A 802.11 MAC protocol adaptation for Quantum communications

C. M. Arizmendi†1 J. P. Barrangú†2 O. G. Zabaleta†3

†University of Mar del Plata, Faculty of Engineering, Mar del Plata, Argentina
1arizmend@fi.mdp.edu.ar, 2jparrangu@fi.mdp.edu.ar, 3gzabaleta@fi.mdp.edu.ar

Abstract—In this work, a novel medium access control method for classical and quantum communications purposes is proposed. Near future quantum communications promise secure ways to send valuable information, therefore quantum-device network and quantum medium access control methods which avoids information loss will be necessary. On the other hand, future classical wireless communication systems aim at very high data rates, nevertheless excessive colliding transmissions, especially in congested situation is still a problem, so designing a suitable MAC protocol is critical to fully take advantage of the benefit of high speed transmission. Quantum parallelism and quantum multipartite entanglement are exploited to design a MAC sublayer which provides the devices a fair and efficient access to the channel.

Keywords—Quantum communications, MAC

1. Introduction

Quantum computation and information processing are rapidly evolving fields of physical science. Their practical importance arise from the exponential speedup in computation of certain algorithmic tasks over classical computation [5]. In a world of security-conscious information transmission, the possibility of sending hidden information in quantum states of electrons or photons would be highly desirable. A quantum communication network can be set to many uses: it can transmit classical information, private classical information, or quantum information. Independently of the technology used to built quantum transmission networking, quantum channel access protocols will be necessary.

The main quantum computing drawback is quantum decoherence. The coherence state, fundamental to a quantum computers operation, it is destroyed when it is affected by the environment. As a consequence, the physical requirements of manipulating a system on quantum scale are considerable, touching on the realms of superconductor, nanotechnology, and quantum electronics, as well as others. Despite considerable advances in quantum technology [6, 9, 18] make us think that quantum computing horizons are not so far.

Generally, wireless systems do not have a common goal and do not cooperate with each other, with every device seeking its own “benefit”. Telecommunication systems designed to provide services for more than one subscriber has to cope with the problem of medium access control (MAC), which regulates how to share the common medium (channel) among users. The most widely used standard is 802.11 produced by the Institute of Electrical and Electronic Engineers (IEEE). This is a standard defining all aspects of Radio Frequency Wireless networking. The main goal is to avoid having stations transmitting at the same time, which results in collisions and corresponding retransmissions.

Because of hidden and exposed station problems, it does not use CSMA/CD (Carrier Sense Multiple Access with Collision Detection) protocol as ethernet communications does. Instead, Wireless LANs (WLANs), as standardized in IEEE 802.11, employ CSMA/CA (CSMA with Collision Avoidance) offering the advantage of improved access control, which serves to reduce collisions and, thereby, improve the overall performance of the network. In order to ensure that only one radio device is transmitting on half-duplex medium, the standard supports two operating methods, DCF (Distributed Coordination Function) and PCF (Point Coordination Function).

DCF is the fundamental access method of 802.11 communications and is widely used in most simulations for ad hoc network research. Ad hoc networks are defined by the manner in which the network nodes are organized to provide pathways for data to be routed from the user to and from the desired destination. In other words, nodes sense the medium and transmit when the medium is idle. Flexibility, independence from central network administration, scalability, low cost, among others advantages, have made this type of networks be extensively studied in recent years. On the other hand, for base station (BS) oriented networking, where access is centralized by a coordinator device or Access Point (AP) which enables other devices to use the medium, PCF is used. BS-oriented networks are more reliable and have better performance than Ad hoc ones [20]. Both, the BS-oriented networks (also called infrastructure networks) and ad hoc networks have some drawbacks. An infrastructure network takes a bit more work than setting up an ad-hoc network. Infrastructure networks cut the data transfer
rate about in half, because of the time it takes to send
the signal to and from the access point rather than
directly to its destination, as in an ad-hoc network. The
other drawback is expense: Infrastructure networks
are more expensive than ad hoc networks because an
access point has to be purchased. As we already men-
tioned, however, that expense may be compensated
by considering all the benefits an AP provides. Mean-
while, in the non-infrastructure networks connections
are hard to rebuild or maintain. When the connec-
tion is built it will be disrupted anytime a mobile
host moves out of the connection range, so route and
communication connectivity result fairly weak. Hy-
brid wireless network protocols combining the advan-
tages of BS-oriented and ad hoc wireless networks are
proposed in [3, 12]. Furthermore, new wireless net-
works aim to be increasingly flexible while the devices
are becoming smarter.

