DOI : 10.15613/sijrs/2016/v3i2/157299
ISSN (Print): 2349–8919
ISSN (Online): 2350–0999
ScieXplore: International Journal of Research in Science, *Vol 3(2), 57–65, July-December-2016*

Quantum Based Cryptography for Secure Data Communication in Mobile Ad-Hoc Network

S. Sangeetha* and S. Sathappan

Department of Computer Science, Erode Arts and Science College, Erode – 638112, Tamil Nadu, India;
sgeethact2k7@gmail.com, devisathappan@yahoo.co.in

Abstract

A Mobile Ad-Hoc Network (MANET) is an infrastructure-less network of mobile devices that are linked without any wire. Every mobile device in MANET moves in any direction. Security is a key problem in MANET of providing the secured communication with routing and packet forwarding process. In order to improve the security during the data communication, Quantum Key Distribution based Secured Data Communication (QKD-SDC) technique is designed in MANET. In QKD-SDC technique, quantum based cryptography used the quantum mechanics for secured data communication. Initially, Quantum based Cryptography performs Quantum Key Generation and Quantum Key distribution process. In Quantum Key Generation process, quantum key is generated and the key is shared to the receiver. With help of the quantum key, the original data gets encrypted as qubits. In Quantum Key distribution process, the qubits are sent to the receiver end through quantum communication channel along with the quantum key. At the receiver end, when the quantum key gets matched with receiver's quantum key, the qubits are decrypted to obtain the original data. When the key is not matched, the qubits get dropped. This in turn helps to improve the secured data communication in quantum communication channel. Experimental evaluation of QKD-SDC technique is carried out with the performance metrics such as data loss rate, throughput and time for secured data delivery. Experimental analysis shows that the QKD-SDC technique is able to reduce the data loss rate and also improves the throughput when compared to the state-of-the-art works.

Keywords: Mobile Ad-HOC Network (MANET), Quantum Key Generation Process, Quantum Key Distribution Process, Quantum Communication Channel, Secured Data Communication

1. Introduction

A Mobile Ad-hoc Network (MANET) is a collection of mobile nodes that do not depend on the predefined infrastructure. In MANET, nodes communicate with other nodes that are within their radio range and by using routed messages to communicate with nodes that are not directly accessible. This flexibility makes sure that mobile networks can be set up in an Ad-hoc manner where there is no infrastructure available. In MANET, ensuring a secure communication and also provides security properties such as authentication, secrecy, integrity are significant. Recently, many research works have been developed for secure data communication with the help of different techniques in mobile networks.

2. Literature Survey

Secure secret key agreement protocol Ning Wang, Ning Zhang et al.,[1] was designed with three-node cooperative wireless communication system over block-fading channels. The key agreement scheme attained the positive secret key rate while the adversary has higher channel provisions. But, the data confidentiality and data integrity was not guaranteed for secured communication.

An Aggregated-Proof based Hierarchical Authentication scheme (APHA) was introduced to Huansheng Ning et al.,[2] for attaining enhanced data confidentiality and data integrity with the directed path descriptor and homomorphism based Chebyshev chaotic maps. Homomorphism based Chebyshev chaotic maps

**Author for correspondence*

created the trust relationships of lightweight mechanisms and used dynamically hash values to attain the session freshness. However, key agreement protocol causes other channel noise utilization by adversaries.

A novel Self Organized B+ Tree Indexed Key (SOBTIK) mechanism is proposed Sangeetha S and S Sathappan[3], in which efficient transmission of the neighboring mobile node is performed based on the instance of mobile node deployment.

The symmetric key cryptography scheme was introduced to Amol Bhosle and Yogadhar Pandey[4] for improving the security of mobile network. However, the security is not at required level during the data communication with MANET. Position-based Opportunistic Routing (POR) protocol was designed in Shengbo Yang et al[5] for geographic routing and broadcast of wireless medium.

A framework called High-Rate Uncorrelated Bit Extraction (HRUBE) was introduced to Neal Patwari et al.,[6] changes the decorrelation and encoding channel measurements by multibit adaptive quantization scheme. However, the security level was not improved.

