QUANTUM THREE-PASS PROTOCOL AUTHENTICATION WITH GENETIC ALGORITHM BASED HILL-CIPHER ALGORITHM FOR NETWORK SECURITY ENHANCEMENT

Dr. G. Mohammed Nazer

Principal and Head-Dept., of Computer Science, RAAK Arts and Science College, Villupuram District, TamilNadu.

Abstract

In present times, the study of security in computer networks is a quickly growing area of interest due to the creation of networks and the scarcity of security measures in numerous existing networks. Cryptography is the science of defense of confidential data from illegal access, assuring data integrity, authentication, and other processes. For attaining this aim, a cryptographic technique is applied to generate a cryptogram with extra information. The quantum cryptography is a rising technology depending upon quantum mechanics, the phenomenon of light and the characteristics of light. It enables a transmission of data between two users without sharing any secret details. This paper presents a quantum three-pass protocol (QTPP) authentication based on Genetic algorithm (GA) with Hill-cipher algorithm. The matrix in Hill Cipher is developed to carry out the encryption and decryption processes. GA provides an optimized manner of determining the key employed to encrypt and decrypt the data using Hill Cipher. By computing the evaluation function in GA, the key which fits the composition will be attained. An elaborate experimentation takes place to ensure the goodness of the presented model. The attained simulation outcome strongly pointed out the better performance of the presented model over the compared methods.

Keywords: Cryptography, Network Security, Hill Cipher, Quantum Three Pass Protocol, Genetic Algorithm

1. Introduction

Cryptography is the discipline of defense of secret data from illegal access, ensure data integrity, authentication, and other processes. For attaining this intention, a cryptographic technique is utilized for producing a cryptogram with few extra details, known as key. The traditional cryptographic technique can be classified into two major kinds based on the sender and receiver namely symmetrical and asymmetric models. In the former one, both parties utilize same key and the latter one employs different keys. The one time padding technique comes under the traditional cryptography [1]. The quantum cryptography is a rising field developed using the

fundamentals of quantum mechanics, the phenomenon of light and the characteristics of light. The quantum cryptography has begun in the year of 1984 by a physicist named Bennett where unconditionally secure quantum key distribution protocol known as BB84 has been presented. It enables two users to securely communication data with no use of secret data transmission [2]. With respect to the uncertainty principle, it is verified in a scientific way in 1992 [3]. Then, [4] showed that the deterministic quantum key distribution is proposed where the quantum secure direct communication has been developed through the communication of individual photons with normal channel. The Ping-Pong quantum secure direct communication makes use of the entanglement [5]. In [6, 7] the limitations of the PingPong model has been simultaneously enhanced. A quantum secure direct communication model utilizing individual photons as discussed in [8, 9].

Quantum dense key distribution utilizes quantum key distribution and quantum dense encoding [10] to prove the key distribution improvement on the capacity of transmission [11–13]. A novel type of quantum cryptography approach depending upon Shamir's three-pass protocol (TPP) of traditional cryptography has been presented [14], and then the quantum three-pass protocol (QTPP) with respect to quantum superposition state has been devised [15] indicating that none of the keys were communication between two parties in contrast to BB84 protocol.

At recent days, quantum encryption model has been presented and pointed out that the quantum encryption models are found to be identical to the traditional encryption technique apart from that the quantum approach which depends upon the quantum laws and the traditional mathematical oriented concepts. The growth in the domain of quantum computation might poses a threat to classical encryption models due to the Shor's quantum factor, discrete and quantum Grover's searching approaches. Therefore, several studies have designed novel models for protecting data with the progresses made in this field. Due to the essential features which are defined by the quantum models which differentiate it from traditional models where the attacker can be identified under quantum in an easier way, the nonorthogonal quantum states could not be effectively differentiated. In addition, an unconditionally security model is very important on the traditional way of protecting data. So, the quantum approaches are found to be the optimal ones for accomplishing the present requirements.

The quantum cryptography is a rising technology depending upon quantum mechanics, the phenomenon of light and the characteristics of light. It enables a transmission of data between two users without sharing any secret details. This paper presents a QTPP authentication based on Genetic algorithm (GA) with Hill-cipher algorithm. The matrix in Hill Cipher is developed to carry out the encryption and decryption processes. GA provides an optimized manner of determining the key employed to encrypt and decrypt the data using Hill Cipher. By computing the evaluation function in GA, the key which fits the composition will be attained. An elaborate experimentation takes place to ensure the goodness of the presented model. The attained simulation outcome strongly pointed out the better performance of the presented model over the compared methods.

The rest of the paper is formulated as follows. Section 2 describes an outline of QTTP. Section 3 explains the presented model in an elaborate way. Section 4 performs experimental validation and section 5 provides conclusion.

2. Quantum Three-Pass Protocol (QTPP)

Currently, TPP has been generally utilized in several applications, for example, cryptography. The QTPP is a new addition to the protocols of the quantum cryptography protocol and based on Shamir's TPP of usual cryptography. The main feature in this protocol is to utilize only the quantum channels different from other quantum protocols to utilize the quantum as well as usual channel. The process of this protocol is utilizing the photon as a qubit; then every usual bit is encrypted to the qubit. Behind the usual bit of encrypting to photon, the polarization to photon is turn around with the angle θj that is arbitrarily selecting every qubit. The rotation function can be signified as

$$R(\theta j) = \begin{Bmatrix} \cos\theta j & \sin\theta j \\ -\sin\theta j & \cos\theta j \end{Bmatrix}. \quad (1)$$

