Secured IPsec Multicast Architecture Based on Quantum Key Distribution

A.F.Metwaly[1], M. Z. Rashad[2], F.A. Omara[3], and A.A.Megahed[4]

[1]Information Technology Department, Al-Zahra College for Women, Oman
[2]Faculty of Computer and Information Sciences, Mansoura University, Egypt
[3]Faculty of Computer and Information Sciences, Cairo University, Egypt
[4]Faculty of Engineering, Cairo University, Egypt

Dr.ahmedfarouk85@yahoo.com , ahmed@zcw.edu.om

ABSTRACT

Multicasting reveals to the delivery of a message or information from one source to multiple recipients simultaneously through a single transmission channel. Securing the transmitted multicast information can be achieved through IPsec multicast architecture. The process of IPsec involves the sender and destinations to agree on IPsec keys. These keys are used for protection transmitted information among communicated peers over IPsec network. IPsec depends on classical algorithm for key generation and distribution. These algorithms proved their conditional security which means intruder can break the algorithm and intercept the communication process. In this paper, a new IPsec multicast architecture is proposed. The proposed architecture is divided into five main processes. The most important process is key generation and distribution. The key generation and distribution through IPsec multicast network is achieved using quantum algorithms. Quantum keys proved their unconditional security according to their physical characteristics. Sender and receivers communicate through two channels which quantum and classical. Encryption and decryption processes depend on agreed quantum keys and classical cryptographic algorithms. IPsec depends on quantum key distribution for creating keys for IPsec security associations. The confidentiality and authentication of proposed architecture is analyzed

KEYWORDS

IPsec, Multicast, Quantum Key Distribution, Quantum Keys and cryptography

1 INTRODUCTION

IPsec delivers security for IP communications at the network layer of the Open System Interconnections Model (OSI Model). Sensitive information sent over the internet can be encrypted via IPsec to maintain the secrecy of the information. IPsec encrypts data at layer 3 IP packet layer proposing exhaustively secured solution through providing data authentication, anti-replay protection, data confidentiality, and data integrity protection [1, 2]. IPsec consists of set of protocols which each protocol concentrates on particular characteristics of the IPsec purposes to protect IP communications over untrusted networks. Internet key exchange is an example of IPsec protocols which focus on message delivery authenticity as well Encapsulating Security Payload which focus on data confidentiality. IPsec uses encapsulated security payload (ESP) and authentication header (AH) to accomplish desired security objectives [1, 2, 3, 4, 11, 12, 13].

AH is constructed to enhance the security principles by protection IP packet header. The protection objective is delivered by cryptographic authentication [5, 7]. The authentication service confirms that any interference with IP traffic will be identified. ESP provides protection and confidentiality for IP packet data. This protection objective is achieved by encoding the content of data packet using symmetric encryption algorithm as Data Encryption Standard (DES), Triple Data

Encryption Standard (3DES), and Advanced Encryption Standard (AES) [5, 7, 9, 11, 12].

Traditional multicast IPsec architecture's based on classical key generation and authentication. The Diffie -Hellman algorithm is mainly used for securing key transmission over unsafe media, furthermore is used excessively in present key management for delivery keying information for IPsec [1, 2, 17]. Key generation and management based on Diffie -Hellman algorithm impaired from many weaknesses. Firstly, the frequency of changing the distributed keys between the communicated IPsec peers is limited. Secondly, the generated keys are conditional security which means intruder can spy on the communication channel and copy keys without any given warning for the communicated IPsec peers. Lastly, the whole architecture of traditional multicast IPsec deteriorates from man in the middle attack [3, 4, 17]. Many approaches discussed multicast quantum cryptography [23,24]
In 1984, Bennett and Brassard [14, 15, 16] achieved that the transfer of quantum states is very essential for securing communication system. Consequently, they developed the first quantum key distribution method which latterly is known as BB84 protocol. BB84 protocol was applied practically in 1989. Quantum communication delivers an innovative technique for securing the confidentiality and authentication of modern communication systems. Unlike the classical communication, the quantum communication relies on physical characteristics of used quantum signals. Quantum communication security depends on the corresponding quantum physics laws, such as the well-known Heisenberg uncertainty principle and no-cloning theorem [18, 19, 22].

