The Role of Quantum Cryptography under Distributed Protocols for Secured Communication in Ad Hoc Networks

Rajaram Jatothu1,
Research Scholar1 , Department of Computer Science and Engineering ,
Sri Satya Sai University of Technology and Medical Science, Sehore,
Madhya Pradesh , India
rajaram.jatothu@gmail.com

Dr. R. P. Singh2
2Department of Computer Science and Engineering ,
Sri Satya Sai University of Technology and Medical Science, Sehore,
Madhya Pradesh , India

Abstract : Most of the cryptographic methods employed so far has been using symmetric and asymmetric cryptography, and had involved cryptographic keys extensively. Usually it is observed that many of the cryptographic algorithms are infeasible as the key distribution system is feeble. As an emerging approach Ad Hoc networks is subjected to Quantum cryptography concept or quantum key distribution in distributed environment and has drawn a good attention as an appropriate solution to the Key Distribution issue. QKD extends unconditional secured inter-communication by means of quantum mechanics. The paper focuses on quantum theory as a substitute to conventional key distribution protocols and a comprehensive narration is offered illustrating implementations of quantum key distribution protocols. This paper depicts quantum key distribution protocols (QKDP) to preserve safety in large and Ad hoc networks, guiding towards novel direction. It is aimed to narrate the efficiency of communication in terms of effort, security, suitability and confidentiality by the use of QKDPs.

Keywords: *Communication, wireless, quantum cryptography, authentication, quantum key distribution; Ad hoc, protocol.*

*****

1. Introduction

The wireless networks do not possess any limitations and boundaries, hence, they are much liable to be exposed to security threats than the wired systems. It is evident that there is clear probability that an intruder to sneak on secret communications or alter the information to obtain access to the wireless or mobile networks. Consequently, offering secured communication for networks has turned into one of the chief concerns. The IEEE has introduced to the previous release of 802.11 standard or norms in 2004 release i.e. 802.11i. Since , then previous version is found to be obsolete and found to have security disadvantages in the terms of authentication and confidentiality. Quantum Key Distribution rely on quantum cryptography and offers to undertake unconditional security. QKD extends a provision to two parties to share a random bit string identified by both only, which could be utilized to transform messages in terms of encrypt and decrypt process.

Cryptanalysis is a pertinent stream of e study of cryptography, which includes now Classical Cryptography along with the Quantum cryptographic systems. In paper analyzes the security of Quantum Key Distribution Protocols proposed in the recent times, and point out how effective and simple they are for implementation than the conventional Cryptographic algorithms. The main focus is on operations on key generation and measurement in the trusted environment using DKD. In symmetric key encryption process, the intruder is restricted from gaining the confidential messages between the valid users. It is evident that the eavesdropper might entirely obtain the session key by transmitting the bits as fake signal to sender making the sender commit mistake of trusting the intruder. The means that attack procedure is like a dense-coding interaction amid between Eve and sender, wherein a particular measurement basis is engaged[4][1].

An ad-hoc network is the mobile network of the modernized age. It is the accumulation of mobile hosts that goes wireless without any assistance of integrated administration or a well-established foundation to form a momentary network. There is a necessity for the mobile hosts to aid the transfer of packet to its final destination in such networks because of the limited range of transmission in the wireless networks of the mobile hosts. To ensure secure communication in Ad hoc networks, there is a need to authenticate the user globally by providing security characteristics like cryptography, privacy and reliability[11][3].

Quantum cryptography is a novel approach in the contemporary world that was established to safeguard the privacy and confidentiality of data which will be shared among two parties. More often than not, these two parties are theoretically named as Bob and Alice and by this technique one can attain the faulty or illogical action done by them. The quantum system of communication provides virtual encryption that lasts for ever. As opposed to the classic encryption that transmits the secured information over the network, the quantum cryptography system splits the key of encryption from the information to transfer. In this way, the intruder cannot decipher the key even he/she have access to the information. Nevertheless, quantum encryption can be responsive to hacking according to the researchers. In quantum cryptography, the classic assumption is that the two parties, Bob and Alice use the detectors and sources of photons that make them trust each other completely which in turn provides them with a secure region that no one can intrude, whereas the connecting channel between them can be manipulated by other intruders or opponents[5][7].