This function can be regarded as encryption with an angle θj signifies the encryption key, although the rotation function can be regarded in decryption by angle$-\theta j$. In the QTPP there is no distributed key among sender as well as receiver; the sender creates its own confidential $K_{\theta \mathrm{SEN}}$ where $(K_{\theta \mathrm{SEN}} = \{\theta_{SEN} | 0 \leq \theta_{SEN} < \pi\})$ to every session. With the receiver creates its own confidential key $K_{\theta REC}$ where $(K_{\theta REC} = \{\theta_{REC} | 0 \leq \theta_{REC} < \pi\})$ for every session. Assured the opponent never determined these keys. For n-qubits, the key to sender as well as receiver altered with every qubit and every key is utilized only twice with creator that maintained to other n-qubits of the key. Thus, the new key will avoid several data connected to the key with data from being infiltrated. At present, if supposed that the plaintext P is single photon encryption to the qubit as $P = |1\rangle$, the sender as well as receiver creates their own key, sender key $= K_{\theta \mathrm{SEN}}$, and receiver key $= K_{\theta REC}$. The sender encrypted the plaintext P with its making of key as the subsequent:

$$E_{\mathrm{K}_{\theta \mathrm{SEN}}}[P]: REC(\theta_{\mathrm{SEN}})|1\rangle = \begin{bmatrix} \cos\theta_{\mathrm{SEN}} & \sin\theta_{\mathrm{SEN}} \\ -\sin\theta_{\mathrm{SEN}} & \cos\theta_{\mathrm{SEN}} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \sin\theta_{\mathrm{SEN}}|0\rangle + \cos\theta_{\mathrm{SEN}}|1\rangle$$
$$= |\emptyset_1\rangle \, (2)$$

where E is the encryption through sender key $K_{\theta \mathrm{SEN}}$, and the resultant is the superposition state $|\emptyset_1\rangle$where the sender will transmit to receiver. The receiver receives the photon in $|\emptyset_1\rangle$ and encrypted it through its own key as the subsequent:

$$E_{\mathrm{K}_{\theta REC}}\left[E_{\mathrm{K}_{\theta \mathrm{SEN}}}[P]\right]: REC(\theta_{REC})|\emptyset_1\rangle$$

$$= \sin(\theta_{REC} + \theta_{\mathrm{SEN}})|0\rangle + cos(\theta_{REC} + \theta_{\mathrm{SEN}})|1\rangle = |\emptyset_2\rangle, \quad (3)$$

where $|\emptyset_2\rangle$ is the superposition state. The receiver transmits $|\emptyset_2\rangle$back to the sender. The sender obtains $|\emptyset_2\rangle$and decryption it with utilizing the angle θ_{SEN} but through rotation of $-\theta_{SEN}$ as there is decrypted in this case; next the outcomes $|\emptyset_3\rangle$ transmit back to the receiver as the subsequent:

$$D_{\mathrm{K}_{\theta\mathrm{SEN}}}\left[E_{\mathrm{K}_{\theta REC}}\left[E_{\mathrm{K}_{\theta\mathrm{SEN}}}[P]\right]\right]$$

$$= E_{\mathrm{K}_{\theta REC}}[P] : REC(-\theta_{SEN}) = \sin\theta_{REC}\,|0\rangle + \cos\theta_{REC}|1\rangle = |\emptyset_3\rangle, (4)$$

where D is the decryption by sender key $K_{\theta\mathrm{SEN}}$. The receiver receives $|\emptyset_3\rangle$ and decrypted it with utilizing angle θ_{REC} although with rotation of $-\theta_{REC}$as there is decrypts in this case; after that the receiver obtains the plaintext P that the sender sends it $|1\rangle$ as the subsequent:

$$D_{\mathrm{K}_{\theta REC}}\left[E_{\mathrm{K}_{\theta\mathrm{SEN}}}[P]\right] : REC(-\theta_{REC})\,|\emptyset_3\rangle$$

$$= \begin{bmatrix}\cos-\theta_{REC} & \sin-\theta_{REC}\\ -\sin-\theta_{REC} & -\cos\theta_{REC}\end{bmatrix}\begin{bmatrix}\sin\theta_{REC}\\ \cos\theta_{REC}\end{bmatrix} = |1\rangle. \quad (5)$$

At last, the receiver has the plaintext$j1i$. The entire process of the protocol is in Fig. 1 and every protocol is presented, proposed and increased.

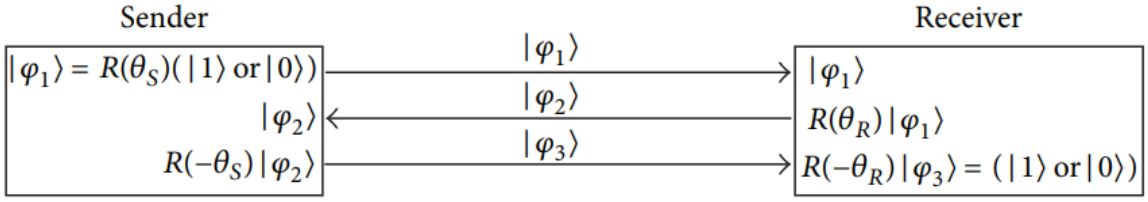

Fig. 1. QTPP procedure

3. The proposed model

In this section, a QTPP authentication based on GA with Hill-cipher called QTTP-GA-HC algorithm has been presented. The matrix in Hill Cipher is developed to carry out the encryption and decryption processes. GA provides an optimized manner of determining the key employed to encrypt and decrypt the data using Hill Cipher. By computing the evaluation function in GA, the key which fits the composition will be attained.

3.1. Hill cipher based GA

GA is a computational technique that stimulated the hypothesis of development that was afterwards accepted into computational techniques is utilized to solve a search value in an optimized problem. This technique is creating on the genetic methods in living organisms. Fig. 2 describes the steps involved in the GA method. There are 3 important phases exist in GA namely

crossover, selection and mutation. Selection is utilized to rejoin the population with the maximum probability. The arbitrary number created is joined with the cumulative probability. The nearby value is occupied to return the actual value of the population.

