TEST Engineering & Management

January – February 2020
ISSN: 0193-4120 Page No. 15213 - 15216

QIDS for N Party Secret Sharing using GA

S. Madhavi ,
Professor , Department of Computer Science and Engineering India , PVP Siddhartha Institute of Technology, India
mmadhavi@pvpsiddhartha.ac.in

Article Info
Volume 82
Page Number: 15213 - 15216
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 28 February 2020*

Abstract:
Security plays a major role in network communication. With the advances in the field of security and communication technology new trends have evolved for secured transmission. Quantum communication is one such advancement where the laws of physics and mechanics are combined for achieving security in transmissions. Shamir secret sharing system can be used for secured communications. Little research is done to use such methods for detecting the attacker. Here we proposed a Quantum intrusion detection system using Genetic Algorithm to punish the malicious nodes and when finally ignore them from the communication network. In the proposed qIDS n party message sharing protocol one system distributes the message to n users such that any subset of users can construct the secret like in (28)

Keywords—GA , QKD , Quantum teleportation , Quantum Entanglement , QuTip

I. INTRODUCTION

However powerful are the traditional cryptography methods to establish a safe and secure communication system , there exists still a smart eavesdropper to break the key and the intrude into the system. This intrusion degrades the system performance. Hence an intrusion detection system to detect the attacker had become a research problem nowadays. The traditional cryptographic algorithms requires lengthy keys, large memory and huge computational power requirements. With the advances in the field of security and communication technology, new trends have evolved to detect the intruder. Quantum Entanglement, Quantum Key Distribution (QKD) , quantum Teleportation and quantum gates uses the fundamental laws of nature to detect the intruder in the system[8-10,14-17,21-27,30].

The success of the traditional cryptographic methods depends on

a. The Key Length From A Given Mathematical Model
b. The Computational Power Of The System
c. The Efficiency Of The Attacker.
d. Powerful Random Number Generators.

The traditional cryptographic methods fails if the attacker uses high computational power. The security in QKD relies on fundamental characteristic of quantum mechanics: With the principle of no cloning an eavesdropper cannot intercept a quantum exchange without going unnoticeable. Once the eavesdropper / errors in transmission is suspected the the nodes are punished and discarded from transmitting. Generally there exists quantum channel to share the secret along with a traditional classical channel between the nodes in the network. Many QKD protocols have emerged using the principles of quantum mechanics using Discrete Variable QKD, and single photon detectors to measure the obtained quantum states. BB84 protocol is the first protocol for implementing the quantum methods for securely transmitting the data using no – cloning method. The figure 1.0 shows the implementation procedure for BB84 protocol.

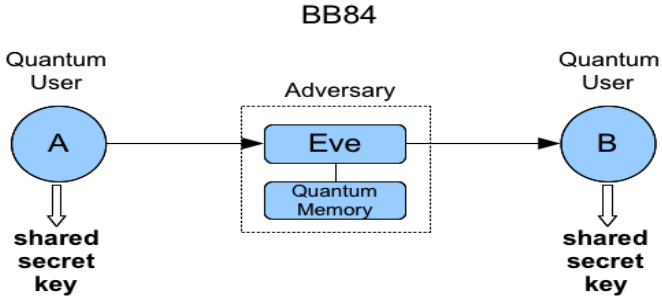

Figure 1.0 BB84 protocol

In Section 2 we discuss briefly various secret sharing protocols using quantum key distribution for sharing a secret. In Section 3.0 we proposed a new qIDS using GA method. In section 4 we present our conclusions and future scope of study.

II. SECRET SHARING USING QUANTUM KEY DISTRIBUTION

Shamir in [28] proposed a method for sharing a secret securely The basic procedure is to divided into n parts and each of the n users shares a part.. Later many researchers developed it by using the BB84 protocol and Ekert protocol,

January – February 2020
ISSN: 0193-4120 Page No. 12873 - 12879

which is proposed in [29]. In [28] authors implemented a method using t/n shares threshold for finding the malicious nodes. Many researchers have proposed methods for sharing a secret in [1-30] like using graph states, quantum methods, , distributed quantum methods , threshold methods, cryptanalysis methods, Grover's algorithm and QKD.
However, little research is done using the Genetic methods to share a secret securely in the communication network. In this paper, we proposed a method for securely transmitting the message using the method proposed by Shamir and method in [28] by applying the Genetic method to find the malicious.