In our proposed scheme, the sender can communicate and exchange information with multiple destinations through a secured IPsec multicast network. The proposed architecture is divided into five main processes. The most important is replacing the classical key generation and distribution by quantum one. The sender and multiple receipts have to go through quantum key distribution steps for generating and distributing keys. Sender and receivers communicate through two channels which quantum and classical. Quantum channel is used for generation and distributing quantum keys. Classical channel is used for negotiation for policies, security associations and security parameters. Encryption and decryption processes depend on agreed quantum keys and classical cryptographic algorithms. The entire process of quantum key generation and distribution inside the multicast IPsec architecture is managed by quantum key distribution. Based on agreed security parameters and policies, sender and receipts starting the negotiation of IPsec security associations. After negotiation is finished, IPsec rely on quantum key distribution for creating keys for IPsec security associations. The confidentiality and authentication of proposed architecture is analyzed

This paper is organized as; in section 2 the preliminaries of Diffie Hellman algorithm, IPsec modes and relation with OSI model, quantum bit, no cloning theory and quantum key distribution are summarized. In section 3 the proposed architecture with steps and its operations is discussed in details. In section 4 the operation of encryption and decryption processes are discussed in details. In section 5 demonstrate confidentiality and authentication analysis. Section 6 concludes the paper

2 PRELIMINARIES

2.1 Diffie Hellman Algorithm

In 1976 Whitfield Diffie and Martin Hellman introduced Diffie-Hellman algorithm [17]. The Diffie -Hellman algorithm is used for securing key transmission over unsafe media, furthermore is used excessively in present key management for delivery keying information for cryptographic algorithms as RSA, DES or

keyed-MD5 (HMAC). It obtains its protection from the complexity of computing the discrete logarithms for each large numbers [1, 2, 13]. Figure 1 summarize the operation of Diffie-Hellman algorithm between two participants called Alice and Bob. The two participants agreed on two random numbers one has small number called generator (g) and other has large number called modulus (p). Every participant randomly create secret (x). According to g, p and x, each participant creates and transmits public values.

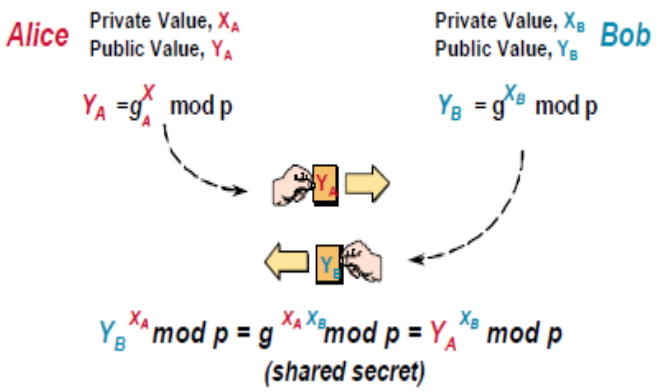

Figure 1. Diffie Hellman Summarized Operation

In Figure 2 demonstrate an example of Diffie Hellman operation with p = 23 and g = 11. The result of common secret key is 8

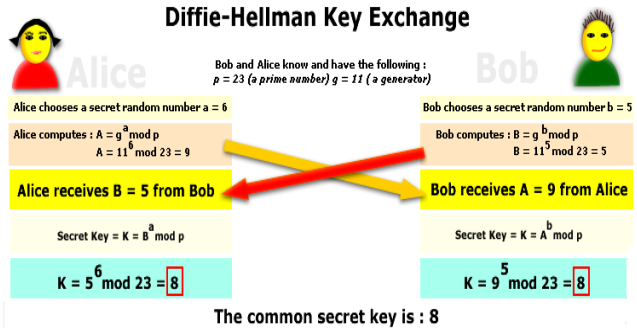

Figure 2. Diffie Hellman Example

2.2 IPsec

IPsec delivers security for IP communications at the network layer of OSI model as well IPsec depends on supportive components for securing transmitted traffic among communicated peers. In Figure 3 showing the encapsulation a de-capsulation process of IPsec and its supportive components over OSI layers.

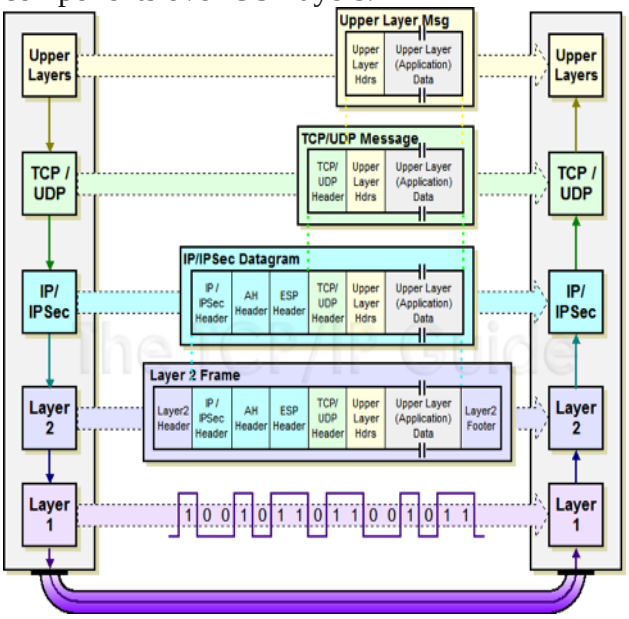

Figure 3. Diffie Hellman Summarized Operation

Encapsulation means when a user sends data, the data is sent down the protocol stack through each layer until it is sent as a stream of bits across the network. Each layer adds information to the data by adding headers. The unit of data that TCP sends to IPsec is called a TCP Segment. The unit of data that IPsec sends to the Network Interface is called an IP datagram. The stream of bits that flow across the Ethernet is called a Frame. Decapsulation is the reverse process of encapsulation and it's done on receiver side. When a user receives encapsulated frame, he extracts each header until retrieve original data sent by sender [1, 2, 3, 4].