Quantum entanglement is one of the most striking
features of quantum mechanics and has been used as
an essential resource of quantum information process-
ing such as quantum teleportation [1], quantum cryp-
tography [11], quantum computation [17]. In entan-
gled states measurements on different particles are cor-
related, even if the particles are widely separated. It
is also possible to entangle more than two particles,
and even to spread out the entanglements over time,
so that a system may be only partly entangled at the
start and fully entangled later on. Entanglement will
be defined in the next section.

This paper proposes a medium access control
(MAC) protocol relevant both for classic and quantum
communications. In order to make migration easier, it
takes advantage of quantum parallelism and quantum
entanglement strengths taking into account the cur-
rent standards.

As proposed by Bérces and Imre in [2], the MAC
protocol for quantum communications uses a slotted
time system. Stations send a request to reserve the
medium according to the data load for transmitting
during the next interval of time. The difference lies
in the fact that users can act as routers, so request is
sent by the both users and AP.

Aiming to find the destination, sender broadcasts a
“search” message which arrives to all users, included
the AP, within the covering region. Every other user
receiving the message checks the destination address
for a match. So, if matching is affirmative, the receiver
is within the signal coverage range, therefore he creates
an EPR pair and sends one part of the entangled qubit
to the sender which will allow the sender to teleport
data to the receiver. Note that in such case users are
interconnected without the BS intervention.

When the receiver cannot hear the signal from the
sender, BS-oriented mode begins. If AP accept con-
nexion, it creates an EPR pair and sends a part to
the sender and the other to the receiver. After that,
sender and receiver proceeds as stated above. When
two users want to send a message to the same receiver
simultaneously, some priority rules must be created: If
both of them are far from the receiver coverage range,
the AP must control the channel access. Hence, it
creates a three partite entangled state and sends one
part to each sender remaining one for her. The AP
is able to control probability amplitudes in order to
give higher priority to one of the users. In any case
users measure their state and depending on the mea-
sure outcome they know if they can start transmitting
or not. The case of more than two users accessing the
channel is fairly straightforward.

The paper is organized as follows. Section 2 gives a
brief overview of quantum computation and quantum
channels. The system model for the network scenario
under consideration is described in Section 3. Next,
section 4 describes the proposed protocol. Finally, con-
clusions and further work are depicted in section 5.

2. Quantum computation and quantum chan-
nels

As the bit is the minimum information in classical
computation, the quantum bit or qubit is the mini-
num information for quantum computation and quan-
tum information[17]. The qubit is typically a micro-
scopic system, such as an atom or polarized pho-
ton. The Boolean states 0 and 1 are represented by a
fixed pair of distinguishable states of the qubit (for
example, electron states: spin up $|0\rangle = \uparrow$ and spin
down $|1\rangle = \downarrow$) where “$\uparrow$ ” is called Dirac notation,
see [15, 17] for a complete introduction to quantum
computation and quantum information. A qubit can
also exist in a continuum of intermediate states, or
“superpositions”, represented mathematically as unit
vectors in a two-dimensional complex vector space (the
“Hilbert space”) spanned by the basis vectors,

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

Then the qubit state is mathematically represented by
a linear superposition:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$
where $\alpha$ and $\beta$ are complex numbers which must
satisfy the normalization condition $|\alpha|^2 + |\beta|^2 = 1$