2. Basic Distributed Protocols for Networks

The two basic issues of distributed protocols are[1] :

1. No global state possible , this means the knowledge about the current state of any process cannot be precisely ascertained .
2. The time factor relating to the process clock cannot be defined in a global scenario.

In spite of these inconsistencies in real time application implementations, following are some of the conventional principles to achieve the synchronization under distributed systems[6].

A. Causal relations : This is a synchronization relation to serialize the processes.

It uses a relation i.e. a happens-before b if either:

- *Event a* and *b* take place on the same node and *a* take place before *b* in the program.
- *Event a* sends a message on sender node and event *b* receives the same message on the target node.
- There exist a transitive link between *a* to *b* based on two cases mentioned above.

B. Lamport clocks

- Lamport clocks were also popular for synchronization , wherein every local event increments the value of local clock
- Every message is expected to carry the message sending timestamp
- Whenever a message is reached the destination process sets the clock onward, so that the local clock has bigger time than message timestamp
- Process Identification could be used to tie-break to gain complete strict order
- Employed for gaining sequential stability or consistency.

Vector clocks

Vector clocks are the variant of Lamport clocks with additional functionality:

- Every timestamp dealing with event for the process in recorded as a clock into a vector;
- The incrementing is done by the local clock processing;
- By receiving a message all the clocks are set to forward.

C. Consistency models

This model is used when there is a requirement of shared memory concept and need arises for broadcasting of events to n number of nodes seamlessly.

- Sequential consistency: all the events appear to happen in the identical order for all processes;
- Casual consistency: two events that are casually associated emerge in the casual order for all processes;

concurrent events may become visible in different orders for dissimilar processes.

- Aquire/release model of consistency

D. Distributed transactions

- Completes in 2 phases;
- Phase 1: At the end, every process sends a message "ready" or "failed" to the process coordinator; if the message happens to be ready, the process can commit;
- Phase 2: The coordinator transmit "commit" or "abort" signal

3. AD Hoc Networks

An ad Hoc network is a type of Local Area Network (LAN) that is assembled by integrating the devices over the network with the medium of wireless and mobile connections. It neither relies on any central control nor any prior infrastructures unlike wired networks. Hence, these kind of wireless networks are named as ad Hoc networks. It

sets a novel example for wireless communication on mobile hosts. The mobile devices or the nodes which come under the range of the radio waves tends to detect the network spontaneously and can directly correspond with the hosts over wireless networks. The factors that make an ad Hoc network more pertinent to situations of crisis are its rapid formation of network and minimum configuration. The ad hoc network follows a certain security model that incorporates the following essential aspects that are required for a secure communication[10][11].

i) SECURITY

For a network to be reliable, it needs to be secure first. The main attributes of security used in the ad hoc networks are its confidentiality, reliability, accessibility, non-repudiation and substantiation.

ii) RELIABILITY

It is mainly important for crucial aspects of safety and also the manipulation of financial activities of data. The information or data that is made significant might be abolished resulting in inaccessibility. It denies the authorized people to attain the necessary information .

iii) ACCESSIBILITY

The service oriented architectures which wholly depends on the information and data transferred, accessibility is the major aspect. It is the primary feature of the network as the total business depends on the wireless network connections or else they encounter the denial of service attack.

iv) SECRECY

It is the aspect that mainly concerns with the security and disclosure of information that is sensitive. It is ensured that this sort of information is never leaked to unknown sources, if so then the consequences will be disastrous. The information that is passed over a channel in a wireless network must be carefully transmitted as that info may also be essential to the end users and it would definitely be a threat if its accessed by enemies.

v) ATTACK USING FABRICATION

During the transmission of the mobile packets in the wireless networks, there are also the data packets which are created falsely into the wide area network. These messages are known as fabrication messages and are very difficult to identify.

vi) NON-REPUDIATION

It is an attack in which either the sender or the receiver cannot deny that they have neither sent nor received any messages which they have or haven't. It is mainly helpful for exposing and isolating the nodes that are compromised .

