

# Quantum-based wireless sensor networks: A review and open questions

Mario E Rivero-Angeles

## Abstract

Applications of quantum computing are growing at a very fast pace, for example, from quantum computers to quantum algorithms and even to the development of the quantum Internet. However, the use of quantum technology in wireless sensor networks has not been thoroughly investigated just yet. This is in part due to the complexity of using big, costly, and highly energy-consuming machines that are quantum computers to this date, compared to the nodes used in wireless sensor networks which are small, inexpensive, and operate with very low energy consumption requirements. However, we can expect that in the future (possibly in the next decade) quantum computers will be commercial and reduced in size, and hence, they can be used for sensor network applications which are the basis of the Internet of Things. In this review, we study the road from quantum computing to quantum wireless sensor networks and how the analysis and design of these systems have to change to accommodate quantum capabilities in sensors, processors, communication links, and overall performance of these monitoring networks.

## Keywords

Wireless sensor networks, quantum computing, quantum communications, quantum sensors, quantum security

Date received: 3 December 2020; accepted: 8 September 2021

Handling Editor: Peio Lopez Iturri

## Introduction

Quantum computers are still a long way from becoming a commercial alternative for everyday computing tasks. The main limitations of quantum computing are noise-related issues in the environment. Indeed, any temperature, vibration, or electromagnetic variation in the surroundings may cause errors in the qubits effectively degrading the performance of these machines. These limitations are more important still in Wireless Sensor Network (WSN)-related applications considering that nodes may be placed outside a laboratory's controlled environment, such as streets, roads, agricultural fields, rivers, vehicles, or even in people or animals. Nodes in a WSN are limited in resources, processing, and usually battery powered. As such, the operations they can perform are also limited, and the system lifetime becomes a major performance metric to consider in the design of the network.

However, there are now fully operational quantum computers performing algorithms for chemistry, machine learning, and cryptography applications.<sup>1,2</sup> Furthermore, many hybrid approaches have been proposed where classical machines are used for certain tasks in conjunction with quantum machines or quantum-based algorithms to improve certain computer operations. For instance, running simulations using a quantum processor while the rest of the operations are performed in a classical machine. An example of this approach is the variational quantum eigensolver

Computer Research Center—Instituto Politécnico Nacional (CIC-IPN), Ciudad de México, México

### Corresponding author:

Mario E Rivero-Angeles, Computer Research Center—Instituto Politécnico Nacional (CIC-IPN), 07738 Ciudad de México, México.  
Email: [mriveroa@ipn.mx](mailto:mriveroa@ipn.mx)



Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (<https://creativecommons.org/licenses/by/4.0/>) which permits any use, reproduction and distribution of the work

without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

(VQE) that is used for electronic-structure, material science, and condensed matter physics problems where the complexity of finding numerical results increases exponentially with the size of the system.<sup>3</sup> Also, the variational quantum factoring (VQF)<sup>4</sup> algorithm is a good example of these hybrid applications. These approaches are mainly used to solve specialized problems where classical machines may find it hard to provide results, but can these same approaches be used for WSNs applications? In the subsequent sections, this question will be addressed.

In addition to quantum computing, that is, the algorithms used to analyze, store, or treat information or simulate different processes in quantum computers either fully or partially, we also have to look for the quantum communication efforts where data can be transmitted (data have to be previously generated and stored) via the laws of quantum mechanics, effectively constructing a quantum network. In 2016, China demonstrated the functionality of a quantum satellite system, and both the European Union and the United States have ongoing projects regarding the transfer of quantum information, that is, qubits instead of classical bits.<sup>5,6</sup> However, the logical choice for these networks is based on optical fiber cables due to their capacity to transmit photons over large distances. Although these networks are an important step toward providing quantum communications at large distances, it is problematic for WSN applications since the use of fiber optics is not practical or even possible when nodes are placed randomly in hostile environments. Even in cases where the entanglement property is used to entangle matter nodes instead of using qubits in fiber optics directly, there is a previous phase that still uses optical fiber communications.<sup>7</sup>

In this regard, the team of Chinese scientists achieved the transmission of entangled photons over 1,200 km in a satellite link, using the Micius satellite, without the need for fiber optics.<sup>6,8</sup> In this case, the quantum communication network generates entangled photons that can be received at ground stations at a rate of one pair of entangled particles per second, which is a very low data rate to be used in general communication networks and especially for the quantum Internet but maybe sufficient for WSNs, where low-length data packets are generated. Indeed, many WSNs are used to detect a certain event, which requires a very low bit rate, for example, “1” when the event is detected and “0” when it is not, with additional bits for assuring correct communications. The question is, whether if this satellite network can be used in *conventional* WSNs to provide secure communications in terms of the relation cost/benefit that they can provide?

Finally, the development of mobile and portable quantum sensors that can be mass-produced in a reduced cost fashion opens the door to consider a

complete quantum WSN from the point where the measurement is taken until the information it conveys reaches the sink node or the cloud where it can be stored and accessed by any person in the planet, providing high data security levels.

Because of this, there are many open questions such as: Can quantum sensor nodes reduce energy or increase the overall system performance? Is it possible to use quantum sensor nodes and if so, what are the main design paradigms for these nodes? Can conventional sensor nodes be used in quantum physics experiments, and if so, what are the main design guidelines? Can quantum sensors be used in conventional WSNs effectively providing an acceptable system lifetime? Can the quantum theory be used for the design and analysis of WSNs?

In this review, we first discuss quantum computing and quantum communication technologies which would be the basis for providing *quantum capabilities* in WSNs. Then, we study the current research to develop and use quantum sensors and even quantum processors and quantum communications in WSNs. Also, the use of hybrid approaches in the context of sensor networks. Then, we focus on understanding the road to use quantum mechanics and quantum computing as tools to the mathematical model and study the performance of WSN. In this case, there is no direct use of quantum processors or sensors but rather apply the *quantum philosophy* to provide an accurate and efficient mathematical framework. Following this, we review the use of quantum security in the context of WSNs, where nodes have considerably less processing and storage capacity compared to classical or quantum computers in laboratory settings. Then, the key generation and cyphering are completely different from typical quantum key distribution (QKD) schemes. The review ends by considering the use of WSNs in quantum experiments, where sensors are used to measure entangled particles and how a careful design in these scenarios can render an overall lower energy consumption.

## Quantum computing in general

In the last years, many research groups and companies have focused their efforts on achieving quantum supremacy, where quantum computers outperform classical computers in a given field. This has produced an important impulse to construct practical (and eventually) commercial quantum machines that, at first would be used by specialized operation, but then, they could be used in conjunction with classical computers for more generalized use.

As proposed by Gibney<sup>9</sup> and Mohseni et al.,<sup>10</sup> some companies developing quantum computers use superconducting wires to process and store qubits reaching

temperatures close to absolute zero, such as the ones developed by Google and IBM. Others are focused on the use of magnetic fields and lasers. Yet another approach is generating photons inside silicon chips.

However, there is no need to wait for a commercial quantum machine in order to develop quantum algorithms or quantum communications. As explained in this section, the quantum-based computer science area has been growing in different parallel lines even if no access to a quantum computer is widely available.

