A Quantum Fuzzy Logic for a Secure and Safe Wireless Network Communication

Varun Pande, Khaled Elleithy, Wafa Elmanna, Elham Geddeda
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, USA
vpande@my.bridgeport.edu, elleithy@bridgeport.edu, welmanna@my.bridgeport.edu, egeddeda@my.bridgeport.edu

Abstract—Due to the wireless network’s features and the flexibility that it provides over the communication, it has become the most common used network. That motivates many researchers to introduce and discover new techniques in order to improve this environment. However, the huge use of wireless networks leads to lack of secure communication. Especially, with wireless local area networks (WLAN); where many public places such as airports and banks are equipped with those networks. In order to transmit the secret key between two parties, quantum cryptography uses a new method called quantum key distribution (QKD). It has been created to solve the problem of secret key distribution. In this paper we provide a secure and safe wireless network communication using quantum logic (QKD) and fuzzy logic; where fuzzy logic is an approximation process, in which crisp inputs are turned to fuzzy values based on linguistic variables, set of rules and the inference engine provided. This process is called fuzzification which is a process that enables us to determine a value within sets. Similarly in quantum computing we determine the probability of a qubit inclined towards the 1 or 0. Since a qubit can be a function that is closely related to fuzzy logic, our protocol creates a rule based engine that implements fuzzy logic to show the output on a quantum based rule engine during the communication. The algorithm detects an intruder who tries to intercept the communication.

Keywords— Wireless Networks, Communication, Security, Fuzzy Logic, Quantum key distribution.

I. INTRODUCTION

Nowadays, wireless networks are used over the world due to its rapid advancement during past years. The number of its users is being increasing every day [1, -3]. Therefore, it would not be long when the industry’s communications will be controlled by the wireless network due to its appealing features. Although the wireless networks and their applications became the most popular ones to provide a smooth communication; security of information remains a major concern. Therefore, in this paper we address this problem by introducing an algorithm that provides a high level of security over the wireless networks using Quantum Key Distribution (QKD) and fuzzy logic.

Radio frequency signals makes wireless communications are more exposed and vulnerable to the attackers than its corresponding wired communications. Most of wireless networks’ security applications such as encryption and protocols become widespread; that increases the security risk with such applications [4, 5]. Several methods can be used by the attackers such as man-in-the-middle attacks, Identity theft (MAC spoofing), denial of service attack (DOS), and ARP poisoning.

Quantum Key Distribution (QKD) technique is used to distribute the secret key between the two communicating parties. Recently, optical communications have used QKD protocols with optical fiber schemes [6]; for example, six-state [7], B92 and BB84 [8]. In particular, BB84 is considered as the most used technique [9]. In optical networks, QKD shows noteworthy improvements [10, 11].

In 1965, Lotfi A. Zadeh introduced Fuzzy logic at the University of California in Berkeley [12, 13]. However, it was a long debate between the thoughts of multivalued logic and the notion in the field of Fuzzy Logic which was considered as multivalued logic; that permits moderate values such as: true/false, right/wrong, big/small, yes/no, and so on. While, other methods were described as notions; that can be processed mathematically using computers. It can be applied as human way of thinking through programming of computers. Furthermore, the developed ideas of Fuzzy logic yielded a profitable tool for the steering and controlling of complex systems in serial processes, households and many other applications in our daily life [14].

II. RELATED WORK

In this section we are presenting some techniques that have been used to support security over the wireless networks using fuzzy logic and QKD. The two dimensional fuzzy dynamic switching is the main focus in [6]; where it switches between the sender and receiver through long distance. The authors provide a solution for Line-Of-Sight (LOS) issue using Fuzzy logic. The authors used QKD system using fuzzy logic with the IEEE 802.11i protocol for wireless network. The authors argue that their work would provide secure communications over the network.

Based on the privacy amplification phase of IEEE 802.11, the authors tested their results using quantum cryptography [15]. They have tested their application based on obtained data from a quantum station against combinations of inputs. Their analysis showed that the adjustment which they made on IEEE 802.11 protocol does not have any major effect on general key distribution system. The results displayed the 4-phase handshake was finished within rational time limits even under high error rate. In the end, they have claimed that their suggested solution is resourceful enough to be combined in the IEEE 802.11 standard.
One of the most profitableness of fuzzy Logics is to convert heuristic control rules to be operated automatically instead of being operated manually [12, 13]. Modern applications of technologies and science are greatly benefited and developed by fuzzy logic techniques. For example, steam engine controller, complex systems signal processing and many other fields of science and technologies cannot ignore the parole that played by the importance of fuzzy logic [14]. There are still some difficulties that need to be overcome such as the interference of inputs and outputs in engine maps for instance.