In existing work Panagiotis Papadimitratos et al.,[7] secured data transmission against the subjective malicious behavior of nodes was introduced. But, the throughput was not at required level. A secure privacy preserving architecture in Muthumanickam Gunasekaran et al.,[8] presented for data communication in wireless mobile ad-hoc networks. The designed architecture comprises idea of observer anonymity for presenting nodes with better privacy and security. However, the security level was not improved.

Security based algorithmic approach was designed in Rajinder Singh et al.,[9] for mobile ad-hoc networks. Though the security level gets increased, the execution time remained unaddressed.

A danger theory-based artificial immune algorithm termed Mobile Dendritic Cell Algorithm (MDCA) in Maha Abdelhaq et al.,[10] to recognize flooding-based attacks in MANETs. MDCA uses the Dendritic Cell Algorithm (DCA) for the secure data transmission.

A collection of mobile nodes communicating together with wireless links is called as Mobile Ad-Hoc Network (MANET). In Gautam M. Borkar et al.,[11] the standard ad-hoc on-demand multi-path distance vector protocol was introduced to increase the packet delivery ratio with lesser delay and overhead. However, the intermediate nodes failed to confirm the node was trusted node for packet transmission.

A low-overhead identity based distributed dynamic solves the problems of configuration scheme in Uttam Ghosh and Raja Datta[12] for secure allocation of IP addresses. However, the throughput performance of this algorithm was not improved.

A secure, lightweight, on-demand routing protocol was presented in H. N. Saha et al.,[13] for MANETs with fidelity approached to allocate the trust value to the neighbor for secured data transmission. But, the time for secured data delivery remained high using this protocol.

A secure and energy-efficient stochastic multipath routing protocol was introduced in Sajal Sarkar and Raja Dattab[14] with Markov chain for mobile ad-hoc networks that improve security level against the attacks.

Identity (ID) based protocol Waleed S. Alnumay et al.,[15] secured the AODV and TCP in dynamic and attack prone environments of mobile ad-hoc network. It creates the session key for every pair of source-destination nodes of MANET during end-to-end data transmission. However, the time for data communication was high for MANETs.

Many wireless ad-hoc technologies were surveyed in R. Di Pietro et al.,[16] and emphasized the security/privacy features.

A protocol in Jeevaa Katiravan et al.,[17] used many metrics like residual energy and link quality for route selection. It has monitored mechanism that finds route for poor link to reduce the overhead and to increase the throughput of the network. However, the security issue remained unsolved during data communication.

Efficient Secure Routing Protocol (ESRP) Dipayan Bose et al.,[18] in MANET presented new routing scheme based on trust. The protocol was integer values that select the administrator inside the network for routing. But, the security in ESRP was not increased.

Biometric perception is new method in Zafar Sherin and M. K. Soni[19] to extend the security in different networks with the limited identification features. A new routing protocol called an Authenticated Anonymous Secure Routing (AASR) in Wei Liu and Ming Yu[20] to address the attacks.

A new technique was designed in Srinivas Aluvala et al.,[21] for providing the node authentication when new node joins into network of mobile ad-hoc networks.

Based on the above said methods and techniques, an efficient Quantum Key Distribution based Secured Data Communication (QKD-SDC) technique is developed to improve the security during the data communication in MANET. The Quantum Key Generation and Quantum Key Distribution is explained in next section.

3. Methodology

Secure secret key agreement protocol was introduced in[1] to attain the positive secret key rate. However, attackers hack the individual sensitive information with intercepted messages. In addition, an Aggregated-Proof based Hierarchical Authentication scheme (APHA) was presented in[2] for improving the data confidentiality and data integrity during the data transmission. A novel Self Organized B+ Tree Indexed Key (SOBTIK) mechanism is proposed[3], in which efficient transmission to the neighboring mobile node is performed based on the instance of mobile node deployment. However, key agreement protocol calculated the lower bound using minimization function that causes other channel noise utilization by adversaries. Therefore, there is a need for secured data communication in MANET.

In order to improve the secured data packet transmission, Quantum Key Distribution based Secured Data Communication (QKD-SDC) Technique is introduced. In QKD-SDC technique, quantum based cryptography employs the quantum mechanics for secured data communication. In this technique, it uses the shared random quantum key for both encrypting and decrypting the information between sender (i.e., source node) and receiver (i.e., destination).