IPsec have two modes transport and tunnel as shown in Figure 4. IPsec uses transport and tunnel mode to establish a secure communication channel between network nodes. In transport mode only transport layer protocols which communicate between two

ISBN: 978-1-941968-06-2 ©2015 SDIWC

IPsec hosts together encapsulated using AH/ESP.

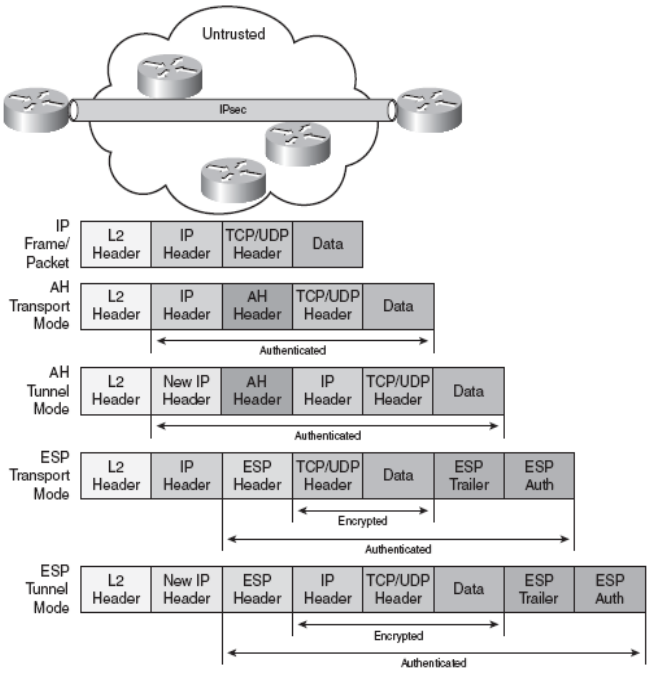

Figure 4. IPsec Modes

In tunnel mode the entire IP packet which communicate between two security gateways encapsulated using AH/ESP and a new IP packet will be generated. Security associations (SAs) are essential to IPsec. An SA is a suite of components including the protocols (AH, ESP or both), encapsulation mode (transport mode or tunnel mode), encryption algorithm (DES, 3DES, or AES), shared key used for flood protection and key lifetime. An SA can be created manually or with IPsec supportive components [5, 6, 7, 8, 13].

2.3 Quantum Bit

The classical bit is the fundamental element of information. It is used to represent information by computers. Nevertheless of its physical realization, a classical bit has two possible states, 0 and 1. It is recognized that the quantum state is a fundamental concept in quantum mechanics. Actually, the quantum bit is the same as the quantum state. The quantum bit can be represented and measured using two states |0> and |1> which well known as Dirac notation [19, 22] as shown in Figure 5.

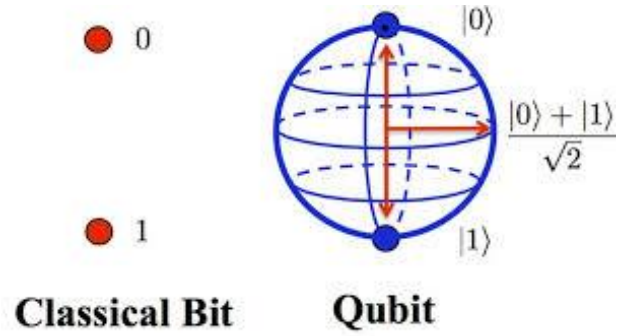

Figure 5. Classical and Quantum Bits

A pure quantum bit is a linear superposition of the basis states which indicates that the quantum bit can be denoted as a linear combination of |0> and |1> [19, 22] using equation 1

$$\Psi = \alpha\,|0> + \beta\,|1> \qquad (1)$$

Where Ψ represents the quantum bit and α , β represents complex numbers.

The quantum bit can be measured in the traditional basis equal to the probability of effect for α^2 in |0> direction and the probability of effect for β^2 in |1> direction [19, 22] which α and β must be constrained by the equation 2 and showing in Figure 6

$$\alpha^2 + \beta^2 = 1 \qquad (2)$$

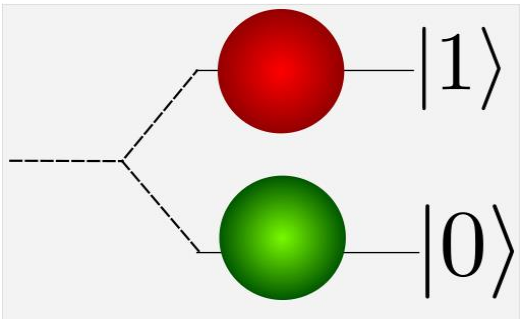

Figure 6. Quantum Bit Measurement

2.4 Quantum Key Distribution

Innovative communication systems depend on cryptographic methods to guarantee confidentiality and integrity of transmitted traffic among communicated peers over the communication network. Basically, cryptographic methods rely on generated and distributed secret keys for encryption, decryption and authentication process. According to Basic characteristics of quantum physics a new model for key generation is initiated and known as Quantum Key Distribution, QKD [19, 20, 21, 22].