The modern science of cryptography is used to as a safe guard for protecting private information from the attackers, as well as authentication and insuring data integrity. By using key distribution quantum (KDQ) technique, the eavesdropping can be detected [16]. However, authentication needs a partner in communication progression who could share some amount of secret information. However, for an unlimited secret key growing, quantum cryptography will be essential. Recently, Heisenberg uncertainly was suggested to provide secure communications [17].

The authors in [18] used quantum cryptography mechanism which is called fuzzy logic controller (FLC) over the social networks. Thus, its purpose is to prevent the attacker of being involved inside the network. They have compared their proposed fuzzy quantum cryptography method with PKI methods. This approach showed improvement in the results compared to PKI methods. The main reason of the proposed method is to recognize the irregular behavior over the networks.

III. PROPOSED WORK

A. Proposed Algorithm:

In this section, we introduce an algorithm to provide a high level of security over wireless networks using quantum fuzzy logic. Our algorithm is based on Gaussian principal and membership sets of fuzzy logic. In order to demonstrate the security level of this algorithm, an application was developed using C sharp programming language.

As we demonstrated in previous sections, fuzzy logic is an estimate process, in which crisp values are turned to fuzzy values based on semantic variables, set of rules and the inference engine provided. This method is called fuzzification. Fuzzification is a method that allows us to control a value within sets. Likewise in quantum computing we define the probability of a qubit inclined towards the 1 or 0. Furthermore, the qubit has a rotation that defines its positive or negative attribute. Since a qubit can be a function that is closely related to fuzzy logic, we are going to use the fuzzy logic’s features of maximizing qubit value to be optimized. Our main goal is to get the closed values to determine whether the qubit is 0 or 1. Therefore, the optimization model of fuzzy can be presented over multi-objective software design issues as following:

\[
\max, \min\{\mu_1(D)\} & \min\{\mu_2(U_l)\} \forall s \in S \& \forall l \in L
\]

Such that \(A_1 < C_1\)

\[
\sum_{r \in R}^{\mathbb{P}} X_{rs} = 1 \quad \forall p \in P \& \forall s \in S
\]

\[
X_{rs} = 0 \text{ or } 1 \quad \forall r \in R \& \forall s \in S
\]

Our goal is to maximize the minimum qubit value of all delay which is donated by D and the difference between the measured and recommended values donated by U.

\[
f(x) = \begin{cases} \text{Negative spin}, & x = 0 \\ \text{Positive spin}, & x = 1 \end{cases}
\]

\[
\mu_{b,a}(x) = \exp\left(-\frac{(x - \mu_0)^2}{2\sigma^2}\right)
\]

At-Norm \(T: [0,1]^2 \rightarrow [0,1]\) is a commutative and associative function satisfies:

\[
T(a,1) = a \text{ and } a \leq b \Rightarrow T(a,c) \leq T(b,c)…(1)
\]

A t-Conorm: \(\downarrow [0,1]^2 \rightarrow [0,1]\) is a commutative and associative function satisfies:

\[
\downarrow (a,1) = a \text{ and } a \leq b \Rightarrow \downarrow (a,c) \leq \downarrow (b,c)…(2)
\]

From equations 1 and 2, we understand that the spin sets of a single qubit can be derived. Once the spin value is derived, then n subsets will be stored under the probability set. The Gaussian principal allows us to determine the point of access between any of the two qubits. Thus, it is enabling us to determining a path without overwhelming it. Theoretically, we can determine the spin function based on each node that is adjacent other nodes. That is to make subsequent sets as showing in equation 3 in order to define the number of qubit sets having the same spin state. Since it is an exponential function, a delta spin value is generated from the total set of qubits. This enables us to determine three sets of spinning qubits. One of the sets that have a positive spin and flow towards path is more probable to have the value one. One set of qubits that have a spin in the negative direction and flow towards the value 0 in a probability function. Finally a set of qubits that have no spin function determined. A vice versa case again gives output to multiple probabilities. Thus, this process makes the whole communication faster, and more secure without overwhelming and creating a large overhead.