III. PROPOSED QIDS USING GA

Let Gr be the graph, where V is set of vertices say Alice and Bob are users. Let A denote Alice and B denote Bob = {Bob1, Bob2, …, Bobn}. There are a set of edges, with (E,V,Gr ,) E E edges and V vertices. Graph will be referred as Gr to simplify the notation. As in [28] the proposed qIDS too constructs the secret iff at least t shares are collected. GA are adopted to find the t/n shares to select to establish a quantum communication and to eliminate/punish the Eavesdropper.

The proposed qIDS scheme uses the basic three phases in [28] and the methods

- Select_Trusted_Consructor:
- Find Qualified_k_subset:
- Evidence of Malicious_acitivity:
- GA:

To identify the compromised nodes in the channel and to establish a secure communication..

A. *Initialization Phase.*

Alice select a prime number say d such that $n \le d \le 2n$ and within a finite field Zd and divides

Secret is divided into n parts.

Alice randomly selects $f(x) = a_0 + a_1x^1 + a_2x^2 + ...a_{i-1}x^{i-1}$,

With degree t–1

where the

$$a = (a_1....a_{i-1}) \in Z_d^{t-1}$$

coefficients

are chosen, using + addition modulo d.

B. *Share Distribution Phase.*

Alice[28] compute n shares f (xi) € Zd for (i = 1, 2, …, n) using distant nonzero values xi € Zd to. The f(xi) is shared on a quantum channel using the no cloning method in BB84 protocol.

Alice shares the qubits f(xi) to Bob i for (i = 1, 2, …, n) on a quantum channel.

Each Bob $_i$ has a share f(xi)

The secret is shared among a the n users.

Alice calls Trusted_Reconstructor method to find the trusted reconstructor for Bob1

Bob1=Trusted_Constructor Method(Set P of Privilidges).

Now Bob1 receives all the t shares and then reconstructs the final secret.

Alice selects a any Hash function to find a values and thares it to the Bob1 so that the value is used in the secret reconstruction process

C. *Reconstruction Phase.*

- Generate the qualified subsets using the Qualified_k_subset (Set P of privileges) method. Each participant is assigned a privilege(shortest indegree) in this method which specifies the qualified subset number to which the participant is listed in. The values returerned by the Qualified_k_subset (Set P of privileges can reconstruct the secret. Each qualified subset need not belong to the same set. In the k shares the share with largest entropy is selected and is denoted by R = {Bob1, Bob2, …, Bobt}.
- Bob1 prepares qudit particles with each having m qubits where m = [log2 d][28].
- Bob1 implements QFT to the first share to obtain a t shares and they are denoted as follows

$$|\varphi_1\rangle = (QFT\,|0\rangle_1)\,|0_2\,|0\rangle_3 ... |0\rangle_t \rightarrow 1[28]$$

$$= \left[\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{0-k}\,|k\rangle_1\right]|0\rangle_2\,|0\rangle_3\,|0\rangle_t \rightarrow 2[28]$$

where ω = e2πi/d is a primitive d-th root of unity[28].

- Bob1 implements d-level CNOT[28] operation on the every |0⟩r to get the entangled states

$$|\varphi_2\rangle = (CNOT((QFT\,|0\rangle_1),|0\rangle_2)) \otimes (CNOT((QFT\,|0\rangle_1),|0\rangle_3)) \otimes (CNOT((QFT\,|0\rangle_1,|0\rangle_1)))$$

$$\rightarrow 3[28]$$

- Bob1 sends the shares to the Bobr

TEST Engineering & Management

January – February 2020
ISSN: 0193-4120 Page No. 12873 - 12879

- Once all the users obtains their shares particles they calculate f(xr) on their share sr which is the shadow of the share f(xr) which are shown as follows

$$s_r = f(x_r)\Pi_{1\le j\le t, j\ne r}\frac{x_j}{x_j - x_r} \quad \text{mod } d \rightarrow 4[28]$$

- On each share a generalized Pauli operator U0,sr is applied where

$$U_{0,S_r} = \sum_{k=0}^{d-1}\omega^{s_r.k} \mid k\rangle rr\langle k \mid\mid \rightarrow 5[28]$$

$$\mid \varphi_3\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{s_1.k} \mid k\rangle_1 \omega^{s_2.k} \mid k\rangle_2 \omega^{s_3.k} \mid k\rangle_3 ... \omega^{s_t.k} \mid k\rangle t \rightarrow 6[28]$$

