Enhanced Secured Delegation Based Authentication Protocol for Communication Systems Using Quantum Key Distribution

Prudhviraj Pallam, K.Palanivel

Abstract— This article provides an up-to-date survey of secure delegation authentication protocol. Portable devices play a major role in our daily routine life. For portable communication Systems authentication is needed to provide data security and user privacy. A secure delegation based authentication protocol is used to provide authentication, Ellipctical curve cryptography is used for authentication in portable communication systems.It will restricts Denail Of service attacks.Reduces computational cost while authenticating a communication session. User Unlink ability is achievied.In this paper we propose a protocol with the help of quantum cryptography using quantum key distribution mechanism for detecting eavesdropping by the third party.

Index Terms— Portabledevices, authentication, Denial of Service (DOS) attacks, unlinkability, ellipcticcurvecryptography, quantum cryptography, quantum key distribution

1 INTRODUCTION

THE portable devices are being widely used by the people for communication and mobile applications for accessing the wireless networks. In interconnected electronic world, the communication among the devices and the people is rapidly increased. Accessing the internet has become mandatory in many of the areas.Secure and fast transmission of private information over wireless channels has become crucial.The use of public key cryptography to facilitate authentication for data over medium. Portable devices use the wireless medium to communicate.Radio waves are being transmitted in medium. It is very easy to eavesdrop and manipulate the message.So we must be concern about security and privacy for portable communication systems.The concept of delegation based authentication is proposed to solve the problems of computational cost,user privacy,dos attacks.One of the most serious security issues between service providers and enterprises is to achieve robust authentication mechanism.If a user temporarily hand over his authorization to another legitimate user then the process is known as delegation.Ellipctical curve cryptography is used for authentication. (ECC) is a mechanism which uses smallest keys to provide high security for data and high speed in low bandwidth channels. Elliptic Curve Cryptography has become the important cryptographic technique for networks and communication devices due to its size and efficiency in performance.Dos attacks will be eliminated by the secure based delegation authentication protocol.In proposed work we will explain about quantum cryptography and quantum key distribution for preventing eavesdropping potential threat.

- *Prudhviraj Pallam is currently pursuing masters degree program in network and internet engineering in Pondicherry University, Pondicherry, India PH-09943916567. E-mail: prudhvipallam@gmail.com*
- *K.Palanivel is currently working as System Analyst in Pondicherry University, Pondicherry, India, PH-09488824888. E-mail: kpalani@yahoo.com*

2 BACKGROUND AND RELATED WORKS

This section discusses the results obtained from the previous researches.

In this paper [1], they proposed a delegation based authentication protocol to provide solutions to the security issues for portable communication systems.Proxy signature is the major technique used in this protocol.This protocol provides more data security and user privacy when compared to previous protocols.It reduces computational cost for mobile stations.

In this paper [2], they proposed a novel and efficient mobile authentication scheme and analysis of security properties has been done.Two messages and one scalar point multiplication is provided on mobile stations for establishing each session after the verification of one time delegation key.

In this paper [3], they proposed an enhanced version of secure delegation based authentication protocol in which mobile station uses a backward hash chain to guarantees that no one can manipulate the authentication message to trick home location register.It reduces computational cost in mobile stations.

In this paper [4], they proposed a improved delegation based authentication protocol to achieve the user unlinkability.It shows user identity privacy and user unlikability are required for mobile users to communicate.

In this paper [5], they proposed an enhanced delegation based authentication protocol with user unlinkability and prevents denial of service attacks.It uses less computational cost for authentication of messages in each session.

In this paper [6], they analyzed the performance of elliptic curve cryptography in secure socket layer. Elliptic curve cryptography provide the same level of security afforded by an

RSA-based system with a large modulus and correspondingly larger key .Elliptic curve cryptography uses smaller keys and reduces power consumption.ECC will be utilized properly for portable devices having lesser memory space and small hardware.

In this paper [7], they examined why ECC is most suitable for constrained environments. Many devices are constrained devices that having small storage space to be applied. They explore its performance wireless communication systems. In wireless communication network devices like Cellular phone, PDA's can be used for providing security.

In this paper [8], they proposed hyper elliptic curve cryptography mechanism to provide better performance for mobile devices of less battery power and supporting small key sizes, less storage memory. The performance of this algorithm is better than RSA.

3 PROBLEM STATEMENT

In present generation all devices are portable and they are using wireless communication medium. In wireless communication, data security and user privacy is mandatory.There are enormous potential threats in wireless communication medium like DOS attacks ,brute force attacks, eavesdropping ,smurf attacks, spoofing etc.

