Improved Security in WSNs with Quantum Logic Gates and Quantum Teleportation

Pawan Bharadwaj[*], Divya. S[**]

[*] Electronics and Communications Engineering, NIEIT, Mysore
[**] Electrical and Electronics Engineering, NIEIT, Mysore

Abstract- Recent developments in technology have made possible the widespread deployment of small, low power and dense wireless networks, known as wireless sensor networks which collect and disseminate environmental data. In such networks communications can be easily monitored and hence data transmission and reception between the nodes must be encrypted using a secret key. Furthermore, the distribution of secret key used in encryption of data in a very large network is a cause for the reduced efficiency of the network. The scheme of using quantum teleportation as a mechanism to distribute quantum data over a sensor network offers huge advantage over traditional methods. In this paper an EPR-Pair scheme is implemented in terms of quantum gates to achieve higher degree of immunity from eavesdropping of malicious nodes.

Index Terms- EPR-Pair, Quantum Gates, Quantum teleportation, Wireless sensor network (WSN).

I. Introduction

A wireless sensor network is a large collection of nodes which are organized into a network which are co operative in nature. The nodes communicate wirelessly and often self organize after being deployed in an ad hoc fashion. Numbers of nodes anticipated range from 100s to1000s in number. In recent times, WSNs are being deployed at a highly accelerated pace. In a few years wireless sensor networks will cover the whole world with access to the internet. This can be considered as the Internet becoming a physical network. The main properties of a wireless sensor network is that they are wireless, have low power resource and are real-time, have dynamically changing sets of resources, aggregate behaviour is important and location is critical. Many wireless sensor networks also utilize minimal capacity devices which places a further strain on the ability to use past solutions. [1]

The sensors in a WSN report the changes in a physical parameter to a centralized system. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base stations or sinks. As sensor nodes typically have short range of transmission and scarce resource, an attacker with high processing power and larger communication range could attack several sensors at the same time to modify the actual information during transmission. [2]

To overcome the above disadvantage of eavesdropping, an entanglement pair, better known as the Einsten-Podolsky-Rosen (EPR) pair is used to distribute quantum data over a wireless sensor network. Using quantum gates to generate this entanglement scheme, the overall power consumption in this sensor network drastically reduces.

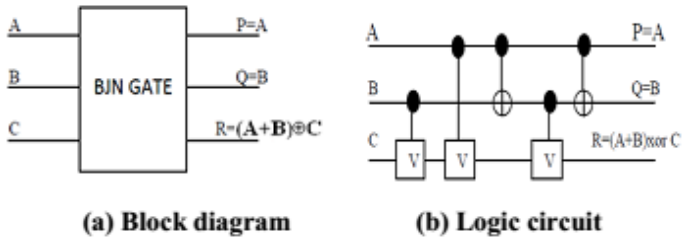
II. Quantum Gates

In the field of quantum computing and specifically in the domain of quantum circuit model of computation, a quantum gate, and otherwise known as a quantum logic gate is a basic quantum circuit operating on a small number of qubits. Just as the basic gates are the building blocks of a classical computer, quantum gates form the building block for a quantum computer.

Unlike many classical logic gates, quantum logic gates are reversible. However, classical computing can be performed using only reversible gates. For example, the reversible Toffoli gate can implement all Boolean functions. This gate has a direct quantum equivalent, showing that quantum circuits can perform all operations performed by classical circuits. Quantum logic gates are represented by unitary matrices. The most common quantum gates operate on spaces of one or two qubits, just like the common classical logic gates operate on one or two bits. This means that as matrices, quantum gates can be described by 2×2 or 4×4 unitary matrices. [5].The quantum gates used in this paper are: Hadamard gate and BJN gate. The description of BJN and Hadamard quantum gates are given below.

BJN Gate (BJN):

Figure.1 shows a BJN Gate which is a 3*3 gate with inputs (A,B,C) and outputs P=A, Q=B, R=$(A \oplus B) \oplus C$. Its logic circuit and its quantum implementation are as shown.



(a) Block diagram (b) Logic circuit

Figure 1: BJN Gate

Hadamard Gate (H):

The Hadamard gate acts on a single qubit. It maps the basis state $|0\rangle$ to $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ and $|1\rangle$ to $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$.

It is represented by the Hadamard matrix:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Figure 2 is the circuit representation of this gate is as shown:

Figure 2: symbol of Hadamard matrix

III. PROPOSED SECURITY MODEL

The proposed work uses a teleportation scheme to distribute quantum data within the sensor network. In previous works, the entanglement is generated using the CNOT gate [4]. A teleportation scheme for sensor data distribution is implemented using a Feynman gate in [6] wherein the mathematical steps involved are more complex and hence more secure [6]. In this paper a BJN gate is used to implement the same.

The final analytical result received by this proposed model with that of the CNOT gate is computationally identical. Figure. 3 shows a sensor environment in which node A and node B are communication to a remote base station. Node A and node B are assigned a qubit pair [6].

These nodes communicate using quantum teleportation. This makes the environment more secure and reliable with very low power consumption.

