Implementation of a Modified BB84 Algorithm for Secure Key Exchange in a Normal Network

Sandeep V,
Fouth Semester, M.Tech in Digital Communication,
Acharya Institute of Technology,
Bangalore.

Niranjan A.
Senior lecturer,
M.N.Technical institute,
Bangalore.

Abstract - The basic idea behind cryptography as a discipline was to research how valuable data & information can be protected? from unauthorized parties. Quantum cryptography is one of the recent advancements occurred within that discipline. Many research papers have been done to develop the algorithms, while others, to propose new implementations of these algorithms to tackle a specific problem. A conventional security mechanism such as Symmetric Key Encryption demands for the usage of a single key by the two parties (principals) involved in communication. Hence it is required for the parties to exchange the key in a secured manner. There are several public key algorithms such as RSA. However these algorithms are becoming untrustworthy because an attacker by using a modern technology may easily determine the contents of exchange and use this key to recover the data that is getting exchanged. Quantum cryptography involves the use of a number of Quantum Key Distribution (QKD) protocols such as BB84, B92, EPR. In this paper, an attempt is made to establish the secure communication channel by modifying the existing BB84. The proposed approach is tested on a wide range of inputs to analyse the required key size to be chosen by the user to obtain a key that is suitable for DEA, TDEA &AES.

Keywords: Symmetric Encryption, Public Key Encryption, Quantum Cryptography, QKD, BB84

1. INTRODUCTION

Cryptography generally aims at providing confidentiality, integrity and authentication services to the parties involved in communication. Symmetric Encryption and Asymmetric Encryption are two different existing encryption techniques, where Symmetric encryption uses single key by both the parties for the exchange of data while Asymmetric encryption uses two different keys called the public and private key pairs. For both techniques to succeed the key must be exchanged in a secured manner (Secure Key Distribution). The parties after agreeing upon the key use it for encryption and decryption of the data.

The QKD model provides a mechanism to exchange secret keys based on a security method that is rooted in the laws of Physics [3] [4]. Since this approach is still at its early stages, many researches and developments have been proposed and some had been implemented to improve it. Quantum cryptography uses our current knowledge of physics to develop a cryptosystem that is not able to be defeated - that is, one that is completely secure against being compromised without knowledge of the sender or the receiver of the messages. The word ***quantum*** refers to the fundamental behavior of the smallest particles of matter and energy: ***quantum theory*** explains everything that exists and nothing can be in violation of it. Quantum cryptography uses the ***Heisenberg Uncertainty Principle***, which holds that when a phenomenon is observed its characteristics are always affected by the act of observation.

1.1 Related work

Diffie and Hellman, presented a secure key agreement protocol that can be carried out over public communication channels and is still widely used. Even though the protocol seems to be quite simple, it is vulnerable to certain attacks. Diffie-Hellman key agreement protocol (DH protocol) has vulnerability is compounded by the fact that programmers often do not have a proper understanding of the security issues. Brassard and Bennett during the year 1984, presented BB84 to demonstrate an efficient procedure for safe key distribution. The main objections to QKD have been the expense.

Until now, the idea of leasing fibers from telecoms providers has put potential users off from the first hurdle. Also, BERs (bit error rates) caused by a combination of the Heisenberg Uncertainty Principle and microscopic impurities in the fiber make the system unworkable.

2. The BB84 protocol

The BB84 protocol [3] was proposed by Bennet & Brassard during 1984. This protocol makes use of four non-orthogonal polarization states (0º, 90º, 45º,135º) that are classified as

- Rectilinear states (0º, 90º) and
- Diagonal states (45º,135º).

The Rectilinear states are represented by the " +" symbol and the Diagonal states by the " X" symbol. The "+" & " X" are considered the "photon bases" and their equivalent binary values are called the "quantum bits" or "qubits" . The conventions used are listed in Table-1.