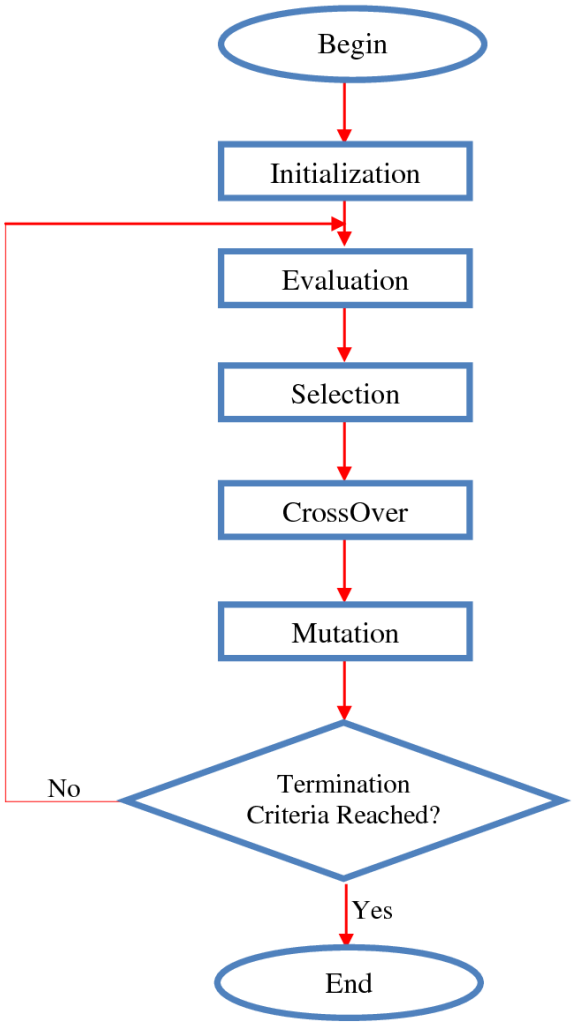

Fig. 2. Step involved in GA

Crossover is a GA operator to combine the chromosome through additional chromosome select to make child chromosome from one generation to next. It generally chooses some qualified parents [16]. The qualification is the crossover rate value. This value relates to choose the parent chromosome. Mutation is a genetic operator utilized to continue genetic diversity from one generation of a population of GA chromosomes to next. This operator relocates the chromosomes with replacing the value of chromosome. The chromosome index does not modify, however the value of index is replaced to other value in the other index. Mutation causes progress in the search space and can generate stronger chromosome. Each chromosome in Hill Cipher contains of 9 numbers. Every gene has a value among 0 to 255 that signifies the number

of byte. Because the ASCII value does not over 255, we do not obtain an integer as the modular expression. There are 3 important phase in GA namely crossover, selection and mutation. Selection is utilized to rejoin the population with the maximum probability. The arbitrary number created is joined with the cumulative probability. The nearby value is occupied to return the actual value of the population.

K11	K12	K13
K21	K22	K23
K31	K32	K33

K11	K12	K13	K21	K22	K23	K31	K32	K33
x	x	x	x	x	x	x	x	x

Fig. 3. Hill Cipher Chromosome

Fig. 3 illustrates the form of the Hill Cipher chromosome. The matrix is transformed into one-dimension vector. Every cell is filled with an arbitrary integer number (x). The fitness function estimates the determinant of the chromosome by this subsequent formula.

$$F = D\ (1) \tag{6}$$

Where F denotes Fitness and D denotes Determinant. The GA of this technique is rather straightforward than the one of a usual technique to scheduling as we do not have to search till the fitness value reaches no error. We just search the ideal fitness that does not contain equal value. Because the determinant is in the odd number, it is optimal to Hill Cipher. However, we still to find until the determinant reaches 1.

3.2. GA based Hill-Cipher Algorithm on QTPP

In this case, the unique feature in the QTPP is to there is no requiring to traditional channel similar to BB84 although there is require to only quantum channel, in order that every data and data that manage this protocol is quantum data [17]. It is recognized that the replace, saved, and procedure of data are performed with utilizing elementary entities known as bits, where these bits are signified with separate values 0 and 1. Newly through the tremendous progress in the domain of data, cryptography and communication, these usual bits are accepted with light pulses, equivalent to macroscopic packets of photons, permitting a usual explanation of their performance as well as propagation. Physicists have appreciated that separate quantum objects, for sample, photons, could also be utilized to manage another variety of data. Now data is no longer encoding on the number of occupied photons, but separate photons simply serve as carrier and quantum data and photons are encoding on their quantum assets, similar polarization or

time-bins of arrival. Certainly, with choosing 2 orthogonal states spanning the Hilbert space, $|0\rangle$ and $|1\rangle$ now encoding the zero and one values of quantum bit (qubit), and quantum superposition creates it probable to make states of the form:

$$|\emptyset\rangle = \alpha|\,0\rangle\ + \beta|\,1\rangle\,, \tag{7}$$

where $\alpha, \beta \in C$ and $|\alpha^2| + |\beta^2| = 1$.

Quantum superposition is very essential to quantum communication protocols. We supposed that a photon is utilized as a qubit. The photon is utilized as a qubit and 1 polarization base set horizontal or vertical to signify a usual 2-level system. The horizontally polarized photon signifies logic 0, $|0\rangle = (1\ 0)^T$, and a vertically polarized photon signifies logic 1, $|1\rangle = (1\ 0)^T$. At present, behind the sender executes the usual Hill-cipher technique and encoding the plaintext, every letter in encode plaintext is transformed to binary code (BC). Behind the alteration of the letters to BC, the whole data binary bit is encrypted into a single particle known as qubit or encoding plaintext qubits $|E\rangle$ and after that transmits every qubits to the receiver with utilizing the QTPP as follows. Initial, sender as well as receiver create their session keys $K_{\theta SEN}$ and$K_{\theta REC}$. Sender encrypts the encoded plaintext qubits $|E\rangle$ by its encrypted key$K_{\theta \mathrm{SEN}}$:

$$|\emptyset_1\rangle = |E\rangle \cdot K_{\theta \mathrm{SEN}}\,. \tag{8}$$

Sender transmits the resultant state to receiver. Receiver obtains the photon and encrypted through its key$K_{\theta REC}$. The resultant state is until a superposition state and the receiver transmits it back to sender:

$$|\emptyset_2\rangle = |\emptyset_1\rangle \cdot K_{\theta \mathrm{REC}}\,. \tag{9}$$

