Quantum Phase Shift for Energy Conserved Secured Data Communication in MANET

E.Selvi[1], M. S. Shashidhara[2]

[1]Department of Computer Science, Asan Memorial College of Arts and Science, Chennai, India
[2]Department of MCA, The Oxford College of Engineering, Bangalore, India

***Abstract*:** A Mobile Ad-Hoc Network(MANET) is a structure-less network where the mobile nodes randomly moved in any direction within the transmission range of the network. Due to this mobility, wide range of intrusion occurs in MANET. Therefore, Intrusion Detection Systems (IDS) are significant in MANETs to identify the malicious behavior. In order to improve the secured data communication an efficient Quantum Phase Shift Energy Conserved Data Security (QPSEC-DS) technique is introduced. The Quantum Phase Shift (QPS) technique is used for ensuring the security during the data transmission from sender to receiver in MANET. Initially, the quantum based approach is used to encrypt the information using QPS at the sender through secret key distribution. The receiver side also performs the same QPS, and then the encrypted bit is received successfully. This in turns attains the secured packet transmission without any malicious node in the MANET. Based on the phase shifting, the energy conservation between the sender and receiver is measured for transmitting the data packet using QPSEC-DS technique. Also, the enhanced Dynamic Source Routing (DSR) protocol is applied in QPSEC-DS technique is implemented to improve the energy management and secured data communication between the source and destination in an efficient manner. The QPSEC-DS technique conducts the simulations work on parameters including packet delivery ratio, energy consumption, communication overhead and end to end delay.

Keywords: Mobile ad hoc network (MANET), Quantum phase shift (QPS), Energy conservation, Intrusion Detection Systems (IDS), Dynamic source routing (DSR) protocol.

1. Introduction

A MANET is arranged with a group of mobile nodes based on the multi-hop approach without any centralized administration. In MANET, every mobile node act as a sender and a receiver via bidirectional wireless and it does not contain any permanent network infrastructure. Intrusion-detection mechanisms effectively protect MANET from attacks. Most recently, intrusion attacks are created by forming the black hole attacks in MANET. Therefore, IDS is developed in MANET to improve the security level and to detect the malicious attackers in the network. Several secured
data transmission and energy efficient techniques are explained with the help of literature.

An Enhanced Adaptive Acknowledgment (EAACK) intrusion-detection system was developed in [1] for detecting the malicious activities. However, EAACK does not reduce the network overhead and also energy efficient secured data transmission is the difficult issue. Energy-Aware and Error Resilient (EAER) routing protocol was designed in [2] for improving the packet delivery with minimum energy consumption. However, the secured transmission remained unaddressed.

In [3], standard ad hoc on-demand multi-path distance vector protocol was introduced to improve packet delivery ratio with minimum delay, overhead and it also offered security against vulnerabilities and attacks. A Report-based payment scheme (RACE) was developed in [4] for securing the payment and accurately detecting malicious nodes without false declaration. However, intermediate nodes cannot make confirmation for packet transmission.

A MANET has been highly susceptible to several attacks because of random motion of mobile nodes in network. Due to this, a risk-aware response approach was introduced in [5] to systematically handle identified routing attacks. However, it included node reputation and attack frequency with adaptive decision model and energy management was considered to be a challenging issue. In [6], Reliable and Energy Efficient Protocol was developed for improving packet delivery ratio, energy consumption, and throughput. Danger-theory based artificial immune algorithm was designed in [7] to improve security through multipath routing by means of attack detection. However, the performance of this method was not proved to be efficient.

Residual Energy based Reliable Multicast Routing Protocol (RERMR) was designed in [8] to improve network lifetime and also increased packet delivery rate. However, security in optimized multicast routing was unaddressed. Hybrid method was developed in [9] for minimizing energy consumption and execution time through multipath routing in MANET. Different routing protocol was designed in [10] for identifying malicious activities during secured data transmission in MANET.

With the above considerations, main contribution of the research work is arranged as follows. An efficient Quantum Phase Shift Energy Conserved Data Security (QPSEC-DS) technique is proposed with the objective of improving the security during data packet transmission with minimum energy conservation in MANET. Then the Quantum phase shift is carried out to improve the security for transmitting the data packet from the sender to the receiver side. Initially, the Quantum based approach utilizes the shared random key to encrypt and decrypt the information using phase shift between the sender and the receiver in a secured manner. Next, the Quantum key distribution is efficiently detects the intrusion node and improves the security for packet transmission in MANET. With the aid of energy conserved data communication, the shifting position is evaluated for preserving the data transmission with lesser energy

conservation. Finally, the improved Dynamic Source routing (DSR) protocol is applied in QPSEC-DS technique which enhances efficient energy management and data communication with secured manner between the source and destination. Therefore, the performance of proposed QPSEC-DS technique in MANET identifies the optimized route path for secured data transmission with minimum communication overhead and delay in an efficient manner.

The rest of this paper is categorized as follows: Section 2 presents a brief introduction of related works. Section 3 describes the Quantum Phase Shift Energy Conserved Data Security (QPSEC-DS) technique with neat diagram. In Section 4, the simulation environment is presented and the simulation results are obtained in section 5. Finally, the concluding remarks are explained in section 6.

2. Related Works

A MANET contains the set of mobile nodes that performs fundamental networking services such as packet forwarding, routing etc. A node in an ad hoc network depends on another node for packet transmission, due to restricted number of mobile host's in wireless transmissions. Therefore, security is considered to be an important factor for packet forwarding and routing in MANET.

A secure, lightweight, on-demand routing protocol was designed in [11] for MANETs which uses fidelity approach to assign trust to a neighbor for secured data transmission. This protocol also improved packet delivered fraction. However, energy conservation was considered as a major issue and hence was difficult to send more number of packets.