QKD uses two channels one is quantum channel and other is public channel. The quantum channel is used for transmission quantum keys through light pulses. The public channel is used for transmission of cryptographic protocols, ciphered traffic and key agreement protocols. By the nature of quantum physics, any attacker that spies on the quantum channel will produce a measurable interruption to the movement of single and continues fire of photons [19, 20, 21, 22] as shown in Figure 7.

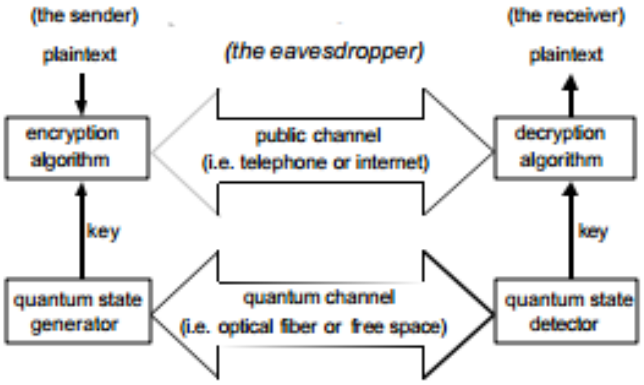

Figure 7. Quantum Key Distribution

2.4 Quantum No-cloning Theory

The quantum cloning [21, 22] is a procedure that takes a random, unidentified quantum state and creates an exact replica without modifying the original state in any way. The process of quantum cloning is specified by equation 3

$$U\,|\Psi>_A|e>_B = |\Psi>_A|\Psi>_B \quad (3)$$

Where U represents the actual cloning action, $|\Psi>_A$ is a quantum state to be copied, $|e>_B$ is an initial state of the copy and $|\Psi>_B$ represents the final copy state which is exact same as the state , $|\Psi>_A$.

In 1982 Wootters, Zurek, and Dieks [18, 19, 22] identified the no-cloning theorem and its deep effects in the quantum computing and associated areas. The no-cloning theorem is a consequence of quantum system which prevents the formation of duplicate copies of an unidentified random quantum bit. The property of quantum no-cloning is a fundamental component in the quantum cryptography, as it prevents eavesdroppers from creating copies of a transmitted quantum cryptographic key. Quantum no-cloning theorem proves that there is no such operation *U* that can perform the cloning operation for any arbitrary quantum state which means an arbitrary, unknown quantum state cannot be copied exactly without altering the original state in any way.

3 The Proposed IPsec Multicast Architecture

The sequence of procedures for communicating between sender and multiple receipts in our proposed scheme

(1) Sender wishes to transmit a packet to multiple receipts simultaneously. Since no security associations created yet for protecting transmitted traffic, IPsec start for creating security associations

(2) Sender's IPsec process starts the Conferring with each receiver's IPsec process. This Conferring involves policy negotiation, transmission of quantum keys for securing established IPsec session and identity verification of communicated participants. This step known as phase one.

(3) Based on agreed security parameters and policies from phase one. Sender and receipts starting the negotiation of IPsec security associations. After negotiation is finished, IPsec rely on quantum key distribution for creating keys for IPsec security associations.
(4) Now , sender and receipts can exchange packets securely over IPsec tunnel
(5) After transmission is over, the established session will be terminated.

3.1 Phase One

The goal of the first phase in our proposed scheme is to exchange the policy , distribute and manage security keys, check the identity of the communicated participants and establish a secured media among the sender and his perspective multiple receipts. With the purpose of finalize first phase, the communicated participants must agree for security factors as verification process, encryption method and key generation process as specified in Figure 8.

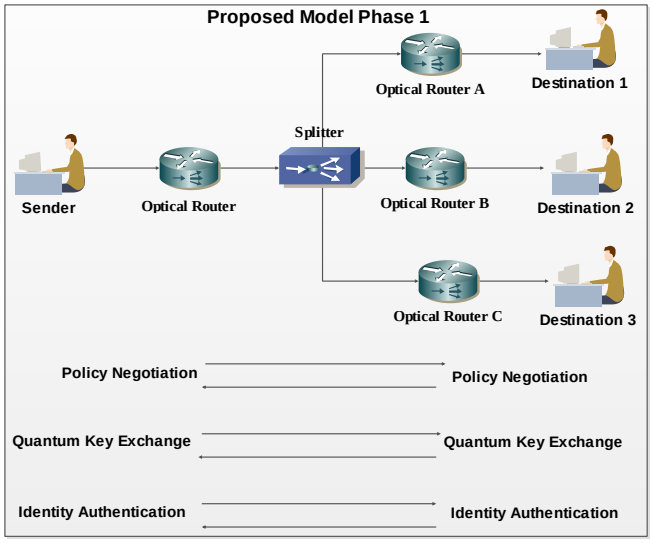

Figure 8. Proposed Model Phase 1 Process

The steps required for establishing phase one is demonstrated In Figure 9 as showing the process of symmetrical key agreement between sender and destination 1