The sender obtains and decrypts it with rotating it reverse through angle $K_{-\theta \mathrm{SEN}}$ and transmits the resultant superposition state to receiver another time:

$$|\emptyset_3\rangle = |\emptyset_2\rangle \cdot K_{-\theta \mathrm{REC}}\,. \tag{10}$$

Receiver obtains and decrypts it with rotating it reverse through the angle$K_{-\theta REC}$:

$$|E\rangle = |\emptyset_3\rangle \cdot K_{-\theta \mathrm{REC}}. \tag{11}$$

This method maintains through every qubit of the encoded plaintext qubit $|E\rangle$ still the receiver obtains entire encoding plaintext qubits $|E\rangle$, afterwards alter every BC to letters that are then decoding to the plaintext with utilizing the key inverse of Hill-cipher algorithm (KIHCA) where the sender and receiver agree on the key of Hill-cipher algorithm (KHCA). Here, the receiver has the actual plaintext.

4. Experimental Validation

In this section, a detailed validation of the presented QTTP-GA-HC model takes place. The QTTP-GA-HC has been simulated using OPNET simulator and the results are measured in terms of throughput, end to end delay, jitter, latency, security strength and average power. The results are calculated by executing the QTTP-GA-HC under a set of ten iterations.

4.1. Throughput analysis

Table 1 and Fig. 4 provide a comparison of the throughput analysis of diverse methods under varying rounds of simulation. Under the first round of simulation, the Ipv4 and SIPv4 offers minimum throughput of 872Mbps and 883Mbps. Afterwards, the SIPv6 exhibits even better results over the IPv4 and SIPv4 with the throughput value of 988Mbps. Though the IPv6 offers minimum ETE delay over the earlier methods with the maximum throughput value of 1000Mbps, it does not outperform the GABFO-TPP and the QTTP-GA-HC models. The GABFO-TPP model shows competitive performance by obtaining a higher throughput of 1077Mbps which is higher than all the compared methods except QTTP-GA-HC. At last, the QTTP-GA-HC offers maximum throughput of 1200Mbps which is significantly higher than all the other existing models. These values proved that the QTTP-GA-HC shows effective outcome interms of throughput.

Table 1 Comparison of different models under various simulations interms of throughput

Sim No	IPv4	SIPv4	IPv6	SIPv6	GABFO TPP	PROPOSED
1	872	883	1000	988	1077	1200
2	924	945	1001	1089	1151	1223
3	822	993	1068	978	1077	1189
4	797	953	1036	1078	1066	1150
5	935	892	1093	954	1074	1255
6	854	995	1093	1125	1044	1145
7	817	865	1094	1150	1186	1226
8	875	826	927	992	1056	1240
9	950	866	991	1148	1140	1218
10	928	903	961	1043	1055	1141

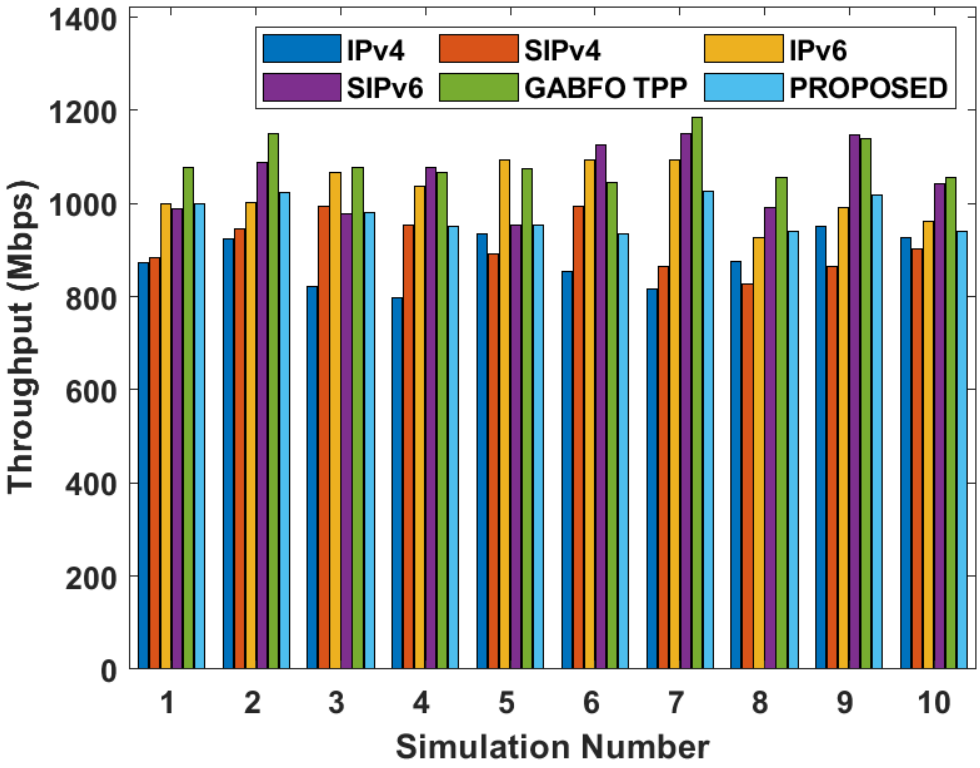

Fig. 4. Throughput analysis of diverse models

4.2. Security strength analysis

Table 2 and Fig. 5 provides a comparison of the Security Strength analysis of diverse methods under varying rounds of simulation. Under the first round of simulation, the Ipv4 model offers poor performance by attaining highest Security Strength of 85%. Then, the Secured SIPv4 mode provides slightly lower Security Strength compared to IPv4 of 91%. Afterwards, the IPv6 exhibits even better results over the IPv4 and SIPv4 with the Security Strength of 93%.