To address this issue, a Secure and Energy Aware Routing Protocol (ETARP) was designed in [12] for energy efficiency and security for wireless sensor networks (WSNs). However it did not ensured security at the required level. A secure and reliable routing mechanism was presented in [13] for providing different levels of security in an energy-efficient manner. A secure and energy-efficient stochastic multipath routing protocol was developed in [14] based on Markov chain for mobile ad-hoc networks (MANETs) to improve security against attacks and at the same time reduced energy consumption.

In [15], a machine learning technique was developed in ad hoc network security and improved packet delivery ratio with minimum delay and energy consumption. New multi-hop cognitive cellular network architecture was designed in [16] to provide better data transmissions in cellular networks and also reduced energy consumption. Different MANET routing protocol was developed in [17] for improving security against attacks in MANETs. In [18], Cluster-based routing protocol using Network Coding provided an insight into reducing energy consumption and therefore improving network lifetime. A symmetric key cryptography scheme was developed in [19] to improve network security. An energy-efficient inter-domain routing protocol was developed in [20] for reducing the energy with minimum overhead in MANET. In [21], proactive MANET protocol OLSR was considered with the objective of improving the network lifetime with the aid of novel multiple metric routing scheme, based on energy efficient and path reliability metrics. This scheme was called as, standard OLSR and Energy Efficient and Path Reliability OLSR (EEPR-OLSR) in which cross layer parameters were investigated to introduce the prediction-based link availability estimation. On the other hand, multi-criteria weights were investigated in [22] using Genetic algorithm to improve signal-to-noise ratio that was a main drawback inn cross layer scheme. For mission critical communication, Network Condition Aware WMSN routing protocol was introduced in [23] to ensure minimal retransmission that in turn reduced energy consumption in cross layer design.

Based on the above said methods and techniques, an efficient Quantum Phase Shift Energy Conserved Data Security (QPSEC-DS) technique is developed to improve the security and also reducing the energy consumption in MANET. The brief clarification about the intrusion detection is explained in next section.

3. Quantum Phase Shift Energy Conserved Data Security technique

In this section, an efficient Quantum Phase Shift Energy Conserved Data Security technique is described to improve the security and minimum energy consumption with the help of structural diagram in MANET. Before explaining the proposed QPSEC-DS technique, the major problem that arises during the data transmission from sender to receiver is explained as follows.

Problem statement: A MANET includes the set of nodes that has the ability to communicate both wireless transmission and networking without any centralized administrator. Also, the MANET dynamically creates the network in order to exchange their information without any constant network infrastructure. In MANET, the mobile nodes are distributed in a random manner. Due to the mobility of the nodes, the intrusions occur during the data packet transmission from sender to receiver. Therefore, security is most significant during the data packet transmission. The conventional IDS improve the network security level. However, the energy efficient secured data communication is a challenging issue in MANET.

Quantum Phase Shift technique for secured data transmission: An Enhanced Adaptive Acknowledgment intrusion-detection system identifies the malicious activities. Though, it improves the network overhead and reduces energy efficient secured data transmission. Also, Energy-Aware and Error Resilient routing protocol improves the packet delivery with lesser energy utilization. But, security and several intrusions are simply affecting the performance of the system due to the variation in network transmission range. Therefore, the proposed Quantum Phase Shift Energy Conserved Data Security (QPSEC-DS) technique is applied for adjusting the transmission range of the mobile nodes efficiently. In order to enhance the security in MANET, Quantum mechanism is utilized with minimum transmission interference. Next, the energy conservation is attained during the secured data packet transmission from sender to receiver for achieving the efficient energy routing. Then the quantum key distribution improves the security for transmitting the data using routing protocol without any intrusion node occurs. The Block diagram of the quantum based approach is illustrated in fig 1.

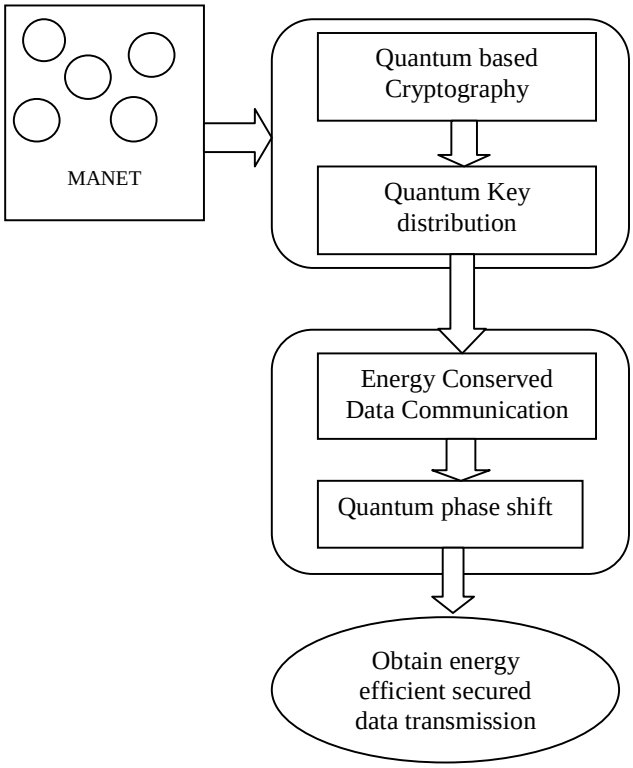

Fig. 1. Block diagram of quantum phase shift energy conserved secured data transmission

Fig.1 illustrates the two processes for efficient data packet transmission in MANET. Initially, the quantum mechanism is applied for secured transmission through quantum key distribution to reduce the intrusion in MANET. The quantum mechanism provides a secret encryption key which is shared between the sender and receiver within the transmission range. This in turns effectively improves the security during the data packet transmission. After that, based on the quantum phase shifting position, energy efficient measurement is carried out with the objective of reducing the energy consumption on transmission and communication overhead. The detailed explanation of the proposed QPSEC-DS technique is discussed in next sub section.