Figure 1 explains the design architecture of Quantum Key Distribution based Secured Data Communication (QKD-SDC) Technique. Initially, Quantum based Cryptography performs Quantum Key Generation and Quantum Key distribution process. In the sender side, Quantum Key Generation process is carried out. After generating the quantum key, the data gets encrypted using quantum key and sent to the receiver side along with the key. In the receiver side, when the quantum key gets matched, the data gets decrypted using the same random key. Finally, the original data is obtained.

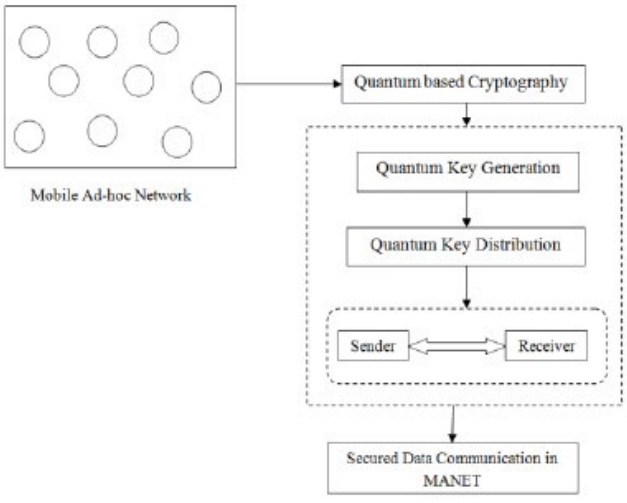

Figure 1. Design of Quantum Key Distribution based Secured Data Communication (QKD-SDC) technique.

3.1 Quantum Key Generation Process

Quantum cryptography in QKD-SDC technique provides safety and security during the data communication through executing the cryptographic tasks by quantum mechanical effects. The quantum states of photons are used and the security key information is sent by means of polarized photons with message represented by bits (0 or 1). The quantum approach uses two polarization states, namely rectilinear basis and the diagonal basis. Sender generates an input bit either 0 or 1 and then chooses any one of the bases (rectilinear or diagonal) to transmit the information. After that, randomly selected bases are used to convert the binary bits into qubits. Then, the relationship between the qubit and binary bits are expressed as follows,

The two polarization states are explained with qubit and binary bit in Table 1. Every photon with one bit of quantum information termed as Qubit. Quantum communication involves the encryption process in quantum states to form qubits. The sender transmits the qubits to the receiver end. The sender and receiver are connected by quantum communication channel which permits the quantum states to be transmitted as described in Figure 2.

During the transmission, qubits are sent to the receiver end through communication channel. Based on above table, each photon is selected at random manner and the sender node repeats till it sends all the photons to the receiver. The sender of key is encrypted with above said non-orthogonal states of information and it sends to the receiver end. This helps to increase the secured data packet transmission at the receiver end.

3.2 Quantum Key Distribution Process

Quantum Key Distribution (QKD) is an application of quantum cryptography and addresses the faults of conventional cryptography. The Quantum key distribution employs the property of quantum states for enhancing the security. Quantum based key distribution is used for

Table 1. Relationship between qubit and binary bits

Basis	Classic Bits	
	0	1
Rectilinear basis (+)	SHAPE * MERGEFORMAT	SHAPE * MERGEFORMAT
Diagonal basis (x)	SHAPE * MERGEFORMAT	SHAPE * MERGEFORMAT

Figure 2. Data communication over quantum channel.

privately sending the data packet in MANET. QKD creates secure distribution of key between different parties with properties of physics. At receiver end, the user finds out the photon polarization through sending it through filter and verifies for any changes in received bits of photons when evaluated to bits measured by receiver.

Figure 3 explains that the process of Quantum communication systems for secured data packet transmission from sender to receiver. The quantum key distribution enables sender and receiver to create shared quantum key. A Quantum state generator creates a random key and it distributes to sender for encryption. Also, it distributes the same key to the quantum state detector at the receiver side for decryption. Both the sender and receiver keeps the quantum key in secret manner for secured data packet transmission. After sending the encrypted qubits to the receiver end, it checks whether quantum key gets matched. When the quantum key matches with receiver quantum key, the decryption is carried out and original data is obtained or else, the qubits get dropped. The flow diagram of the shared key distribution is organized as shown in Figure 4.