4. Modern Distributed Algorithms Using MANETS

A). Mobile Ad Hoc network (MANETs)

The modern mobile application are based on the scenarios extended by the MANES dynamic topologies which changes the network dynamically by means of arrival/leaving of nodes in a network. Following are the scenarios utilized by the Ad hoc networks to create and function[1] :

(i) MANET Initialization

All the nodes in Ad-hoc wireless networks share a familiar wide band communication channel, permitting all the nodes that have data to transfer simultaneously hence, results in a poor throughput, as a plenty transmissions would not receive correct data owing excessive interference. The Medium Access Control (MAC) system is can be employed to resolve the problem. The MAC permits a subset of the nodes craving to transmit at any specified time. A superior MAC algorithm plan the transmissions in a way to enhance the data throughput in a network by avoiding delays, and controlling the level of fairness. It is achieved through a central controller[10].

(ii) Joining new nodes in the network

Adding is not an easy task in a MANET as the data is subjected to collision and congestion. In a large network, the distributed algorithm employs a TDMA based channel i.e. control channel (CC) running parallel to data channel. The algorithm role is to sense every node and need to "know" its immediate neighbours under one-hop distance. The CC consists of n mini-slots, one slot for every node in the network. The nodes make use of CC to swap control information with their neighbours, every node should know only the mini-slots allocated to its neighbours. It is evident that there is a definite need for a central entity to control the TDMA frame, which would read, add nodes, control the size of the network and transmit the information to every node.

(iii) Graceful exit of nodes

The member node of MANET may depart the network at any point of time. Node departure must be a graceful act. In case of departing nodes they must inform other MANET nodes about the departure event and surrender their IP address. It is obvious that node congestion or network partitioning may suffer due to abrupt departure of the node.

In that case the remaining nodes are accountable ultimately for detecting the leaving and regaining of IP address from the departed node(s).

iv) Abruptly departure of the nodes

If a node member of MANET, with a given IP address crashes unexpectedly or depart the network. In this case it does not have any opportunity to transmit a Address_Cleanup message to any other nearby MANET nodes. In such situation the other nodes maintain to consider that crashed node is still part of the MANET and continue to have their allocated sets. For example, let initiator node j begin a process to configure a freshly arrived node. The node j floods an Initiator Request message to every MANET node and expects a clear reply in turn from all other nodes, including the crashed i node. In this case as the node has already departed it would never send a response to node j. This exercise to initiated by all the nodes now and then based on the protocol chosen is to ascertain the departed nodes in the neighborhood.

(v) Concurrent Address Requests

If a node gets concurrent IP address requisitions, and if it possess a nonempty free ip set, then it allocates disjoint IP address blocks from its free ip set to the requesting nodes. If two allocators perform IP address reclaiming concurrently , then one of them defer allocation process. To explain this , Let us assume two allocators be X and Y with X's IP address higher than Y's. Let both the nodes flood the network with Free Address messages. A node that receives the TentativeFreeAddresses message from Y prior to X, sends a NoConflict / ConflictNotification message (based on whether there is conflict amid its address and addresses in the broadcast message) to Y and a Defer message to X. A node that gets a TentativeFreeAddresses message from X earlier than receiving that from Y, responds with NoConflict / ConflictNotification message to both the allocators . The X suspends the IP address allotment process on receiving a Defer message. While Y continues the IP address allotment process. After finishing the address assignment process, Y sends the IPAddressUpdate message to every nodes in the network. The nodes that had sent the Defer messages to X, now transmit Resume messages to X. Node X, on receiving the Resume message, rebroadcasts TentativeFreeAddresses
signal and maintain the address reclamation procedure. After the reclamation process at Y, free ip sets at nodes in the network may have altered. Therefore, it is probable that the addresses that were in absent addresses set of X are either in usage or are in redistributed between nodes to create their free ip set. By means of rebroadcasting TentativeFreeAddresses after suspension, it is assured that X has the updated network related information. In the nonexistence of such Defer messages, the timer at the allocator would have elapsed and the allocator process at would continue to lead the duplicate IP address assignment. The approach described above avoids such duplication.

