Indian Journal of Science and Technology, Vol 10(22), DOI: 10.17485/ijst/2017/v10i22/109504, June 2017
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

# Self Organized Quantum Key Authentication Technique 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

**Background /Objectives:** To improve the security in Mobile Ad Hoc network (MANET) by means of a Self Organized Quantum Key Authentication (SO-QKA). **Methods/Statistical Analysis:** The key objective of SO-QKA technique is to improve data security and mobile node authentication in MANET. Initially, SO-QKA technique generates quantum key for mobile node data transmission along the route path in MANET. Next, SO-QKA technique formulates self organized key for every mobile node with its quantum key for corresponding data transmission at specific instances. With the help of generated self organized key, SO-QKA technique finds secure route for transmitting the data in MANET. Finally, SO-QKA technique is performs key matching at the destination node where the verification of the mobile node is checked with the mobile node id of self organized key and data authentication is verified with quantum key and destination id. **Findings:** Experimental evaluation of SO-QKA technique is done with the performance metrics such as data loss rate, data transmission rate, security, execution time. Experimental analysis shows that the SO-QKA technique is able to improve the security and also improves the data transmission rate comparable to the state-of-the-art works. **Applications/ Improvements:** It can be further enlarged with implementation of new algorithm model with different parameters which improves high authentication and confidentiality.

**Keywords:** Data Communication, Key Matching, Mobile Ad Hoc Network, Mobile Node, Quantum Key, Self Organized Key

## 1. Introduction

In MANET, security properties such as authentication, secrecy and integrity are significant. Recently, many research works has been developed for secure data communication with the help of different techniques in mobile networks.

In[1] presented secure secret key agreement protocol three-node cooperative wireless communication system over block-fading channels. The key agreement scheme attains a positive secret key rate while an adversary has higher favorable channel conditions. Designed in an Aggregated-Proof based Hierarchical Authentication scheme (APHA) for achieving data confidentiality and data integrity by means of the directed path descriptor and homomorphism based Chebyshev chaotic maps[2]. In APHA, homomorphism based Chebyshev chaotic maps constructs trust relationships with the aid of the light-weight mechanisms and employed dynamically hashed values to achieve session freshness.

In[3] developed three-round anonymous roaming protocol that employed a pseudo-identity-based sign cryption scheme to accomplish effective revocation with short revocation list and efficient authentication in wireless mobile networks.

An Efficient and Privacy-Aware Data Aggregation in Mobile Sensing with Sum aggregation protocol to support large plaintext space for secured sensed data aggregation in mobile sensor networks was discussed in[4]. In[5] Presented Social-aware approach for optimizing Device-to-Device

*Author for correspondence

(D2D) communication to achieve stable transmission link with D2D communication. But, D2D (mobile node to mobile node) need to provide neighbor mobile node data transmission services that are typically handled with secured data communication.

In[6] designed, RACE a report-based payment scheme for multi-hop wireless networks to motivate node cooperation, control packet transmission and provide fairness. However, the intermediate nodes cannot provide evidences due to computational complexity. A new scheme using in[7] Localized Secure Architecture for MANET (LSAM) routing protocol for providing security in MANETs. Though, the packet drop rate was higher. A secure dispersed data transfer method with a secret sharing scheme was designed in[8] to improve reachability of the source and destination nodes in both dense and sparse networks with minimum security degradation.

In[9] proposed An Ad hoc On-demand Multicast Distance- Vector–Secure Adjacent Position Trust Verification named AOMDV–SAPTV to determine the optimal path for routing and achieving the security in MANETs. But, avoiding various attacks was remained unaddressed. An Unobservable Secure On demand Routing (USOR) aiming at enhancing the privacy during routing[10].

In[11] Introduced an energy efficient communication framework called Random Cast using dynamic source routing resulting in minimizing total energy consumption during routing. An Efficient data transfer in MANET was ensured during Cooperative Opportunistic Routing in[12]. A novel trust mechanism was used in[13] to improve the throughput and packet delivery ratio in MANET. In[14] designed a novel routing protocol to enhance the reliability of data delivery in MANET.

Progressive Energy Efficient Routing protocol in[15] derived a new link cost model to more accurately track the energy consumption. This protocol achieved minimum routing overhead, path setup delay with reduced energy consumption compared to other protocols. Anonymous Location-based Efficient Routing Protocol (ALERT) with the objective of enhancing the routing efficiency through geographic routing mechanism was followed in[16].