Table 2 Comparison of different models under various simulations interms of security strength

Sim No.	IPv4	Secured IPv4	IPv6	Secured IPv6	GABFOTPP	PROPOSED
1	85	91	93	94	97	99
2	85	90	93	96	97	99
3	85	91	93	94	95	97
4	86	89	92	96	97	98
5	85	89	93	94	96	97
6	86	90	93	94	95	96
7	87	90	94	95	96	97
8	86	90	94	94	97	98

9	87	89	93	95	97	97
10	86	91	94	96	95	96

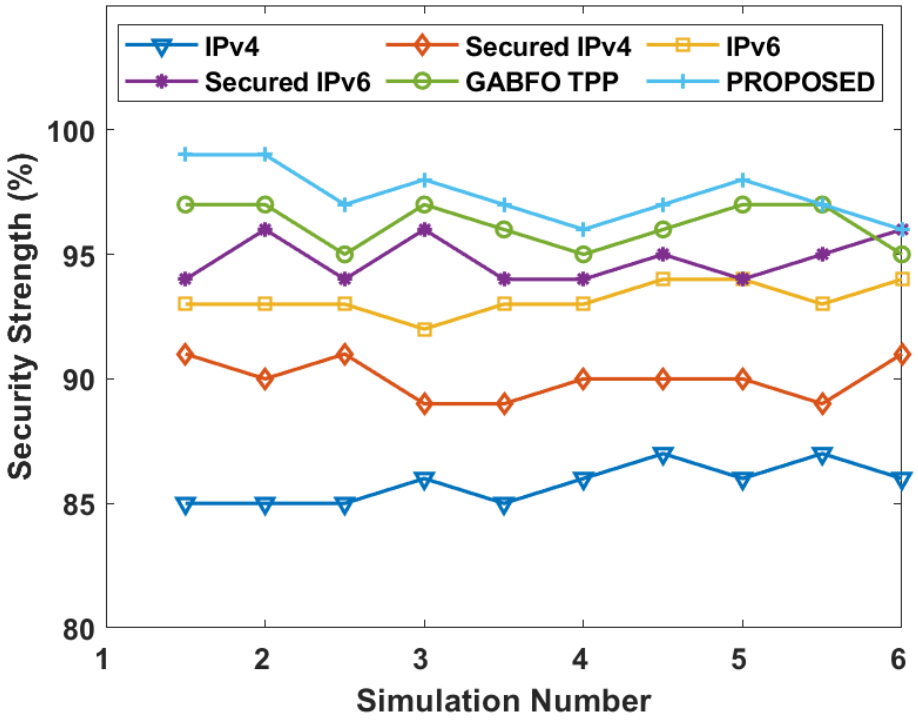

Fig. 5. Security Strength analysis of diverse models

Next to that, the Secured IPv6 model gives moderate performance by offering a moderate Security Strength of 94%. Though the IPv4 offers minimum Security Strength over the earlier methods, it does not outperform the IPv6 and the GABFO-TPP models. The GABFO-TPP model shows competitive performance by obtaining a Security Strength of 97%, which is lower than all the compared methods except QTTP-GA-HC. At last, the QTTP-GA-HC offers least Security Strength of 99% which is significantly higher than all the other existing models. These values proved that the QTTP-GA-HC shows effective outcome interms of Security Strength.

4.3. ETE delay analysis

Table 3 and Fig. 6 provides a comparison of the ETE delay analysis of diverse methods under varying rounds of simulation. Under the first round of simulation, the Ipv4 model offers poor performance by attaining highest ETE delay of 938ms. Then, the Secured IPv4 mode provides slightly lower ETE delay compared to IPv4 of 768ms. Afterwards, the secured IPv6 exhibits even better results over the IPv4 and Secured IPv4 with the ETE delay of 745ms. Next to that, the IPv6 model gives moderate performance by offering a moderate ETE delay of 715ms.

Table 3 Comparison of different models under various simulations interms of ETE delay

Sim No.	IPv4	Secured IPv4	IPv6	Secured IPv6	GABFO TPP	PROPOSED
1	938	768	715	745	688	640
2	945	779	741	754	679	630
3	945	798	727	763	678	629
4	919	771	719	753	675	626
5	944	793	709	763	649	606
6	955	775	709	758	674	624
7	957	778	712	737	653	616
8	916	754	729	765	645	602
9	920	750	731	773	660	620
10	920	782	726	777	676	627