(vi) Migration of the Requester

Let X be a requester moved away from the allocator node Y before Y could allocate an IP address to X. Node X sends node Y' s IP address to the fresh allocator , say Z node. The node Z sends IPAddressForward message to Y. The node Y, on obtaining the IPAddressForward message, updates the entry for the respective transaction id in the transaction info_set record with the IP address of Z node. Node Y then sends the IPAddressAssign message to node X through node Z. Alternately , the previous allocator Y could terminate the IP address allotment process when the requester drift and the new allocator Z begins the allocation process freshly. In the previous concept, the communication overhead is condensed by retaining state information at the nodes. The latter theory do not maintain such state information however, it requires the address allocation process to be initiated all again.

(vii) Loss of Messages

The loss of message is apparent similar to abrupt node departure. The solution for such problem can be resolved in the same pattern employed for the abrupt node departures. The event initiator keeps on retrying for a maximum number of request response retry times. If the message loss is due to a constant communication crisis in the MANET, any one of the retry attempts would succeed in gaining a response. Though, there will be a message loss situation wherein the initiator might not be of great help. Assume IP address x be allotted to some node. Let the flood of message about this allocation fail to arrive at some of the nodes in MANET. Subsequently, those nodes do not append x to their corresponding allocated sets. At those nodes the allocated pending timer is connected with x will conclude and x will be removed from the respective allocated pending sets. Thereafter , one of those nodes can operate as an originator and suggest that address x can be allocated to freshly arrived node. In this address assignment stage, at least one node which has received the previous flood about x's assignment will refuse the request. Hence, the probability of duplicate address assignments can be prevented.

(viii) Partitioning of network followed by merging

During MANET process, nodes can divide from a network and form or join other networks. These networks can afterward combine into one. In order to sense merging of networks, each network needs a unique identifier i.e. network id. The network id of the network initially has 4-tuples: Initiator's IP address, Initiator's MAC address, random number , timestamp, where Initiator happens to be the first node that creates the network. The possibility of two nodes possessing exactly same MAC address is very low. The probability of nodes retaining the same MAC address receiving allocated identical IP addresses with equivalent timestamps is still lower. When a random number field is added to the 4-tuple, then the probability of redundant network-id is insignificant. Thus, for all realistic reasons, network ids can be taken as unique.

B). CDS - Connected Dominating Set (CDS)

CDS is extensively used theory by various protocols for broadcasting and routing in MANETs environment.
It is based on computations of dominating set in a given network. Assume all nodes in a MANET are distributed in a 2-Dimensional plane and possess an identical maximum broadcast range which can be set during the simulation based on the need. This algorithm initiates with every host holding no information of the neighbourhood nodes and also uses one-hop neighbour data in the later part of the algorithm post broadcasting stage. When the information is attained from its neighbour nodes, every node organizes the neighbour nodes in the descending order by means of number of neighbours to it. The algorithm then begins from the node with highest number of neighbours and starts the marking process which continues till all the nodes in the MANET are covered. The CDS algorithm maintains node mobility capably as compared to other similar algorithms. The experimentation has exhibited the results and has validated that CDS algorithm constructs a set with reasonable size and very low message overhead.
The CDS algorithm comprise of 3 stages and requires no neighbourhood information to begin with.

