Comparison of Cryptographic Techniques:Classical,Quantum and Neural

1st Minal Ghute
Research Scholar
Yeshwantrao Chavan College of Engineering
Nagpur,India
mrsminalghute@gmail.com

2ndYogesh Suryawanshi
Electronics dept
Yeshwantrao College of Engineering Nagpur, India
Nagpur,India
yogesh_surya8@rediffmail.com

2022 6th International Conference on Electronics, Communication and Aerospace Technology (ICECA) | 978-1-6654-8271-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICECA55336.2022.10009164

Abstract—**Now days, the necessity of highly secured and reliable network is tremendously increased in the wireless communication network. There are various routing attacks occurs in wireless communication network there for secure routing is one of the most challenging research area in a mobile ad-hoc network-MANETs. Several methods are available for providing safety of the MANET, still various attacks are there which reduces network performance. Hence a strong cryptography technique is required to secure communication in MANET.An efficient cryptographic method is required, which will not only generate and maintain key also distribute it safely to the nodes which are not malicious.The method proposed here detects the nodes which are malicious and keeps them away from communication in the network so that packet delivery rate is increased by reducing delay in the network. The reliable communication in MANET is achieved by applying strong cryptography methods. In this paper comparison of classical, quantum and neural cryptography are given.**

Keywords—Classical Cryptography, Quantum cryptography, Neural Cryptography, Attacks, Security

I. Introduction

MANETs has a dynamic topology i.e. nodes enter and leave the network randomly, due to which it often undergoes attacks. To prevent the attacks on the network the essential cryptographic techniques play vital role. In MANETs due to unavailability of central administrator nodes have to communicate and coordinate with each other for the successful data transmission from source node to destination node. When nodes become spiteful it does not takes part in the communication. Malicious node does not send information to other nodes in the network. Cryptography is the method in which the original data which is called plain text is encrypted by using a particular key. The modified data is called cipher text which is not possible for the malicious node to decrypt it without licensed key.

Cryptography is an essential and efficient technique for reliable data transfer. It converts plaintext into encrypted data called cipher text. There are two approaches of cryptography first is symmetric-key approach and second is asymmetric key approach.

Paper is organized as, problem statement given in section II. Section III describes survey of literature. Section IV describes Methodology. Conclusion is section V.

II. Problemstatement

Network performance and security are two major issues related to MANET. Some security-related challenges are present in the existing network are given below:

i. Attacks and security service are two essential processes for a highly secured network.

ii. The nodes within the MANET are randomly placed there is no limitations on the boundary of the network.

iii. Data encryption is utilized to maintain data privacy. If the cryptographic keys are not encoded and stored in the node then additionally compromised nodes create risk to secrecy.

III. Literature Survey

In 2021, Alejandro Cohen has done work on post quantum cryptography which is network coding-based. When the data transmission rate is very much high then quantum cryptography is used. Hybrid universal network coding cryptosystem is designed [1]. A secure mobile sensor data transfer protocol called secure sensor protocol (SSP). SSP is depend on Elliptic Curve Cryptography (ECC). But still there is a scope for utilization of ECC for Android based network [2]. An optimal cluster head-based signcryption technique for a reliable MANET is proposed in 2020. The MDPSO algorithm was developed which is used to select the head of the cluster. For data security the estimated distance, energy consumed and trust value of each cluster members were calculated. The proposed method obtained packet delivery ratio of 92.22, a security level of 93% and an accuracy of 80-82% [3]. Yaswanth Kumar Alapati, provided efficient cryptography algorithm for safe data transfer in MANET.A node act as MANET key calculator and another node is considered as a MANET Key distributor [4] .In 2019 Fatma Mallouli, presented a survey of asymmetric cryptographic algorithms like Elliptic curve cryptography (ECC), Rivest , Shamir, Adleman (RSA) and El-Gamal . As compared to RSA algorithm Elliptic curve cryptography i.e. ECC is more complicated for designing. As per experimental results ECC is more efficient and safe than RSA [5]. Eljilani Hmouda proposed the EAACK Protocol which is implemented using hybrid techniques. Combinations of DES and RSA algorithms are used. DES algorithms have higher efficiency. The proposed scheme EAACK (DES-RSA) improves network performance in terms of increased packet delivery ratio and reduced network overhead. Due to higher efficiency of DES algorithm in block encryption it is preferred in cryptography [6].In 2016, Ankita Singh, described Encryption technique which play important role in network security. Done survey on existing cryptography techniques like AES, DES, RSA algorithms based on their characteristics and performance. The AES algorithm takes least encryption time whereas RSA consumes longest encryption time .In terms of security RSA have strong security [7]. Rohit Kumar et al. proposed Elliptic curve cryptography based lightweight authentication scheme in MANET. For mutual authentication one extra encryption needed which increase security of the network, which is requirement of the MANET [8].

IV. Methodology

Secure communication in MANET can be achieved by using powerful cryptographic techniques. In this paper classical cryptography, quantum cryptography and neural cryptography are studied as follows.