Figure 4 explains the flow process of quantum based key distribution. In this diagram initially, the sender requested for the quantum key generation. After generating the quantum key, the key is shared with the receiver. In the sender side, the original data gets encrypted to form qubits. Then, the qubits are sent to the receiver through the quantum communication channel along with the quantum key.

When the quantum key gets matched with the receiver's quantum key, the qubits are decrypted using the quantum key to obtain original data. When the key is not

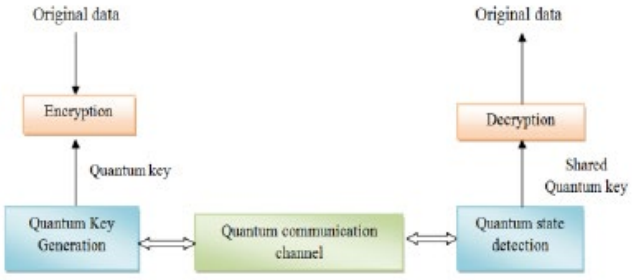

Figure 3. Architecture of quantum communication systems.

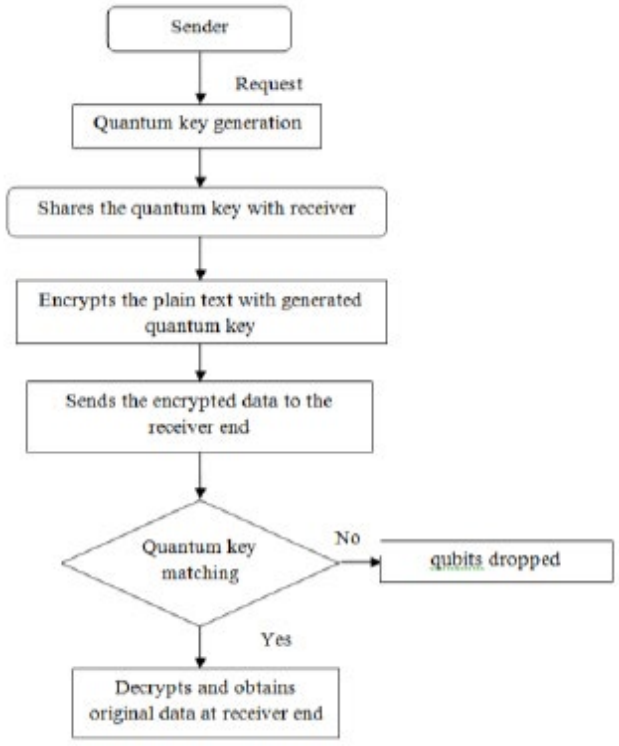

Figure 4. Flow process of quantum based key distribution.

matched, the qubits get dropped. The algorithmic process of quantum key generation and quantum key distribution is shown in below.

// Quantum Key Generation and Quantum Key Distribution Process
Input: Source Node 'SN', Destination Node 'DN', Mobile Nodes '$MN_i = MN_1, MN_2, \ldots, MN_n$', Quantum Key value '$QK_i = QK_1, QK_2, \ldots, QK_n$', Data Packets '$DP_i = DP_1, DP_2, \ldots, DP_n$'
Output: Improved security of data transmission
Step 1: Begin
Step 2: Source node generates quantum key
Step 3: Shares the quantum key with destination node
Step 4: Encrypts the original data with help of quantum key
Step 5: Binary bits converted into qubits
Step 6: Sends the encrypted data along with the quantum key
Step 7: Destination node perform key matching
Step 8: if key matching
Step 9: Transaction allowed
Step 10: destination node obtains original data
Step 11: Else
Step 12: Transaction declined
Step 13: End if
Step 14: End

Algorithm 1. Quantum key generation and quantum key distribution process.

With the help of above process, QKD-SDC technique performs secure data transmission in MANET efficiently. This process helps to increase the data transmission rate and also reduces time taken for secured data transmission in an effective manner.