• Broadcasting: Originally, every node in the network has nil information about its neighbour. The algorithm starts with broadcast of packets that consists of count of neighbours (initially set to zero for every node) with a node ID (MAC address). After some period of time, which is determined based on broadcast range of every node, every node contain information concerning its one-hop neighbours and their subsequent MAC IDs.

• Sorting of nodes: N(v) is the number of open neighbours of node v. Nodes in V are now sorted and arranged in the decreasing order of the number of neighbours they have. The node with the highest number of neighbours will be placed first followed by the node with next highest number of neighbours.

• CDS formation: There are two major phases in the arrangement of CDS. The first phase executes the coloring process and the second stage concludes the CDS process .

Phase 1:

1. All nodes denoted by V are initialized with color white.
2. The first node in V set alters its color to black and transmits a notice to all its neighbours. On receiving this indication, the white neighbours of this node is modified to gray color.
3. Consider the second node in V. 3.1, if it has white color, then replicate the above procedure.
- If it has gray color, then test for any white neighbours. If yes, then the color of the second node is altered to black and its white neighbours turns gray after receiving the warning from the second node.
4. The above procedure continues till there are no white nodes in the network. The noteworthy issue to understand is that this phase is conceded only until the network gets worn out of white nodes hence, it is not needed to check all the nodes in the network. This would save computation time.

5. Following above steps once completed, if some gray node in the network is identified which has at least two black neighbours, it is a probable contender for a CDS and thus, it must be colored with yellow.

Phase 2.

1. Make sure that yellow nodes persist in the network, and if they are present

- If the neighbours of the yellow node are not at all there in the neighbour set of both of the two black neighbours, the colour of the node is transformed from yellow to black color. If not, the colour is altered from yellow to gray.

2. If a black node has at least two black neighbours,
- If the neighbours of the black node are all there in the neighbour set of both the two black neighbours, then the colour of the node is altered from black to gray.
3. Now, ultimately every black node in the network creates a CDS.

 ISSN: 2321-8169
1089 – 1096

5. Quantum Key Distribution for Secured Ad hoc Networks

Quantum Key Distribution (QKD) deals with the challenges posed by the Ad hoc networks by employing quantum properties to swap secret information between properties with cryptographic keys[2]. The protection of QKD depends on basic laws, which are invincible to increase the computational influence, fresh attack algorithms or quantum based computers. It is secured against the arbitrarily dominant eavesdroppers. QKD efficiently faces the challenges met by the classical key distribution concepts, by offering a verifiable secured cryptographic building blocks for remote parties to distribute cryptographic keys. In order to introduce highest security requirements, QKD enables the nonstop generation and sharing of actual random one-time pad keys as shown in figure 1.

Quantum Key Distribution (QKD) protocols offers a means to two parties, a sender, Alice and a receiver, Bob to commonly share an unconditional secured key in the presence of eavesdropper say Eve. Contrast to the classical process of key distribution that depends on unverified computational hypothesis, the security of QKD protocols is assured by the philosophy of quantum mechanics[8][9].

The trespasser or the eavesdropper is commonly termed as Eve, attempts to interrupt or grasp the message travelling in the channel, then finally the data is segregated into bits and will show up a variation in the pattern that would be noticed by both the valid parties i.e. Bob and Alice. This notice is adequate for them to identify that the route has been compromised due to interception by the intruders. If no interception is detected, then the secret key and the related data is assumed to be intact and the channel is expected to be safe for transferring messages that are encoded via unreliable channels.