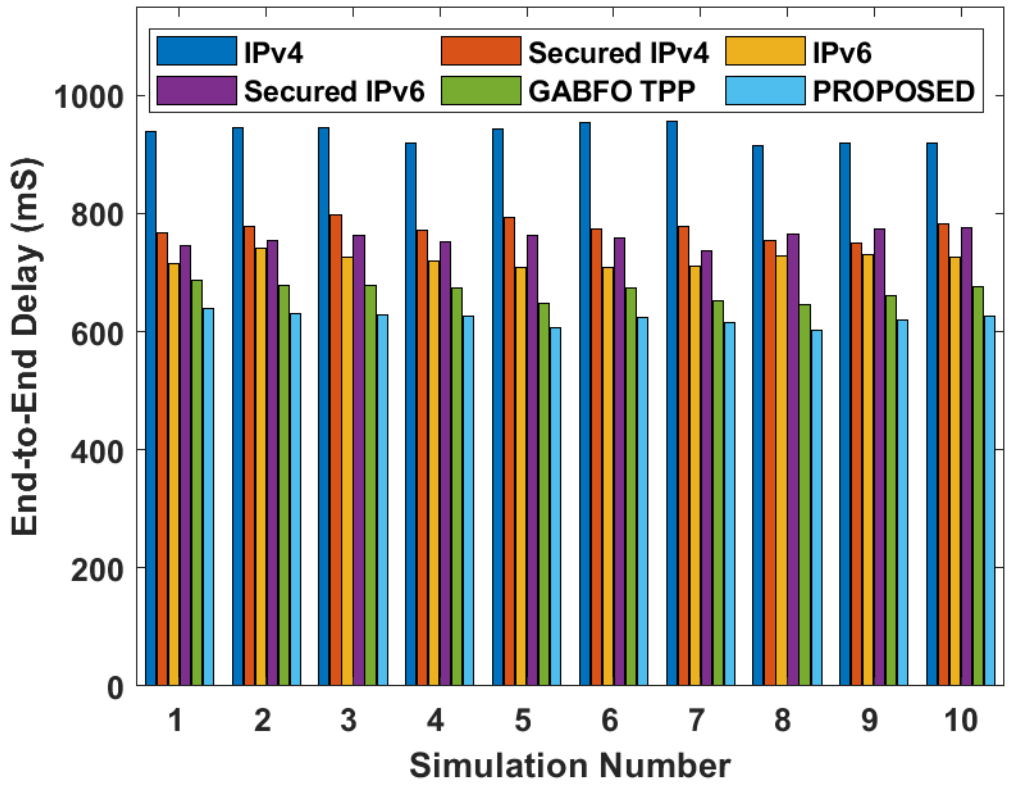

Fig. 6. ETE delay analysis of diverse models

Though the IPv4 offers minimum ETE delay over the earlier methods, it does not outperform the GABFO-TPP and the QTTP-GA-HC models. The GABFO-TPP model shows competitive performance by obtaining a ETE delay of 688ms, which is lower than all the compared methods except QTTP-GA-HC. At last, the QTTP-GA-HC offers least ETE delay of 640ms which is

significantly lower than all the other existing models. These values proved that the QTTP-GA-HC shows effective outcome interms of ETE delay.

4.4. Jitter analysis

Table 4 and Fig. 7 provides a comparison of the Jitter analysis of diverse methods under varying rounds of simulation. Under the first round of simulation, the Ipv4 model offers poor performance by attaining highest Jitter of 83ms. Then, the Secured IPv4 mode provides slightly lower Jitter compared to IPv4 of 60ms. Afterwards, the secured IPv6 exhibits even better results over the IPv4 and Secured IPv4 with the Jitter of 49ms. Next to that, the IPv6 model gives moderate performance by offering a moderate Jitter of 45ms. Though the IPv4 offers minimum Jitter over the earlier methods, it does not outperform the GABFO TPP and the QTTP-GA-HC models. The GABFO TPP model shows competitive performance by obtaining a Jitter of 37ms, which is lower than all the compared methods except QTTP-GA-HC. At last, the QTTP-GA-HC offers least Jitter of 32ms which is significantly lower than all the other existing models. These values proved that the QTTP-GA-HC shows effective outcome interms of Jitter.

Table 4 Comparison of different models under various simulations interms of jitter

Sim No	IPv4	Secured IPv4	IPv6	Secured IPv6	GABFO TPP	PROPOSED
1	83	60	45	49	37	32
2	86	58	48	54	40	35
3	88	54	47	49	42	37
4	85	55	44	54	39	34
5	84	56	47	52	37	32
6	87	56	45	53	39	34
7	86	56	44	54	42	37
8	88	55	44	55	37	32
9	84	59	48	51	39	34
10	88	57	47	53	40	35

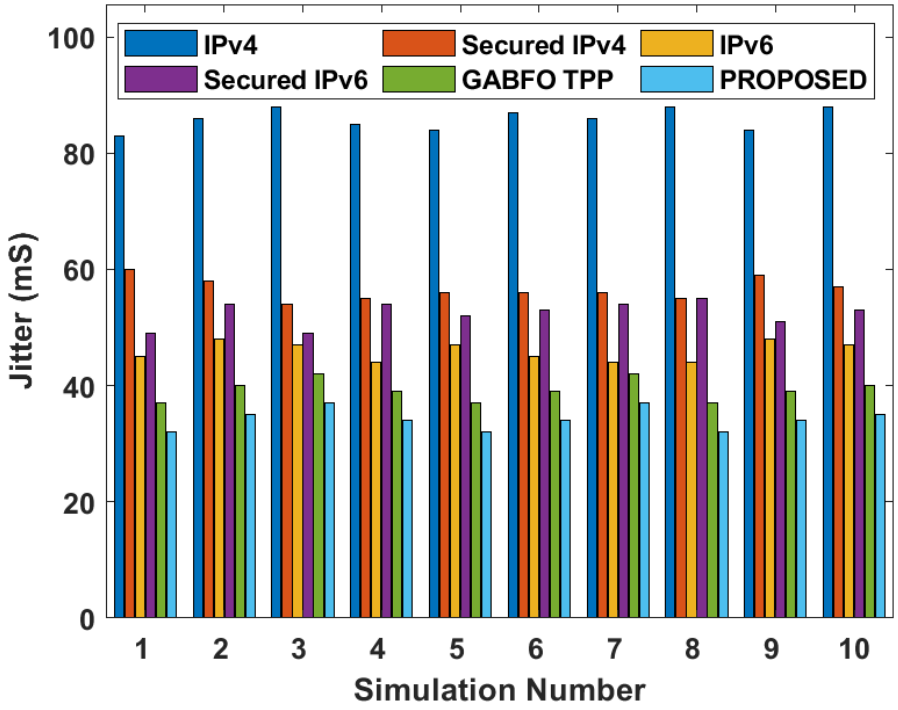

Fig. 7. Jitter analysis of diverse models

4.5. Latency analysis

Table 5 and Fig, 8 provides a comparison of the Latency analysis of diverse methods under varying rounds of simulation. Under the first round of simulation, the Ipv4 model offers poor performance by attaining highest Latency of 335ms. Then, the Secured IPv4 mode provides slightly lower Latency compared to IPv4 of 235ms. Afterwards, the Secured IPv6 exhibits even better results over the IPv4 and Secured IPv4 with the Latency of 212ms. Next to that, the IPv6 model gives moderate performance by offering a moderate Latency of 191ms. Though the IPv4 offers minimum Latency over the earlier methods, it does not outperform the GABFO TPP and the QTTP-GA-HC models. The GABFO TPP model shows competitive performance by obtaining a Latency of 178ms, which is lower than all the compared methods except QTTP-GA-HC. At last, the QTTP-GA-HC offers least Latency of 170ms which is significantly lower than all the other existing models. These values proved that the QTTP-GA-HC shows effective outcome interms of Latency.