### Hybrid approaches

In the following algorithms, the use of classical algorithms that can be implemented in quantum computers or quantum circuits is proposed. Hence, these works propose an important hybrid approach for using classical algorithms but to be used by quantum computers.

The limitations posed by classic computers to find numerical solutions of complex systems, where the computational cost increases exponentially with the size of the system (such as electronic-structure or material science-related problems), has led to different research teams to look for alternative solutions in the quantum computing area. One of these works is the one presented by Kandala et al.,<sup>3</sup> where the authors prove an experimental optimization of Hamiltonian problems using up to six qubits using the VQE algorithm specifically designed to work and take advantage of the interactions that take place in quantum processors.

In order to solve combinatorial problems on graphs, Farhi et al.<sup>11,12</sup> proposed the quantum approximate optimization algorithm (QAOA) that is implemented in a quantum circuit. Both the complexity of the circuit and the approximation accuracy increase as the positive integer  $p$  of the proposed algorithm increases. The authors found that this quantum algorithm finds a cut in three-regular graphs that is at least 0.6924 times the size of the optimal cut, proving a clear pathway to develop efficient algorithms to be implemented in quantum circuits. Also, the authors study if the quantum algorithm requires the information from the complete graph or if it can efficiently work with a partitioned graph, which would also reduce the complexity of the system.

On the contrary, integer factorization is one of the main applications for quantum computers, given the high number of operations required. In this sense, the work by Anshuetz et al.<sup>4</sup> develops an algorithm to map the factoring problem using well-known techniques, known as VQF. The main idea is to simplify the equations in a preprocessing phase to reduce the number of qubits required by a subsequent variational circuit using the QAOA. Hence, VQF is a good example of how conventional algorithms are being developed in conjunction with quantum computing-enabled techniques.

Another relevant line of research in this class of hybrid algorithms is the Entanglement-Assisted Quantum Error Correcting Codes (EAQECCs)<sup>13</sup> that produce quantum codes using classical codes but without the “1” and “0” duality for the value of the bits and considering a pre-existing entanglement between the transmitter and receiver. In this regard, the work presented by Guenda et al.<sup>14</sup> provides different methods to construct such EAQECC codes with an adequate number of entanglements to produce codes with good error correction performance. This research is a basic requirement to achieve efficient communications in quantum systems, as we explore in the following sections.

### Quantum communications

Wehner et al.<sup>15</sup> reviewed the road to achieve quantum communications, which will be the fundamental function of the *quantum Internet*. The main characteristic of the quantum Internet is to provide quantum communications between two geographically separated points, connecting quantum processors that can potentially provide higher information rates and inherent security. This is achieved by transmitting qubits, that, unlike classical bits that take values of “0s” and “1s,” can be in a superposition of states (0 and 1 simultaneously). To this end, Pfaff et al.<sup>16</sup> proposed the use of defects in diamonds in order to develop a quantum teleportation protocol that may be the fundamentals of this aforementioned quantum Internet. The authors generate remote entanglement to control and read multiple qubits per node that can be used to send information through large distances. Also, Humphreys et al.<sup>7</sup> proved that extended quantum networks are viable using these diamond spin qubits nodes achieving extended entangling rates.

Building on this, an entanglement between matter-based quantum nodes over 50 km in a fiber optic is reported by Krutyanskiy et al.<sup>17</sup> This is done using an efficient source of ion-photon entanglement via cavity QED techniques. These advancements are the basis for providing quantum networks where quantum nodes store, process, and convey quantum information. In this work, the authors were able to avoid drastic photon absorption typical in the wavelengths where the entangled matter is generated by frequency conversion in the telecommunication range where the fiber optic acts as an ideal waveguide, allowing such extended communication distances.

### Quantum security

One of the first applications of quantum theory in computer-related subjects is *Quantum Cryptography*

and probably the first quantum-related computer algorithm to be mature enough to become commercial.<sup>18–20</sup>

The basic idea in QKD is that two nodes create a shared key, kept in secret from the rest of the nodes in the system, that can be used to decrypt messages. This key is shared among the *legal* nodes within a quantum channel. The main advantage of QKD is its ability to detect when a third unauthorized party attempts to gain knowledge about the secret keys. The reason for this is that, measuring a quantum system changes the state of the system. For instance, one way to implement this key distribution scheme is through the entanglement of particles, where an intruder that intercepts the distribution of the keys changes the state of the system and the cyberattack is detected. Building on this, QKD is used to distribute the secret key, while the encrypted information is transmitted through a classical verified channel. Specifically, a pair of nodes are connected through a quantum channel, that can send quantum states (qubits), either using fiber optic cables or wirelessly to share the keys. Unlike classical security protocols, the keys are nearly identical but they can have an estimation of the discrepancy between them that arise due to imperfections in the quantum channel but can also arise due to eavesdropping. They are also connected via a classical communication channel where messages are encrypted using the aforementioned keys.

## Quantum computing in WSNs

Given the current advances in quantum computers and quantum processors, the direct use of these machines seems to be impractical to be used in WSNs. Given the high cost, dimensions, and stability conditions required to operate these machines, their use in field monitoring, where hundreds or thousands of nodes are used in a sensor network, it is not ost-effective nor practical to consider the direct deployment of quantum computers as nodes in a WSN.

