Indian Journal of Communication Engineering and Systems(IJCES)
Vol.2.No.1 2014 pp 43-48.
available at: www.goniv.com
Paper Received :08-03-2014
Paper Accepted:22-03-2013
Paper Reviewed by: 1. R. Venkatakrishnan 2. R. Marimuthu
Editor : Prof. P.Muthukumar

A NOVEL APPROACH FOR HASTY ERROR REDUCTION TO SAFEGUARD THE NETWORKS

A.DIVYA, R.KAVITHA
Department of Computer Science and Engineering,
IFET College of Engineering,
Tamilnadu, India.
Email:anjali.rec@gmail.com kavithayuppy@gmail.com

ABSTRACT

In many cases error reconciliation is a obstruction in Quantum Key Distribution Systems. The QKD protocol is used to safeguard security in large networks by the use of key agreement. By exchanging the identical key, the information is shared between the sender and receiver, also there is no reduction in the case of error. To improve this, each time the data is transferred, a unique key is generated, trusted center being the third party authenticates and generates the shared secret key using Algorithms and Quantum Mechanisms. Two Reconciliation Techniques are used for avoiding the loss of data and to secure the key. As a result, the error is reduced along with the generation of secure key at high speed.

***Keywords*:** Quantum Key Distribution (QKD), Information Reconciliation, Privacy Reconciliation.

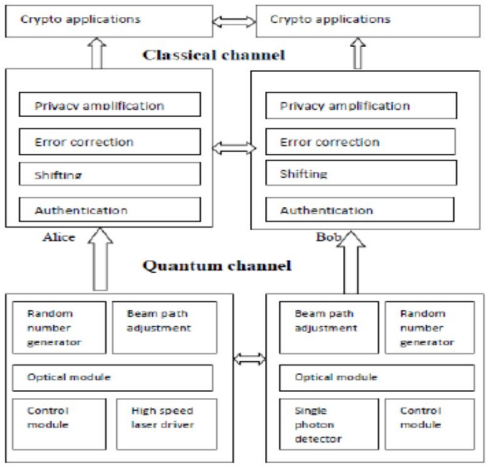
I. INTRODUCTION

Network Security involved in the authorization of access to data in the network, which is controlled by the network administrator. User gives an ID and Password or other authenticating information that allows them access to information which is needed. Network Security covers a variety of computer networks, both public and private, that are used in everyday jobs. A Peer to Peer network is a network which is of decentralized and distributed network and the architecture in which individual nodes in the network act as both suppliers and consumers of resources. Quantum Cryptography is the first practical skill in Quantum Communication.

Articles give an overview about the QKD system. The aim of QKD is to generate a secure key string between Alice and Bob, and thus the key is used for the communication. QKD generally consists of three steps, i)raw key shifting ii)error reconciliation iii)privacy amplification. The first step in QKD is raw key shifting that is generating of unique key by the trusted center using the qubit combinations. The second step is error reconciliation in which the errors must be eliminated by exchanging information through a public channel. The first error reconciliation protocol was BBBSS.

Later on other new protocols such as Cascade , Low Density Parity Check (LDPC) protocol were used to reduce the error in data transferring. The Third step is privacy amplification it is achieved by applying universal hash functions that map a longer bit to a shorter one.

The Information Reconciliation is used for error correction in between Alice's and Bob's keys, to ensure both keys are identical. It safeguards from the hackers by reading the information. In this it has common protocol in information reconciliation is cascade protocol.



The Privacy Reconciliation is a method for reducing hackers partial information about Alice's and Bob's key. Privacy amplification uses the key to produce a new, shorter key, which is updated in such a way that hackers has only negligible information about the new key. This can be done by universal Hash Functions.

Till now Error reconciliation has been completed using software on PC. The final key rates is a demand which gives rise to a obstruction in the QKD system. Thus a hasty error reduction is needed.To achieve this a unique key is generated by the QKD system .In which trusted center being the third party authenticates on sender and receiver and a session key is shared on both sides.