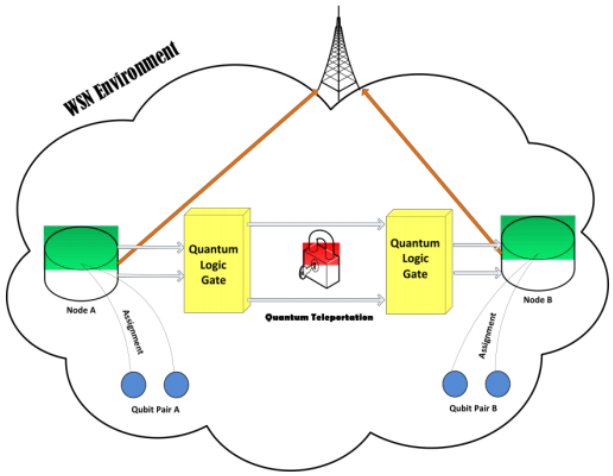


Figure 3: Teleportation between two nodes in a WSN

Suppose a qubit denoted by $|\chi\rangle = \alpha|0\rangle + \beta|1\rangle$ is to be teleported between the node A to Node B. Assume the qubit is normalised. Consider an entangled quantum state $|\Psi\rangle$ formed by a tensor product of three separate states represented as

$$|\Psi\rangle = |\chi\rangle \otimes |0\rangle \otimes |0\rangle$$

$$|\Psi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |00\rangle$$

$$|\Psi> = \alpha|000> + \beta|100> \quad (1)$$

Applying Hadamard gate to the second qubit, we obtain

$$|\Psi> = \alpha|0> \otimes \frac{1}{\sqrt{2}}(|0> + |1>) \otimes |0> + \beta|1> \otimes \frac{1}{\sqrt{2}}(|0> + |1>) \otimes |0> \quad (2)$$

$$= \frac{1}{\sqrt{2}}(\alpha|000> + \alpha|010>) + \frac{1}{\sqrt{2}}(\beta|100> + \beta|110>) \quad (3)$$

Now applying a BJN gate to equation (3),

$$|\Psi> = \frac{\alpha}{\sqrt{2}}(BJN|000> + BJN|010>) + \frac{\beta}{\sqrt{2}}(BJN\ |100> + BJN|110>) \quad (4)$$

$$= \frac{\alpha}{\sqrt{2}}(|000> + |011>) + \frac{\beta}{\sqrt{2}}(|101> + |110>) \quad (5)$$

Lastly, apply a Hadamard gate to the first qubit in equation (5) we get,

$$|\Psi> = \frac{\alpha}{2}(|000> + |100> + |011> + |111>) + \frac{\beta}{2}(|001> - |101> + |010> - |110>) \quad (6)$$

Rearranging the terms we get,

$$|\Psi> = \frac{1}{2}|00> \otimes (\alpha|0> + \beta|1>) + \frac{1}{2}|01> \otimes (\alpha|1> + \beta|0>) + \frac{1}{2}|10> \otimes (\alpha|0> - \beta|1>) + \frac{1}{2}|11> \otimes (\alpha|1> - \beta|0>) \quad (7)$$

This equation (7) represents the possible outcomes of measuring the first two qubits. If node A measures |00>, then the state collapses and node B has $|\chi> = \alpha|0> + \beta|1>$ in its possession. If |01> is measured by node A then the desired state at node B can be obtained using an X-gate. Similarly if node A measures |10>, then a Z-gate is to be applied at node B and finally if node A measures |11>, then a ZX- gate combination must be applied to the qubit at node B for obtaining back the qubit in its original form. The information of what state has been measured at node A must be sent classically by node A to node B.

IV. Conclusion and Future Scope

In this paper we have seen that a secure communication of quantum data in a wireless sensor network can be achieved using quantum teleportation. The above methodology gives a far superior data protection than the traditional approach. The mathematical results clearly indicate that from gates used at intermediate stages we can extract the same quantum information at the output as is generated at the input and intermediate communication can be made more secure with the use of quantum gates. This paper can be extended to teleporting two qubit states as well. Different quantum gates can also be used in the future to produce successful teleportation.

References

[1] J. Stankovic, "Wireless Sensor Networks", Handbook of Real-Time and Embedded Systems, CRC, 2007.

[2] Al-Sakib Khan Pathan, Hyung-Woo Lee, ChoongSeon Hong ,"Security in Wireless Sensor Networks: Issues and Challenges", International conference on Advanced Computing Technologies, Page1043-1045, year 2006.

[3] Prof. Sujata S. Chiwande, Prashant .R.Yelekar, Introduction to Reversible Logic Gates & its Application,2nd National Conference on Information and Communication Technology (NCICT) 2011 Proceedings published in International Journal of Computer Application.

[4] Jung-Shian li, Ching-Fang Yang, 2009. Quantum Communication in Distributed Wireless Sensor Networks, IEEE.

[5] http://en.wikipedia.org/wiki/Quantum_gate

[6] S. Ahmed, N. Javaid, S. H. Bouk, A. Javaid, M. A. Khan, Z. A. Khan, Quantum Cryptography Using Various Reversible Quantum Logic Gates in WSNs , Journal of Basic and Applied Scientific Research (JBASR), 2013, http://arxiv.org/abs/1304.0980.

Authors

First Author – Pawan Bharadwaj is an Assistant professor at Department of Electronics and Communications Engineering at NIEIT, Mysore. Email: pbsjce@gmail.com

Second Author – Divya.S is a lecturer at Department of Electrical and Electronics Engineering at NIEIT, Mysore. Email: divya.srp@gmail.com