\[
|S_f| = f(1)^1 f(2)^1 \ldots f(n)^1 |11 \ldots 1
\]

\[
> + f(1)^1 (-f(2)^2)\ldots f(n)^1 |10 \ldots 1
\]

\[
> + \cdots + (1 - f(1))\frac{1}{2} (1 - f(2))\frac{1}{2} \ldots (1 - f(n))\frac{1}{2} |00 \ldots 0 \quad (3)
\]

Our main goal is to show the possibility of deriving a quantum based rule engine that implements fuzzy logic to determine the possibility of multiple logical outputs to provide a secure wireless communication. Figure1 demonstrates a logic based interference engine which we are going to use. We are showing how a number of probable if statements and a number of if else statements logic, all go to a main interference engine.
B. System Architecture:
Figure 2 presents an overview of the system. The algorithm receives a set of quantum-based inputs and fuzzy logic-based inputs into our interference engine. Then, we determine the sets based on the fuzzy logic for the inputs. Based on the fuzzy sets, a logic-based decision is taken via logic engine and a probability of location or spin is derived. The value needs to be checked for each qubit. These output values help define a path in the unlimited network, and then the data transmission begins under secure communication.

Figure 3 is the presentation of the node network. We can call it a quantum spin or qubit spin node network. As each of the nodes in the network transmits data to each other based on the qubit’s spin which is presented in the data stream based on [19]. Basically, the presence of the nodes shows how the data is passed across the network based on the qubit’s spin and its position between 1 and 0. It is a similar concept to the P2P [20] networking for data transmission across a node network, but we define the set of data value to be transmitted based on the spin notation and the probability of the location of the qubit between 0 and 1. Thus, the path determination for the data transmission is based on the probability of the qubit location which is between 0 and 1.

C. Results:
Based on our implemented idea, we could provide a secure communication between the nodes. Figure 4 shows the implementation that creates an interference engine using quantum and fuzzy logic.

We first use a fuzzy-based logic for using multiple attributes of a sensor node in a network to generate the value ranges between 0 and 1. Then, we define a condition or expression to classify how the transmission process will occur throughout the network. Although the choice can be defined by the user, default definitions can be selected to access the whole network.

Figure 5 shows that the data transmission decreases as the number of nodes increases as well as the energy and the transmission power were not at maximum value. Thus, based on the node properties, we can determine the amount of input data transmitted. Theoretically, based on quantum computation this should not be an issue even with infinite nodes as the transmission packets will be qubits, since the
log function cannot be displayed in relation to other attributes. We show that the transmission power will not be at its maximum.

The final result which is based on the fuzzy logic is that the data is transmitted. That is the data is sent completely without any loss of packets of any data size and any condition. There was no packet loss throughout the network in either scenario as showing in figure 6.

The quantum logic function window is allowed us to see and modify the attributes of the individual qubits. We can determine the qubit sets based on the fuzzy logic here and determine the number of qubits that have a positive negative and no spin. We tend to reach a crossover point via fuzzy logic to determine sets before the transmission of the qubit data as shown in Figure 7.

Delta spin basically determines the difference between the number of qubits in the whole network whether or not it is ready to be transmitted against the amounts that are having the positive spin and the negative spin. Again using fuzzy logic as a subset of qubits are defined based on the probability of these bits toward the whole binary value 1 or whole binary value 0 as showing in figure 8. Qubit’s position displays the result of the number of qubits and their final probable locations as showing in Figure 9.

IV. CONCLUSIONS

In this paper, we have shown a novel and secure way using quantum logic and fuzzy logic over wireless network. The development of an interference engine was demonstrated using an application developed in C# programming language which determines how the fuzzy logic can support secure communication over a network of unlimited nodes without loss of data using qubits of quantum logic and set theory derived via fuzzy logic. Since there is no quantum machine to actually determine the ability of such an engine, we statistically used the properties of both functions to verify a fast and secure method using a quantum fuzzy logic interference engine. In the future we plan to apply this logic on large node network sizes and observe how the behavior of fuzzy logic changes based on set determination and the path selection as a network grows exponentially.
REFERENCES