In this paper, we are proposing a secure delegation based authentication protocol by using quantum key distribution mechanism of quantum cryptography over elliptic curve cryptography algorithm to detect and prevent eavesdropping potential threat.

4 PROPOSED MODEL

4.1 Eavesdropping

Eavesdropping is a potential threat in network security. Eavesdropping is the behaviour of listening secretly to a private conversation of other individuals without their consent. Eavesdropping is commonly thought to be unethical. Eavesdropping can be done over telephone communications (wire tapping),email messages,instant messages and other means of communication considered to be confidential.In the following fig(1) shown gives a general scenario of eaves dropping.

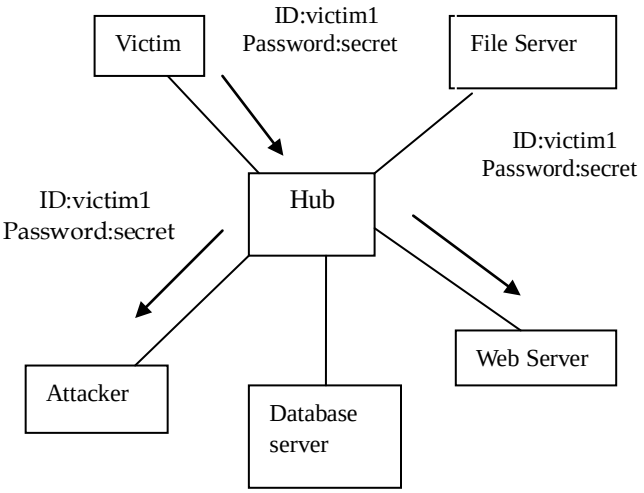

Fig (1): Eavesdropping scenario

4.2 Quantum Mechanics

Quantum mechanics (quantum theory or quantum physics) is a branch of physics dealing with physical phenomena at microscopic scales, where the action is on the pattern of the Planck constant(h).Quantum mechanics differs from classical mechanics firstly at the quantum realm of sub atomic length and atomic scales. Quantum mechanics provides a mathematical description of much of the dual particle-like and wave-like interactions and behaviour of energy and matter.

In advanced theories of quantum mechanics, some of these attitudes are macroscopic and only emerge at extreme (i.e., very high or very low) temperatures or energies. The term quantum mechanics derived from the observation that some physical quantities can change only in discrete (non-continuous) amounts, and not in a continuous way. For example, the angular momentum of an electron bound to an molecule or atom is quantized. In the definition of quantum mechanics, the wave particle duality of energy and matter and the uncertainty principle provide a unified view of the behaviour of photons, electrons, and other atomic-scale objects.

The mathematical formulations of quantum mechanics are complex. A mathematical function called the wave function provides notification about the probability amplitude of position, momentum, and other physical assets of a particle. Mathematical manipulations of the wave function usually involve the bra-ket notation, which requires an accepting of complex numbers and linear functions. The wave function treats the object as a quantum harmonic oscillator, and the mathematics is related to that describing acoustic resonance. Many of the results of quantum mechanics are not easily created in terms of classical mechanics, for instance, the ground state in a quantum mechanical scenario is a non-zero energy state that is the lowest permitted energy state of a system, as opposed to a more "conventional(traditional)" system that is thought of as simply being at rest, with zero kinetic energy.

$$P=hk$$

4.3 Planck Constant

The Planck constant is a physical constant that is the quantum of action in quantum mechanics branch. The Planck constant was first detailed as the proportional constant between the frequency (ν) of its associated electromagnetic wave and the energy (E) of a photon This relation between the energy and frequency is called the Planck relation:

$$E=h\nu$$

Since, the frequency ν, wavelength λ, and speed of light c are connected by $\lambda\nu = c$, the Planck relation can also be explained as below

$$E=hc/\lambda$$

4.4 Quantum Computer

A quantum computer is a computing device that makes direct usage of quantum mechanical scenario such as superposition and entanglement, to carry out operations on data. Quantum computers are unlike from digital computers based on transistors. Whereas a digital computer needs data to be encoded into binary digits (bits), quantum computation uses quantum properties to represent data and execute operations on these data. An abstract model is the quantum Turing machine, also called as the universal quantum computer. Quantum computers contribute theoretical similarities with non-deterministic and probabilistic computers. One example is the capability to be in more than one state simultaneously.

Although quantum computing is still in its beginning, experiments have been carried out in which quantum computational operations were completed on a very small number of quantum bits .Both practically and theoretically research work is continued, and many national government and military funding organizations support quantum computing research to expand quantum computers for both civilian and national security needs, such as cryptanalysis.