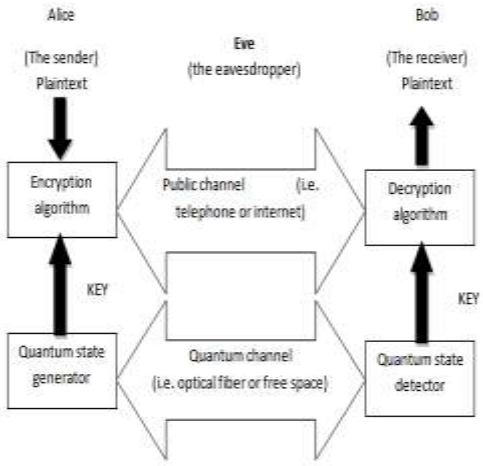

Figure 1. QKD communication System for secured transmission of random key

The working principle QKD:

The security of QKD relies on a fundamental attribute of quantum mechanics. The act of determining quantum of a system is lengthy and may disturb the system. Thus, an intruder tend to intercept a quantum swap will unavoidably leave noticeable traces. The rightful exchanging parties can choose either to abandon the corrupted information, or to decrease the information accessible to the eavesdropper to nil by distilling to a smaller key.

The coding of QKD usually involves the steps or the components given below:

- Information leakage and errors of potential information are removed during ensuing error correction and privacy strengthening post-processing steps, extending both valid parties to share a key known only to them.
- A fiber or free-space quantum path to transmit quantum states of light among the transmitter (Alice) and receiver (Bob) is extended.
- A public but authentic communication connection between the two parties to perform post-processing steps and distil an accurate and secret key is establishment.
- Key exchange protocol that uses its quantum nature to guarantee security by discovering eavesdropping or errors, and by computing the quantity of information that has been interrupted or lost.

The safety and protection of the Quantum Key Distribution systems is finite and counts on the three ideal hypotheses. The first one is the primary confidentiality of the password, secondly is the accuracy and integrity of the quantum ideology and the last one is the trustworthiness of the devices used in the systems of quantum communications.

There may be a possibility of exploitation by an alert hacker that precedes the transmission deficiency in the quantum systems of communication, if the physical world mechanisms and devices fail to be hundred percent dependable and stable. For instance, at any time of action if a photon is identified, then the indicators of photon present in the Quantum Key Distribution systems must notify either by a click or a snap with a certain expectation of encountering a photon. In a more regular use, the device detectors are blocked or darkened not by a click or snap but by a very strong pulse of light. The opponent misuses this strong pulse of light to control these device detectors from very far off sights. This hacking methodology of using

 ISSN: 2321-8169
1089 – 1096

comparable bright light have a led a way to an interesting field of study known as device-independent cryptography. This study explored the ways of security concerns of the quantum encryption techniques being independent of the authenticity concerns of the detector devices. In this cryptography, the attention towards security and privacy of the quantum systems is primarily based on the direct and perceptible interaction among the sender and receiver parties and this provides the security proof of the system. In between this interaction provided that they generate appropriate equivalence despite the fact of blocking out the detectors, the secret key or password can be derived from them. It is quite opposite to the conventional approach of calculating the security of quantum encryption where only the cases are considered corresponding to the actual hypothetical specifications.

The current research works presents the concept-based computations of the Quantum Key Distribution systems that demonstrate the security factors independent of device. The latest technique that provides evidence to possibly evaluate the system's security is attained through the concept of failure probability. This makes it likely to form assertions upon the statistic figure of specific Quantum Key Distribution systems.

The concept of Quantum Key Distribution also depends upon the classic theory of information apart from the basic standards of quantum physics. The secret key or password distributed between the two parties ought to be both private and common. Initially, the errors caused during the data communication must be rectified by recognizing the source of causing them by the intruders or also due to any weakness or flaws in the system setup. Secondly, the trace of key must be unknown to the intruder or an eavesdropper. Secret-key distillation, a technique from classic theory of information must be used to attain these two goals. The approach of both Quantum Cryptography and Quantum Key Distribution are identical. Quantum cryptography involves applications of quantum mechanics pertinent to cryptography like quantum secret sharing whereas the idea of the secret key is principle to the cryptography theory in which the Quantum Key Distribution intends to a play a major role. Table 1 depicts the list of some mechanisms using QKD principles.