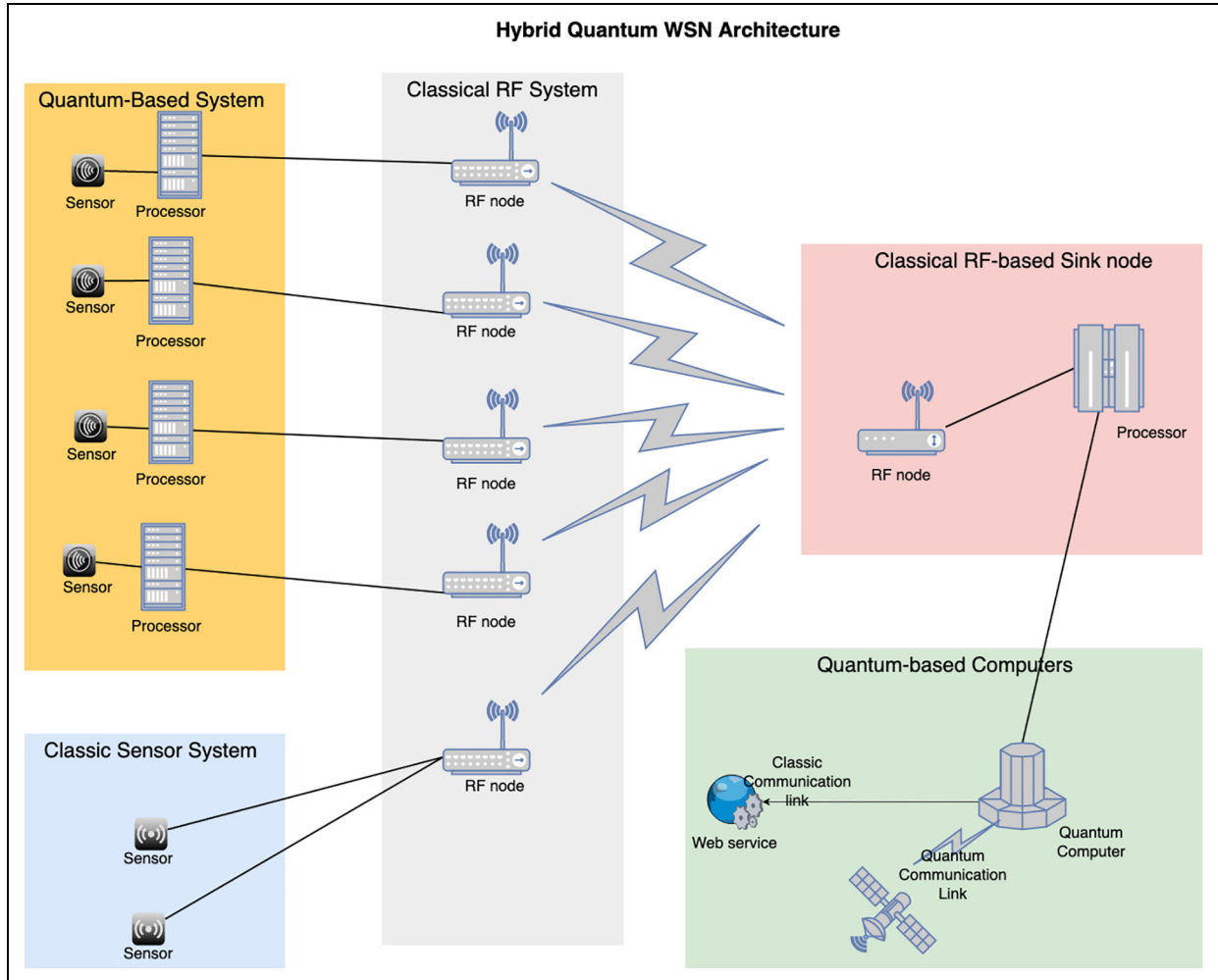
Nonetheless, quantum machines can still be used at the sink node or as part of the information processing unit, outside the physical deployment of the network, used to perform operations like machine learning-related algorithms or optimization procedures. In this case, only a few (or even one) quantum machine is required in a laboratory setting. Hence, hybrid approaches, like the ones discussed above, can be directly used in the WSN context.

On the contrary, quantum sensors can be used instead of conventional sensors where high accuracy is required as we discuss in this section.

In Figure 1, we can see the communication architecture that could be used in quantum wireless sensor networks (QWSNs), which corresponds to a hybrid approach. For one part, we would have classic sensors

taking measurements for typical environmental variables. These sensors, even if sophisticated and accurate, do not possess the sensing capacity, at the particle level, as quantum sensors, as discussed later on. Indeed, quantum sensors would be used only for the monitoring of specific variables and are not meant to be used for all phenomena. Hence, it is expected to have both types of sensors in the same surveilled area. For the quantum sensors, they would require some type of processing/conversion to obtain classic bits, since qubits are not likely to be transmitted in WSNs composed of hundreds of nodes, due to implementation cost restrictions. A much cheaper option is to obtain classic bits from the quantum sensors in order to be transmitted using low-cost radio frequency (RF)-based nodes. Classic sensors do not require such processing considering that many commercial sensor nodes are already equipped with RF capabilities. Hence, the sink node may also be based on a RF transceiver. At this point, bits may be stored, processed, and sorted in a classical processor to be transmitted to the gateway, which can be composed of both classic communication links, either RF or fiber optics, and quantum-based computers can be used to transmit sensitive data using a quantum communication link by satellite or fiber optics. Again, not all information packets are greatly benefited by such quantum communication links that require specialized equipment and for non-critical data, low-cost communication links can be used.

It is important to note that there may be applications where the hybrid approach is not attractive or efficient. For instance, when the number of sensor nodes is reduced, two or three as opposed to hundreds of nodes in typical WSNs. Also, when all the monitored variables have a *particle-level* accuracy measurement, and no classic variable is of any interest. Conversely, classic sensor data (bits) can be converted to qubits if the sensor nodes are using a quantum communication link. Hence, nodes would use a satellite or fiber optic quantum communication system that does not require the conversion of bits-qubits and vice versa. Even if these links are much more expensive at this time (and may remain more expensive in the future compared to classic communication links), there is an interest on using such links when information is sensitive or when all the system is quantum-based, that is, sensors, nodes, links, and computers, avoiding the need to have conventional bits. For example, experiments that take place in particle colliders where information is quantum in nature can be stored and transmitted by quantum sensors using quantum links. In this scenario, sensor nodes are placed in specialized facilities under very secure conditions with specialized electrical and physical conditions. This information can be processed and classified using quantum computers considering that the raw data are already in a quantum state given by the particles



**Figure 1.** General architecture for hybrid QWSNs.

obtained in the collider. In turn, this information may be classified and highly sensitive due to its potential uses in military applications. Hence, quantum-based security protocols are more than justified.

### Quantum sensors

Quantum sensors have been developed for a variety of applications such as navigation systems, earthquake detection, and brain monitoring.<sup>21</sup> The main characteristic of such quantum sensors is their precision, far beyond what classic sensors can achieve due to the fact that they use atomic properties, like electrons in different energy states, to sense the environment, that conventional sensors cannot do. For instance, quantum sensors can detect minuscule changes in local gravity. Most of these sensors have been confined in laboratory settings, but the research presented by Ménoret et al.<sup>22</sup> develop a portable quantum gravimeter that functions in real-world conditions that are capable to measure absolute gravitational acceleration below  $1 \mu \text{ Gal}$ .

Other research teams have focused on developing quantum sensors based on diamonds placed on silicon chips for the detection of magnetic fields, effectively opening the path to low-cost quantum sensors that are capable of operating in temperatures found in most sensor network applications, that is, room, open field, and street-focused applications.<sup>21</sup>

Once these quantum sensors are available for commercial usage, the question remains on their impact on the performance of the network. Specifically, it would be interesting to see the energy consumption of these types of quantum sensors and their adaptation capabilities in the sense that if they are easily configurable to work in continuous monitoring or event-based detection manner or even in a hybrid operating mode.

Also, it will be of major importance to determine if these sensors are benefited in any way using quantum nodes and/or quantum communication systems. Imagine the case where measurements from these nodes can be provided in qubits that are best stored and processed in quantum processors without losing their

properties and then be transmitted in a quantum communication link, either wirelessly or using a fiber optic channel. Would this reduce energy consumption in the overall system? Would this provides a secure end-to-end WSN, from the point where the measurement is done until it reaches the sink node or even the cloud? Or would this be a highly unstable, costly, and complex system to be installed in fields or streets? To the best of our knowledge, these questions have not been fully addressed to this date and research efforts would have to answer them before considering the implementation of such quantum systems.