- Bob1 calls QFT−1 to share |k⟩1 and obtains the secret ′ = $f(0)' = \sum_{r=1}^{t} s_r \ mod\ d.$. → 7[28]
- Bob1 verifies the shared is the same as the reconstructed using a hashed function as in [28]
- If the value is the same

  he distributes the message s to the users;

- otherwise

  identifies the malicious activity and ignores the transaction

- ends the reconstruction phase
- calls Evidence_of_ Malicious_acitivity.
- End

Select_Trusted_Consructor(Set P of privileges)

- Let Pi denote the privileges of each participant
- Choose a Random Number RNDi
- Let Pri=Pi*RNDi
- Return TC=Max(Pri)

Find Qualified_k_subset(Set P of privileges)

- k=k + 1
- Generate RAND
- Call Generate_sequences_number(Set P of privileges,RAND)
- Call GA(Si) to find the QSk and selected qualified subset R
- If Sizeof(QSk > 1)

  repeat step 1

- else

  return k

- End

Evidence of Malicious_acitivity ()

- For each k = 1 to t do
- If (Search(Trustedset(QSk) = false) then
- Add QSk to UnTrustedset
- P(QSk) = P(QSk) – Fine
- If if P(QSk < threshold) then
- Mark user as malicious and
- Ignore user from the communications.
- Else
- Add QSk to Trustedset
- P(QSk) = P(QSk) + promote
- End if
- End

GA(Gr)

- A candidate solution is a collection of complex vectors Gji and takes the real part of the numbers.
- Obtain a n qubit from the quantum system
- Obtain the density matrix ρ
- Read input parameters including nodes in the system, distances, degree of the graph , neighbor for every node ,crossover probability, mutation probability.
- Build a neighbor table with indices of smallest indegree neighbor's of each node.
- Using the neighbor table, create adjacency matrix Ad .
- Generate initial population as G XOR ρ XOR Ad
- Take any two chromosomes as initial population
- Generate sequence number from G for Tr
- For a given number of generations repeat: –
- Allocate two arrays, "generation0" and "generation1" composed of chromosomes.
- Apply crossover and mutation operators to get childi

January – February 2020
ISSN: 0193-4120 Page No. 12873 - 12879

- Find distance between Tr and childi and if childi is close to Tr call it BEST child.
- Include the BEST child in the qualified subset.

IV. CONCLUSION AND FUTURE WORK

The proposed is a Quantum intrusion detection system using GA. In the proposed quantum n party message, sharing protocol one system distributes the message to n users such that any subset of users can access the secret. We modeled the n user system as a quantum graph and used the GA AND the method in [28] to share the message securely among the n users. The laws of physics are employed to identify the eavesdropper and a threshold limit is imposed on every user for their misbehavior. When the misbehavior reaches the threshold, the user is marked as malicious and ignored in the rest of the communication.

REFERENCES

[1] Xiu-Li Song1, Yan-Bing Liu1, Hong-Yao Deng2 & Yong-Gang Xiao1 " (t, n) Threshold d-Level Quantum Secret Sharing" , scientific reports 25 July 2017 SCienTifiC REPOrTS | 7: 6366 | DOI:10.1038/s41598-017-06486-4

[2] Hillery, M., Buzek, V. & Berthiaume, A. Quantum secret sharing. Phys. Rev. A 59, 1829–1834 (1999).

[3] Deng, F., Zhou, H. & Long, G. Circular quantum secret sharing. J. Phys. A. Gen. 39, 14089–14099 (2007).

[4] Lin, J. & Hwang, T. New circular quantum secret sharing for remote agents. Quantum Inf. Process. 12, 685–697 (2013).

[5] Zhu, Z. C., Hu, A. Q. & Fu, A. M. Cryptanalysis of a new circular quantum secret sharing protocol for remote agents. Quantum Inf. Process. 12, 1173–1183 (2013)

[6] Karimipour, V. & Asoudeh, M. Quantum Secret Sharing and Random Hopping: Using single states instead of entanglement. Phys.Rev. A 92, 030301 (2015).

[7] Markham, D. & Sanders, B. C. Graph states for quantum secret sharing. Phys. Rev. A 78, 42309 (2008).