Table 1. List of some protocols using QKD concept

No	Year	Name of Protocol	Principles	Applications
1	1984	BB84	Heisenberg Uncertainty Principles	It uses Photon Polarization state to transmit the information it has four polarization states (0^0,45^0,90^0,135^0).
2	1991	E91	Quantum Entanglement	It uses entangled pair of photons
3	1992	BB92	Heisenberg Uncertainty Principles	The only difference between the BB84 is that only two states are necessary rather than four polarization states i.e. (0^0,45^0)
4	1999	SSP	Heisenberg Uncertainty Principles	It is BB84 protocol with an additional basis i.e. it has 6 states are ±x, ±y, ±z on the Poincare sphere
5	2003	DPS	Quantum Entanglement	It has certain advantageous feature including a simple configuration, efficient time domain use and robustness against PNS attack
6	2004	SARG04	Heisenberg Uncertainty Principles	It is an equivalent to BB84 but more robust when using attenuated laser pulses instead single photon sources. The QBER of SARG04 is twice that of BB84 i.e. more sensitive to losses. But provide more security than BB84 in the presence of PNS attack
7	2004	COW	Quantum Entanglement	To work with weak coherent pulses at high bit rates. The setup is experimentally simple and tolerant to reduced PNS attack Hence no information will be lost
8	2009	KMB09	Heisenberg Uncertainty Principles	In this two parties used two bases: one for encoding '0' and the other for encoding '1' instead of using two direction of one single base
9	2012	S09	Public private key cryptography	It allows massive key distribution between n-1 computers and one key message distribution centre.

Conclusion

This paper discuses a distributed, dynamic host configuration protocols for MANET. The protocol extends facility to MANET nodes to configure the networking elements for entering , leaving , allocating, message loss, migration, partitioning parameters for old and new nodes in the network. The study has revealed the limitations and solution approaches to the problems faced in the Ad hoc networks. The paper further highlights some security issues that are relevant to MANET protocols. The distributed protocols and some of the popular Ad hoc networks mechanism have been discussed . Finally the Quantum Key Distribution for Cryptographic security has been discussed which is emerging as an ultimate solution for secured networks.

References

[1] Distributed Network Protocols by Adrian Segall, Senior member IEEE, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-29, NO. 1, JANUARY 1983.

[2] Pratap M S, Drishya Nair, Ponnu Narayanan, Nitha Kamar, Aneesa C V, Three Party Authentication Using Quantum KeyDistribution Protocol by International Journal of Advanced Networking & Applications (IJANA).

[3] D N Kartheek, M Abhilash Kumar, M R Pavan Kumar, Security Using Quantum Key Distribution Protocols (QKDPs) by International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012.

[4] Suganya Ranganathan1, Nagarajan Ramasamy2 , Senthil Karthick Kumar Arumugam3, Venkateswaran Radhakrishnan6, and Ramesh Karpuppiah7 , A Three Party Authentication for Key Distributed Protocol UsingClassical and Quantum Cryptography, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 5, September 2010.

[5] Gabriela Mogos, Quantum Key Distribution Protocol with Four-StateSystems – Software Implementation, Procedia Computer Science 54 (2015) 65 – 72.

[6] Yoshito Kanamori1 and Seong-Moo Yoo, Quantum Three-Pass Protocol: Key Distributionusing Quantum Superposition States, , International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009.

[7] Introduction to Quantum Cryptography and Secret-Key Distillation.

[8] Gilles Van Assche , Quantum Safe Cryptography and Security-An introduction, benefits, enablers and challenges, ETSI, June 2015.

[9] Shirantha Wijesekera, Quantum Cryptography for Secure Communication in IEEE 802.11 Wireless Networks, June 2011.

[10] Sumee Rai, Nidhi Tyagi and Pradeep Kumar ,Secure communication for mobile Adhoc network using(LPIT) Lagrange polynomial and Integral transform withExponential Function , International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163Volume 1 Issue 6 (July 2014).

[11] Gaurav Vishwakarma, Ensure Secure Communication in Ad Hoc Network by, International Journal of Wired and Wireless Communications Vol.2, Issue 1, October, 2012.