1.Classical cryptography:

In classical cryptography at the transmitter side the input data which is called as plain text is encrypted using a sequence of code called key. Now the encrypted data is called cipher text [9]. The cipher text is transmitted over the wireless channel. At the receiver side the cipher text is converted into plain text by decrypting the data and using same or different key. Depending on the key use the classical cryptography having two types symmetric and asymmetric cryptography. In symmetric cryptography same key is used at the transmitter for encryption and decryption of data at the receiver as shown in fig.1. In asymmetric cryptography one key is use at receiver to convert plain text into cipher text and different key is use to get original data from ciphertext as shown in fig2. In classical cryptography information is transfer in the form of bits represented by "0" and "1" [10].

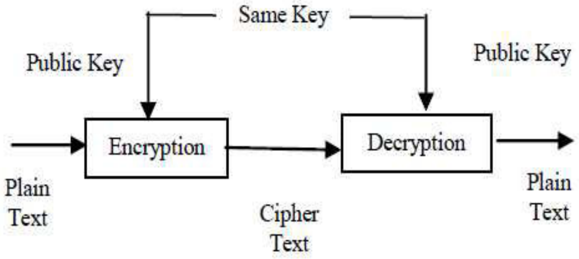

Fig. 1. Symmetric Cryptography

2.Quantum Cryptography:

The principle of quantum cryptography is depended on quantum physics. Quantum cryptography is based on Heisenberg uncertainty and Photon Polarization Principle [11]. In this sender generate the polarized sequence of photons which are polarized by 0^0,45^0,90^0, 135^0. Then sender transmits the information in the form of photons.

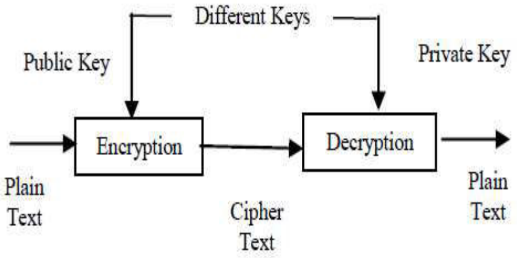

Fig. 2. Asymmetric cryptography

After receiving these photons by receiver, it will decide whether to use diagonal or rectilinear pattern of photons to get the data and it announces it publicly [12]. In quantum cryptography, information is transfer in the form of qubit. Qubit are in superposition of both the states at a same time. Due to which it is difficult to copy. Rectilinear and Diagonal Polarization Base in shown in fig.3.

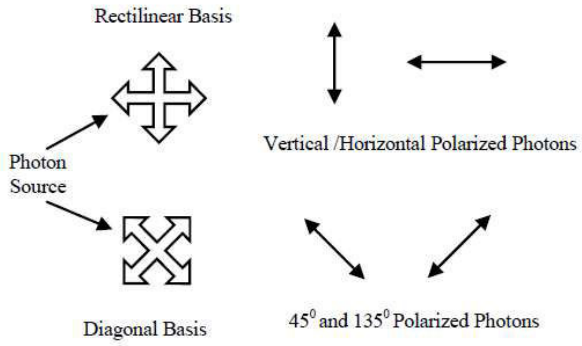
Rectilinear Basis
Vertical /Horizontal Polarized Photons
Photon Source
Diagonal Basis
45⁰ and 135⁰ Polarized Photons

Fig. 3. Rectilinear and Diagonal Polarization Base

3.Neural Cryptography:

Neurons play a crucial role in human body. Artificial neural network plays an important role in decision making, whose idea is taken from biological neural mode [13][14]. Neuron is nothing but the node which takes input from other node. A simple artificial neuron is shown in fig.4.Weight value w is assigned to each input. The weight value assigned is random. All the inputs are multiplied with assigned weight and then applied to the summer block [15]. The output of the summer block is given to some activation function which will generate the final output [16]. Permutation parity machine is one of the examples of neural cryptography. Activation function is step function, sigmoid function or rectified linear unit. Activation function decides which neuron is activated at what time.

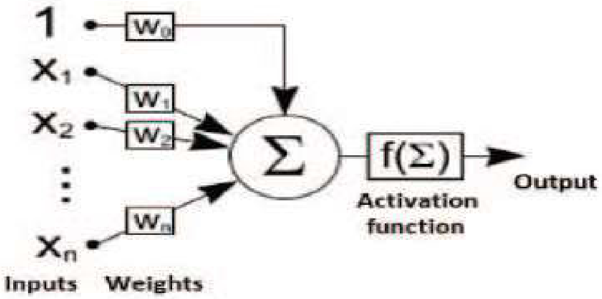

Fig.4. A simple artificial neuron

V. Conclusion

The MANET is a self-maintained, self-organized network due to which it is popular in natural disaster management, military applications where the wired network fails. Various cryptography techniques are compared as shown in table 1. Neural cryptography provide good security against conventional attacks. This algorithm cannot hack easily due to their structure.