Quantum based secure transmission in MANET: Quantum based cryptography uses quantum mechanics for enhancing the security of the data communication in MANET. It uses the shared random key to encrypt and decrypt the information between the two parties, sender (i.e. source node) and receiver (i.e. destination). The main objective of the Quantum key distribution is to detect the intrusion node and improve the secured data packet transmission. The quantum based approach is clearly illustrated in fig. 2

Fig.2 shows the Block diagram of Quantum communication systems with shared secret key for efficient data packet transmission from sender to receiver. The quantum key distribution enables sender and receiver to create a shared secret key although there is a potential presence of an intrusion in MANET. In order to ensure the security, the Quantum key distribution utilizes the accurate property of the quantum states. Quantum based key distribution is used for detecting the intrusion without disturbing the data packet transmission in MANET. A Quantum state generator creates the shared secret key and then 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 keep the secret key with contact to achieve the perfect secret key for transmission in a significant manner

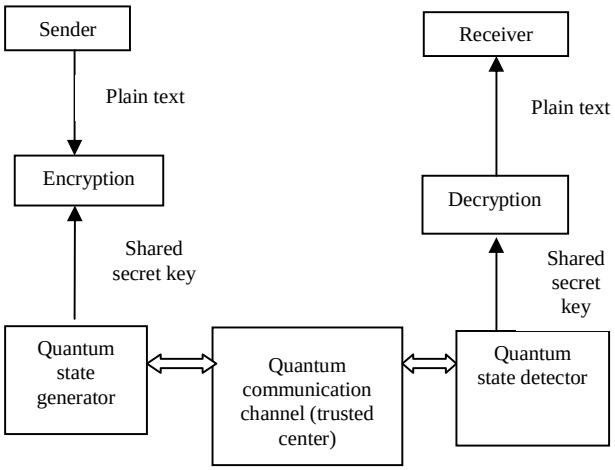

Fig. 2. Block diagram of quantum communication systems with shared secret key

The Quantum communication involves the encryption process in quantum states, or qubits. The sender and receiver are connected by a quantum communication channel which permits the quantum states to be transmitted. Generally, four possible states are available such as (|0> + |1>), (|0> - |1>), |0>, |1>. During the transmission, the input bits of the data packets are transmitted. After that, randomly selected bases (rectilinear or diagonal) are used to coverts the binary bits into qubits. The quantum approach uses two polarization states namely, the rectilinear basis or 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. Then the relationship between the qubit and binary bits are expressed as follows,

Table 1. Relationship between the qubit and binary bits

Basis	Bits	
	0	1
Rectilinear basis (+)	↑	→
Diagonal basis (x)	↗	↘

From the table 1, the two polarization states are explained with qubit and binary bit. The node has the ability to detect the third party (i.e. intrusion) trying to obtain the knowledge of the key, the quantum cryptography is utilized. The sender of the key is encrypted with the above said non orthogonal states of the information and it sends to the receiver which resulting in increases the secured data packet transmission at the receiver end.

The information is phase shifted by 0° and 180° with separated time and the difference in their time is Δt. The encrypted

information is transmitted to quantum state detector through the communication channel. After that, the encrypted information is decrypted with the help of shared secret key (i.e. 0 or 1). The different possibilities of phase shifting are measured by sender and receiver with two measurement bases such as rectilinear basis and diagonal basis. The two non-orthogonal bases consists of four possibilities is clearly described as follows.

Sender encrypts the information bit 0 in quantum state by using a phase shift of 0° and receiver measurement basis is also with a phase shift of 0°.Then it concludes that the information is encrypted in 0 is within the one time unit.

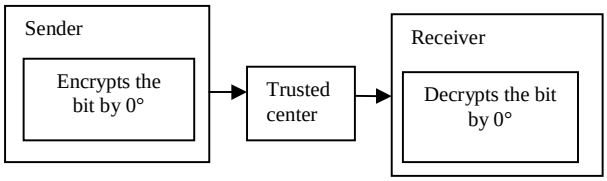

Fig.3. Phase shift by sender is 0° and phase shift by receiver is 0°

Fig.3 clearly illustrates the similar phase shift is obtained between the sender and receiver. Therefore, the information bit is transmitted in a secured manner. The next possibilities is that the sender encrypts the bit 0 in state by using a phase shift of 0° with the time unit. Then the receiver provides the incorrect measurement due to a phase shift of 180°. This indicates that the measurement basis was wrong due to which information is lost and it does not conclude whether the transmitted information was 0 or 1. From the result, the key is not matched between the sender and the receiver. Therefore, the intrusion node is identified and packet dropping is reduced in MANET. The above process is described in fig.4.

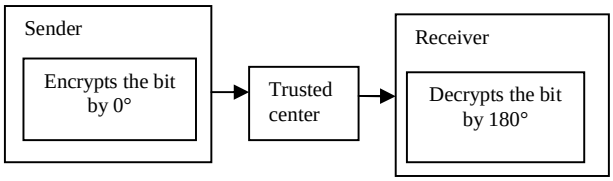

Fig.4. Phase shift by sender is 0° and phase shift by receiver is 180°

The third case is that sender encrypts the bit 1 in quantum state with the phase shift of 180°. Similarly, the receiver decrypt the bit with the measurement basis is correct, i.e., a phase shifts of 180°. The schematic diagram of the quantum phase shift approach is shown in Fig.5

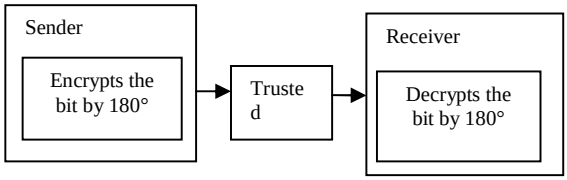

Fig.5. Phase shift by sender is 180° and phase shift by receiver is 180°

From the fig.5, quantum phase shift is obtained between the sender and receiver with similar secret key. The figure shows that the information is encrypted and the phase shifted by 180° and hence correct information is observed at the receiver. The receiver measures the phase of the information and it concludes that the encrypted information is 1.