In[17] designed a new method to improve the security between the nodes by enhancing and improving the authentication and confidentiality between the nodes in MANETs. In[18] described that it does not provide more authentication service. An ID based Secure AODV routing protocol for providing security to the route identification and maintenance process which in turn enhanced the routing security against the attacks. But, establishing secure communication was challenging process. Self organized key management using server signed public keying technique[19] was suggested to improve security. A high Rate Uncorrelated Bit Extraction (HRUBE) framework[20] was aimed at improving the rate of security.

## 2. Methodology

Self Organized Quantum Key Authentication (SO-QKA) technique is designed in this work. During data transmission, the SO-QKA technique generates quantum key to guarantee secure communication in MANET. SO-QKA enables two users to generate a quantum key known only to them and which can then be employed to encrypt and decrypt secret messages.

SO-QKA creates self organizing key for each mobile node in MANET to identify the route path through which a source node transmits the secured data to destination node. In destination node, SO-QKA technique performs key matching to verify whether the secret data send to the exact node in MANET.

### 2.1 Quantum Key Generation

SO-QKA generates quantum key $\mathbf{QKey_i}$ for mobile node data transmission along the route path in MANET with the support of quantum key distribution. The security of QKA is based on a primary characteristic of quantum mechanics. MANET is subject to diverse security risks. Data transmission over a mobile network must be secured since traffic interceptions in mobile networks are very easier. Therefore, SO-QKA is used quantum key in which two parties can secure network communications by applying the phenomena of quantum physics.

In SO-QKA, the sender node generates quantum key $\mathbf{QKey_i}$ which is used to encrypt the secured data while performing the data transmission in MANET. During data transmission, the secret message to be transmitted is converted into the binary form. After that, following randomly selected bases (rectilinear or diagonal) are used to coverts the binary bits into qubits. This qubits is transmitted over a MANET with aiming at improving the security of data transmission.

**Table 1.** Basis and encoding value

| Bits | Rectilinear Basis + | Diagonal Basis × |
|---|---|---|
| 0 | ↑ | ↗ |
| 1 | → | ↘ |

Table 1shows, each photon is selected at random and the sender node repeats this in order to send all the photons to the receiver.

The overall architecture diagram of Self Organized Quantum Key Authentication technique is shown in Figure 1.

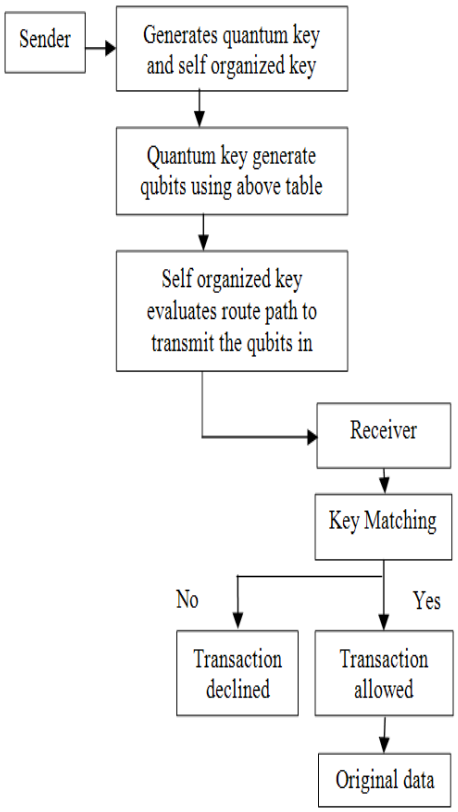


**Figure 1.** Architecture diagram of self organized quantum key authentication technique.

Figure 1 shows that, SO-QKA technique initially generates quantum key for mobile node data transmission which provides unique identification of data. This quantum key is used for encrypting and decrypting the secret message. With the aid of quantum key, the qubits is generated. This qubits is transmitted over an unsecure communication channel with aiming at improving the security of data transmission in mobile ad hoc network.

Next, SO-QKA formulates self organized key for every mobile node with its quantum key for identifying the route path to transmit the secret data in MANET. Finally, Key Matching is performed in receiver side to validate the whether the secret data send to the accurate destination node in MANET. As a result, SO-QKA technique achieved secure data communication in MANET.

