key distribution. Thus we can achieve 100% efficiency by bringing classical cryptography to quantum cryptography.

8. REFERNCES

[1] "A Survey of Quantum Key Distribution Protocols" Mobin Javed and Khurram Aziz NUST School of Electrical Engineering and Computer Science

[2] "Authentication in Wireless Mesh Networks", Raphael Frank

[3] "Man-in-the-middle in tunneled authentication protocols", N. Asokan, Valtteri Niemi, Kaisa Nyberg..

[4] "A Symmetric Key Cryptographic Algorithm", Ayushi, Lecturer, Hindu College of Engineering

[5] "Public Key Cryptography Applications Algorithms and Mathematical Explanations", Anoop MS

[6] "Wireless mesh networks: a survey" Ian F. Akyildiz a, Xudong Wang b, Weilin Wang b

[7] "Quantum Key Distribution Protocols and Applications", Sheila Cobourne

[8] " Quantum cryptography: Public-key distribution and coin tossing". Bennett, C. H. and Brassard, G.1984. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, pp. 175 - 179.