TABLE1. COMPARISON OF CLASSICAL , QUANTUM AND NEURAL CRYPTOGRAPHY TECHNIQUES

Features	**Cryptography Techniques**		
	Classical Cryptography	***Quantum Cryptography***	***Neural Cryptography***
Requirements	Software and hardware	Hardware and communication link	Software and hardware
Methodology	1.It uses encryption of digital data and cryptography at the transmitter 2.At the receiver ,received data is decrypted using same or different key	1. It uses quantum physics and cryptography 2.It is based on Heisenberg uncertainty and Photon Polarization Principle	1.It combines neural network and cryptographic techniques 2.Artificial neural network is used
Data transfer medium	communication medium not required	Required communication medium	communication medium not required
Digital signature	Yes	No	Yes
Development	Network generation and testing	After network generation in the initial stage it is not tested	After creation of neural network in the 1st stage training of the network is done and in later stage testing is done
Advantages	1. It has large communication range. 2.One time pad provide perfect security	1. This is more secure than classical cryptography. 2. Random secret key generation based on the process used by the sender and receiver.	1.Without knowing the architecture it is difficult to crack the network and to hack the information 2.Tolerate large noise
Disadvantages	It requires modifications as computing power increases	1. Implementation is quite difficult. 2.Communication range is restricted upto 10 miles 3.Bit error rate is large	In this network weight and network architecture itself act as key which are required for encryption as well as decryption.
Applications	Transfer videos and images securely	Mostly use to transfer videos and images securely	Cloud security

REFERENCES

[1] Alejandro Cohen, “Network Coding-Based Post-Quantum Cryptography”, IEEE journal on selected areas in information theory, Vol. 2, No. 1, march 2021

[2] NoumanKabir , “Secure Mobile Sensor Data Transfer using Asymmetric Cryptography Algorithms”,Internationalconferemce on cyberwarfare and security(ICCWS),DOI:10.1109/ICCWS48432.2020.9292392,2020

[3] Mohamed Elhoseny and K. Shankar, “Reliable Data Transmission Model for Mobile Ad Hoc Network Using Signcryption Technique”, IEEE transactions on reliability, Vol. 69, No. 3, September 2020

[4] Yaswanth Kumar Alapati, Suban Ravichandran, “Secure Data Transfer in Manet with Key Calculator and Key Distributer Using Cryptography Methods”, International Journal of Safety and Security Engineering ,Vol. 10, No. 4, pp. 567-572, August 2020

[5] FatmaMallouli, AyaHellal, NahlaShariefSaeed, Fatimah AbdulraheemAlzahrani, “A Survey on Cryptography: comparative study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms” , 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud), 2019

[6] EljilaniHmouda, Wei Li, “Detection and Prevention of Attacks in MANETs by Improving the EAACK Protocol”, Southeast Con 2018, DOI: 10.1109/SECON.2018.8478999

[7] Ankita Singh, Mahima Sharma, “Cryptography Techniques based on Security of AODV in MANETs - A Survey”, International Journal ofScience and Research , ISSN: 2319-7064, Volume 5 Issue 4, April 2016, PN.1002 – 1007

[8] Rohit Kumar, YashendraShiv , Vimal Kumar , ManojWairiya , “An Authentication Technique in Mobile Ad hoc Network using Elliptic Curve Cryptography” 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence),2018, DOI: 10.1109/CONFLUENCE.2018.8442504

[9] Anindya Kumar Biswas,Mou Dasgupta, “A secure hybrid routing protocol for mobile adhoc networks(MANETs)”,11th international conference on computing, communication and networking technologies ,Oct.2020,DOI:10.1109/ICCCNT49239.2020.9225474

[10] Muhammad Asghar Khan, “An Efficient and Provably Secure Certificateless Key-Encapsulated Signcryption Scheme for Flying Ad-hoc Network”, IEEE acess ,Vol.8, 2020.

[11] Bindu, V. ,“Cyber Security Analysis for Quantum Computing”,Journal of IoT in social ,mobile,analytics and cloud,Vol 4,Issue 2,pp. 133-142,2022

[12] Harshad R.Pawar“Classical and quantum cryptography for image encryption and decryption”,international conference on research in intelligent and computing in engineering,2018,DOI:10.1109/RICE.2018.8509035

[13] Mohammad Reza Khalili-Shoja, “Secret Common Randomness From Routing”, IEEE transactions on information forensics and security, Vol. 11, No. 8, August 2016

[14] Deepshikha Sharma “Big data protection via neural and quantum cryptography”,International conference on computing for sustainable global development,pp.3701-3704,2016

[15] Roberto De Prisco and Alfredo De Santis, “On the Relation of Random Grid and Deterministic Visual Cryptography”, IEEE transactions on information forensics and security, Vol. 9, No. 4, April 2014

[16] Cai, R.J., Li, X.J., Han, P., Chong, J. , “An evolutionary self-cooperative trust scheme against routing disruptions in MANETs”. IEEE Transactions on Mobile Computing, Vol. 18, Issue 1, Jan.2019,DOI:10.1109/TMC.2018.2828814, pp.42 - 55