II. LITERATURE SURVEY:

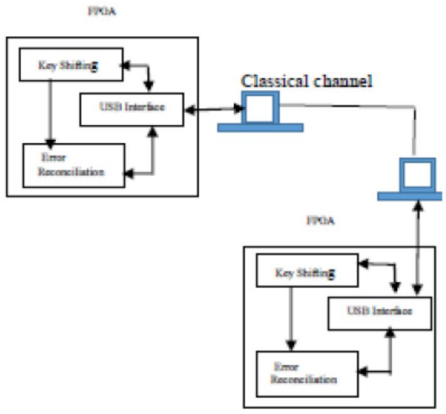
N.Gisin proposed a Quantum Mechanism [1] to send the message, the hackers hack any one of the position this can be avoided using trusted center. Won-Young Hwang, this author implements a decoy pulse method [2] to overcome the photon splitting, to decrease it a key is used in final process. Ivan Rech, in this SPAD and SPCM techniques are proposed to provide a clock rate upto 2khz, [3] this clock rate is extended to 2.5khz in this paper. W.T.Buttler, Hamming code technique [4] is proposed in this for large data set, the data can be easily hacked it can be avoided by information and privacy reconciliation to avoid the errors in a process. G.Van, this author describes a spectrum quantum carriers [5] to get a binary key which list the correlated variables and it is shared. Lijun Ma, this author describes a QKD system with clock synchronization at 1.25 gbps clock rate [6], this can be done more effectively by 2.5 gbps clock rate. D.Elkouss, LDPC and BSC methods [7] are proposed by this author in which a common string is shared between the users which can be easily hacked to overcome this dynamic key is used. D.Lancho, Information Reconciliation technique [8] is implemented to reduce the error rate by setting N to 64 bits. Viente Martin, in this Information Reconciliation based LDPC technique [9] is proposed by predefining the error rate which can be made efficient in using privacy reconciliation method in this paper. P.Youplao, Privacy Reconciliation [10] is proposed by this author in Wavelength router by generating identical secret key, this can be avoided by generating dynamic key. David Elkouss, proposesd a method of Information reconciliation [11] used to reduce the error rate, for longer distance which is one of technique used in this paper. Paul Jouguet, Polar codes [12] is used to exchange the information through a physical channel which requires a large block for better efficiency. Zhi Ma, In this a new schema called RCEV with LDPC [13]is implemented which is for decoding process only the error in encryption process is not reduced. Zhu Chang-Hau. This author describes a frequency and time coding method [14] for security, and it is not efficient in all cases as it can be easily hacked. K.Chen, Decoy state [15] is used by this author to detect the eve attacks, but it is not secured as it can be easily hacked ,it can also be reduced by random strings. Y.Zhao, A signal state [16] is proposed for securing the data, the signal state can be easily hacked.

III. ERROR RECONCILIATION BY HAMMING TECHNIQUE

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to encrypted form. The user of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients. In classical Cryptography Challenge-Response Authentication Mechanism (CRAM) was used. In Challenge-Response Authentication Mechanism is the two-level (basic authentication and digest authentication) scheme for authenticating network users that is used as part of the Web's Hypertext Transfer Protocol (HTTP).The basic authentication scheme is based on the model that the client must authenticate itself with a user-ID and a password for each real. Web Browser or other client Program provides credentials in the form of username and Password. Although the scheme is easily implemented, it relies on the assumption that the connection between the client and server computers is secure and can be trusted. Digest authentication is out of date unencrypted Basic access authentication, allowing user identity to be established securely without having to send a password in plaintext over the network. Digest authentication is basically an

application of cryptographic hashing with usage of nonce values to prevent cryptanalysis. While sending in a network the key generation is done by the sender, the key is a static key in which it is easily hacked by the Eve.Does not protect fully from man-in-the-middle attacks.The error rate is not also fully reduced in using the Hamming technique.