Large-scale quantum computers will be capable of solving certain problems much faster than any other classical computer using the best currently known algorithms such as integer factorization using Shor's algorithm or the simulation of quantum many-body systems. There exist quantum algorithms, such as Simon's algorithm, which run quicker than any other possible probabilistic classical algorithm. Given enough computational resources, a general computer could be made to affect any quantum algorithm; quantum calculation does not violate the Church–Turing concept.

5 QUANTUM CRYPTOGRAPHY

Quantum cryptography explains the usage of quantum mechanics to perform cryptographic works. Examples of quantum cryptography are the use of quantum communication to securely exchange a key between individuals which is known in quantum key distribution and use of quantum computing.

The advantage of quantum cryptography is to perform various cryptographic tasks. For example, it is used to detect eavesdropping in quantum key distribution.In the fig (2) shown below illustrates how the communication will be done using quantum channel.

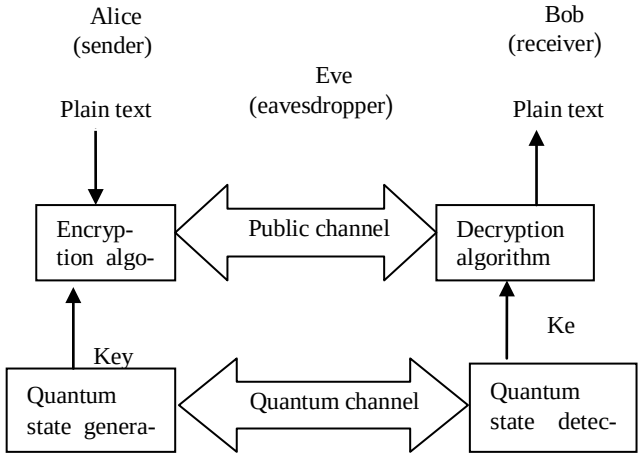

Fig (2): communication between two users using quantum Channel

5.1 Basic phenomenon of quantum cryptography

Quantum mechanics explains a general scenario that relates with the polarization states of a single photon.There are four possible polarization positions of a photon namely vertical, horizontal,45 degrees,135 degrees.Using these polarization states, communication will be done confidentially and generation of a secret key or shared key will be provided securely. Below fig(3) shows diagrammatic representation of polarization states.

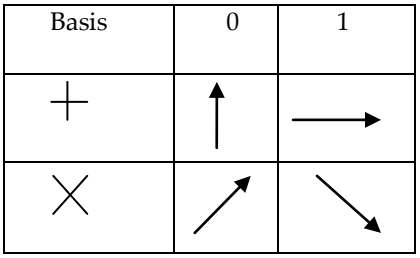

Fig (3): Polarization States of a photonQuantum key distribution

Quantum mechanics is used in quantum key distribution to guarantee secure communication over wireless medium. Quantum key distribution enables two parties to produce a shared random secret key which is known only to them .This key can be used to encrypt and decrypt messages .An unique and important property of quantum key distribution is the ability given to the two communicating users to detect the presence of any third party willing to know the detects of the key. This is from a basic fundamental aspect of quantum mechanics: the process of measuring a quantum system in normal scenario disturbs the system. If the third party trying to eavesdrop on the key (secret key) must in some way measure it, thus introducing detectable

mechanisms. By using quantum entanglement or quantum super positions and transmitting information into quantum states, a communication system can be implemented which detects eavesdropping potential threat. If the level of eavesdropping is below a certain threshold value, a shared random key can be produced that is guaranteed to be secured. Otherwise no secure key will be generated and communication is aborted.

Security of quantum key distribution relies on the basis of quantum mechanics, it is totally contrast to traditional key distribution protocol which relies on the computational ambiguity of certain mathematical functions and cannot provide any indication of restricting eavesdropping or wont guarantees key security.QKD is only used to generate and distribute a key, not to transmit any message data to other. So this key can then be used with any chosen encryption algorithms to encrypt an decrypt a data message, which can be then transmitted over a standard communication medium.OTP (one time pad) is the algorithm most commonly associated with quantum key distribution as it is proved secure when we use secret key and random key.

Quantum key distribution protocols which are used for quantum cryptography are given below:

1) SARG04
2) BB84
3) E91
4) COW
5) DPS
6) KMB09

The quantum key distribution protocols described above provides Alice and Bob with nearly unique shared keys, and also with an approximate calculation of the discrepancy between the keys. These differences can be done by eavesdropping potential threat, but also by fault in the transmission line and detectors. As it is impossible to differentiate between these two types of errors, guaranteed security requires the assumption that all errors are caused due to eavesdropping threat. Provided the error rate between the keys is lower than a certain threshold value, two steps can be performed to first remove the error bits and then reduce Eve's knowledge of the key to an arbitrary small value. There are two steps to detect and rectify as information reconciliation and privacy amplification respectively.