In this regard, the work presented by Lee et al.<sup>23</sup> focuses on a general architecture for the development of quantum sensors in the context of Quantum WSNs. Specifically, they propose the use of four elements that any quantum node should have, namely: transducer (to convert the physical phenomena that the system is monitoring), classical to quantum (C/Q) converter, quantum to classical (Q/C) converter, and quantum processor and memory core. Specifically, the transducer should return electrical signals that represent the measurement, either physical, chemical, or biological quantity. Then, this electrical signal is represented in qubits using the C/Q converter in such a way as to be processed and stored by the quantum processor. If the WSN has a quantum communication system, then the qubits are directly transmitted to other nodes or the sink node. Conversely, if such quantum capabilities are not available, the Q/C is used to convert qubits to classical bits in order to be conveyed to the sink node. Additional characteristics of each of these components are described in this work.

Also, they develop a mathematical analysis to calculate the achievable data rate from using such architecture, considering that quantum operations require exponentially fewer operations than classical systems. However, this work does not provide an energy-related analysis which may be critical in the context of WSNs. Indeed, if the energy required to operate such quantum nodes is too high, it may hinder the system lifetime which in turn would restrict their use in commercial/practical scenarios. Hence, an energetic analysis should be provided in the near future, regarding the operation of quantum converters and processors directly in WSNs with and without the use of quantum communications in order to have a precise idea on the operation conditions of quantum WSNs.

### Hybrid approaches

Classical computing tasks can be performed by nodes in the field while information processing can be done using quantum processors elsewhere.

First, it is important to mention that the hybrid approaches mentioned before, such as QAOA, VQF,

and VQE, are not of great interest in the area of WSNs. This is because nodes are not typically used to solve such computational intensive problems, such as factorizing or solving combinatorial problems. However, these algorithms can still be used in quantum computers assisting the WSN. Indeed, if the nodes in the system convey information to the sink, it can be processed using the optimization algorithms over quantum computers for certain applications but not directly over the nodes in the network.

On the contrary, quantum-based codes present a promising option to provide efficient communications in quantum WSNs. Given that quantum-assisted error-correcting codes, such as the ones presented in Guenda et al.,<sup>14</sup> use well-known classical correcting codes such as Reed-Solomon and Linear Codes with Complementary Duals, they can be used for communications among sensor nodes in a WSN. However, the energetic and computational costs (in terms of memory and processing requirements) have not been thoroughly studied for such resource-limited systems. In the following years, we expect to find works evaluating the performance of such codes showing the impact of EAQECC codes in the system lifetime in order to decide if these codes are adequate in the sensor networks or in which applications. For instance, if the energetic cost for generating these codes is too high, they can still be used in event-driven applications, where nodes only transmit when specific events occur which may rarely happen. Hence, the rate of event occurrence may be the main parameter to decide if quantum correcting codes are implemented in WSNs.

### Quantum philosophy to design WSNs

In the following works, the authors use quantum theory or some relevant parameters of quantum mechanics to propose new algorithms to optimize the performance or even to design or model WSNs. As such, there is no use of quantum nodes, nor quantum processors nor quantum communications. Only the main ideas or *philosophy* of quantum mechanics are used.

### Optimization

We begin by reviewing the works focused on optimizing the performance of sensor networks.

Topology control is used to decide the number of connections among nodes and determining the adequate neighbor nodes that each sensor should connect to in order to reduce energy consumption and still provide a good connectivity level, allowing information exchange in the system. In general, there is an inverse relation between node connectivity and energy consumption in the sense that when a node has more connections, there are more packet transmissions and more

active links which consume more energy. As such, balancing these two parameters is not straightforward. Sun et al.<sup>24</sup> proposed a quantum genetic algorithm, quantum genetic algorithm (QGA), to select the connection among nodes and establish routes for packet exchange. The idea is to combine genetic algorithms (where an initial setting is proposed and then it evolves according to the laws of genetics to select the optimal final setting, that is, the connection among nodes) and quantum theory using qubits to represent genes instead of the binary values typically used. The authors prove an energy reduction in the system while maintaining good connectivity in the network.

Clustering is a technique aimed at reducing energy consumption in the network by forming clusters of neighboring nodes, that is, nodes close to each other that can communicate directly or by multiple hops. Nodes inside a cluster, also called cluster members (CMs), transmit to a selected cluster head (CH). By doing so, transmissions are short-ranged and local, avoiding highly energy-consuming long-range transmissions that rapidly deplete the energy in the system. Clustered-based WSNs are also scalable since the number of nodes implies a higher number of clusters but transmissions remain local. In Rathee and Kumar<sup>25</sup> and Tsai et al.'s study,<sup>26</sup> quantum-based genetic/evolutionary algorithms are also used, but in this case, focused on achieving efficient cluster formation. The advantages of using the quantum-based algorithm are that it introduces parallel processing to the genetic algorithm reducing the computational cost of finding the optimal clustering configuration in terms of selecting the appropriate CHs and CMs, increasing the system lifetime. Kanchan et al.<sup>27</sup> also study the use of quantum-based algorithms for clustering but using a particle swarm optimization proposal called QPSOEEC (quantum-inspired particle swarm optimization for energy efficient clustering). In this work, the node's position updates are performed using the quantum-inspired methods and the CH selection is done using the particle swarm optimization algorithm.

Wenlan et al.<sup>28</sup> consider a heterogeneous system where nodes may have different characteristics in terms of energy and communication range among others. In this heterogeneous setting, the problem of node localization is complicated due to the error in distance estimation among nodes. To this end, this work uses a quantum particle swarm optimization (QPSO) algorithm to improve the accuracy of the position estimation of nodes.

A related work is presented by Guo et al.,<sup>29</sup> where coverage optimization is achieved through the use of a quantum-inspired evolutionary algorithm. Adequate coverage in a sensor network aims at efficiently distributing nodes in the area of interest in such a way as to detect possible events that occur inside this region. In

many cases, it is not feasible to achieve complete coverage due to the deployment cost required (either by installing many nodes or using expensive nodes with high coverage radii). Hence, it is essential to place the available nodes most efficiently also reducing coverage redundancy and blind spots in the system. Building on this, Guo et al.<sup>29</sup> proposed to achieve optimal coverage using a quantum-inspired cultural algorithm (QCA), where evolutionary individuals are generated from quantum individuals effectively obtaining maximum coverage and minimum redundancy ratio (where the same region is covered by multiple nodes) in WSNs.

Finally, Ishizaki<sup>30</sup> uses a quantum annealing scheme to find near-optimal scheduling solutions in time division multiple access (TDMA)-based WSNs. TDMA is a collision-free access protocol that allows nodes to transmit in an orderly fashion in a shared channel. By dividing the access opportunities into multiple time slots, each node is assigned a particular slot to convey its information to the sink or other nodes while the rest of the nodes remain silent effectively avoiding collisions. However, the number of slots is usually lower than the number of nodes. Hence, channel assignment, that is, time slot assignment, is no easy task. As such, the quantum annealing scheme provides an efficient computational solution to finding near-optimal channel assignments that can be performed offline and not by the resource-constrained nodes in the system.