Polarization State	Photon base	Symbol	Degrees	Qubit
Rectilinear state	+	—	0º	0
		|	90º	1
Diagonal state	**X**	/	45º	0
		\	135º	1

Table 1: conventions used

The BB84 typically involves the following steps

1. a. Polarization state generation phase
   b. Selection of polarization states within the chosen polarization state (—, | , /, \)
2. Transmission of the polarization states to the Reciever.
3. Measurement of the received states with randomly chosen polarization states.
4. Valid state determination by comparing the received states with the generated states.
5. Saving the valid states and transmitting them to the sender.

Both the parties can now choose to use the qubits of the valid states as the one time session key for the secure exchange of data. Consider the following example shown in figure 1 to understand the working of BB84.

ACTIONS	Photon bases, polarization states and qubits							
Sender(S) randomly generates photon bases	+	+	X	+	X	+	X	+
S selecting the polarization states within the chosen base and transmits the bases	-	|	/	|	/	-	\	-
Reciever(R) randomly generates photon bases	X	+	+	+	X	+	X	X
R's polarization states within the chosen base	/	|	-	|	/	-	\	\
Valid data		1		1	0	0	1	
Transmitted & added to their sequences		1		1	0	0	1	

Figure 1: Working of BB84

3. PROPOSED APPROACH

Unlike the BB84 protocol which simply relies on the public channel for the exchange of polarization states, the proposed approach uses a secured channel for the exchange of this information. The sender in the proposed approach, encrypts the polarization states before transmission. The reciever decrypts the received states and follows the same procedure as that of the standard BB84 approach upto the transmission of the valid states. However instead of sending the valid states in plain text format the sender encrypts the valid states before transmitting to the Receiver. The reciever has to decrypt the incoming message and finally before sending the valid state message back to the sender it encrypts the message which is decrypted by the Sender.

The proposed approach typically involves the following steps

1. Polarization state generation phase
   a. Random generation of photon bases (+ or X)
   b. Selection of polarization states within the chosen polarization state (—, | , /, \)
2. **Encrypting the polarization states using a pre-shared secret key**
3. **Transmission of the encrypted polarization states to the Reciever.**
4. **Decrypting the polarization states using the sameshared key**
5. Measurement of the received states with randomly chosen polarization states.
6. Valid state determination by comparing the received states with the generated states.
7. Saving the valid states.
8. **Encrypt the valid states using the pre-shared secret key.**
9. **Transmit back the resultant message**
10. The Sender recovers the message using the same pre-shared secret key and stores the qubits for the future use as a secret key.

Additional steps included into the proposed modified BB84 are steps 2,3,4,8 & 9. These steps are highlighted for convienience. As the proposed modified BB84 protocol [1] is adopting encrypted communication, the fear of Beam Splitting, Intercept/Resend may be avoided[2].

4. RESULTS AND ANALYSIS

We developed a simulation software providing a thorough simulation of the working of a modified BB84 algorithm. Our software had two modules Secure QKD Sender & Secure QKD Receiver that were necessarily implemented on two heterogenous systems with different Operating systems.They were interconnected via a wireless router to examine its performance in terms of speed and security.
The software was tested on a wide range of inputs to analyse the required key size to be chosen by the user to be able to obtain a key for the use with different algorithms such as DEA, TDEA, IDEA, AES etc.,.

After executing the application several times with different key lengths results were obtained as shown in figure 2.

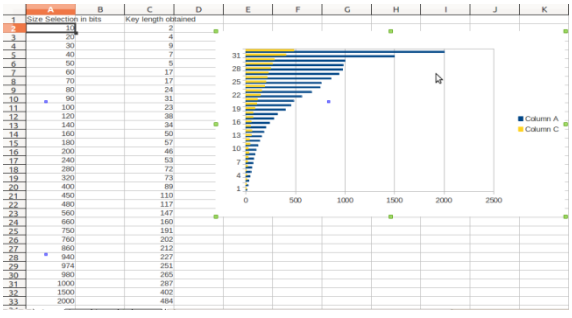

Figure 2 : A run of the application with different key sizes

Inspired by these findings we decided to show the range of key size that could be chosen to be used along with DES or TDEA or AES. These findings are shown in
figure 3.