In the FPGA to receive and for sending the information Interface module is has been used during the reconciliation process. The First in First Out (FIFO) is used in it as there is one incoming data and one outgoing data. To process the whole system a data bus and a control bus is used for coordinating the FIFO among different modules. For calculating and comparing the parities on both sides the parity comparison module is used. This is achieved using the single data operator. Hamming code module is used for sending the data without error, in which the data is converted into a matrix form. Permutation module needs a pseudo random number with a long cycle period. These are the modules which are used for the error reconciliation process in existing for a better security.



QKD System with Error Reconciliation

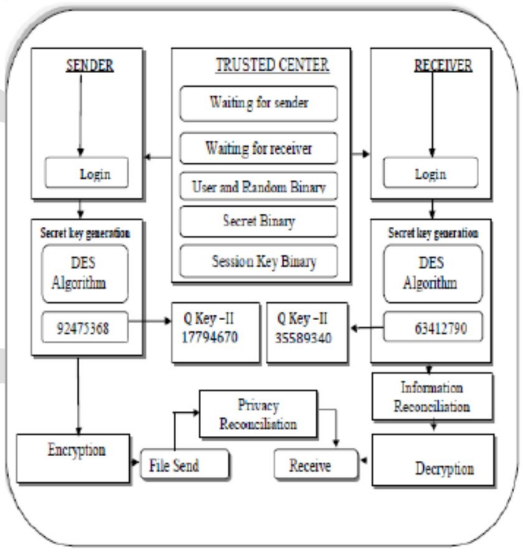
IV. ALGORITHM

RC4 Algorithm is used for the data encryption and decryption. But it is complicated when related keys or a non-random keys are used. There are many possibility for insecure Cryptosystems. In this algorithm it does not take a separate nonce alongside the key. A nonce is of a number or a string which is used for the encryption and decryption process.

There are some of the advantages in using this algorithm and techniques in which the data loss occurs when it is received as the bits can be easily hacked when it is send through a public channel. The error occurrence is also more when it passed through a system. Though some of the modules has been developed in avoiding the error reconciliation, it cannot be said a efficient process is done to avoid it. For a better result and for a efficient process a proposed system has been developed which is free from above complexities.

V. ERROR RECONCILIATION BY INFORMATION AND PRIVACY RECONCILIATION

The Quantum Key Distribution Protocols is used to safeguard security in large network. QKD protocol which works on network security by the use of key agreement. The sender and receiver should register themselves into the separate databases maintained for them and then whenever each user either on the sender or the receiver side makes a login request, an individual secret key is created. Trusted Center considered being the third party authenticates both the sender and the receiver, the secret key is generated by the Trusted Center at both sides using Algorithms and Quantum Mechanism.



Structure for Generating the Key with Error Reconciliation

The secret key will take part in the final key (Quantum key).At this instance our system will store every detail such as username, password etc. While sending the data Hashing technique is applied inorder to get the two key values. This is to prevent the data from hackers and also it enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages. To reduce the error rate two techniques is used such as information reconciliation to secure the key and

privacy reconciliation to reduce the loss of data. In this for data encryption and decryption DES Algorithm is used, to reduce the error information reconciliation and privacy reconciliation is used.

VI. ALGORITHM FOR KEY GENERATION

DES ALGORITHM:

The Data Encryption Standard (DES) algorithm, is a block cipher that transforms 64-bit data blocks under a 56-bit secret key, by means of permutation and substitution. The DES algorithm is widely used and is still considered reasonably secure. The working of DES algorithim is as follows,

Step 1:

I). Process the key

Get a 64-bit key from the user which is considered a parity bit. For a key to have correct parity, each byte should contain an odd number of "1" This key can be entered directly, or it can be the result of hashing

II).Calculate the key schedule

i) Perform the permutation on the 64-bit key. The parity bits are discarded, reducing the key to 56 bits. Bit 1 of the permuted block is bit 57 of the original key, bit 2 is bit 49, and so on with bit 56 being bit 4 of the original key.

ii) Split the permuted key into two halves. The first 28 bits are called C[0] and the last 28 bits are called D[0].

iii) Calculate the 16 sub keys.