### Uncertainty in WSNs

In this research area, quantum properties can be used to mathematically model WSNs. Specifically, we focus on the intrinsic property of the superposition of states, where a bit can be both "1" and "0" simultaneously and its value is only known when a measurement or observation is performed. This concept can be directly applied to the state of a sensor node in the field surveilling its environment.

Indeed, in most cases, it is not possible to know if a node is sensing an ongoing event, even if the sensor lays inside the event radio. This is because there could be obstacles between the sensor and the event or due to the sensibility of the node or due to a noisy environment or simply a malfunction of the node. This uncertainty issue is rarely captured in the mathematical modeling of the system.<sup>31</sup> Indeed, in many models, whenever a node is inside the event radio, it is assumed to be correctly detected. Recall that mathematical models in WSNs aim at determining the average performance metrics, such as system lifetime, average packet delay, and probability of successful event detection. These models allow to carefully select the system variables where an adequate operation is guaranteed, like the number of nodes, the position of nodes, detection range, transmission range, and packet size among

others. By overlooking this event detection uncertainty, the derived models can (over)underestimate the system lifetime and hindering the system performance in general, resulting in different behavior from the practical system compared to the estimation of the model. This issue does not only impact the accuracy of the model, it can negatively impact the system dynamics. Given that the network is installed to operate under certain variables when a different environment is encountered, the number of packet collisions can increase or the traffic at certain regions can vary, resulting in a poor monitoring system.

In many works, this uncertainty of detection can be modeled using a detection probability, like the one developed by Villordo-Jimenez et al.<sup>32</sup> However, in Quantum WSNs, where sensors are enabled with quantum capabilities or even if quantum processors are being used, the use of the superposition of states would render a more accurate analysis. Furthermore, this accuracy could be even more important if the network is monitoring quantum events where particles in superposition states are being detected.

Similar research, where the *quantum uncertainty* is used to model classical systems in different states not known apriori has been presented before. For instance, the works developed in previous works,<sup>33–39</sup> consider the game of life, developed by John Conway in 1970, where the evolution of life is emulated using cellular automata with very simple rules for the survival or death of cells in a given environment. In this game of life, cells are either dead or alive at a certain moment and their state is defined by the state of the cell's neighbors. Namely (1) a live cell with less than two live neighbor cells dies; (2) a live cell with more than three live neighbor cells dies; (3) a live cell with two or three live neighbor cells survives (remains alive); and (4) a death cell with three live neighbor cells becomes alive in the following iteration (birth) and remains death otherwise. In the quantum-based game of life, cells can be in a superposition of life and death states, and their state is only known when the next iteration of the game is performed according to the specific quantum rules or quantic logic gates used in each case.

Following this idea, a node can be in a superposition of *event detection* and *no event detection* that can be introduced to the model to determine the number of reporting packets transmitted to the sink node. To this date, it is an open question if these models would render a more accurate representation of classical WSNs or quantum WSNs and in which conditions or cases this happens. Also, it is still to be known if this line of research would provide enhanced performance of the system by establishing different medium access control schemes with this consideration of having nodes in a superposition of states.

## Quantum communications in WSNs

In general, we can considerate that the use of fiber optics in WSNs is not feasible, given the implementation cost of connecting thousands of nodes randomly placed in certain regions, that in many cases are in hostile environments (high temperatures, exposed to rain, where animals can transit, etc.). However, there are some applications where fiber optics can be used. Namely in domotic applications to monitor different variables in indoor environments inside a building, like sensors in doors or windows, temperature sensors, and seismographers to detect earthquakes. In these applications, nodes are usually placed in strategic locations (not randomly), away from people, and can easily use fiber optic channels. This would allow the use of qubits to transmit small information packets (only a few bits are required to indicate if a door or window is open or if the temperature has risen above a certain level), with the advantage of providing a secure channel. Note that this application is not intended for common house environments but rather for governmental buildings, hospitals, and military bases among others, due to the restrictive implementation costs. A careful design should be developed in order to clearly show performance metrics like system lifetime, packet error rate, and packet delay, considering the specific characteristics of the quantum channels which, to the best of our knowledge have not been presented before.

For other applications, where fiber optics are not feasible, a wireless channel can be used. However, it would not be practical to consider a satellite channel since in this case, nodes have to be aligned to the satellite antenna, and nodes placed randomly, are very unlikely to perfectly align to the satellite. Also, nodes may probably suffer from non-line of sight channels due to obstacles, walls, trees, and other objects. However, they may communicate directly using a wireless channel in low-distance communications. Indeed, through multi-hop communication architectures, nodes can reach their destination using multiple intermediate nodes using a wireless quantum channel. For instance, Maier et al.<sup>40</sup> explored quantum communications where environmental noise can enhance the efficiency of the communication system. Hence, this type of communication can be used in noisy environments such as the one usually present in WSNs. These research lines should be further developed in order to know practical communication distances and design the monitoring systems accordingly.

## Quantum-based security in WSNs

Given the fact that WSNs are battery operated and limited on memory and processing capabilities, the use of classical cryptographic techniques, that require the



generation of big prime numbers or high processing demanding tasks is not recommended in WSNs. Hence, different approaches to provide security in these networks have been developed in the last few years.<sup>41–46</sup> In this regard, some works have focused on reducing the number of entangled qubits required to encrypt data in quantum-based schemes.<sup>44</sup> Also, in view of the limitations of establishing quantum channels in WSNs, there are many proposals to use quantum-based security algorithms by providing off-line, previous to the implementation of nodes, solutions.

For instance, Li and Yang<sup>41</sup> and Li et al.<sup>45</sup> present a random Einstein–Podolsky–Rosen (EPR) pair allocation scheme pre-assigned to sensor nodes to form a secure link. This scheme aims at reducing the effect of the man-in-the-middle attack.

Ma et al.<sup>42</sup> focused on underwater communications, where nodes communicate using acoustic signals that propagate efficiently in water, rather than radio-frequency or light signals, commonly used in conventional WSNs. Their proposal involves a quantum communication channel between a surface base station and an autonomous underwater vehicle, where keys are shared, and a classical communication acoustic channel between the autonomous vehicle and underwater sensor nodes using symmetric cryptography, reducing the complexity and overhead at the resource-constrained nodes.

Agarkar et al.<sup>43</sup> focused on providing a secure scheme for aggregation in WSNs. Aggregation is the process of extracting relevant information from a set of data packets in an intermediate node. For instance, consider the case of a cluster-based WSNs, where the CH collects the data from all of its CMs. Instead of transmitting all the packets directly to the sink node, which would convey a highly energetic transmission, the CH only sends the average values, or the maximum and minimum values, greatly reducing energy consumption in the system. In addition to data aggregation, these intermediate nodes can perform data compression either using lossless schemes or lossy schemes. Compression, unlike aggregation, is used to eliminate or reduce redundancy from the data. Typically, WSNs can use encryption schemes like elliptic curve cryptography (ECC) that become vulnerable if a quantum machine is used to break the codes. Hence, in this work, the authors propose the use of lattice cryptography applying the learning with errors over rings (R-LWE) technique that proves a better solution than elliptic curves.