## 2.2 Self Organized Key Generation for Identifying Secured Route Path

In SO-QKA technique, the self organized key is generated for every mobile node to discover the rout path through which a source node transmits the secured data to the destination node. The self organized key comprises of four components such as mobile node id, quantum key, destination id and the instance id. In SO-QKA technique, a self organizing key '$SKey_i$' for each mobile node '$N_i$' is generated with mobile node id, quantum key, destination id which is formulated as,

$$\textbf{self organizing key} \rightarrow N_i, QKey_i, \textbf{destination id}, \textbf{instance id} \quad (3..1)$$

The structure of self organized key in SO-QKA technique is shown in below Figure 2.

| Mobile node id | Quantum key | Destination id | Instance id |
|---|---|---|---|

**Figure 2.** Structure of self organized key.

Figure 2 shows that, mobile node id represents the mobile node id of that node and Quantum key contains the qubits of secured data and their secret key for decryption process. Instance id refers the subsequent neighbor nodes id (i.e. trust factor of subsequent neighbor nodes id) and destination id help for intermediate nodes to identify the receiver node. The process of self organized key generations for identifying the neighbor node to perform secure data communication in MANET.

Figure 3 shows that, SO-QKA technique secured neighbor node to transmit the secret data efficiently in MANET. Let us consider the two mobile nodes '$N_i$' and '$N_j$' in MANET. If the mobile node '$N_i$' believes that a self organized key $SKey_i$ belongs to another mobile node '$N_j$', then the mobile node '$N_i$' grants a self organized key certificate in which $SKey_i$ is bounded to '$N_j$' by the signature of '$N_i$' which is mathematically formulated as,

$$N_i \rightarrow N_j : SKey_j \forall N_j, (i \in 1, 2, \ldots, n) \quad (3.2)$$

From 3.2, $SKey_j$ indicates the trust factor of neighbor node. In order to estimate the trust factor $Trust\ factor_{i,j}$, the difference between the percentages of data packets forwarded $DPF_{i,j}$ to the percentage of data packets dropped $DPD_{i,j}$ over the total number of data packets $DP_n$ offered to the neighboring mobile nodes '$NMN_i$' is measured.

In SO-QKA technique, the data packets forwarded is the percentages of data packets initiated from $N_i$ that was forwarded by $N_j$ over the total number of data packets provided to '$N_j$'. Therefore, the data packets forwarded is mathematically formulated as,

$$\sum_{i,j=1}^{n} DPF_{i,j} = \frac{DPF(N_j)}{DP_i} \quad (3.3)$$

Besides, the data packets dropped is the percentages of the packets that were dropped over the total number of data packets provided to $N_j$. Therefore, the data packets dropped is mathematically formulated as,

$$\sum_{i,j=1}^{n} DPD_{i,j} = \frac{DPD(N_j)}{DP_i} \quad (3.4)$$

Further, the difference between the percentages of data packets forwarded to the percentage of data packets dropped over the total number of data packets offered to the neighboring mobile nodes i.e. trust value is mathematically formulated as below,

$$Trust\ factor_{i,j} = DPF_{i,j} - DPD_{i,j} \quad (3.5)$$

With the help of acquired trust value of the neighboring nodes, the decision regarding the data packet forwarding is performed in an efficient manner which in turn enhances the security of data communication in MANET.

### *2.2.1 Self Organized Key Neighbor Node Authentication Algorithm*

Algorithm 1 shows that, generated self organizing key for each mobile node, a route path through which the source node '$SN$' transmits the secured data packets '$DP_i$' to the destination mobile node '$DN$' is determined. In SO-QKA technique, Self organizing key helps the mobile nodes to authenticate themselves with the neighboring mobile nodes in the network before they perform data packet transmission. As a result, SO-QKA technique establishes secured data communication in MANET which in turn improves the security of data transmission in a significant manner.