An $n$ qubits system is capable of exiting in $2^n$ basis
states, as well as all possible superpositions of them.
Thus, states of a pair of qubits, for example, lie in a
four-dimensional Hilbert space $\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$. When state $|\psi^{\otimes n}\rangle$ is separable, it can be written as

$$|\psi^{\otimes n}\rangle = |\psi\rangle_0 \otimes |\psi\rangle_1 \otimes \ldots \otimes |\psi\rangle_{n-1}.$$
Quantum states evolution are determined by

$$|\psi(t)\rangle = U|\psi(0)\rangle,$$
where $U$ are unit operators (a necessary condition to
satisfy quantum computation reversibility) in a Hilbert
Entanglement is also possible with more than two qubits, as in the W-states, entangled states used in n-qubit systems. For example, a 3-qubit W-state is

$$|W⟩ = a|001⟩ + b|010⟩ + c|100⟩,$$

where $a, b, c$ are the probability amplitudes associated with each state. This kind of entangled states have an interesting property: if one particle is measured then an entanglement can be observed in the remaining particles. Several methods are used to achieve this kind of states [13, 19, 22, 23]. A sample circuit generator of W-states is shown in figure 3, see for example [7, 8] as helpful references of n-qubits quantum gates circuits and applications. In the circuit depicted in figure 3, the $U_a$ gate operates on the three upper states, originally initialized to $|0⟩$, obtaining the system state $|ψ_i⟩$.

$$|ψ_i⟩ = (∑_{i=0}^{7} α_i|i⟩) ⊗ |0⟩^3,$$

$$|ψ_f⟩ = (α_0|000⟩ + α_3|011⟩ + α_6|110⟩)|001⟩ + (α_1|001⟩ + α_4|100⟩ + α_7|111⟩)|010⟩ + (α_2|010⟩ + α_5|101⟩)|100⟩$$

Thus, probabilities $p_i$ can be modified by controlling $α_i$ values.

$$p_1 = |a|^2 = |α_0|^2 + |α_3|^2 + |α_6|^2$$

$$p_2 = |b|^2 = |α_1|^2 + |α_4|^2 + |α_7|^2$$

$$p_3 = |c|^2 = |α_2|^2 + |α_5|^2$$

A quantum channel is a formal description of how qubits in a given setting are affected by their environment. It is possible to think a quantum channel as a pipe that transmits a qubit, such as a spin-half particle (an electron for example) or a polarized photon.

The measurement operator $M$ must satisfy the completeness equation

$$∑_m M^\dagger_m M_m = I,$$

where the elements $M_i$ are the measurement matrices of the qubit $|i⟩$. Furthermore, the probability of the result of the quantum system $|ψ⟩$ is equal to $m$

$$p(m) = ⟨ψ|M^\dagger_m M_m|ψ⟩$$
Similarly, measurement operators of the outer product of each state of the basis with itself, created from the outer product of each state of the basis with itself, after measurement is performed the system state is

$$M_m |\psi\rangle = \sqrt{\langle \psi | M^\dagger_m M_m |\psi\rangle}$$

The completeness equation states that the sum of probabilities is equal to one, that is

$$\sum_m p(m) = \sum_m \langle \psi | M^\dagger_m M_m |\psi\rangle = 1.$$

Measurements of qubits were made using a collection of measurement operators. These operators are created from the outer product of each state of the basis with itself, i.e.: 

$$M_{00} = |00\rangle \langle 00| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$M_{11} = |11\rangle \langle 11| = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Suppose the qubit $|\phi\rangle = a|00\rangle + b|11\rangle$ is measured, the probability of obtaining measurement outcome 00 is

$$P(00) = \langle \psi | M^\dagger_{00} M_{00} |\psi\rangle = |a|^2$$

Similarly,

$$P(11) = \langle \psi | M^\dagger_{11} M_{11} |\psi\rangle = |b|^2$$

The state after the measurement is

$$\frac{M_{00} |\psi\rangle}{|a|} = \frac{a}{|a|} |00\rangle = |00\rangle$$

or

$$\frac{M_{11} |\psi\rangle}{|b|} = \frac{b}{|b|} |11\rangle = |11\rangle,$$

$^2(\text{ is the } | \text{ vector conjugate transpose version.})$

Figure 3: Circuit to obtain a quantum W-state

where $\frac{a}{|a|}$ and $\frac{b}{|b|}$ have modulus one, so they can be ignored [17].

For quantum teleportation the circuit shown in figure 4 is used, where $|\varphi_j\rangle$ is the qubit to be transmitted and $|\phi\rangle$ is the EPR pair.