3.3 Simulation Settings

The Quantum Key Distribution based Secured Data Communication (QKD-SDC) Technique in Mobile Ad-hoc Network uses NS-2 simulator. The number of mobile nodes used for experimental purpose is 100. The 100 mobile nodes are randomly distributed in rectangular area of 1500m 1500m. The dynamic changing topology uses the Destination Sequence Based Distance Vector (DSDV) routing protocol to perform the experimental work with network range. The mobility of nodes for QKD-SDC technique in MANET is about 10 m/s for each mobile node with simulation rate of 45 seconds for secure data transmission between mobile nodes. Table 2 illustrates the input parameter.

Table 2. Simulation setup

PARAMETER	VALUE
Protocols	DSDV
Network range	1500 m 1500 m
Simulation time	45 s
Number of mobile nodes	10, 20, 30, 40, 50, 60, 70, 80, 90,100
Packets	9, 18, 27, 36,45, 54, 63, 72, 81, 90
Network simulator	NS 2.34
Mobility speed	10 m/s
Pause time	15 s

3.4 Simulation Results

Experiment is conducted on the factors such as data loss rate, throughput and time for secured data communication in MANET. The results of the metrics of QKD-SDC technique is compared against the existing methods such as secure secret key agreement protocol[1], Aggregated-Proof based Hierarchical Authentication scheme (APHA)[2] and SOBTIK Mechanism[3] respectively.

3.4.1 Impact of Data Loss Rate (DLR)

During the data transmission in MANET, data loss occurs when number of sent packets at sender end is not same as the number of received packets at the receiver end. For measuring the data loss rate 'DLR', the difference between size of data packets sent 'Size(DP_s)' and the size of data packets received 'Size(DP_r)' was calculated. It is measured in terms of Kilo Byte (KB). The data loss rate is formulated as,

$$DLR = \sum_{i=1}^{n} [[Size\ (DP_s) - Size\ (DP_r)]] \quad (1)$$

From Equation (1), data loss rate in QKD-SDC technique is evaluated using the size of data packet sent 'DP_s' and data packet received 'DP_r'.

Table 3 illustrates the data loss rate with respect to data packet size ranging from 15-150 during the secured data communication in MANET. This table represents the data loss rate of four different methods such as QKD-SDC Technique, SOBTIK Mechanism, Secure Secret Key Agreement Protocol and APHA Scheme. From the table value, it is clear that proposed QKD-SDC technique has achieved minimum data loss rate than existing works.

Figure 5 illustrates the impact of data loss rate with respect to the data packet size in range of 15 to 150.

Table 3. Tabulation for data loss rate

Data Packet size (KB)	Data loss rate (KB)			
	QKD-SDC Technique	SOBTIK Mechanism	Secure Secret Key Agreement Protocol	APHA Scheme
15	1	2	4	6
30	3	5	7	10
45	6	8	9	15
60	12	14	16	20
75	8	10	13	17
90	15	18	22	26
105	20	22	24	29
120	23	25	27	33
135	25	28	32	36
150	27	31	35	40

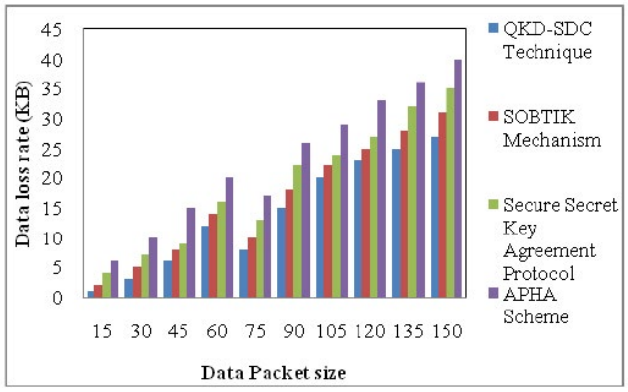

Figure 5. Measure of data loss rate.

From the Figure, it is clear that proposed QKD-SDC technique has lesser data loss rate compared to SOBTIK Mechanism, Secure Secret Key Agreement Protocol and APHA Scheme. When data packet size gets increased, data loss rate also gets increased correspondingly. But, data loss rate in proposed QKD-SDC technique is lesser because of using quantum key distribution process. This type of distribution helps to avoid the data distribution to the malicious user at the receiver end. From the result, the data loss rate of proposed QKD-SDC technique is reduced by 20%, 33% and 47% compared to existing SOBTIK Mechanism, Secure Secret Key Agreement Protocol and APHA Scheme respectively.