Table 5 Comparison of different models under various simulations interms of latency

Sim No.	IPv4	Secured IPv4	IPv6	Secured IPv6	GABFO TPP	PROPOSED
1	335	235	191	212	178	170
2	348	251	202	216	175	167
3	346	235	196	216	187	175
4	351	248	199	210	183	173

5	334	245	203	211	175	168
6	352	237	207	214	182	172
7	344	242	204	206	185	173
8	352	235	195	217	179	169
9	339	245	192	204	189	178
10	345	252	198	209	182	172

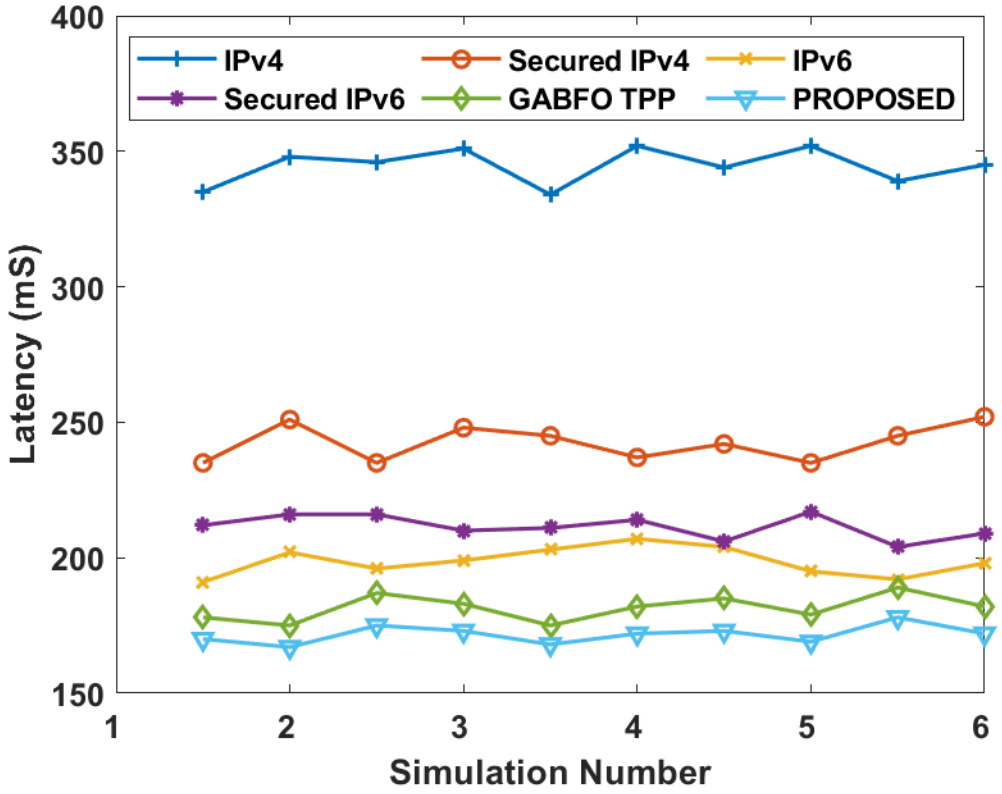

Fig. 8. Latency analysis of diverse models

4.6. Average Power analysis

Table 6 and Fig. 10 provides a comparison of the Average Power analysis of diverse methods under varying rounds of simulation. Under the first round of simulation, the Ipv4 model offers poor performance by attaining highest Average Power of 845mW. Then, the PROPOSED mode provides slightly lower Average Power compared to GABFO TPP of 830mW. Afterwards, the Secured IPv4 exhibits even better results over the GABFO TPP and PROPOSED with the Average Power of 2074mW. Next to that, the Secured IPv4 model gives moderate performance by offering a moderate Average Power of 1274mW. Though the GABFO TPP offers minimum Average Power over the earlier methods, it does not outperform the Secured IPv6 and the QTTP-GA-HC models.

Table 6 Comparison of different models under various simulations interms of average power

Sim No.	IPv4	Secured IPv4	IPv6	Secured IPv6	GABFO TPP	PROPOSED
1	2074	1274	1031	1052	845	830
2	2057	1240	985	1098	890	860
3	2025	1300	939	1059	842	828
4	2050	1286	1011	1107	844	835
5	2056	1319	1010	1119	805	785
6	2006	1264	975	1040	838	830
7	2052	1237	942	1094	868	845
8	2021	1274	984	1067	831	827
9	2018	1313	959	1012	871	855
10	2049	1283	1006	1060	846	837