Step 2:

I) Process a 64 bit data block

i).Get a 64-bit data block. If the block is shorter than 64 bits, it should be padded as appropriate for the application.

ii).Perform the permutation on the data block.

iii).Split the block into two halves. The first 32 bits are called L[0], and the last 32 bits are called R[0].

iv).Apply the 16 sub keys to the data block. Expand the 32-bit R[i-1] into 48 bits according to the bit-selection

v). Perform the permutation on the block R[16]L[16].

This has been a description of how to use the DES algorithm to encrypt one 64-bit block. To decrypt, use the same process, but just use the keys K[i] in reverse order. That is, instead of applying K[1] for the first iteration, apply K[16], and then K[15] for the second, on down to K[1].

DES vs RSA ALGORITHM:

DES algorithm is more efficient in encryption and decryption than a RSA algorithm. RSA algorithm is for integer factorization and it is still in theorem. The security is carried out by mathematics.Encryption and Decryption is less efficient as it cannot done for larger blocks of data.DES algorithm is a group cipher algorithm in which it encrypts data by 64-bit and it is suitable for encrypting large number of message.

Table : Results for DES-RSA

Packet Size	20 kb	40 kb	60 kb
Time to Encrypt	61342.1ms	109415.3ms	123754.0ms
Time to Decrypt	5175.1ms	6852.3ms	10892.3ms

This table denotes the time taken for encrypting an decrypting various packet size both by RSA and DES algorithm.

VII. TECHNIQUES FOR ERROR RECONCILIATION

A.INFORMATION RECONCILIATION:

The information reconciliation is a technique to reduce or avoid the error which occurs in key and securing the key while it is generated on both sides. Information reconciliation is conducted over the public channel and it is vital to minimise the information sent about each key, as this can be read by hacker. A common protocol used for information reconciliation is the cascade protocol. This operates in several rounds, with both keys divided into blocks in each round and the parity of those blocks compared. If a difference in parity is found then a binary search is performed to find and correct the error. If an error is found in a block from a previous round that had correct parity then another error must be contained in that block; this error is found and corrected as before. This process is repeated, which is the source of the cascade name. After all blocks have been compared, Alice and Bob both reorder their keys in the same random way, and a new round begins. At the end of multiple rounds Alice and Bob have identical keys with high probability, however Eve has additional information about the key from the parity information exchanged. Information reconciliation is essentially a source coding with side information, from coding point of view.

B.PRIVACY RECONCILIATION:

Privacy Reconciliation is a method for reducing Hackers partial information about Alice and Bob's key. This partial information could have been gained both by eavesdropping on the quantum channel during key transmission thus introducing detectable errors, and on the public channel during information reconciliation where it is assumed hacker gains all possible parity information. Privacy amplification uses Alice and Bob's key to produce a new, shorter key, in such a way that hacker has only negligible

information about the new key. This can be done using a universal hash function, chosen at random from a publicly known set of such functions, which takes as its input a binary string of length equal to the key and outputs a binary string of a chosen shorter length. The amount by which this new key is shortened is calculated that is updated key, based on how much information hacker could have gained about the old key in order to reduce the probability of Eve having any knowledge of the new key to a very low value.

VIII. COMPOSITION OF MODULES

This system consists of three main modules: 1.Sender 2.Trusted Center 3.Receiver for secure sending of data and to reduce the error.

A.SENDER MODULE:

Getting Authorization is the first stage in sending phase. This phase or Sender Module has Sub Modules.

