International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 10 Issue 1 –OCTOBER 2014.

An Efficient Data Sharing Using Quantum Cryptography in Wireless Sensor Network

Yogapriya.D[*1], and Mr.R.Rameshkumar[#2]

[*]PG Student, *Department of Computer Science and Engineering, Gnanamani College of Technology, Namakkal,India*

[#] Asst Professor, *Department of Computer Science and Engineering, Gnanamani College of Technology, Namakkal,India*

Abstract— Wireless Sensor Network is the network in which the communication can be done easier without any cable media. During the wireless network communication the hackers can be able to attack the information in easy manner. We propose a Quantum Cryptography called "An Efficient Data Sharing Using Quantum Cryptography in Wireless Sensor Network" to protect the network from the attacks by the hacker. The quantum cryptography is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network. Recently, A new quantum cryptography scheme is claimed its security by providing well-organized security arguments. In this paper, however, we illustrative that their scheme is actually insecure as it fail to meet credential privacy and soundness of authentication. Specifically, we present two enhancement attacks. The intermediate nodes along the path to the sink are able to verify the authenticity and integrity of the incoming packets using a predicated value of the key generated by the sender's cybernetic energy, thus requiring no need for specific rekeying messages. AES is able to efficiently detect and filter false data injected into the network by malicious outsiders.

Keywords: WSN (Wireless Sensor Network), Quantum Cryptography, AES (Advanced Encryption Standard) Algorithm, Attacks, Authentication.

I. Introduction

Sensor Network is used to convert any type of physical signal into electrical signal. In Distributed Network the environmental conditions can be monitored by using WSN. The environmental conditions are humidity, temperature, soil moisture etc. In WSN the communication can be done through the Sensor node.

Cryptography is the technique in which the information will be protected from the third parties (HACKERS) to avoid the interception. There are different types of cryptography such as public key cryptography, cryptanalysis, symmetric key cryptography etc.

Public key cryptography has two types of keys, one is Public key and the other is Private Key, these keys are linked mathematically. Encryption of the plaintext can be done in public key while the decryption of the ciphertext can be done in private key. In encryption of the plain text the information is passed to the authorized persons and hence the information will not be stolen by the hackers. There are different kinds of encryptions available to pass the information such as symmetric key encryption and public key encryption. In Decryption the message will be converted from the ciphertext to the plaintext.

Cryptanalysis will be useful to find out the hidden information from the system. It analysis the hidden information and helps us to access the information from the encrypted messages.

Symmetric key cryptography: The Another name of symmetric key cryptography is secret key cryptography. This secret key cryptography is used to share the secret key between the sender and receiver.

Quantum key cryptography has the technique of Quantum Key Distribution (QKD) in which the key is distributed between the sender and receiver in a secure way. The advantage of using quantum key cryptography is it detects the scheme of eavesdropping.

Quantum key distribution has the list of protocols; they are BB84, decoy state protocol, E91 protocol, SARG04, COW protocol, DPS protocol, KMB09 protocol, S09 protocol, S13 protocol. These protocols are used to exchange the key securely.

The working principle of Quantum Key Distribution is that it consists of the individual photons. Those photons exchange the key between the sender and receiver in the form of binary digits (a 1 or a 0) and the photon is determined by the polarization. The sender will send the information to the receiver that time the laser generates a single photon consists of horizontal or vertical polarization. If an eavesdropper interrupt into the communication then the photon will destroy the process and the eavesdropper have to generate a new one, and the creation of duplicate photon is passing to the receiver. By means of destroyed process the hacker will be identified and the information is send to the receiver successfully. The eavesdropper cannot be able to send the fake data's to the receiver because it is impossible to create a replica path because of the photon created by the sender.

ERROR RATE: If the sender's information and the receiver information is same without any error then the information is passed securely, otherwise the error rate has to be calculated. If the sender's information is not matched with the receiver information then there is an intercept occurred in the communication, and hence the receiver should calculate the error rate. Because of the destroyed process of photon the session is secure in the network and the photons cannot be used in the creation of key. But the error rate should be calculated to find out the communication process is secure throughout the network.

II. Related Works

We are unacquainted of the earlier technique of Automatic test packet generation [1] from the performance and requirements to transfer the information between the sender and receiver [7]. The ATPG is used to send the packet to check the network whether it has the faulty links [8] and then the packet will clear the problem [5] through the data plane with the help of anteater [2] [6]. A NICE way of open flow application is used to reduce the identified bugs and KLEE technique is used to automatically generate the test packets and find the similar differences between the tools used in the complex system programs [3] [4]. The closest related article we know is the Quantum cryptography.