In order to achieve quantum teleportation the qubit $|\varphi_j\rangle = \alpha|0\rangle + \beta|1\rangle$ interact, where $\alpha$ and $\beta$ are unknown amplitudes which comply with $|\alpha|^2 + |\beta|^2 = 1$, with the half of the EPR pair through a CNOT gate. Thus, the input state to the circuit is

$$|\psi\rangle = |\varphi_j\rangle |\phi\rangle = \alpha|0\rangle (a|00\rangle + b|11\rangle) + \beta|1\rangle (a|00\rangle + b|10\rangle)$$

The next step is to pass the qubit $|\varphi_j\rangle$ for a Hadamard gate and then the two resulting qubits are measured. After the Hadamard gate the resulting state is

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} [\alpha|0\rangle + |1\rangle) (a|00\rangle + b|11\rangle) + \beta(0) - |1\rangle) (a|10\rangle + b|01\rangle)]$$

replacing $a$ and $b$ by $a = b = 1/\sqrt{2}$ and regrouping, the expression is

$$|\psi_2\rangle = \frac{1}{2} [\alpha|0\rangle + |1\rangle) (a|0\rangle + b|1\rangle) + |01\rangle (a|angle + b|0\rangle) +$$

$$+ |10\rangle (a|\rangle - |1\rangle) + |11\rangle (a|\rangle - |0\rangle)]$$

According to this expression, the measurement of the transmitter's qubits determines the state of the qubit holding by the receiver. The measurements outcomes are sent to the destination through a classical channel. According to the result received, one of the four possible operations will be made, given by the different combinations of the gates $X^{M_2}$ and $Z^{M_1}$ in the circuit. The qubit $|\varphi_j\rangle$ is got at the receiver.
If the measurement result is 00, then the receiver has the qubit $|\varphi_j\rangle$ in its possession, if it is 01 the gate $X$ is needed to be applied, if it is 10, it applies the gate $Z$ and if it is 11 it must apply first an $X$ and then a $Z$ gate to obtain the qubit $|\varphi_j\rangle$.

3. MAC protocols and Network description

Classical network communications use a layer structure based on OSI (Open System Interconnection) model which defines the functions of several layers of communication protocol. Each layer fulfills a specific function and the information proceeding from one layer is used as data by the next layer. MAC (Medium Access Control) and PHY (physical access) layers of protocol 802.11 are shown in figure 5. These layers also are subdivided into other sublayers [20].

The medium access control (MAC) Layer provides a variety of functions that support the operation of 802.11-based wireless LANs. In general, the MAC Layer manages and maintains communications between 802.11 stations (radio network cards and access points) by coordinating access to a shared radio channel and utilizing protocols that enhance communications over a wireless medium. Often viewed as the “brains” of the network, the 802.11 MAC Layer uses an 802.11 Physical (PHY) Layer, such as 802.11b or 802.11a, to perform the tasks of carrier sensing, transmission, and receiving of 802.11 frames.

Recent work in quantum wireless computation are [2, 4]. In [2] is presented that quantum algorithms can be used to improve actual classical MAC protocols. There, the authors propose a MAC layer modification by adding a Quantum Channel Access Sublayer, as is shown in Figure 6. This sublayer is responsible for controlling the access to the channel by quantum methods. However, whole modification of the layer stack will be necessary for quantum communications. Namely, all layers and sublayers must be able to manage quantum data. Moreover, in [4], a quantum routing mechanism is proposed to teleport a quantum state between quantum devices that do not share quantum EPR pairs mutually. Authors also set a precedence of a simple protocol for wireless communications purposes.

Recent technological advances show that wireless quantum transmission is possible [21]. In this work, the wireless network analyzed is based on cellular structure, i.e. the system is divided into cells. Each cell (named Basic Service Set, BSS) is controlled by a Base Station (BS) also called Access Point (AP), although it can work without BS when communication is between computers.

The protocol supports both Ad Hoc networks, which use a connection between two devices without using a wireless access point: the devices communicate directly when in range, and BS-oriented where base stations are responsible to communicate with Mobile Hosts (MH) in its cell, see figure 7. Every MH belonging to the cell can hear BS but MHs may be not near enough to hear each other. Besides, Access Points of different cells are connected through a backbone network (Distribution System).