(1) Authentication between a sender and multiple destinations in a multicast network can be achieved through using a pre-shared quantum keys.
(2) Quantum key distribution generates a group of random qubits. Each user derives a private and public keys after negotiation with quantum key distribution through quantum key generation process including key distillation, sifted keys and raw key exchange. Furthermore, public keys are exchanged between the sender and multicast destination users.
(3) Each user produces a shared secret key from their private key and the other's public key. Shared secret key is the generated agreed quantum key
(4) QKD is used to exchange key information as well corresponding methods used for cryptography among the users.
(5) Based on QKD and agreement key material, each user produces an independent symmetrical key.

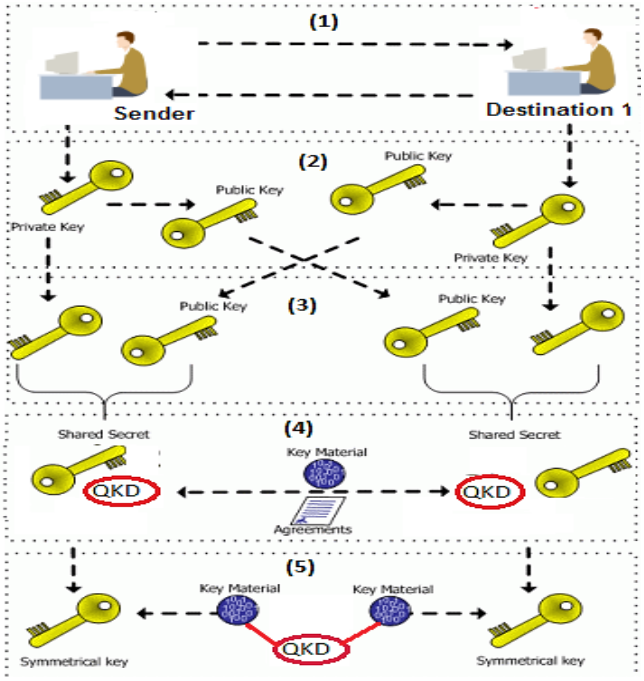

Figure 9. Phase 1 Steps

3.2 Quantum Key Generation and Distribution

The key generation and distribution among he communicated peers will go through four phases. The four phases are Quantum coding, Quantum transmission, Eavesdropper detection and Key distillation as described in Figure 10 and 11.

In Quantum coding phase, the quantum key distribution generate qubits from a quantum source to encode a random-bit string. Each random-bit string encodes with a probabilistic distribution function. The resulted qubits transmitted to the multicast user in the second phase

After having finished the first phase, communicators participate the quantum transmission phase. In this phase the encoded qubits are transmitted physically from the quantum key distribution to the multicast user over a transmission channel. Apparently, a QKD technique requires a transmission channel so that encoding qubits are transmitted from one transmitter to another through quantum carriers. Two common types of transmission channels are optical fiber and open air often used for telecommunication networks and satellite communications respectively. The multicast user generates measurements on received encoded qubits by selecting basis on his realized.

In Eavesdropper Detection phase, during the transmission between sender and a destination; eavesdropper might listen on quantum channel and recover possible secret key bits. Using quantum laws, eavesdropper operation on quantum channel can be detected. Eavesdropping is discovered as follows: An arbitrary subset of the raw key is agreed upon by communicators, and those bits are evaluated openly. If whichever two agreeing bits vary this specifies the existence of an eavesdropper and so communicators go back to stage one. Otherwise, the exchanged bits will be aborted and the rest of the raw key used as the final secret key.

In key distillation phase, both sender and a destination use several bases for measurements purpose. The objective of this step is to recognize and exclude those bit positions where communicators use different bases. These positions are then discarded by both communicators over a public channel. Furthermore, improve the security of the key string by correcting resulted errors during transmission and eavesdropper detection phases.