The final case is that sender encrypts the information bit 1 in quantum state with 180° phase shift. However, the receiver measurement basis is incorrect, i.e., a phase shift of 0°. Fig.6 shows the quantum phase shift measurement.

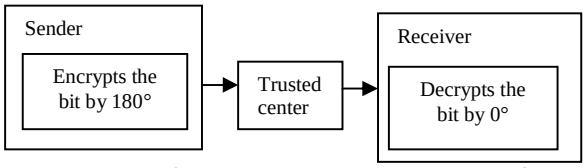

Fig.6. Phase shift by sender is 180° and phase shifted by receiver is 0°

Fig.6 clearly illustrates the phase shift is obtained between the sender and receiver. The information occurring at the receiver side is wrong due to which the bit is lost and the system cannot state whether that information is 0 or 1.Therefore, the receiver informs the sender of the instances where it got accurate results. As a result, the sender and receiver keep these bits as their key bits and remove the all other bits. Table II shows the generation of secret key transmitted by sender and the measurement basis used by receiver.

Table. 2. Secret key for sender and receiver

Sender random bit	0	1	1	0
Phase shift	0°	180°	180°	0°
Receiver measurement bases	0	0	1	1
Shared secret key	0	-	1	-

Table 2 is used to check the presence of a malicious node in MANET. Therefore the shared secret key is used to decrypt the information. From the table, the shared secret key is 01. The sender and receiver utilize this secret key for secured transmission which helps to ensure the security from the sender to receiver without any malicious node (i.e packet dropping) occurred in MANET. The algorithmic description of the quantum phase shift approach is shown below:

Algorithm I: Quantum Phase Shift Secured Data Transmission

Input: Sender (S), Receiver (R), Quantum Key value '$QK_i = QK_1, QK_2, .., QK_n$', Data Packets '$DP_i = DP_1, DP_2, \dots, DP_n$', input bits 0 and 1

Output: Improved secured data transmission

Step 1: Begin

Step 2: If (S encrypts bit '0' and R measurement basis is 0) then

Step 3: Resultant bit is '0'

Step 4: End if

Step 5: If (S encrypts the bit '0' and R measurement basis is 1) then

Step 6: Resultant bit is cannot state '0' or '1'
Step 7: End if
Step 8: If (S encrypts the bit '1' and R measurement basis is 0) then
Step 9: Resultant bit is cannot state '0' or '1'
Step 10: End if
Step 11: If (S encrypts the bit '1' and R measurement basis is 1) then
Step 12: Resultant bit is '1'
Step 13: End if
Step 14: Obtained the secret key at the quantum state detector
Step15: If (the shared secret key is matched at the receiver) then
Step 16: Secured transmission is obtained
Step 17: else
Step 18: Transmission is declined
Step 19: end if
Step 20: end

The above algorithmic description is clearly described for secured data transmission from source node to destination node in MANET. The proposed quantum phase shift key approach is applied to shift the phase of the information bit at the sender. The receiver side also obtains the similar phase shift and then the encrypted bit is received successfully or else it cannot conclude whether the information is 0 or 1. Then the other possibilities are also measured in order to attain the shared secret key. Finally, the secret key is attained and it is matched with receiver end to perform the effective transmission. If the secret key is not matched, then the transmission is declined which in turns improve the secured packet delivery ratio with minimum overhead.

Energy Conserved Data Communication

After performing the quantum phase shift, energy efficient secured transmission is a significant part in MANET. The shifting position is determined for transmitting the data packet in a secured manner with minimal energy consumption. The energy consumption is used for transferring the data packet from sender to receiver is expressed as follows,

$$EC(n,D)=[E\_d(n)+E\_r(n,D)] \quad (1)$$

From Eq. (1), 'n' denotes the quantum bits and 'D' is the distance between sender and the receiver in the mobile network, whereas 'E_d' and 'E_r' are energy dissipated per bit to forward the data packet and receive the data packets respectively. The distance between the sender and receiver is measured as,

$$D=\text{Min}(\text{dist}(x,y)) \quad (2)$$

From Eq. (2), the 'D' distance between the sender (x) and receiver (y) is measured with minimum energy conservation. From the result, the energy conservation is attained during the secured data packet transmission from sender to receiver. The algorithmic description of the energy consumption is shown below.

Algorithm 2: Energy Conserved Data Communication

Input: Sender 'S', receiver (R), quantum bits '0' and '1'
Output: Energy efficient routing
Step 1: Begin
Step 2: For each sender (S) and receiver (R)
Step 3: Evaluate distance using Eq.(2)
Step4: Evaluate energy consumption using Eq. (1)
Step 5: End for
Step 6: End

The above algorithm clearly describes the energy measurement of data packet for improving the security and energy conserved data communication. Based on the quantum phase shift mechanism, the energy dissipated per qubit and the distance between the sender and receiver is being computed. Therefore, the quantum phase shift approach is used in MANET for encoding the quantum bits with the phase shift of input bits. The encryption and decryption process is carried out between the sender and receiver ensures the secured transmission. Based on the shifting that takes place, the data packets are transmitted successfully and it also used for identifying the malicious nodes in MANET. This helps to ensure the secured data transmission with minimum energy conservation between the sender and receiver. An enhanced Dynamic Source routing (DSR) protocol is also applied in QPSEC-DS technique to improve the efficient energy management and secured data communication between the source and destination in MANET. In addition, the secured data communication take place between the source and destination using DSR protocol, the optimal route is identified for secured data transmission and the communication overhead is reduced in MANET.