Quantum cryptography technique is used to transfer the information from the sender to receiver in a secure way by means of quantum key distribution. The QKD is used to generate the polarised photon that is used to transmit the digital information. The polarization technique is used in this cryptography to find out the eavesdropper intercept into the communication and the photon destroys the process of eavesdropper and therefore the interrupter can be found out.

In the earlier technique of ATPG(Automatic Test Packet Generation), it cannot be able to model the boxes because the test packets will change the internal state and the failed rule can take a backup rule active and hence the information can be hacked in easy way.

The quantum key cryptography consists of the protocols; they are BB84, decoy state protocol, E91 protocol, SARG04, DPS protocol, S09 protocol, S13 protocol. These protocols are used to exchange the quantum information (qubit). The two quantum mechanical system is used to produce the polarization of a single photon. Vertical polarization or Horizontal polarization is used as a two states in the quantum computing.

The operation of a pure qubit is quantum logic state and standard basic measurement Quantum logic state is used to transfer the information as a unitary transformation and standard basic measurement is used to gain the state of the information.

AES (Advanced Encryption Standard) is used in this quantum key cryptography to transfer the information securely without hacking by the third party. AES is used as a substitution and permutation network. AES has the block size of 128 bits and the size of key is 128,192 or 256 bits. AES calculation was done in finite fields. It operates on 4X4 matrix to transfer the information from the plain text to the cipher text.

AES algorithm: This algorithm has high-level description such as KeyExpansion, InitialRound (AddRoundKey), Rounds (SubBytes, ShiftRows, Mixcolumns, AddRoundKey) and Final Round (SubBytes, ShiftRows, AddRoundKey).

The strength of AES algorithm is that it able to protect the shared information up and around the secret level. The key length used in the TOP SECRET information is either 192 or 256 bits and the performance of the AES algorithm is high, It requires low RAM and a wide variety of hardware is used from 8-bit smart cards to the high-performance computers and hence the AES technique is used in the Quantum Cryptography to share the information.

III. PROPOSED WORK

A new quantum cryptography scheme has claimed its security by providing well-organized security arguments.

The intermediate nodes along the path to the sink are able to verify the authenticity and integrity of the incoming packets using a predicted value of the key generated by the sender's cybernetic energy, thus requiring no need for specific rekeying messages.

AES (Advanced Encryption Standard) is able to efficiently detect and filter false data injected into the network by malicious outsiders.

The performance of the quantum key cryptography is high and the time taken to transfer the information to the receiver is low.

IV. References

[1] Hongyi Zeng, Member, IEEE, Peyman Kazemian, Member, IEEE, George Varghese, Member, IEEE, Fellow, ACM and Nick McKeown, Fellow, IEEE, ACM,"Automatic Test Packet Generation," in IEEE/ACM TRANSACTIONS ON NETWORKING,vol.22,NO.2,APRIL 2014.

[2] H. Mai, A. Khurshid, R. Agarwal, M. Caesar, P. B. Godfrey, and S. T.King, "Debugging the data plane with Anteater," Comput. Commun.Rev., vol. 41, no. 4, pp. 290–301, Aug. 2011.

[3] M. Canini,D.Venzano, P. Peresini,D.Kostic, and J. Rexford, "A NICEway to test OpenFlow applications," in Proc. NSDI, 2012, pp. 10–10.

[4] C. Cadar, D. Dunbar, and D. Engler, "Klee: Unassisted andautomatic generation of high-coverage tests for complex systemsprograms," in Proc. OSDI, Berkeley, CA, USA, 2008, pp. 209–224.

[5] A. Dhamdhere, R. Teixeira, C. Dovrolis, and C. Diot,"Netdiagnoser:Troubleshooting network unreachabilities using

end-to-end probes and routing data," in Proc. ACM CoNEXT, 2007, pp. 18:1–18:12.

[6] N. Duffield, F. L. Presti, V. Paxson, and D. Towsley, "Inferring linkloss using striped unicast probes," in Proc. IEEE INFOCOM, 2001,vol. 2, pp. 915–923.

[7] N. Duffield, "Network tomography of binary network performance characteristics," IEEE Trans. Inf. Theory, vol. 52, no. 12, pp.5373–5388, Dec. 2006.

[8] Y. Bejerano and R. Rastogi, "Robust monitoring of link delays andfaults in IP networks," IEEE/ACM Trans. Netw., vol. 14, no. 5, pp.1092–1103, Oct. 2006.