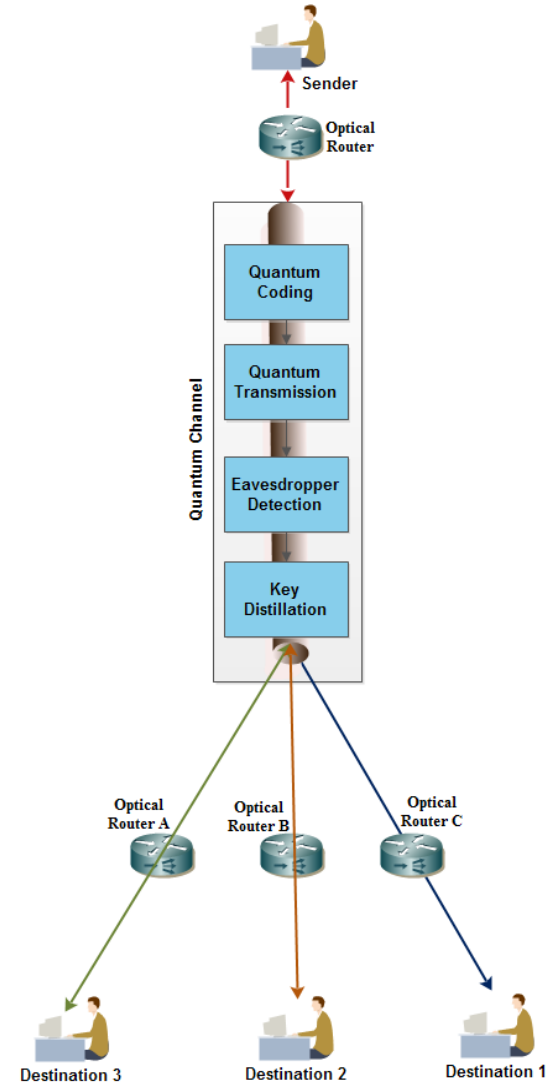

Figure 10. Quantum key Distribution Process

Sender's bit	0	1	1	0	1	0	0	1
Sender's Basis	+	+	X	+	X	X	X	+
Sender's Polarization	↑	→	↖	↑	↖	↗	↗	→
Destination's Basis	+	X	X	X	+	X	+	+
Destination's Measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Figure 11. Quantum Shared Secret Key

3.3 Phase Two

In phase two, IPsec start for protecting the transmitting packets between the communicated participants by negotiation and establishing security associations of IPsec. This achieved by protection of established IPsec policies and appropriate keying information exchanged using Quantum Key Distribution system as shown in Figure 12

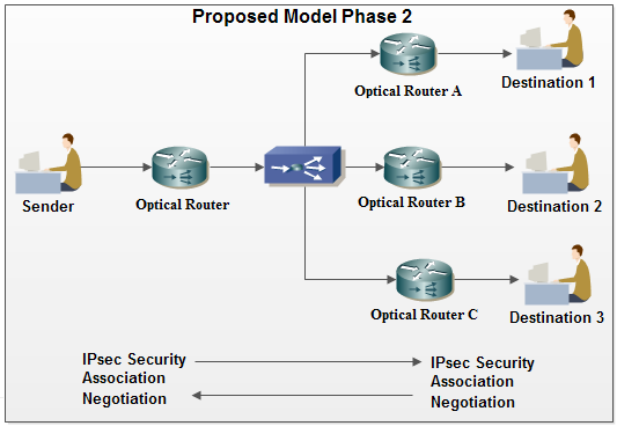

Figure 12. Proposed Model Phase 2 Process

The steps required for establishing phase one is demonstrated In Figure 13 as showing the process of IPsec key agreement between sender and destination

(1) Sender and destinations exchange more key material and agree on encryption and integrity methods for IPsec

(2) Quantum keys are combined with the key material to generate the symmetrical IPsec keys

(3) Symmetrical IPsec keys used for protecting transmitted data between sender and multiple receipts simultaneously

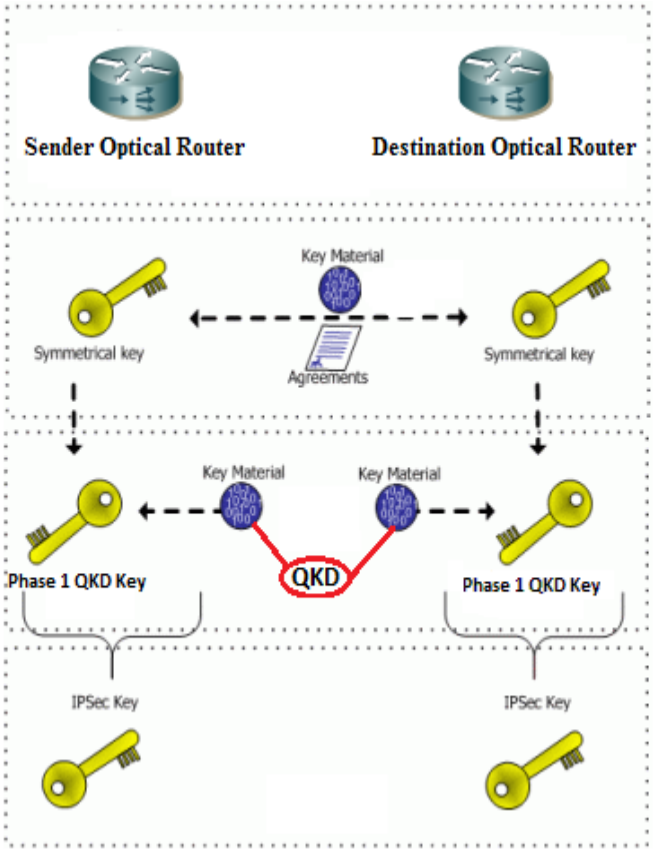

Figure 13. Phase 2 Steps

4 Encryption and Decryption

Before starting a secured communication process between sender and multiple receipts, they must agree upon an IPsec key and keep it secret between themselves. For distributing and generating IPsec keys, sender and destinations are communicated through two channels which quantum and classical channels as shown in Figure 14. Quantum channel is responsible for generating agreed IPsec keys. IPsec keys have to go through quantum key distribution steps to make sure the confidentiality of generated keys.