4. Experimental Evaluation

A proposed Quantum Phase Shift Energy Conserved Data Security (QPSEC-DS) technique is implemented in NS-2 simulator with the network range of 1500*1500 m size. The mobile network consists of 500 nodes in the network structure and uses the Random Way Point (RWM) model. The RWM uses typical number of mobile nodes for locating the movable nodes. The dynamic changing topology uses the Dynamic Source routing (DSR) protocol to implement efficient energy management and secured data communication between the source and destination in MANET. The node speed is varied between 2m/s and 25m/s with the mobile node pause time is varied from 0 seconds to 300 seconds. The simulations parameters are obtained that are used in the experiments listed in table 3.

Table 3. Simulation parameter

Node density	50,100,150,200,250,300,350,400,450,500
Network area	1500*1500m
Transmission range	250m
Packets	9, 18, 27, 36, 45, 54, 63
Simulation period	600s
Minimum node speed	2m/s
Maximum node speed	25m/s
Node pause time	0 – 300 seconds
Routing protocol	Dynamic source routing protocol (DSR)

An efficient Quantum Phase Shift Energy Conserved Data Security (QPSEC-DS) technique is analyzed and compared with the existing Enhanced Adaptive ACKnowledgment (EAACK) [1] and Energy-Aware and Error Resilient (EAER) routing protocol [2].The experimental evaluation is carried out with the different parameter such as packet delivery ratio, energy consumption, communication overhead and end to end delay when compared to the state-of-the-art works. Then the performance of proposed QPSEC-DS technique is evaluated based on following metrics with the help of tables and graph values.

A. Impact of packet delivery ratio

Packet delivery ratio is defined as the ratio of data packets that are correctly sent from the sender to the data packets received at the receiver in a secured manner. The packet delivery ratio is mathematically formulated as given below.

$$PDR = \frac{Data\ Packet_R}{Data\ Packet_S} * 100 \quad (3)$$

From Eq. (3), the packet delivery ratio 'PDR' is measured with respect to the data packets sent '$DataPacket_S$' and data packets received '$DataPacket_R$' at the receiver end. Higher the packet delivery ratio, more efficient the method is said to be. The packet delivery ratio is measured in terms of percentage (%).

Table 4. Tabulation for packet delivery ratio

No. of packet sent	Packet Delivery ratio (%)		
	QPSEC-DS	EAACK	EAER
9	90.56	78.59	65.68
18	91.98	81.35	68.52
27	93.44	83.36	70.2
36	94.39	84.12	73.12
45	95.68	85.47	75.46
54	96.12	87.1	76.3
63	96.78	88.33	78.34
72	97.86	88.79	79.11
81	98.95	90.34	80.23
90	99.78	91.36	81.98

Table 4, clearly describes that the measurement of packet delivery ratio based on number of packet sent in an secured manner using three different methods QPSEC-DS technique and existing EAACK [1] and EAER [2]. For the simulation analysis, the number of packets sent is varied from the range of 9 to 90. The result reveals that the proposed Quantum Phase Shift Energy Conserved Data Security (QPSEC-DS) technique increases the packet delivery ratio in a secured manner when compared to two existing methods EAACK [1] and EAER [2].

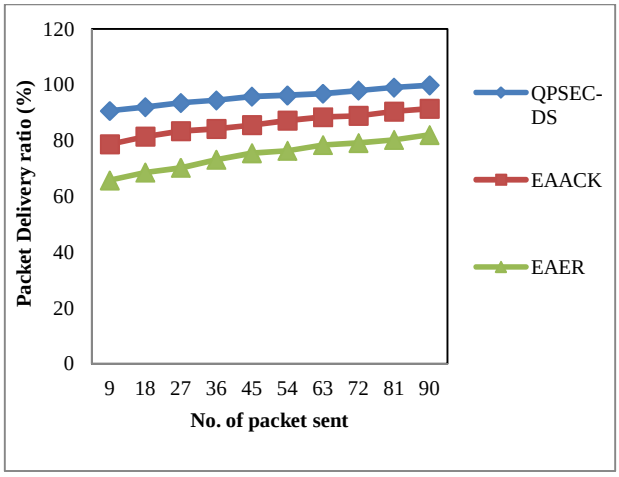

Fig.7. Measure of packet delivery ratio

In fig 7, packet delivery ratio is measured with the packet range of 9 to 90 with varying sizes at different simulation periods using three methods. As shown in figure, the QPSEC-DS technique provides the better packet delivery ratio when compared to other existing methods namely EAACK [1] and EAER [2]. In addition, while increasing the number of packets increases, the packet delivery ratio is also increased using all the three methods. Then the proposed QPSEC-DS technique using the packet delivery ratio is comparatively increased. However, the secured transmission using existing EAER routing protocol remains unaddressed. In order to improve the secured data transmission from sender to receiver, the quantum phase shift approach is applied to encrypt the input bit using QPSEC-DS technique in the network. Then the input bit is encrypted with the phase shift either 0° or 180° during sender side. The receiver also obtains the same phase shift, and then the bit is delivered successfully. Based on phase shifting approach, the shared secret key is attained and it matched with the receiver end to perform the secured and effective data transmission which resulting in improves the packet delivery ratio between sender and the receiver in a secured manner. Hence, packet delivery ratio is increased by 10% and 22% using proposed QPSEC-DS technique when compared to existing EAACK [1] and EAER [2] respectively.