[8] Keet, A., Fortescue, B., Markham, D. & Sanders, B. C. Quantum secret sharing with qudit graph states. Phys. Rev. A 82, 62315 (2010).

[9] Sarvepalli, P. Nonthreshold quantum secret-sharing schemes in the graph-state formalism. Phys. Rev. A 86, 042303 (2012).

[10] Yang, Y. G., Teng, Y. W., Chai, H. P. & Wen, Q. Y. Verifiable quantum (k, n)-threshold secret key sharing. Int. J. Theor. Phys. 50,792–798 (2011).

[11] Yang, Y. G., Jia, X., Wang, H. Y. & Zhang, H. Verifiable quantum (k, n)-threshold secret sharing. Quantum Inf. Process. 11, 1619–1625 (2012).

[12] Song, X. L. & Liu, Y. B. Cryptanalysis and improvement of verifiable quantum (k, n) secret sharing. Quantum Inf. Process. 15,851–868 (2016).

[13] Sarvepalli, P. K. & Klappenecker, A. Sharing classical secrets with Calderbank-Shor-Steane codes. Phys. Rev. A 80, 022321 (2009).

[14] Qin, H. W., Zhu, X. H. & Dai, Y. W. (t, n) Threshold quantum secret sharing using the phase shift operation. Quantum Inf. Process.14, 2997–3004 (2015).

[15] Du, Y. T. & Bao, W. S. Multiparty quantum secret sharing scheme based on the phase shift operations. Opt. Commun. 308, 159–163 (2013).

Liu, F., Su, Q. & Wen, Q. Y. Eavesdropping on Multiparty Quantum Secret Sharing Scheme Based on the Phase Shift Operations. Int.J. Theor. Phys. 53, 1730–1737 (2014).

[16] Hsu, J. L., Chong, S. K., Hwang, T. & Tsai, C. W. Dynamic quantum secret sharing. Quantum Inf. Process. 12, 331–344 (2013)

[17] Wang, T. Y. & Li, Y. P. Cryptanalysis of dynamic quantum secret sharing. Quantum Inf. Process. 12, 1991–1997 (2013)

[18] Yang, W., Huang, L., Shi, R. & He, L. Secret sharing based on quantum Fourier transform. Quantum Inf. Process. 12, 2465–2474 (2013)

[19] Tavakoli, A., Herbauts, I., Żukowski, M. & Bourennane, M. Secret sharing with a single d-level quantum system. Phys. Rev. A 92,030302 (2015).

[20] Hsu, L. Y. Quantum secret-sharing protocol based on Grover's algorithm. Phys. Rev. A 68, 022306 (2003).

[21] Diao, Z. J., Huang, C. F. & Wang, K. Quantum Counting: Algorithm and Error Distribution. Acta Appl Math. 118, 147–159 (2012).

[22] Shi, R., Mu, Y., Zhong, H., Cui, J. & Zhang, S. Secure Multiparty Quantum Computation for Summation and Multiplication. Sci. Rep.6, 19655 (2016).

[23] Thas, K. The geometry of generalized Pauli operators of N-qudit Hilbert space, and an application to MUBs. IEEE International Conference on Systems, Man, and Cybernetic. 5, 3816–3822 (2009).

[24] Yang, Y. H., Fei, G., Xia, W., Qin, S. J., Zuo, H. J. & Wen, Q. Y. Quantum secret sharing via local operations and classical communication. Sci. Rep. 5, 16967 (2015).

[25] Shamir, A. How to share a secret. Commun. Acm. 22(11), 612–613 (1979).

[26] Bennett, C. H., Brassard, G. An Update on Quantum Cryptography. Advances in Cryptology, Proceedings of CRYPTO'84,

[27] Xiu-Li Song,Yan-Bing Liu,Hong-Yao Deng,Yong-Gang Xiao," (t, n) Threshold d-Level Quantum Secret Sharing", Scientific Reports 7, Article number: 6366 (2017) doi:10.1038/s41598-017-06486-425 July 2017

[28] ichael Epping, Hermann Kampermann , Chiara macchiavello and Dagmar Bruß ," Multi-partite entanglement can speed up quantum key distribution in networks", New J. Phys. 19 (2017) 093012

[29] Xiu-Bo Chen,Zhao Dou, Gang Xu,Xiao-Yu He & Yi-Xian Yang,A kind of universal quantum secret sharing protocol, Scientific Reports | 7:39845 | DOI: 10.1038/srep39845