3.5 Impact of Throughput

Throughput is the rate of successful data packets delivery over period of time interval. The average throughput is calculated by total amount of data received by the receiver from the sender divided by time taken by the receiver. It is measured in terms of packet per second (pps). The throughput is formulated as given below,

$$T = \frac{Size(DP_r)}{Simulation\ time * 1000} \quad (2)$$

From Equation (2), throughput 'T' is obtained on size of data packets received 'Size(DP_r)' to the simulation time in mobile ad-hoc network. Higher the throughput, the technique is said to be more efficient.

Table 4 illustrates the throughput with respect to mobile node density ranging from 10-100 during the secured data communication in MANET.

This table represents the throughput of four different methods such as QKD-SDC Technique, SOBTIK Mechanism Secure Secret Key Agreement Protocol and APHA Scheme.

From the table value, it is clear that proposed QKD-SDC technique has achieved higher throughput than existing works.

Figure 6 illustrates the impact of throughput with respect to the mobile node density in range of 10 to 100. From the Figure, it is clear that proposed QKD-SDC technique has higher throughput compared to SOBTIK Mechanism, Secure Secret Key Agreement Protocol and APHA Scheme. When mobile node density gets increased, throughput level also gets increased correspondingly. But, throughput level in proposed QKD-SDC technique is

Table 4. Tabulation for throughput

Mobile node density	Throughput (pps)			
	QKD-SDC Technique	SOBTIK Mechanism	Secure Secret Key Agreement Protocol	APHA Scheme
10	311	278	251	223
20	324	285	265	238
30	335	299	278	246
40	342	310	289	255
50	355	325	303	269
60	364	345	321	278
70	373	359	336	296
80	385	365	345	311
90	395	372	361	325
100	412	391	385	341

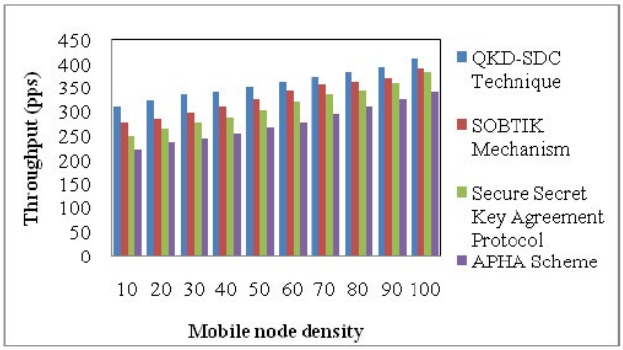

Figure 6. Measure of throughput.

higher because of using the quantum key generation and distribution process. This type of process helps to send the data packets to the receiver end with minimum loss.

From the result, the throughput of proposed QKD-SDC technique is increased by 8%, 15% and 30% compared to existing SOBTIK Mechanism, Secure Secret Key Agreement Protocol and APHA Scheme respectively.

3.6 Impact of Time for Secured Data Delivery

The time for secured data delivery is defined as the product of number of data packets sent and the time taken to deliver the data packets in the mobile ad-hoc network. It is measured in terms of milliseconds (ms). The time for secured data delivery is formulated as,

$$Time = \sum_{i=1}^{n} DP * Time(DP_i) \quad (3)$$

From Equation (3), the time for secured data delivery is calculated where 'DP' represents the number of data packets. Lower the time for secured data delivery, the technique is said to be more efficient.

Table 5 illustrates the time for secured data delivery with respect to data packets ranging from 9-90 during the secured data communication in MANET. This table represents the time for secured data delivery of four different methods such as QKD-SDC Technique, SOBTIK Mechanism Secure Secret Key Agreement Protocol and APHA Scheme. From the table value, it is clear that proposed QKD-SDC technique consumed lesser time for secured data delivery than existing works.

Figure 7 illustrates the time for secured data delivery with respect to the data packets in range of 9 to 90.