B. Impact of energy consumption

Energy consumption is measured based on the amount of energy utilized between the sender and the receiver side in MANET. The energy consumption is measured in terms of Joules (J). The mathematical representation of energy consumption is given as follows.

EC = Node density * Power * Time (4)

From Eq. (4), Energy consumption 'EC' is defined as the amount of energy transmitting the data packet to the receiver side. When the energy consumption is lower, the method is said to be more efficient.

Table 5. Tabulation for energy consumption

Node density	Energy consumption (J)		
	QPSEC-DS	EAACK	EAER
50	824	925	1050
100	869	965	1075
150	880	976	1080
200	881	981	1096
250	945	1045	1135
300	986	1082	1176
350	999	1097	1183
400	1010	1105	1191
450	1065	1153	1250
500	1084	1176	1287

Table 5 describes the measurement of energy consumption based on node density with the aid of three different methods QPSEC-DS technique and existing EAACK [1] and EAER [2]. The node density is taken as input which is varied from the range of 50 to 500 for experimental purpose. The result shows that the proposed QPSEC-DS technique reduces the energy consumption when compared to existing EAACK [1] and EAER [2].

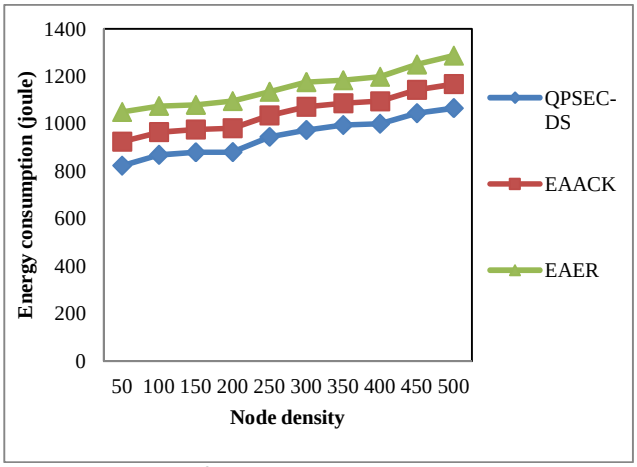

Fig. 8. Measure of energy consumption

In Fig.8, the energy consumption is measured with the node density from the range of 50 to 500 using three methods in MANET. From figure, the proposed QPSEC-DS technique consumes lesser energy when compared to the other existing methods such as EAACK [1] and EAER [2]. Furthermore, when increasing the node density, the energy consumption is also increased using all the technique. Then the proposed QPSEC-DS technique is extensively reducing the energy consumption in MANET. Though, exiting EAACK method consumes more energy in the network. Hence, the proposed QPSEC-DS technique utilizes the quantum phase shift approach for measuring the energy based on the quantum bits and the distance between sender and receiver in the mobile network. The energy dissipated per bit to transmit a data packet from sender and receiver side. In addition, the quantum phase shift approach exchanges the position of the input bit for secured transmission and also measures the lesser energy conservation between sender and receiver. With this approach, both the secured and energy optimized shifting position is attained for efficient transmission in MANET. Therefore, the proposed QPSEC-DS technique reduces the energy consumption in MANET by 10% and 22% when compared to the state-of-the-art methods EAACK [1] and EAER [2] respectively.

C. Impact of Communication overhead

Communication overhead is defined as the amount of time required to secure the data packet during the transmission in MANET. The communication overhead is defined as follows,

CO = No. of packet * Time (secured data packet transmission) (5)

From Eq. (5), 'CO' is represented as communication overhead (CO) in MANET. The communication overhead is measured in terms of milliseconds (ms). Lower the communication overhead, more efficient the method is said to be.

Table 6. Tabulation for communication overhead

No. of packet sent	Communication overhead (ms)		
	QPSEC-DS	EAACK	EAER
9	14.6	20.1	25.6
18	18.1	22.6	27.8
27	20.7	25.8	30.8
36	22.1	26.7	31.4
45	24.7	29.1	33.8
54	29.5	33.7	38.9
63	32.9	36.9	41.7
72	35.8	40.2	44.8
81	37.9	42.8	47.2
90	39.7	44.7	48.9

Table 6 illustrates the measurement of communication overhead during the data packet transmission based on three different methods QPSEC-DS technique and existing EAACK [1] and EAER [2]. For the simulation analysis, the number of packets sent is varied from the range of 9 to 90. In addition, while improving the number of packet sent, the communication overhead is also increased using all the technique. The performance result explains that the proposed QPSEC-DS technique reduces the communication overhead when compared to two existing methods EAACK [1] and EAER [2].

Fig.9 clearly describes the communication overhead is measured with the different number of packet sent is varied from 9 to 90 using three methods. As shown in figure, the proposed QPSEC-DS technique minimizes communication overhead when compared to the other existing methods such as EAACK [1] and EAER [2]. In addition, while improving the number of packet sent, the communication overhead is also increased using all the technique. Then the proposed QPSEC-DS technique is comparatively minimizes the communication overhead in MANETS. However, several intrusions affect the network performance due to increasing the network transmission range in MANET. In order to secure the data packet in MANET, the quantum mechanism is

applied through quantum key distribution. The application of quantum mechanism provides the sharing of a secret encryption key between the senders and receiver within the transmission range. The proposed QPSEC-DS technique uses quantum key distribution approach for encoding the quantum bit with the use of quantum phase shift. Based on the shifting position, the data packets are transmitted from sender to receiver with minimum time. In addition, Dynamic Source routing (DSR) protocol employs the secured data communication and it also reduces the communication overhead in MANET. Hence, the communication overhead is reduced with the aid of QPSEC-DS technique by 21% and 41% when compared to existing EAACK [1] and EAER [2] respectively.