They are as follows:

1. Registration
2. Login and
3. Send Data

1. Registration

Registration is the Initial state for getting Authentication. By Providing username and Password user sets their Authentication. And System provides one more credentials that is Secrete key which is generated by the system for each user. By using username, Password and Secret key system will identify the Authorized person. These values are stored in the reg table

2. Login

A user wants to send a file means, he/she must log in by using his/her authentication credentials. In this module we have to give username, password and Secret key which was generated by the system. If the user does not provide proper information or the given information is mismatched with database then our system shows Exception message immediately. If the user's details are verified and matched with the existing database then our system allows the person to transmit the file. After login the TCP program calls i.e. our Trusted Center program starts listen the client or sender. Through Login we send the sender's secrete key for Identification.

3. Send Data

The main aim of this module is to encrypt a file and send that encrypted file to receiver. Encryption will happen only if the system gets a key from Trusted Center. So after verification of user identification system will send the current user's name and his/her secrete key to Trusted Center.

B.TRUSTED CENTER MODULE:

The Trusted Center as some of the sub modules in it.

1. Secret Key Verification

Verify the secret key received from the user and authenticate the corresponding user for secure transmission.

2. Session Key Generation

It is shared secret key which is used to for encryption and decryption. The size of session key is 8 bits. This session key is generated from pseudo random prime number and exponential value of random number.

3. Qubit Generation

To get secret key and random string, then convert into hex-code and then convert it into binary, find the least bit of two binary values and get the quantum bit of 0 and 1.

To generate the quantum key using the qubit and session key which depends on qubit combinations, such as

1.If the value is 0 and 0, then 1/0.707(p[0]+p[1])
2. If the value is 1 and 0, then 1/0.707(p[0]-p[1])
3. If the value is 0 and 1, then p[0]
4. If the value is 1 and 1, then p[1]

4. Key Distribution

It distributes the original session key and qubit to the sender for encryption. Also, it distributes the qubit and the session key on the receiver side for decryption.

C.RECEIVER MODULE:

Getting Authorization is the first stage in receive phase.

This phase or Receiver Module has Sub Modules. They are as:

1. Registration
2. Login and
3. Receive Data
4. Error Reconciliation

1. Registration

Registration is the Initial state for getting Authentication. By Providing username and Password user sets their Authentication. And System provides one more credentials that is Secrete key which is generated by the system for each user. By using username, Password and Secret key system will identify the Authorized person. These values are stored in the Database quantum key in which reg table.

2. Login

A user wants to send a file means, he/she must log in by using his/her authentication credentials. In this module we have to give username, password and Secret key which was generated by the system. If the user does not provide proper information or the given

information is mismatched with database then our system shows Exception message immediately. If the user's details are verified and matched with the existing database then our system allows the person to transmit the file. After login the TCP program calls i.e. our Trusted Center program starts listen the client or sender. Through login we send the sender's secrete key for Identification.

3. Receive Data

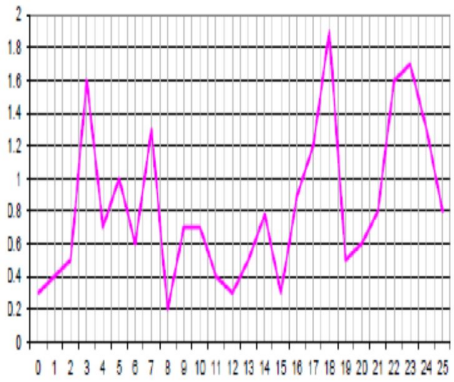
The main of this module is to decrypt a file. Decryption will happen only if the system gets a key from Trusted Center (TC). So after verification of user identification system will send the current user's name and his/her secret key to Trusted Center (TC).

***4.** Error Reconciliation*

Error Reconciliation protocols are used to preserve security by reconciling the errors in the respective keys. The error in key can be reduced by information reconciliation by updating a new key from a old key and the error in the data can also be reduced by privacy reconciliation.