ISBN: 978-1-941968-06-2 ©2015 SDIWC

Classical channel is responsible for encryption, decryption and authentication processes.

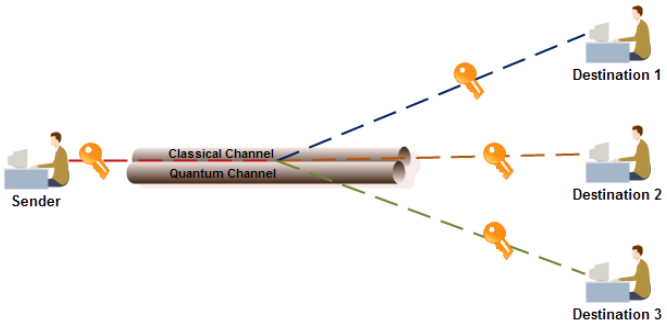

Figure 14. IPsec Key Distribution through Quantum and Classical Channels

These processes depend on generated quantum keys. Sender wish to transmit original message that can be read and understood without any special measures. Encryption of original message is performed at sender side and is achieved by combined original message, sender IPsec key and cryptographic algorithm. A cryptographic algorithm works in combination with a key to encrypt the original message. Encrypting original message results in unreadable form called cipher message. Sender use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data as shown in Figure 15.

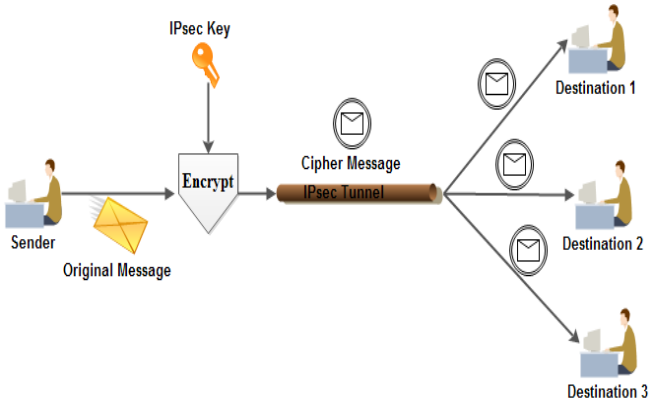

Figure 15. Encryption Process

Decryption of received cipher message is performed at receipt side and is achieved by combined cipher message, receipt IPsec key and cryptographic algorithm. Each receipt use its own IPsec key and cryptographic algorithm. Decryption cipher message results the original message which sent by sender as shown in Figure 16. The security parameters are agreed between IPsec peers before transmitting information between the communicated peers as well after connection is established the transmitted traffic is encrypted through IPsec tunnel.

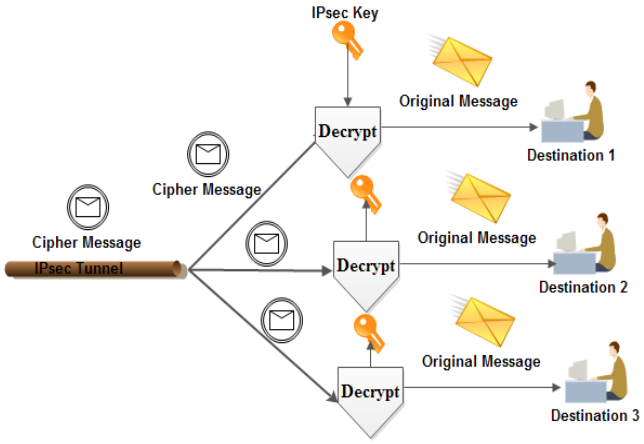

Figure 16. Decryption Process

5 Confidentiality and Authentication

The confidentiality of transmitted messages between sender and multiple receipts over a communication channel is reached based on quantum no-cloning and Heisenberg uncertainty principle. So the eavesdropper or even the intruder cannot retrieve any useable information or be familiar with contents of transmitted messages. According to Heisenberg uncertainty principle when the eavesdropper try to spy the communication channel , the eavesdropper operation intercept the quantum channel and create a result with erroneous probability 50%. So, eavesdropper has no any information about transmitted messages.