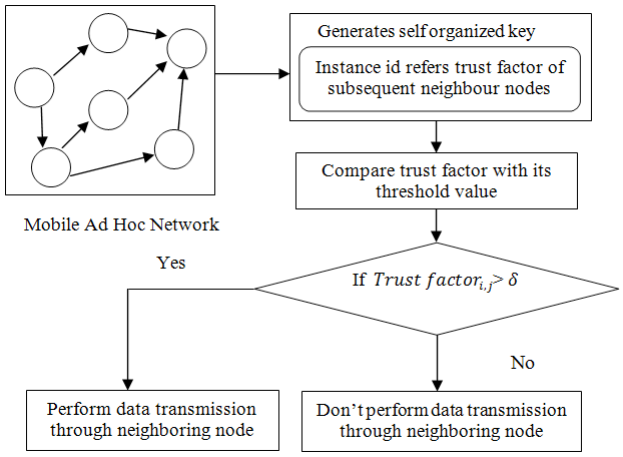


**Figure 3.** Block diagram of self organized key generation for identifying secured route path.

**Algorithm 1.** Self organized key neighbor node authentication algorithm

Input: Source Node '$SN$'; Destination Node '$DN$'; Mobile Nodes '$N_i = N_1, N_2, \ldots, N_n$'; Quantum Key value '$QK_i = QK_1, QK_2, \ldots QK_n$'; Self Organizing Key '$SKey_i = SKey_1, SKey_2, \ldots, SKey_n$'; Data Packets '$DP_i = DP_1, DP_2, \ldots, DP_n$'; Threshold '$\delta$'

Output: Secure data communication in MANET

Step 1: Begin

Step 2: For each Mobile Node '$N_i$'

Step 3: If ($N_i$ is neighbour to the $N_j$ th node)

Step 4: Evaluate Data Packet Forwarding Rate using (3)

Step 5: Evaluate Data Packet Drop Rate using (4)

Step 6: Determine trust factor using (5)

Step 7: If ($Trustfactor_{i,j} > \delta$ )

Step 8: Neighboring nodes are highly secured nodes

Step 9: Perform data transmission through neighboring nodes
Step 10: Else
Step 11: Neighboring nodes are not secured nodes
Step 12: Do not perform data transmission through neighboring nodes
Step 13: End if
Step 14: Else
Step 15: Go to step 3
Step 16: End if
Step 17: End for
Step 18: End

### 2.3 Key Matching

In Self Organized Quantum Key Authentication SO-QKA technique, key matching is performed in receiver side to authenticate whether the secret data send to the exact node in MANET.

In SO-QKA technique, the verification of the mobile node is checked with the mobile node id of self organized key and data authentication is verified with quantum key and destination node id as shown in Algorithm 2.

**Algorithm 2.** Overall process of SO-QKA technique
// Overall Process Of SO-QKA Technique
Input: Source Node '$SN$'; Destination Node '$DN$'; Mobile Nodes '$N_i = N_1, N_2, \ldots, N_n$'; Quantum Key value '$QK_i = QK_1, QK_2, \ldots QK_n$'; Self Organizing Key '$SKey_i = SKey_1, SKey_2, \ldots SKey_n$'; 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: Generate self organized key for every mobile node in MANET
Step 4: Identify the secure route path using algorithm
Step 5: Perform data transmission
Step 6: destination node perform key matching
Step 7: if key matching
Step 8: Transaction allowed
Step 9: destination node obtains original message
Step 10: Else
Step 11: Transaction declined
Step 12: End if
Step 13: End

With the help of above process, SO-QKA technique is efficiently performs secure data transmission in MANET. This is turn improves the data transmission rate and also reduces the execution time taken for performing secured data transmission in an effective manner.

## 3. Experimental Settings

The SO-QKA in mobile ad hoc Network is implemented using NS-2 simulator with the network range of 1500*1500 m size. The number of mobile nodes selected for performing experimental purpose is 70 nodes in SO-QKA technique. For conducting experimental work, Destination Sequence Based Distance Vector DSDV is employed as routing protocol for SO-QKA technique. The moving speed of the mobile nodes for SO-QKA technique in MANET is about 10 m/s for each mobile node with a simulation rate of 45 seconds for data transmission between mobile nodes. The parametric values for performing experiments are shown in Table 2.

**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 |
| Packets | 15, 30, 45, 60,75, 90, 105 |
| Key Size | 6 digit |
| Mobility speed | 10 m/s |
| Pause time | 15 s |

Simulation is carried out with numerous time instances for different mobile node density and speed of mobile nodes. In addition, the performance of proposed SO-QKA technique is estimated with various sizes of data for transmission along with multiple malicious adversaries in the network for secured data delivery in MANET.