Ad hoc networks result more adequate in situations such as a quick data exchange because setup is easy and does not require an access point. On the other hand, they demand self configuration, scalability, redundancy, and robustness in dealing with shifting topologies due to node failure and environment changes. Furthermore, sparse networks can have problems, because a sufficient number of available nodes are necessary in order to ensure reliability. Also, large networks can have excessive latency (time delay), which affects some applications. Consequently, the adding of
access points to an ad hoc network capitalizes both infrastructure and non-infrastructure networks positive points.

As was explained in section 2, whatever happens to an “entangled” quantum particle happens to the other party simultaneously. From this basic idea of a set of particles working in tandem, an access permission tool is thought. That is, each user trying to access the channel is “given” one qubit from an entangled pair. So, in order to find out his transmission turn, any of them measures the state of her qubit, in consequence the system collapses to a base state indicating every user if they can transmit or not at the same time. Let suppose that $|\psi_0\rangle = \alpha |01\rangle + \beta |10\rangle$ is the system state. Here the first qubit belongs to user $A$ and the second qubit to the right belongs to $B$. If one them measures her state the system collapses to state $|01\rangle$ with probability equal to $|\alpha|^2$ or to $|10\rangle$ with probability $|\beta|^2$. The first case means that $B$ transmit and $A$ wait, while the second is the opposite condition.

4. Quantum Protocol Description

The new protocol must be able to allow users to communicate each other either directly or through an access point by minimizing collisions. In what follows, a flow diagram depicting the protocol steps that both the MHs and the APs must carry out to have a reliable communication is presented in figures 8 and 9 respectively.

Let us suppose first that user $A$ wants to transmit data to user $B$. Then $A$ senses the channel for availability, if it is not available he waits a random time and then senses the channel again.

When the medium is idle $A$ searches for $B$. If $B$ is available, the sender create an EPR pair and sends a part to $B$ through a quantum channel. Then the information is shared by means of a teleportation process.

In the other case, when $B$ is far from the base station, or even when, regardless the MHs proximity, another user is trying to establish communication with $A$, oriented mode communication begins, that is, AP takes control. The control made by AP is done by creating a W-state with amplitudes $a, b, c$ (see eq. 2) according to the users priority. For example, the first qubit of the multipartite state is kept by AP and the other qubits are sent to the users. AP measures its qubit, so in case it collapses to zero, the probability amplitudes determine which user will transmit, that one who gets 1 when measuring his qubit.

In this way, quantum entangled communications permit to avoid collisions in this protocol.

5. Conclusion

Information exchanged between devices on a classical wireless network is governed by rules or conventions stated by the IEEE 802.11 communication protocol standard. Likewise, the widespread use of quantum communications systems will require quantum protocols. Here a medium access control (MAC) protocol relevant for both classic and quantum communications was proposed. In order to make migration easier, it takes advantage of quantum parallelism and quantum entanglement strengths taking into account the current standards.

For classical communications purposes a MAC sublayer is added. The quantum algorithm takes classical signals as inputs, and gives classical signals output that are taken as input by the other layers in the stack. Quantum entanglement is used to grant a free collision access. This novel protocol takes advantage of both ad hoc and BS-oriented networks. The former is chosen when MHs are near enough in order to permit
point-to-point direct mobile communications. While AP takes the control when direct communication cannot be established or when more than two users wanted to transmit simultaneously.

Some advantages of using the proposed protocol are described as follows. The hidden node problem is avoided in point-to-point method. Since AP manages the transmission authorizations the hidden nodes cannot transmit until the AP creates a new entanglement state or the transmission finishes. Data rate is improved when point-to-point connection is available by removing the AP hop. Multipartite entanglement is presented as an agile method to give permissions to access the channel when multi-user requests transmission authorization.

Future work points to consider quantum errors present in quantum channel. Despite recent research advances, quantum decoherence problems will be present due to environment interactions. Thus undesirable errors can arise and must be mended either through error detection and information retransmission or correction errors codes.

References