Clearly with Diffie-Hellman key exchange, the communicated peers doesn't authenticate each other. So it vulnerable to man-in-the-middle attack. Based on our proposed IPsec multicast architecture, each communicated peer will be

ISBN: 978-1-941968-06-2 ©2015 SDIWC

authenticated before the beginning of transmitted messages. Authentication is done on phase one based on generated shared keys. Authentication mechanism uses combined technique. Which means keys used for authentication comes from quantum and authentication algorithm is a classical one.

6 CONCLUSION

Securing the transmitted multicast information can be achieved through IPsec multicast architecture. Classical multicast IPsec architecture's based on classical key generation and authentication. Classical architecture suffers from man in the middle attacks and conditional security property of the generated keys. A new secured IPsec architecture based on quantum key distribution has been proposed. Which means keys used for authentication and cryptography come from quantum and authentication algorithm is a classical one.
Quantum keys proved unconditional security by no cloning theory which means intruder can't copy the transmitted keys between the communicated IPsec peers. The source of quantum keys is mostly depend on light or laser which means a high exchangeable and changeable rate of keys between the communicated IPsec peers can be achieved. Quantum network proved their ability against man in the middle attack in accordance of quantum key generation process as well Heisenberg uncertainty principle.

REFERENCES

[1] S. M. Bellovin. "Problem Areas for the IP Security Protocols" , "Proceedings of the Sixth Usenix Unix Security Symposium". San Jose, CA. pp. 1–16 , 2006.

[2] K.G. Paterson and A.K.L. Yau. "Cryptography in theory and practice: The case of encryption in IPsec". "Eurocrypt 2006, Lecture Notes in Computer Science Vol. 4004". Berlin. pp. 12–29 , 2006

[3] J.P. Degabriele; K.G. Paterson. "Attacking the IPsec Standards in Encryption-only Configurations". "IEEE Symposium on Security and Privacy, IEEE Computer Society". Oakland, CA. pp. 335–349. 2007

[4] W.Aiello, S.M. Bellovin, M.Blaze, R.Canetti, J.Ioannidis, A.D.Keromytis, and O.Reingold. Just fast keying: Key agreement in a hostile Internet. ACM Transactions on Information and System Security (TISSEC), 7(2):1{32, May 2004.

[5] R. Atkinson. IP Authentication Header. RFC 1826, Internet Engineering Task Force, August 1995.

[6] R. Atkinson. IP Encapsulating Security Payload (ESP). RFC 1827, Internet Engineering Task Force, August 1995.

[7] S. Kent. IP Authentication Header. RFC 4302, Internet Engineering Task Force, December 2005.

[8] S. Kent. IP Encapsulating Security Payload (ESP). RFC 4303, Internet Engineering Task Force, December 2005.

[9] S. Kent and R. Atkinson. IP Authentication Header. RFC 2402, Internet Engineering Task Force, November 1998.

[10] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP). RFC 2406, Internet Engineering Task Force, November 1998.

[11] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. RFC 2401, Internet Engineering Task Force, November 1998.

[12] S. Kent and K. Seo. Security Architecture for the Internet Protocol. RFC 4301, Internet Engineering Task Force, December 2005.

[13] B.Schneier , Applied cryptography: protocols, algorithms, and source code in C. Wiley, New York, (1994)

[14] C. Bennett , G. Brassard, S .Breidbart, et al, Quantum cryptography or unforgeable subway tokens. Advances in Cryptology-Proceedings of Crypto 82, Santa Barbara, California, 24 – 26 August 1982, pp 267 – 275 (1982)

[15] C. Bennett and G. Brassard.An update on quantum cryptography.Advances in Cryptology-Proceedings of Crypto 84, Barbara, California, 19 –22 August 1984. Lecture Notes in Computer Science (LNCS), Springer, Heidelberg,196: 475 – 480, (1984)

[16] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J.Smolin,Experimental quantum cryptography. Journal of Cryptology, 5: 3 – 28, (1992)

[17] W. Diffie, M.E. Helman , New directions in cryptography. IEEE Transactions on Information Theory, 22(6): 644 – 654 , (1976)

[18] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned.Nature (London), 299: 802 – 803, (1982)

[19] G.H. Zeng,Quantum cryptology. Science Press, Beijing, (2006)

[20] A. Shields and Z. Yuan ,Key to the quantum industry. Physics World, 20(24): 24 – 29, (2007)

[21] G.V. Assche, Quantum cryptography and secret-key distillation using quantum cryptography. Cambridge University Press, London, (2006)

[22] G. Zeng, Quantum Private Communication, Springer ,Berlin-Heidelberg, 2010

[23] A.F. Metwaly, M.Z. Rashad, F.A. Omara, A.A. Megahed, Eur. Phys. J. Special Topics 223(8), 1711 (2014)

[24] A.Metwaly, M.Z. Rashad, F.A. Omara, A.A. Megahed, Architecture of point to multipoint QKD communication systems (QKDP2MP). 8th International Conference on Informatics and Systems (INFOS). Cairo , NW-25-NW-31,2012