The performance of SO-QKA technique is tested with metrics such as data loss rate, data transmission rate, security, execution time. The result of the SO-QKA technique is compared against with existing methods such as secure secret key agreement protocol[1] and Aggregated-Proof based Hierarchical Authentication scheme (APHA)[2] respectively.

## 4. Results and Discussion

To validate the efficiency of proposed SO-QKA technique, the comparison is made with existing two methods namely secure secret key agreement protocol[1] and Aggregated-Proof based Hierarchical Authentication scheme (APHA)[2]. The performance of SO-QKA technique is evaluated along with the following metrics.

### 4.1 Measurement of Packet Loss Rate

In SO-QKA technique, the packet loss rate is defined as the amount of packets lost during the data transmission from the source nodes to destination nodes. The packet loss rate is measured in terms of packets per second (pps) and it mathematically formulated as

$$\text{packet loss rate} = (P_s - P_r) \quad (5.1)$$

From the equation (5.1), the packet loss rate is obtained by using packets send '$P_s$' and packets received '$P_r$'. When the packet loss rate is lower, the method is said to be more efficient.

**Table 3.** Tabulation for packet loss rate

| Number of data packets | Packet Loss Rate (pps) | | |
|---|---|---|---|
| | Secure Secret Key Agreement Protocol | APHA scheme | SO-QKA technique |
| 15 | 6 | 5 | 3 |
| 30 | 14 | 10 | 9 |
| 45 | 20 | 16 | 11 |
| 60 | 23 | 17 | 15 |
| 75 | 30 | 26 | 20 |
| 90 | 33 | 30 | 27 |
| 105 | 44 | 34 | 29 |

The data packet loss rate result of three different methods namely secure secret key agreement protocol[1], APHA[2] and SO-QKA technique is shown in Table 3. SO-QKA technique considers the framework with different number of data packets in the range of 15-105 for conducting the experimental works using NS-2 simulator. From the table value, it is expressive that the proposed SO-QKA technique has obtained lower packet loss rate than the other existing works[1,2].

But comparatively data loss rate using proposed SO-QKA technique is lower. This is because of the self organized key generation in SO-QKA technique. With the aid of self organized key generated for every mobile node, SO-QKA technique efficiently identifies secure neighbor node (i.e. minimum data packet drop rate node) to transmit the secret data in MANET. Therefore, the data loss rate of SO-QKA technique is reduced in an effective manner. As a result, proposed SO-QKA technique is reduced the data loss rate by 59% when compared to the secure secret key agreement protocol[1] and 29% when compared to the APHA[2] respectively.

### 4.4 Measurement of Data Transmission Rate

In SO-QKA technique, data transmission rate is defined as the ratio of number of data packets successfully transmitted at the destination node without any false data to the number of data packets sent. The data transmission rate is measured in terms of percentage (%) and it mathematically formulated as below,

$$\text{data transmission rate} = \frac{\text{Number of data packets successfully transmitted}}{\text{Number of data packet sent}} * 100 \quad (5.2)$$

**Table 4.** Tabulation for data transmission rate

| Number of data packets | Data Transmission Rate (%) | | |
|---|---|---|---|
| | Secure Secret Key Agreement Protocol | APHA scheme | SO-QKA technique |
| 15 | 67 | 75 | 83 |
| 30 | 70 | 77 | 87 |
| 45 | 72 | 81 | 89 |
| 60 | 76 | 85 | 92 |
| 75 | 78 | 87 | 95 |
| 90 | 81 | 91 | 97 |
| 105 | 85 | 93 | 99 |

From the table 4 value, it is descriptive that the proposed SO-QKA technique has obtained higher data transmission rate than the other existing works[1,2].

But comparatively data transmission rate using proposed SO-QKA technique is higher. This is because of the quantum key generation in SO-QKA technique. With the aid of quantum key, SO-QKA technique efficiently encodes the secret data into qubits with the objective of improving the security of data transmission in MANET. Therefore, the data transmission rate of SO-QKA technique is improved in an efficient manner. As a result,

proposed SO-QKA technique is improved the data transmission rate by 18% when compared to the secure secret key agreement protocol[1] and 8% when compared to the APHA[2] respectively.