### Post-quantum security in IoT networks

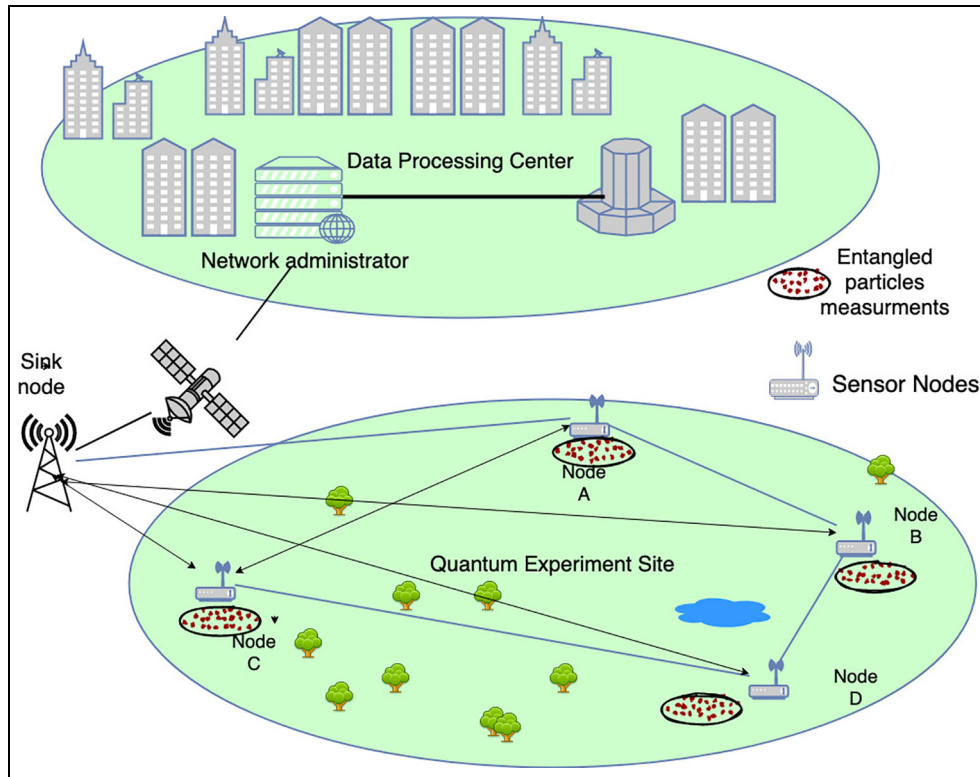
One major research area in cybersecurity is concerned with implementing secure systems in a post-quantum world. In a near future, where quantum computers are

commercially available and conventional (classic) cryptographic schemes are no longer secure due to the increased ability to break such codes that now are practically unbreakable. This is particularly worrisome in the Internet of Things (IoT), where many independent devices are deployed to perform different services in an autonomous manner but are vulnerable to many different attacks due to their open nature, lack of central control, and low computational power.<sup>47</sup> Building on this, IoT devices have to use cryptographic schemes that do not require many operations or memory or energy to perform adequately.

Based on the above, post-quantum security schemes are those that provide secure systems when quantum computers are widely used and available for the general population. Many post-quantum security schemes have been developed recently, such as the ones presented by Lohachab et al.<sup>47</sup> and Fernández-Caramés:<sup>48</sup> lattice-based cryptography, hash-based cryptography, multivariate cryptography. Also, there are many efforts for implementing these schemes in low-processing capacity microcontrollers such as 8 bit and 32 bit ARM processors. Ebrahimi et al.<sup>49</sup> proposed the InvRBLWE scheme that is secure against quantum-based attacks that can be used in resource-constrained nodes. Shahid et al.<sup>50</sup> proposes a distributed ledger scheme, such as the ones used for secure transactions of crypto-currencies, based on a one-time signature that offers low energy consumption and is adapted for IoT nodes.

However, many open questions remain. Most of these works are focused on the computational tasks that the nodes have to perform in order to implement the post-quantum security schemes. But the impact on the system performance has not been thoroughly considered. For instance, the system lifetime, or alternately, the average energy consumption of nodes using such schemes has not been considered in the context of the communication activities, such as the number of packets to be transmitted, if the system operates under an event-driven or continuous monitoring regime. Are there specific conditions where these proposed cyber security schemes can operate adequately or hinder the system operation? Considering that many of these devices are battery operated, it is of major importance that the operations required to provide secure IoT networks do not drastically reduce the operational time of the nodes, since, in many cases, users cannot replace the batteries. Alternatively, considering the *green communication* paradigm, the following question is still open: can IoT systems, with post-quantum security schemes, operate with renewable energy sources, such as solar, wind, or bio-energies? In order to answer this question, a detailed analysis of these networks would have to be done.

Another open question is related to the latency introduced by such post-quantum security schemes. By



**Figure 2.** WSN used for the monitoring of experiments where entangled particles are used.

introducing these additional operations, can IoT systems maintain low latency communications when needed? Indeed, not all nodes require low latency communications, but there are some where nodes are expected to timely report certain events, such as earthquake and fire alarms, and intruder detection. Perhaps, the alternative again is using hybrid schemes where classical cryptography (offering a reduced security level but requires lower computational burden on nodes) can be used when certain events occur while offering an increased security level in normal conditions. Again, a detailed analysis of these tradeoffs has to be developed to accurately answer these questions.

### WSNs in quantum experiments

WSNs can be used in certain experiments where entangled particles have to be measured in some way. Consider for instance the triple slate experiment developed by Sinha,<sup>51</sup> where a photon splits into two lower-energy photons. The team at the Quantum Information and Computing Laboratory from the Raman Research Institute, in India, is performing a series of experiments in open fields next to corn crops. For these experiments, different sensors may be needed to measure different characteristics of the mother or daughter photons. As such, if some of these photons are entangled, like the ones used in the Micius satellite,<sup>6</sup> the measurement of one can be detected in other sensor nodes, further away

and closer to the sink or base station. Hence, the energy consumed to send this information can be reduced by selecting the node closer to the sink to relay this information.

Consider for example the scenario presented in Figure 2. In this case, nodes are placed where the measurements of entangled particles are taken place. Suppose that nodes B and C receive entangled particles, and they have to report relevant data regarding those particles to the sink node. In conventional WSNs, both nodes should report their data (since particles at different nodes are not entangled and probably have different properties), while in this case, for certain conditions and experiments, a single report should convey all the relevant information, reducing in half the energy required to report the measurements. To further reduce energy consumption, node C should be selected instead of selecting node B. Indeed, energy consumption is directly related to the distance between transmitter and receiver. As such, a careful selection of the system setup can produce significant energy consumption reductions, rendering longer network lifetimes. This issue should be carefully studied in the following years in order to determine the type of experiments where this design produces energy consumption reductions and medium access control schemes should be designed considering the distance among nodes with entangled particle measurements and the distance to the sink.