IX. RESULTS

Proposed Efficiency: Most blocks hold errors when the data is transferred it can be detected and removed. In this paper reconciliation techniques are used to avoid the error from the other reported techniques .The information reconciliation is used to avoid the error in the key for a secure key sending. The privacy Reconciliation is a technique used for safe sending of data without any loss in it. To safeguard the network unique keys are been generated at both sides, the encryption or decryption will start only after it receives a key from Trusted Center. In this graph the error is reduced through information and privacy reconciliation techniques in which if in a system any of the error occurs using ns2 two objects are has been used in which any one of the object is used for a better and safe sending of the data.



REFERENCES

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", *Rev. Mod. Phys.*, vol. 74, pp 145-195, 2002.

[2] Won-Young Hwang "Quantum key distribution with high loss", *Phy. Rev. Lett.,* vol. 91, no.5, p 057901, 2003.

[3] Kareni, Gordon, Ivan Rech, Paul.D, Tonsend, Gerald S. Buller,"Quantum key Distribution Syytem clocked at 2kHz",*Opt. Express.,* vol. 13., pp 3015-020, 2005.

[4] W.T .Butttler, S.K. Lamoreaaux, J.R. Torgersonn, G.H. Nickel, " Fast Efficient Error reconciliation for Quantum Cryptography", *Phys. Rev,* vol A.67, no. 5., pp 052303, 2003.

[5] G.Van Asche, J.Cardinal; Cerf, J.Nicolas, "Reconciliation of a Quantum-Distributd Gaussian key" ,*IEE trans. Inf. Theory,* vol. 50,pp 394-400, 2004.

[6] Lijun Ma, Technol, Gaithersbug, Mink, Alan, Hai Xu, "Experimental Demonstration of an active quantum key distribution network with over gbps clock synchronization", *IEEE.,* vol. 11, pp 1019-1021, 2007.

[7] D.elkouss, A.Leverier, R. Alleaume, J.J Boutros, "Efficient Reconciliation protocol for discrete variable quantum key distribution" in *Proc. IEE Int. Symp. Inf. Theory (ISIT 2009),* pp. 1879-1883, 2009.

[8] D.Elkouss, J.Martinez, D.Lancho, V. Martin, " Rate Compatible Protocol for Information Reconciliaiton-An Application to QKD", in *Proc., IEEE Inf. Theory Workshop (ITW),* pp. 1-5, 2010.

[9] Jesus Martinez, MATEO David Elkouss, Viente Martin, "Interactive Reconciliation with LDPC", vol. 1, pp 1006-4484., 2010.

[10] P.Youplao, S.Mithatha, P.P.Yupapin. "Privacy Amplification of QKD Protocol in a Quantum Router", *Procedia Engineering 32,* pp. 536-543, 2011.

[11] David Elkouss, Jesus Martinez, Vicente Martin, "Information Reconciliation for QKD", vol. 11, No 3 &4, pp. 2226-0238, 2011.

[12] Paul Jouguet, Sebastien Kunz-Jacques, "High Performance Error Correction for Quantum key Disribution using Polar Codes", vol. 14, No 3 &4, pp. 0329-0338, 2012.

[13] Zhengchao Wei and Zhi Ma, "Easily Implemented Rate Compatible Reconcilaiton Protocol for QKD",vol. 1, pp. 1305-6244, 2013.

[14] ZHU Chang-Hua, PEI Chang-Xing, YI Yun-Hui, "A New Quantum key Distribution Sheme based on Frecuency and Time Coding", *Chin, Phys. Lett.,* vol. 27, no. 9, 09031, 2010.

[15] H.K.Lo, X.Ma, K.Chen, "Decoy state quantum key distribution", *Phys. Rev. A,* vol. 94, p. 2304, 2005.

[16] X.Ma, B.Qi, Y.Zhao and H-K.Lo, "Practical Decoy state for Quantum key Distribution", *Phys. Rev.A.,* vol. 72,no. 1, p012326, 2005.