## 4.5 Measurement of Security (Data Packets Forwarding in Neighbor Node)

In SO-QKA technique, Security with respect to data packets being forwarded is evaluated on the basis of data packets received by the neighboring node in mobile ad hoc network. Accordingly, security is defined as the difference between the total numbers of packet sent to the packets not received by the neighboring node to the total number of packets sent in MANET. Security is measured in terms of percentage (%) and mathematically formulated as,

$$\text{Security (data packets)} = \frac{DP_s - DP_{nr}}{\text{total number of packets sent}} * 100 \quad (5.3)$$

Figure 4 shows that, proposed SO-QKA technique is provides better security result as compared to secure secret key agreement protocol1, APHA2. Besides, while increasing the number of data packets to be sent, the security is also gets increased using the all the three methods.

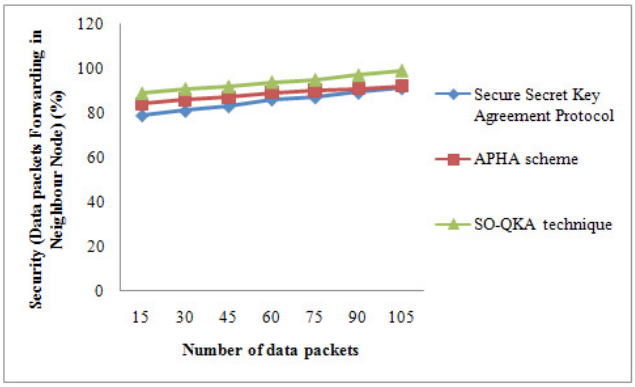


**Figure 4.** Measure of security (Data packets Forwarding in Neighbour Node).

But comparatively security using proposed SO-QKA technique is higher. This is due to the self organized key generation in SO-QKA technique where trust factor is measured to validate whether the neighboring nodes are highly secured nodes for transmitting the secret data.

Therefore, the security of SO-QKA technique is improved in a significant manner. As a result, proposed SO-QKA technique is improved the security by 9% when compared to the secure secret key agreement protocol [1] and 6% when compared to the APHA [2] respectively.

## 4.6 Measurement of Execution Time

In SO-QKA technique, execution time refers the amount of time taken for performing secured data transmission in MANET. Therefore, execution time 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. The execution time of secured data transmission is measured in terms of milliseconds (ms) and formulated as,

$$\text{Execution time} = \sum_{i=1}^{n} DP * \text{Time}(DP_i) \quad (5.4)$$

Figure 5 proposed SO-QKA technique is provides better execution time as compared to secure secret key agreement protocol1, APHA2. Besides, while increasing the number of data packets to be sent, the execution time is also gets increased using the all the three methods.

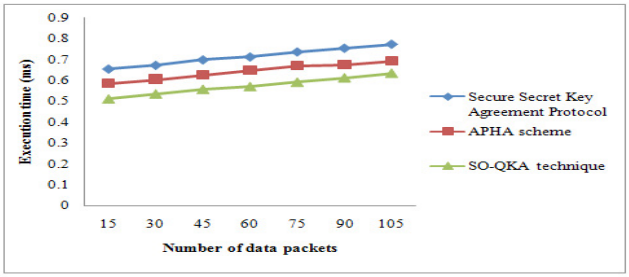


**Figure 5.** Measure of execution time.

But comparatively execution time proposed SO-QKA technique is lower. This is because of the quantum key and self organized key generation in SO-QKA technique. With the aid of quantum key, SO-QKA technique efficiently generates qubits for transmitting the secret data. In addition, with the aid of self organized key, SO-QKA technique efficiently performs secure data transmission in MANET. This in turn helps in reducing the execution time in a significant manner. As a result, proposed SO-QKA technique is reduced the execution time by 25% when compared to the secure secret key agreement protocol[1] and 15% when compared to the APHA[2] respectively.