Table 5. Tabulation for time for secured data delivery

Data Packets	Time for secured data delivery (ms)			
	QKD-SDC Technique	SOBTIK Mechanism	Secure Secret Key Agreement Protocol	APHA Scheme
9	0.559	0.614	0.623	0.654
18	0.571	0.645	0.652	0.679
27	0.582	0.663	0.685	0.693
36	0.593	0.682	0.701	0.710
45	0.605	0.695	0.723	0.731
54	0.613	0.712	0.736	0.756
63	0.636	0.732	0.745	0.772
72	0.651	0.742	0.759	0.795
81	0.684	0.756	0.775	0.812
90	0.698	0.763	0.789	0.825

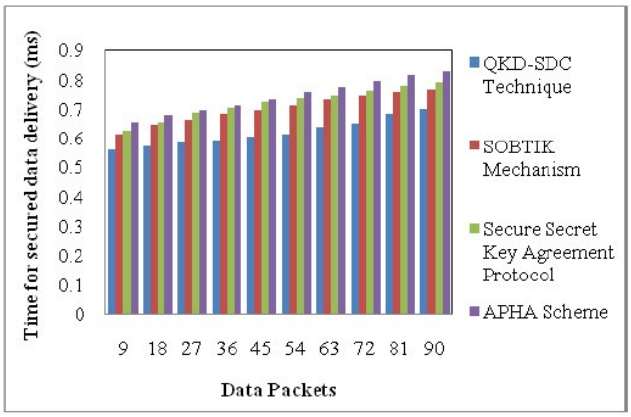

Figure 7. Measure of time for secured data delivery.

From the Figure 7, it is clear that proposed QKD-SDC technique consumes lesser time for secured data delivery compared to SOBTIK Mechanism, Secure Secret Key Agreement Protocol and APHA Scheme. When data packets get increased, time for secured data delivery also gets increased correspondingly.

Time for secured data delivery in proposed QKD-SDC technique is less because of sending the data packets through quantum communication channel. In this channel the data packets get encrypted using quantum key to form qubits and sent to the receiver end. In the receiver side, the data packets get with decrypted in minimal amount of time. This type of communication reduces the time consumption for the secured data delivery. From the result, the time consumption for secured data delivery of

proposed QKD-SDC technique is reduced by 11%, 13% and 16% compared to existing SOBTIK Mechanism, Secure Secret Key Agreement Protocol and APHA Scheme respectively.

4. Conclusion

An effective Quantum Key Distribution based Secured Data Communication (QKD-SDC) technique is designed to improve the security during the data communication in MANET. In QKD-SDC technique, quantum based cryptography used the quantum mechanics for improved secured data communication. Quantum based Cryptography performs Quantum Key Generation process and Quantum Key distribution process. In Quantum Key Generation process, quantum key is generated and shared to the receiver. With help of quantum key, the original data gets encrypted as qubits. After that in Quantum Key distribution process, the qubits are sent to the receiver through quantum communication channel along with quantum key. At receiver end, when the quantum key gets matched with receiver's quantum key, the qubits are decrypted to obtain the original data. When the key is not matched, the qubits get dropped. This in turn helps to increase the security and throughput. The simulation is carried out for different parameters such as data loss rate, throughput and time for secured data delivery. The results show that QKD-SDC technique increases throughput by 17% and also reduces the data loss rate by 33% when compared to the state-of-the-art works.