5.2 Information reconciliation

Information reconciliation is an arrangement of error correction carried out between Alice and Bob's keys, in order to ensure both keys are unique. It is conducted over the public channel and as such it is important to minimize the data information sent about each key, as this can be read by Eve. A common protocol used for information reconciliation mechanism is the cascade protocol. This performs in many rounds, with both keys separated into blocks in each round and the parity of those blocks compared. If any difference in parity is to be found then a binary search is performed to locate and rectify the error. If an error is found in a block from previous rounds that had correct parity then other error must be there in that block; this error is found and corrected as before. This process is done again recursively, which is the source of the cascade name. After all blocks have been compared, Bob and Alice both reorder their keys in the same random way, and again a new round begins. At the end of multiple rounds Alice and Bob have unique keys with high probability value, however Eve has more data information about the key from the parity information exchanged.

5.3 Privacy Amplification

Privacy Amplification is a procedure for decreasing (and effectively eliminating) Eve's partial information about Alice and Bob's key. This limited information could have been acquired both by eavesdropping on the quantum channel during key transmission (thus introducing detectable errors) between Alice and Bob, and on the public channel during information reconciliation (where it is assumed Eve acquires all possible parity information).It uses Alice and Bob's key to generate a new, shorter key, in such a manner that Eve has only negligible information about the newly generated key. This can be performed using a universal hash function, chosen at random from a publicly known group of such functions, which holds as its input a binary string of length equal to the key and outputs a binary string of a chosen shorter length. The quantity by which this newly generated key is shortened is computed, based on how much data information Eve could have acquired about the old key (which is known due to the errors this would introduce), in order to decrease the probability of Eve having any knowledge of the newly generated key to a very low value.

6 BB84 protocol

BB84 is the quantum key distribution protocol scheme developed by Gilles Brassard and Charles Bennett in 1984.BB84 is the first quantum cryptography protocol.BB84 protocol is provably secure and relying on the basics of quantum mechanics properties.BB84 protocol is commonly explained as a method of securely communicating a private key or shared key from one party to another party for use in one time pad (OTP) encryption.

Fig (4): sharing a secret key between Alice and bob using polarization states of a photon

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	×	×	+	×	×	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	×	×	×	+	×	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared secret key	0		1			0		1

7 Conclusion

In this paper, we proposed a secure delegation based on authentication protocol for portable communication systems by using quantum cryptography mechanism quantum key distribution which provides ability to detects and prevent eavesdropping. It strengthens the security of the data over wireless communication medium.

8 References

[1] W. B. Lee and C. K. Yeh, "A new delegation-based authentication protocol for use in portable communication systems," IEEE Trans. Wireless Commun., vol. 4, no. 1, pp. 57–64, 2005.

[2] C. Tang and D. O. Wu, "An efficient mobile authentication scheme for wireless networks," IEEE Trans. Wireless Commun., vol. 7, no. 4, pp.1408–1416, 2008.

[3] T. F. Lee, S. H. Chang, T. Hwang, and S. K. Chong, "Enhanced delegation-based authentication protocol for PCSs," IEEE Trans. Wireless Commun., vol. 8, no. 5, pp. 2166–2171, 2009.

[4] T. Y. Youn and J. Lim, "Improved delegation-based authentication protocol for secure roaming service with unlinkability," IEEE Commun. Lett, vol. 14, no. 9, pp. 791–793, 2010.

[5] Jia-Lun Tsai, Nai-Wei Lo, and Tzong-Chen Wu, "A Secure Delegation-Based Authentication Protocol for Wireless Roaming Service," IEEE Trans. Wireless Commun, IEEE COMMUNICATIONS LETTERS, VOL. 16, NO. 7, JULY 2012.

[6] Vipul Gupta, Sumit Gupta and Sheueling Chang,"Performance Analysis of Elliptic Curve Cryptography for SSL", in *WiSe'02*, September 28, 2002, Atlanta,Georgia, USA.Copyright 2002 ACM1581135858/02/0005.

[7] S. Prasanna Ganesan, Dr. GRD College of Science, "An Asymmetric Authentication Protocol for Mobile DevicesUsing Elliptic Curve Cryptography "978-1-4244-5848-6/10/$26.00 © 2010 IEEE.

[8] S. Prasanna Ganesan, Dr. GRD College of Science, "An Authentication Protocol For Mobile Devices Using Hyperelliptic Curve Cryptography "International Journal of Recent Trends in Engineering and Technology, Vol. 3,No. 2, May 2010.