One variant of this scenario is considering data traffic in different zones of the WSN. In general, nodes closer to the sink node experience higher packet traffic arrival rates since in many cases, nodes transmit in a multi-hop fashion. As such, many transmissions are directed toward nodes closer to the sink node, which have to relay these data in subsequent transmission opportunities. Building on this, an efficient transmission scheme should instead select node B to transmit to node A and then to the sink when traffic at node C is too high or when node C has little energy left. Even if selecting this route includes more packet transmissions and the packet travels a higher distance to reach the sink, system lifetime can be increased by redirecting packet traffic from key nodes, like node C in this case. However, this has to be thoroughly designed and analyzed before implementation to guarantee adequate performance.

Note that, for these applications, nodes in the network are classical nodes, that is, they are not performing quantum-based operations nor transmitting qubits but rather classical bits after the specialized sensors detect the particles of interest. As such, there is no need to use quantum nodes but maybe the use of quantum sensors is required. In this regard, energy consumption would be highly reduced for satellite quantum communications, where nodes may be separated by thousands of kilometers. However, in this case, quantum communication links should be used, adding an intrinsic security level.

## Conclusion

In this work, the road to implement, study, design, and analyze WSNs with quantum capabilities is reviewed. There are many different roads to achieve this, from quantum processors, quantum algorithms, quantum communications, quantum sensors, and even quantum philosophy to design and optimize the system performance.

It is clear that the technological and theoretical advancements quantum WSNs achieve are solid, and there is little doubt that in the near future there will be commercial and fully operational quantum-enabled WSNs in different degrees. Hence, the design and analysis of such systems have to be made accordingly. Specifically, energy consumption and diverse performance metrics of the system (packet delay, packet loss probability, successful event detection, etc.) are calculated differently than in classical WSNs. In order to achieve an adequate operation, mathematical modeling and analysis should be done considering the different capabilities and characteristics of these networks.

Another important issue to consider is the benefit–cost relation of QWSNs. Indeed, even if

quantum-based WSNs provide many benefits, in many current applications of WSNs, there is a need to install dozens or even hundreds of nodes in the area of interest. Hence, this may be restrictive for QWSN applications. Until the commercial cost of quantum sensors and nodes is available, there is a doubt if these systems can be an option for practical applications or if QWSNs would be reserved for very specific environments. Furthermore, there is the possibility that these systems may be contemplated to work in conjunction with classical WSNs, forming hybrid WSNs, taking advantage of both types of networks and also complementing their disadvantages, such as reducing the implementation costs. In this scenario, the design and analysis should be very different from the one in purely classical or purely quantum WSNs.

This is clearly the case for cybersecurity in WSNs. Since key generation and data cyphering require high amounts of operations and memory, a possible scenario is to only apply quantum-based security algorithms in key nodes while other nodes operate using classical cryptographic techniques or even without security capabilities. For instance, only cluster heads can cipher the gathered data to be transmitted to the sink node while cluster members transmit their raw data. The different vulnerabilities in such a system should be studied in detail. Another alternative is to use quantum-based security at quantum nodes, that is, nodes that use quantum sensors and/or quantum processors in cases where the monitored environment is quantum in nature, taking advantage of the reduced complexity of using an *all-quantum node* without converting qubits into bits to be processed, stored, and transmitted, using quantum-based communication channels, that may not be available in all nodes.

## Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was partially funded by Project SIP-IPN No. 20210438.

## ORCID iD

Mario E Rivero-Angeles  <https://orcid.org/0000-0003-1020-6806>

## References

1. Brooks M. Before the quantum revolution. In: Hartle JB (ed.) *Quantum universe*. Harlan, IA: Scientific American, 2020, pp.220–231.

2. Arute F, Arya K, Babbush R, et al. Quantum supremacy using a programmable superconducting processor. *Nature* 2019; 574: 505–510.
3. Kandala A, Mezzacapo A, Temme K, et al. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *Nature* 2017; 549: 242–246.
4. Anschuetz E, Olson J, Aspuru-Guzik A, et al. Variational quantum factoring. In: Feld S and Linnhoff-Popien C (eds) *Quantum technology and optimization problems (QTOP, 2019)* (Lecture Notes in Computer Science), vol. 11413, pp. 74–85. Cham: Springer.
5. Brooks M. The quantum internet is emerging—one experiment at a time. In: Hartle JB (ed.) *Quantum universe*. Harlan, IA: Scientific American, 2020, pp.220–231.
6. Hosseinidehaj N, Babar Z, Malaney R, et al. Satellite-based continuous-variable quantum communications: state-of-the-art and a predictive outlook. *IEEE Commun Surv Tutor* 2019; 21(1): 881–919.
7. Humphreys PC, Kalb N, Morits JPJ, et al. Deterministic delivery of remote entanglement on a quantum network. *Nature* 2018; 558: 268–273.
8. Billings L. Race for the quantum internet. In: Hartle JB (ed.) *Quantum universe*. Harlan, IA: Scientific American, 2020, pp.259–268.
9. Gibney E. Quantum gold rush. In: Hartle JB (ed.) *Quantum universe*. Harlan, IA: Scientific American, 2020, pp.269–283.
10. Mohseni M, Read P, Neven H, et al. Commercialize quantum technologies in five years. *Nature* 2017; 543: 171–174.
11. Farhi E, Goldstone J and Gutmann S. *A quantum approximate optimization algorithm*. Quantum Physics, Report Number MIT-CTP/4610, November 2014, <https://arxiv.org/abs/1411.4028>
12. Farhi E, Gamarnik D and Gutmann S. *The quantum approximate optimization algorithm needs to see the whole graph: a typical case*. Quantum Physics, Report Number MIT-CTP/5198, April 2020, pp.1–19, <https://arxiv.org/abs/2004.09002#:~:text=20%20Apr%202020%5D-,The%20Quantum%20Approximate%20Optimization%20Algorithm%20Needs%20to,Whole%20Graph%3A%20A%20Typical%20Case&text=The%20Quantum%20Approximate%20Optimization%20Algorithm%20can%20naturally%20be%20applied%20to,the%20locality%20of%20the%20graph>
13. Hsieh MH, Devetak I and Brun T. General entanglement-assisted quantum error-correcting codes. *Phys Rev A* 2007; 76: 062313.
14. Guenda K, Jitman S and Gulliver TA. Constructions of good entanglement-assisted quantum error correcting codes. *Des Codes Cryptogr* 2017; 86(1): 121–136.
15. Wehner S, Eikouss D and Hanson R. Quantum internet: a vision for the road ahead. *Science* 2018; 362(6412): eaam9288.
16. Pfaff W, Hensen BJ, Bernien H, et al. Unconditional quantum teleportation between distant solid-state quantum bits. *Science* 2014; 345(6196): 532–535.
17. Krutyanskiy V, Meraner M, Schupp J, et al. Light-matter entanglement over 50 km of optical fibre. *Quantum Inf* 2019; 72(5): 72.
18. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, et al. The security of practical quantum key distribution. *Rev Mod Phys* 2009; 81(3): 1301.
19. Bennett CH and Brassard G. Quantum cryptography: public key distribution and coin tossing. In: *Proceedings of IEEE international conference on computers, systems, and signal processing*, Bangalore, India, 10–12 December 1984, pp.175–179. New York: IEEE.
20. Ekert AK. Quantum cryptography based on Bell's theorem. *Phys Rev Lett* 1991; 67(6): 661–663.
21. Ratti C. Quantum sensors could let autonomous cars “see” around corners. *Scientific American*, 10 November 2020, <https://www.scientificamerican.com/article/quantum-sensors-could-let-autonomous-cars-see-around-corners/#:~:text=Quantum%20computers%20get%20all%20the,brain%20activity%20during%20daily%20life>
22. Ménoret V, Vermeulen P, Le Moigne N, et al. Gravity measurements below 10<sup>-9</sup> g with a transportable absolute quantum gravimeter. *Sci Rep* 2018; 8: 12300.
23. Lee L, Xin X and Kuo G-S. A novel architecture of quantum-based nanosensor node for future wireless sensor networks. In: *Proceedings of the 2005 5th IEEE conference on nanotechnology*, Nagoya, Japan, 15 July 2005, pp.1–4, <https://ieeexplore.ieee.org/abstract/document/1500730>
24. Sun L, Guo J, Lu K, et al. Topology control based on quantum genetic algorithm in sensor networks. *Front Electr Electron Eng China* 2007; 2(3): 326–329.
25. Rathee M and Kumar S. Quantum inspired genetic algorithm for multi-hop energy balanced unequal clustering in wireless sensor networks. In: *2016 ninth international conference on contemporary computing (IC3)*, Noida, India, 2016, pp.1–6, <https://ieeexplore.ieee.org/document/7880239>
26. Tsai CW, Kang CT, Hu KC, et al. A quantum-inspired evolutionary clustering algorithm for the lifetime problem of wireless sensor network. *Int J Internet Technol Secur Trans* 2017; 6(4): 259–290.
27. Kanchan P, Pushparaj SD and Caggiano A. A quantum inspired PSO algorithm for energy efficient clustering in wireless sensor networks. *Cognent Eng* 2018; 5(1): 1522086.
28. Wenlan W, Xianbin W, Haixia X, et al. Accurate range-free localization based on quantum particle swarm optimization in heterogeneous wireless sensor networks. *KSI Trans Internet Inf Syst* 2018; 12(3): 1083–1097.
29. Guo Y, Liu D, Liu Y, et al. The coverage optimization for wireless sensor networks based on quantum-inspired cultural algorithm. In: Sun Z and Deng Z (eds) *Proceedings of 2013 Chinese intelligent automation conference* (Lecture Notes in Electrical Engineering), vol. 254, p. 868. Berlin; Heidelberg: Springer, 2013.
30. Ishizaki F. Computational method using quantum annealing for TDMA scheduling problem in wireless sensor networks. In: *2019 13th international conference on signal processing and communication systems (ICSPCS)*, Gold Coast, QLD, Australia, 2019, pp.1–9, <https://ieeexplore.ieee.org/document/9008543>
31. Vera-Amaro R, Rivero-Angel ME and Luviano-Juarez A. Design and analysis of wireless sensor networks for