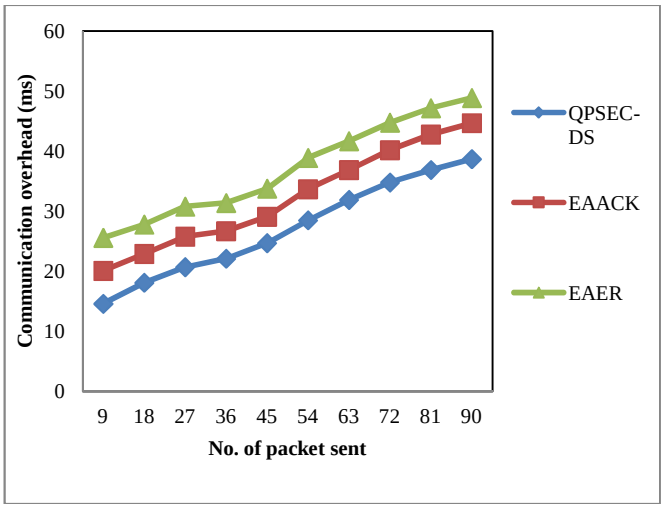

Fig.9. Measure of communication overhead

D. Impact of End to End delay

End-to-end delay is defined as the duration between the time at which the initial bit of the packet is transferred from the sender side and the time at which the last bit of the similar packet is received by the receiver. The end to end delay is mathematically written as.

End to End delay (ms) =Starting time of first bit of the packet - receiving time of the last bit of same packet (6)

From Eq. (6), when the end to end delay gets lower, then the method is said to be more efficient. The end to end delay is measured in terms of milliseconds (ms).

Table 7. Tabulation for end to end delay

No. of packet sent	End to End delay (ms)		
	QPSEC-DS	EAACK	EAER
9	3.5	5.4	7.7
18	5.9	8.4	10.8
27	8.6	11.1	13.9
36	11.8	14.6	17.2
45	13	16.4	19.3
54	17.7	20.7	23.8
63	20.8	23.7	26.7
72	23.3	26.6	29.4
81	24.2	27.8	30.5
90	30.1	33.4	35.9

Table 7 shows the measurement of end to end delay with respect to number of packet sent using three different methods QPSEC-DS technique and existing EAACK [1] and EAER [2]. The number of packets sent is varied from the range of 9 to 90 in a simulation area. The result demonstrates that the proposed QPSEC-DS technique decreases the end to end delay when compared to two existing methods EAACK [1] and EAER [2].

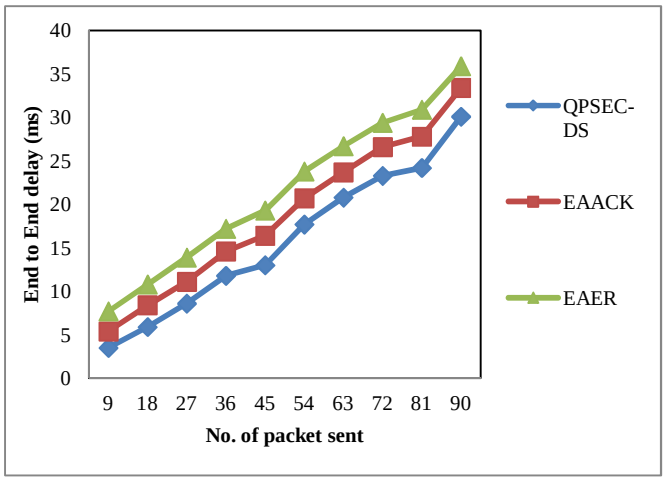

Fig.10. Measure of end to end delay

In fig.10 shows the end to end delay is measured based on the different number of packet sent is varied from 9 to 90 using three methods. From figure, the end to end delay using proposed QPSEC-DS technique is reduced when compared to the other existing methods such as EAACK [1] and EAER [2]. Moreover, when improving the number of packet sent, the end to end delay is also increased using all the technique. But, proposed QPSEC-DS technique is extensively minimizing the end to end delay in MANET. The quantum bit of the packet is transmitted through quantum phase shift. The quantum key distribution is used to achieve the perfect secret transmission. The ability of the source and destination uses the similar shared key to perform the transmission. In addition, a Quantum state generator creates a shared secret key and it distributes to source node for encryption. Also, it distributes the same key to the receiver side for decryption which resulting in improves the packet transmission with minimum end to end delay. Therefore, the end to end delay in MANET using proposed QPSEC-DS technique is minimized by 25% and 49% when compared to existing EAACK [1] and EAER [2] respectively.

5. Conclusion

In this paper, an efficient Quantum Phase Shift Energy Conserved Data Security (QPSEC-DS) technique is introduced in MANET for enhancing the secured data communication with minimum energy conservation. In order to improve the secured data transmission, the quantum phase shift approach based data communication is designed for encoding the information of input bit. Then the quantum key distribution utilizes the certain properties of quantum states for improving the security and also detecting the intrusion without disturbing the data packet transmission in MANET. The Quantum based approach uses the phase shifting operation between the sender

and receiver side through the secret key distribution that helps to enhance the security of packet transmission with minimum overhead. Based on the phase shift, the energy conservation between the sender and receiver in proposed QPSEC-DS technique which is measured to transmit the quantum bit of the data packet this in turns provides efficient energy routing. Finally, an enhanced Dynamic Source routing (DSR) protocol is implemented for efficient energy management and secured data communication between the source and destination with the aid of QPSEC-DS technique in MANET. The efficiency of QPSEC-DS technique is test with the metrics such as packet delivery ratio, end to end delay, energy consumption and communication overhead. With the simulations conducted for proposed QPSEC-DS technique, it is observed that the packet delivery ratio provided more accurate results in a secured manner as compared to state-of-the-art works. The experimental results demonstrate that proposed QPSEC-DS technique provides better performance with an improvement of packet delivery ratio and reduction of energy consumption when compared to the state-of-the-art works