# 5. Conclusion

In this paper, an effective novel framework is designed called as Self Organized Quantum Key Authentication (SO-QKA)

technique to provide secure data communication in mobile ad hoc network. The main objective of SO-QKA technique is to enhance data security and mobile node authentication in MANET. Initially proposed SO-QKA technique generates quantum key for mobile node data transmission. By using the quantum key, the qubits is produced in SO-QKA technique where it ensures secure data transmission. After that, SO-QKA technique generates self organized key for each mobile nodes in MANET to determine secure route path through which the source node transmits the secured data packets to the destination mobile node. Finally, SO-QKA technique is accomplished key matching at the receiver mobile node to confirm whether the secret data send to the precise receiver node in MANET. The effectiveness of SO-QKA technique is tested with the metrics such as data loss rate, data transmission rate, security, execution time. With the experiments conducted for SO-QKA technique, it is observed that the security of data transmission is provided more accurate results as compared to state-of-the-art works. The simulation results demonstrate that SO-QKA technique is provides better performance with an improvement of security by 13% and the data transmission rate by 8% when compared to the state-of-the-art works.

## 6. 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. Crossref
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. Crossref
3. Jo HJ, Paik JH, Lee DH. Efficient privacy-preserving authentication in wireless mobile networks. IEEE Transactions on Mobile Computing. 2014; 13(7):1469–81. Crossref
4. Li Q, Cao G, Porta TFL. Efficient and privacy-aware data aggregation in mobile sensing. IEEE Transactions on Dependable and Secure Computing. 2014; 11(2):115–29. Crossref
5. Zhang Y, Pan E, Song L, Saad W, Dawy Z, Han Z. Social network aware device-to-device communication in wireless networks. IEEE Transactions on Wireless Communications. 2015; 14(1):177–90. Crossref
6. Mohamed MEA, Shen X. A secure payment scheme with low communication and processing overhead for multihop wireless networks. IEEE Transactions on Parallel and Distributed Systems. 2012; 24(2):209–24.
7. Poongodi T, Karthikeyan M. Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks. Wireless Personal Communications. 2016 Sep; 90(2):1039–50. Crossref
8. Murakami T, Kohno E, Kakuda Y. An adaptivity-enhanced multipath routing method for secure dispersed data transfer method in ad hoc networks with varying node density. IEEE 11th International Conference on Ubiquitous Intelligence and Computing and IEEE 11th International Conference on and Autonomic and Trusted Computing, and IEEE 14th International Conference on Scalable Computing and Communications and its Associated Workshops (UTC-ATC-ScalCom); 2014. p. 502–9. Crossref
9. Borkar GM, Mahajan AR. A secures and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks. Wireless Networks. 2016:1–18.
10. Wan Z, Ren K, Gu M. USOR: An unobservable secure on-demand routing protocol for mobile ad hoc networks. IEEE Transactions on Wireless Communications. 2012; 11(5):1922–32. Crossref
11. LimS, Yu C, Das C R. RandomCast: An Energy-Efficient Communication Scheme for Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing. 2009 Aug; 8(8):1039–51. Crossref
12. Wang Z, Chen Y, Li C. CORMAN: A novel cooperative opportunistic routing scheme in mobile ad hoc networks. IEEE Journal on Selected Areas In Communications. 2012 Feb; 30(2):289–96. Crossref
13. Feng R, Che S, Wang X, Yu N. A credible routing based on a novel trust mechanism in ad hoc networks. International Journal of Distributed Sensor Networks. 2013 Mar:1–13.
14. Bosunia MR, Jeong DP, Park C, Jeong SH. A new routing protocol with high energy efficiency and reliability for data delivery in mobile ad hoc networks. Hindawi Publishing Corporation International Journal of Distributed Sensor Networks. 2015; 13(4).
15. Zhu J, Wang X. Model and protocol for energy-efficient routing over mobile ad hoc networks. IEEE Transactions on Mobile Computing. 2011 Nov; 10(11):1546–57. Crossref
16. Shen H, Zhao L. ALERT: An anonymous location-based efficient routing protocol in MANETs. IEEE Transactions on Mobile Computing. 2013; 12(6):1546–57. Crossref
17. Alomari A. Security authentication of AODV protocols in MANETs. Network and System Security. Springer; 2013. p. 621–7. Crossref
18. Alnumay WS, Ghos U. Secure routing and data transmission in mobile ad hoc networks. IJCNC. 2014 Jan; 6(1):111–27. Crossref
19. John S P, Samuel P. Self-organized key management with trusted certificate exchange in MANET. Ain Shams Engineering Journal. 2015 Mar; 6(1):161–70. Crossref

20. 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; 9(1):17–30. Crossref