- animal tracking in large monitoring polar regions using phase-type distributions and single sensor model. *IEEE Access* 2019; 7(1): 45911–45929.
32. Villordo-Jimenez I, Torres-Cruz N, Carvalho MM, et al. A selective-awakening MAC protocol for energy-efficient data forwarding in linear sensor networks. *Wirel Commun Mob Comput* 2018; 2018: 6351623.
33. Cid F and Ivan H. *Implementación y análisis de autómatas celulares cuánticos*. MSc Thesis, Computer Research Center—Instituto Politécnico Nacional (CIC-IPN), Ciudad de México, México, 2019.
34. Arrighi P and Grattage J. The quantum game of life. *Phys World* 2012; 25(6): 23–26.
35. Arrighi P and Grattage J. A simple n-dimensional intrinsically universal quantum cellular automaton. In: *Proceedings of the 4th international conference on language and automata theory and applications*. Berlin; Heidelberg: Springer, 2010, <https://arxiv.org/abs/1002.1015>
36. Bleh D, Calarco T and Montangero S. Quantum game of life. *Europhys Lett* 2012; 97(2): 20012.
37. Watrous J. On one-dimensional quantum cellular automata. In: *Proceedings of IEEE 36th annual foundations of computer science*. IEEE, 1995, <https://ieeexplore.ieee.org/document/492583>
38. Wiesner K. *Quantum cellular automata*. arXiv preprint arXiv:0808.0679, 2008, <https://arxiv.org/abs/0808.0679>
39. Pérez-Delgado CA and Cheung D. Local unitary quantum cellular automata. *Phys Rev A* 2007; 76(3): 032320.
40. Maier C, Brydges T, Jurcevic P, et al. Environment-assisted quantum transport in a 10-qubit network. *Phys Rev Lett* 2019; 122: 050501.
41. Li J and Yang C. Quantum communication in distributed wireless sensor networks. In: *2009 IEEE 6th international conference on mobile adhoc and sensor systems*, Macau, China, 2009, pp.1024–1029, <https://ieeexplore.ieee.org/document/5337016>
42. Ma H, Teng J, Hu T, et al. Co-communication protocol of underwater sensor networks with quantum and acoustic communication capabilities. *Wirel Pers Commun* 2020; 113: 337–347.
43. Agarkar AA, Karyakarte M and Agrawal H. Post quantum security solution for data aggregation in wireless sensor networks. In: *2020 IEEE wireless communications and networking conference (WCNC)*, Seoul, South Korea, 2020, pp.1–8, <https://ieeexplore.ieee.org/abstract/document/9120843>
44. Mohapatra AK and Balakrishnan S. On the number of entangled qubits in quantum wireless sensor networks. *Int J Quantum Inf* 2016; 14(5): 1650025.
45. Li H, Zhao Y and Sun Y. Wireless sensor network based on high-dimensional quantum communication. *Int J Innov Comput Inf Control* 2015; 11(6): 2119–2133.
46. Nagy N, Nagy M and Akl SG. Quantum security in wireless sensor networks. *Nat Comput* 2010; 9: 819–830.
47. Lohachab A, Lohachab A and Jangra A. A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. *Internet Things* 2020; 9: 100174.
48. Fernández-Caramés TM. From pre-quantum to post-quantum IoT security: a survey on quantum-resistant cryptosystems for the internet of things. *IEEE Internet Things J* 2020; 7(7): 6457–6480.
49. Ebrahimi S, Bayat-Sarmadi S and Mosanaei-Boorani H. Post-quantum cryptoprocessors optimized for edge and resource-constrained devices in IoT. *IEEE Internet Things J* 2019; 6(3): 5500–5507.
50. Shahid F, Khan A and Jeon G. Post-quantum distributed ledger for internet of things. *Comput Electr Eng* 2020; 83: 106581.
51. Sinha U. The triple-slit experiment. In: Hartle JB. (ed.) *Quantum universe*. Harlan, IA: Scientific American, 2020, pp.244–258.