References

[1] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, Vol. 60, No. 3, pp. 1089-1098, 2013

[2] Mahfuzur Rahman Bosunia, Daniel P. Jeong, Chanhong Park, and Seong-Ho Jeong, "A New Routing Protocol with High Energy Efficiency andReliability for Data Delivery in Mobile Ad Hoc Networks", International Journal of Distributed Sensor Networks, Hindawi Publishing Corporation, Vol. 2015, pp. 1-8, 2015

[3] Gautam M. Borkar, A. R. Mahajan, "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks", Wireless Networks, Springer, pp. 1-18, 2016

[4] Mohamed M.E.A. Mahmoud and Xuemin Shen, "A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 2, pp. 209-224, 2013

[5] Ziming Zhao, Hongxin Hu, Gail-JoonAhn, and Ruoyu Wu, " Risk-Aware Mitigation for MANET Routing Attacks", IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 2, pp. 250-260, 2012

[6] Bander H. AlQarni and Ahmad S. AlMogren, "Reliable and Energy Efficient Protocol for MANET Multicasting", Journal of Computer Networks and Communications, Hindawi Publishing Corporation, Vol. 2016, pp. 1-13, 2016

[7] MahaAbdelhaq, RaedAlsaqour and ShawkatAbdelhaq, "Securing Mobile Ad Hoc Networks Using Danger Theory-Based Artificial Immune Algorithm" PLoS ONE, Vol. 10, No. 5, pp. 1-16, 2015

[8] S. Gopinath, N. Nagarajan, "Energy based reliable multicast routing protocol for packet forwarding in MANET",Journal of Applied Research and Technology, Elsevier, Vol. 13, No. 3, pp. 374-381, 2015

[9] S. Russia and R. Anita, "Joint cost and secured node disjoint energy efficient multipath routing in mobile ad hoc network", Wireless network, Springer, pp. 1-10, 2016

[10] RatulDey, Himadri Nath Saha, "Secure Routing Protocols for Mobile Ad-Hoc Network (MANETs) –A Review", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol, 5, No. 1, pp. 74-78, 2016

[11] H. N. Saha, D. Bhattacharyya, and P. K. Banerjee, "Modified Fidelity Based On-DemandSecure (MFBOD) Routing Protocol in Mobile Ad hoc Network," International Journal of foundations of computing and decision sciences (FCDS), De Grurter, Vol. 40, No. 4, pp. 267-298, 2015

[12] Pu Gong, Thomas M. Chen, and Quan Xu , "ETARP: An Energy Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks", Journal of Sensors, Hindawi Publishing Corporation, Vol. 2015, pp. 1-10, 2015

[13] HindAlwan and Anjali Agarwal, "A Multipath Routing Approach for Secure andReliable Data Delivery in Wireless Sensor Networks", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, Vol. 2013, pp. 1-10, 2013

[14] Sajal Sarkar and Raja Dattab, "A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks", Ad Hoc Networks, Elsevier, Vol. 37, No. 2, pp. 209-227, 2016

[15] Pratik Gite and Sanjay Thakur, "An Effective Intrusion Detection System for Routing Attacks in MANET using Machine Learning Technique", International Journal of Computer Applications, Vol. 113, No. 9, pp. 37-44, 2015

[16] Ming Li, Pan Li, Xiaoxia Huang, Yuguang Fang, and SavoGlisic, "Energy Consumption Optimization for Multihop Cognitive Cellular Networks", IEEE Transactions on Mobile Computing, Vol. 14, No. 2, pp. 358-372, 2015

[17] Waleed S. Alnumay and UttamGhos, "Secure Routing and Data Transmission in Mobile Ad Hoc Networks", International Journal of Computer Networks & Communications (IJCNC) Vol. 6, No. 1, pp. 111-127, 2014

[18] Srinivas Kanakala, Venugopal Reddy Ananthula, and PrashanthiVempaty,"Energy-Efficient Cluster Based Routing Protocol in MobileAd Hoc Networks Using Network Coding", Journal of Computer Networks and Communications, Hindawi Publishing Corporation, Vol. 2014, pp. 1-12, 2014

[19] Amol Bhosle and Yogadhar Pandey, "Applying Security to Data Using Symmetric Encryption in MANET", International Journal of Emerging Technology and Advanced Engineering, Vol. 3, No. 1, pp. 426-430, 2013

[20] Ziane Sara and MekkiRachida., "Energy-Efficient Inter-Domain Routing Protocol for MANETs", Procedia Computer Science, Elsevier, Vol, 52, pp. 1059-1064, 2015

[21] Abdelkabir Sahnoun1, Ahmed Habbani2 and Jamal El Abbadi1," EEPR-OLSR: An Energy Efficient and Path Reliability Protocol for Proactive Mobile Ad-hoc Network Routing", International Journal of Communication

Networks and Information Security (IJCNIS), Vol. 9, No. 1, 2017,

[22] Nyoman Gunantara1, Agus Dharma1," Optimal Path Pair Routes through Multi-Criteria Weights in Ad Hoc Network Using Genetic Algorithm", International Journal of Communication Networks and Information Security (IJCNIS), Vol. 9, No. 1, 2017

[23] A.Ajina, Mydhili K.Nair," Cross Layered Network Condition Aware Mobile-Wireless Multimedia Sensor Network Routing Protocol for Mission Critical Communication", International Journal of Communication Networks and Information Security (IJCNIS), Vol. 9, No. 1, 2017