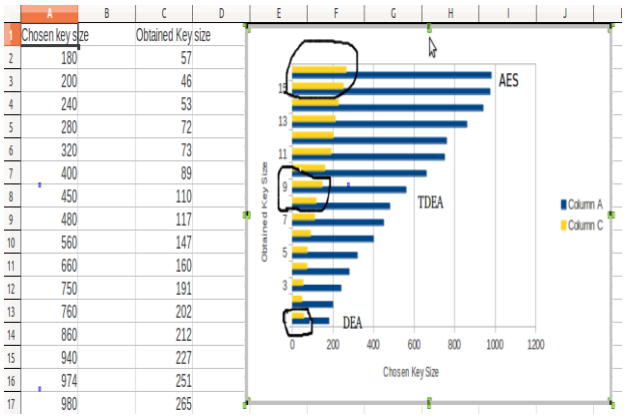

Figure 3: Key Size to be chosen to use with different Algorithms

As seen from the chart above, the user can choose a range of 180-320 to be used with DEA. A range of 400-560 for TDEAand a range of 940-980 is suitable for AES.As the key size obtained is of variable length it may be required to perform a sort of bit stuffing to be able to used for DEA/TDEA/AES.
The modified BB84 protocol combined with Symmetric encryption technology for the exchange of the qubit information provides added security.

4.1 Concerns related to Security

1. The key that is initially used for the Encryption and Decryption must be kept a secret.
2. The communicating parties can also keep the algorithm name a secret to prevent the intruder from trying to recover the key string that will be used for next encryption and decryption.

5. CONCLUSION

A simulation model and also an efficient key management scheme has been proposed for a normal network. This scheme involves a simple Key generation and Key distribution mechanisms influenced by the BB84 protocol while making it possible to be used in a non-optic normal network. It greatly reduces the communication and computation overheads of key setup involved as in Diffie-Hellman Key Distribution Algorithm and RSA. A Symmetric algorithm such as DES was used for the encryption and Decryption of the information that is exchanged between the Sender and the Receiver along with BB84 to further improve the key management scheme for generation and distribution of secret keys. The keys that are exchanged in this manner can be used along with DES, TDEA or AES based on the requirement.

6. REFERENCES

1. "A Modified QKD Approach for Secure Key Distribution Using Quantum Cryptography" Niranjan A. & C.R.Manjunath International Journal Network and Computer Engineering.ISSN 0975-6485 Volume 4, Number 1 (2013) pp. 11-15
2. Miloslav Dusek, Ondrej Haderka,Marlin Hendrych, "Generalized beam Splitting attack in Quantum Cryptography with dim coherent states" optics communication 169 (1999), 103-108.
3. C.H.Bennet & G.Brassard "Quantum Cryptograhy: Public Key Distribution & Coin Tossing"- IEEE, Bangalore, India, December 1984[pp 175-179].
4. Nicolas Gisin, Greoire Ribordy "Quantum Cryptograhy: :Riviews of Modern Physics vol-74, january 2002.
5. C.H.Bennet: "Quantum Cryptograhy using any two non orthogonal staes, physical Review letters,Vol68,pp3121-31124, May 1992.
6. Omer Abd Alkareem Jasim & Anas Ayad Abdulrazzaq "The Goals of Parity Bits in Quantum Key Distribution System"-Volume 56– No.18, October 2012
7. D. Gottesman, H. K. Lo, N. L¨utkenhaus and J . Preskill, "Security of quantum key distribution with imperfect devices", Quant. Inf. Comput. 4, pp.325–360, 2004.
8. K. J. Gordon, V. Fernandez, G. S. Buller, I. Rech, S. D. Cova and P. D. Townsend, "Quantum key distribution system clocked at 2 GHz," Opt. Express 13, pp.3015–3020, 2005.
9. William Stallings, "Network Security Essentials and Standards", Peason education,2000.
10. "A note on Quantum Cryptography", ISSN : 0975-3397 Vol. 4 No. 09 Sep 2012.