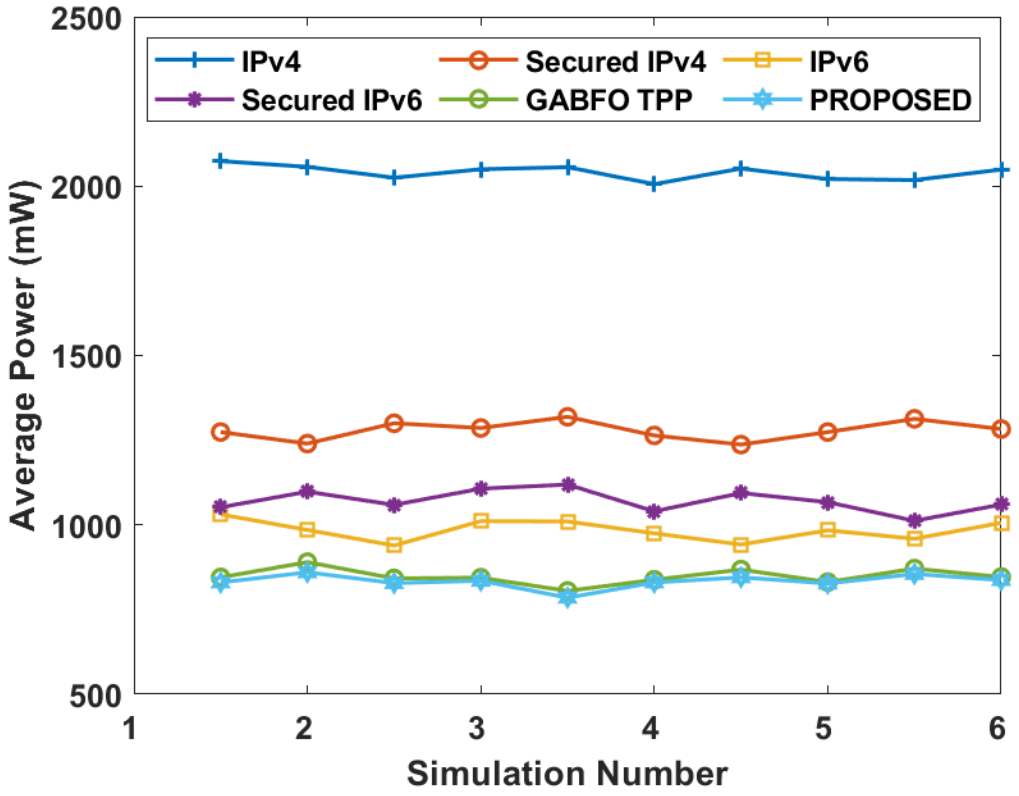

Fig. 9. Average Power analysis of diverse models

The Secured IPv6 model shows competitive performance by obtaining an Average Power of 1052mW, which is lower than all the compared methods except QTTP-GA-HC. At last, the QTTP-GA-HC offers least Average Power of 1031mW which is significantly lower than all the

other existing models. These values proved that the QTTP-GA-HC shows effective outcome interms of Average Power.

From the observation of the values present in the above tables and figures, it can be easily verified that the QTTP-GA-HC outperforms all the compared methods in a significant manner.

5. Conclusion

This paper has introduced a QTPP authentication based on GA with Hill-cipher called QTTP-GA-HC algorithm has been presented. The matrix in Hill Cipher is developed to carry out the encryption and decryption processes. GA provides an optimized manner of determining the key employed to encrypt and decrypt the data using Hill Cipher. By computing the evaluation function in GA, the key which fits the composition will be attained. The QTTP-GA-HC has been simulated using OPNET simulator and the results are measured in terms of throughput, end to end delay, jitter, latency, security strength and average power. The results are calculated by executing the QTTP-GA-HC under a set of ten iterations. The experimental outcome verified that the QTTP-GA-HC outperforms all the compared methods in a significant manner.

References

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, Pearson Custom Computer Science Series, Prentice Hall, 5th edition, 2010.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175, New York, NY, USA, 1984.

[3] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," Journal of Cryptology, vol. 5, no. 1, pp. 3–28, 1992.

[4] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, "Secure communication with a publicly known key," Acta Physica Polonica A, vol. 101, no. 3, pp. 357–368, 2002.

[5] K. Bostrom and T. Felbinger, "Deterministic secure direct ¨ communication using entanglement," Physical Review Letters, vol. 89, no. 18, pp. 187902–187905, 2002.

[6] A. Wojcik, "Eavesdropping on the 'ping-pong' quantum com- ´ munication protocol," Physical Review Letters, vol. 90, no. 15, Article ID 157901, 2003.

[7] Q.-Y. Cai, "The ping-pong protocol can be attacked without eavesdropping," Physical Review Letters, vol. 91, 2003.

[8] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," Physical Review A: Atomic, Molecular, and Optical Physics, vol. 69, no. 5, Article ID 052319, 2004.

[9] H. Hoffmann, K. Bostroem, T. Felbinger, F.-G. Deng, and G. L. Long, "Comment on 'Secure direct communication with a quantum one-time pad'," Physical Review A—Atomic, Molecular, and Optical Physics, vol. 72, no. 1, Article ID 016301, 2005.

[10] *K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, "Dense coding in experimental quantum communication," Physical Review Letters, vol. 76, no. 25, pp. 4656–4659, 1996.*

[11] *I. P. Degiovanni, I. R. Berchera, S. Castelletto et al., "Quantum dense key distribution," Physical Review A: Atomic, Molecular, and Optical Physics, vol. 69, no. 3, 2004.*

[12] *Y. Xia and H.-S. Song, "Controlled quantum secure direct communication using a non-symmetric quantum channel with quantum superdense coding," Physics Letters A, vol. 364, no. 2, pp. 117–122, 2007.*

[13] *J. Liu, Y.-M. Liu, Y. Xia, and Z.-J. Zhang, "Revisiting controlled quantum secure direct communication using a non-symmetric quantum channel with quantum superdense coding," Communications in Theoretical Physics, vol. 49, no. 4, pp. 887–890, 2008*

[14] *L. Yang, L.-A. Wu, and S. Liu, "Quantum three-pass cryptography protocol," in Quantum Optics in Computing and Communications, vol. 4917 of Proceedings of the SPIE, pp. 106–111, Shanghai, China, October 2002.*

[15] *Y. Kanamori and S. Moo-Yoo, "Quantum three-pass protocol: key distribution using quantum superposition states," International Journal of Network Security & Its Applications, vol. 1, no. 2, 2009.*

[16] *Siahaan, A.P.U. and Rahim, R., 2016. Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm.*

[17] *Stallings, W., 2017. Cryptography and network security: principles and practice (pp. 92-95). Upper Saddle River: Pearson.*