5. References

1. Wang N, Zhang N, Gulliver TA. Cooperative key agreement for wireless networking: key rates and practical protocol design. IEEE Transactions on Information Forensics and Security. 2014; 9(2):272–84. https://doi.org/10.1109/TIFS.2013.2293113
2. Ning H, Liu H, Yang LT. Aggregated-proof based hierarchical authentication scheme for the internet of things. IEEE Transactions on Parallel and Distributed Systems. 2015 Mar; 26(3):657–67. https://doi.org/10.1109/TPDS.2014.2311791
3. Sangeetha S, Sathappan S. Securing data retrieval based on tree indexed self organized key in mobile ad- hoc network. IEEE Computation System and Information Technology for Sustainable Solutions (CSITSS). 2016 Dec; 11(2):191–4. https://doi.org/10.1109/csitss.2016.7779412
4. Bhosle A, Pandey Y. Applying security to data using symmetric encryption in MANET. International Journal of Emerging Technology and Advanced Engineering. 2013 Jan; 3(1):426–30
5. Yang S, Yeo CK, Lee BS. Toward reliable data delivery for highly dynamic mobile ad-hoc networks. IEEE Transactions on Mobile Computing. 2012 Jan; 11(1):111–24. https://doi.org/10.1109/TMC.2011.55
6. Patwari N, Croft J, Jana S, Kasera SK. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. IEEE Transactions on Mobile Computing. 2010 Jan; 9(1):17–30. https://doi.org/10.1109/TMC.2009.88
7. Papadimitratos P, Haas ZJ. Secure data transmission in mobile ad-hoc networks. WiSe '03 Proceedings of the 2nd ACM Workshop on Wireless security; 2003. p. 41–50. https://doi.org/10.1145/941311.941318
8. Gunasekaran M, Premalatha K. SPAWN: A secure privacy-preserving architecture in wireless mobile ad-hoc networks. Springer, EURASIP Journal on Wireless Communications and Networking. 2013 Sep; 2013:1–12. https://doi.org/10.1186/1687-1499-2013-220
9. Singh R, Singh P, Duhan M. An effective implementation of security based algorithmic approach in mobile ad-hoc networks. Springer, Human-Centric Computing and Information Sciences. 2014 Dec; 4(7):1–14.
10. Abdelhaq M, Alsaqour R, Abdelhaq S. Securing mobile ad-hoc networks using danger theory-based artificial immune algorithm. PLoS ONE. 2015 May; 10(5):1–16. https://doi.org/10.1371/journal.pone.0120715
11. Borkar GM, Mahajan AR. A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks. Wireless Networks, Springer. 2016 May; 1–18.
12. Ghosh U, Datta R. A secure addressing scheme for large scale managed MANETs. IEEE Transactions on Network and Service Management. 2015; 12(3):483–95. https://doi.org/10.1109/TNSM.2015.2452292
13. Saha HN, Bhattacharyya D, Banerjee PK. Modified Fidelity Based On-Demand Secure (MFBOD) routing protocol in mobile ad-hoc network. International Journal of Foundations of Computing and Decision Sciences (FCDS), De Grurter. 2015 Dec; 40(4):267–98.
14. Sarkar S, Dattab R. A secure and energy-efficient stochastic multipath routing for self-organized mobile ad-hoc networks. Ad-hoc Networks, Elsevier. 2016 Feb; 37(P2):209–27. https://doi.org/10.1016/j.adhoc.2015.08.020
15. Alnumay WS, Ghos U. Secure routing and data transmission in mobile ad-hoc networks. International Journal of Computer Networks and Communications (IJCNC); 2014 Jan; 6(1):111–27. https://doi.org/10.5121/ijcnc.2014.6108
16. Di Pietro R, Guarino S, Verde NV, Domingo-Ferrer J. Security in wireless ad-hoc networks – A survey. Computer

Communications, Elsevier. 2014 Sep; 51:1–20. https://doi.org/10.1016/j.comcom.2014.06.003
17. Katiravan J, Sylvia D, Rao DS. Energy efficient link aware routing with power control in wireless ad-hoc networks. The Scientific World Journal. 2015; 2015:1–7. PMid:26167529 PMCid:PMC4475759. https://doi.org/10.1155/2015/576754
18. Bose D, Banerjee A, Bhattacharyya A, Saha HN, Bhattacharyya D, Banerjee PK. An efficient approach to secure routing in MANET. Advances in Computing and Information Technology, Springer. 765–76. https://doi.org/10.1007/978-3-642-31513-8_78
19. Sherin Z, Soni MK. Secure routing in MANET through crypt-biometric technique. International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA); 2014. p. 713–20.
20. Liu W, Yu M. AASR: Authenticated anonymous secure routing for MANETs in adversarial environments. IEEE Transactions on Vehicular Technology. 2014; 63(9):4585–93. https://doi.org/10.1109/TVT.2014.2313180
21. Aluvala S, Sekhar KR, Vodnala D. A novel technique for node authentication in mobile ad-hoc networks. Perspectives in Science, Elsevier. 2016; 8:680–2. https://doi.org/10.1016/j.pisc.2016.06.057