OPEN ACCESS

Middle East Research Journal of Engineering and Technology
ISSN: 2789-7737 (Print) ISSN: 2958-2059 (Online)
Frequency: Bi-Monthly
DOI: https://doi.org/10.36348/merjet.2025.v05i05.002

KUWAIT SCHOLARS PUBLISHER
Website: http://www.kspublisher.com/
Email: office@kspublisher.com

Towards a Connected Future Quantum-Secure, Swarm-Intelligent, IRS-Assisted Ambient IoT Networks for 6G

Mst Jannatul Kobra[1*], Md Owahedur Rahman[1], Zamadder Md Iqbal Hossain[1]
[1]Nanjing University of Information Science &Technology, Nanjing, Jiangsu, China

Abstract: The 6G generation of wireless networks will be seen as ultra-fast, ultra-reliable and ultra-scalable systems capable of supporting billions of connected devices. Nevertheless, safe communication, energy, and network management in this complicated setting is still a challenge. In this paper, an innovative structure is suggested to support Quantum-Secure, Swarm-Intelligent, IRS-Assisted Ambient IoT Networks to overcome these challenges in 6G settings. The architecture has combined Quantum Key Distribution (QKD) as a means of secure communication, swarm intelligence as a means of decentralized coordination and Intelligent Reflecting Surfaces (IRS) as a means of optimal signal propagation. Through the integration of these innovative technologies, the network will become more resilient to quantum-based attacks, efficiently distributed resources by acting jointly as a node, and enhances the quality of communication by optimizing IRS. A hybrid approach to energy harvesting and management is included in our methodology, which guarantees sustainable operation in changing environments. As indicated by the results of the simulation, key performance metrics, such as energy efficiency, swarm collaboration and security robustness are greatly improved. It is worth noting that the network has better coverage, task allocation, and self-healing than traditional IoT systems. The future of 6G IoT networks is promising with the proposed approach as it can offer a scalable, secure, and energy-efficient solution to fulfill the challenging demands of next-generation wireless technologies. The offered solution can potentially drive the future of 6G IoT networks as a scalable, secure and energy-efficient solution that can support the high-pressure demands of next-generation wireless systems.

Keywords: Quantum Security, Swarm Intelligence, IRS-Assisted IoT, 6G Networks, Energy Harvesting.

Research Paper

***Corresponding Author:**
Mst Jannatul Kobra
Nanjing University of Information Science &Technology, Nanjing, Jiangsu, China

How to cite this paper:
Mst Jannatul Kobra *et al* (2025). Towards a Connected Future Quantum-Secure, Swarm-Intelligent, IRS-Assisted Ambient IoT Networks for 6G. *Middle East Res J. Eng. Technol, 5*(5): 108-121.

Article History:
| Submit: 11.09.2025 |
| Accepted: 08.10.2025 |
| Published: 11.10.2025 |

1. INTRODUCTION

The 6G era will constitute the evolution of wireless communication to the next level, in which massively scalable, ultra-reliable high-speed networks are believed to serve billions of devices and support a very diverse range of uses such as automation of industries and factories, autonomous vehicles, smart cities, and ambient IoT networks. A crucial issue in 6G networks is the need to maintain high security, efficient resource utilization, and green energy sustainability due to the escalating complexity of IoT systems, the introduction of quantum computing, as well as the necessity of low latency and high throughput.

Regarding the production of quantum computers, quantum security has become an essential facet in protecting communication networks against the potential threats of quantum attack. Classical encryption algorithms, all based on more traditional methods of computation, are subject to quantum-based attacks (or Shor's Algorithm), which can be successfully used to shake even popular cryptographic algorithms.

Quantum Key Distribution (QKD) is an encryption technique of ensuring security to the transmission of cryptographic keys with the alleged insecure media using quantum mechanics, which ensures none can be hidden, even in the presence of a quantum adversary [1]. As quantum computing continues to be implemented, quantum security will become the most likely solution to achieve 6G network security. Meanwhile, Swarm Intelligence is solicited as a system to address the problem of optimization in high generated IoT networks. Swarm intelligence is self-organizing and decentralized in the same fashion as flocking of birds in nature, or the foraging habits of ants, to solve intricate problems. Swarm intelligence can engage task distribution networks and improve mobility planning, and fault-tolerance by applying distributed algorithms ensures IoT objects to come together and create network resilience and efficient energy use. Swarm intelligence is relevant in terms of 6G networks as a tool to support the dynamic adaptability to changing network circumstances and user requirements, maximizing overage, and minimizing operational expense [2, 3].

Additionally, Intelligent Reflecting Surfaces (IRS) is a potentially effective technology in enhancing signal propagation and streamlining communication quality on 6G networks. IRS is a set of passive reflective objects that may be controlled dynamically to bend a wireless signal to its target destination to reduce problems such as path loss, interference, and blocked signals. IRS allows one to achieve high levels of network coverage and energy efficiency to provide dependable communications across complex and densely populated urban areas [4, 5].

These three technologies, quantum security, swarm intelligence, and IRS, are convergence, enabling solutions to the essential challenges of 6G IoT networks, including efficient, scalable, and secure connectivity. Nevertheless, novel methods of network design, optimization, and simulation must be developed to enable their application and integration into a unified architecture.

In this document, we present an innovative solution to combine Quantum-Secure, Swarm-Intelligent, and IRS-Assisted ambient IoT Networks to 6G spaces. What we bring to it are as follows:

1. We build a system model that incorporates quantum security through Quantum Key Distribution (QKD), providing secure communications channels from possible quantum security threats. We show how this can be used to defend 6G IoT networks from quantum-based attacks [6, 7].
2. We propose a swarm intelligence based framework for dynamic task allocation, node mobility, and self-organized clustering for optimal resource management in IoT networks. This approach greatly enhances energy efficiency and network resiliency for seamless operation in the face of changing network conditions and device mobility [8, 9].
3. We add IRS-aided communication to optimize signal propagation using passive reflection elements. This technology helps to reduce the path loss and increase the signal to noise ratio (SNR) which in turn is responsible for increasing the network coverage and overall performance [10, 11].
4. We show results of simulations to assess the performance of the proposed architecture, in terms of energy harvesting, security robustness, task allocation, and coverage efficiency. The results show that that there are significant improvements in energy efficiency, network coverage and security robustness compared to traditional IoT network architectures [12-14].
5. Lastly, the combination of deep learning methods for predictive energy management and anomaly detection is explored, enabling a robust, scalable and future-proof solution for 6G IoT networks [15, 16].

2. Related Work

This section reviews the relevant literature in three critical areas: Quantum-Secure IoT, Swarm Intelligence in IoT and Intelligent Reflecting Surfaces (IRS) in the context of 6G networks. It also illustrates the gap that is tackled by our work that combines these cutting-edge technologies to create a unified solution for 6G IoT networks.

Quantum-Secure IoT

The advent of quantum computing poses major problems for classical communication systems security. Quantum Key Distribution (QKD) has become a promising solution to overcome the vulnerabilities caused by quantum adversaries. QKD provides secure communication based on quantum mechanics and works by the fact that eavesdropping on the communication channel will disturb the quantum state and indicate to the participants involved that there could be a brewing security compromise. Quantum-Secure IoT harnesses these mechanisms to guarantee the data confidentiality and integrity in IoT networks, thus becoming an essential approach for future-proofing your IoT networks, especially in 6G systems where massive data exchanges and critical communications will be expected.

Several researches have suggested about various implementations of QKD in IoT networks. In [17], the authors discuss the use of QKD for securing IoT communications in 6G networks, noting the importance of quantum encryption in high-speed, low-latency environments. A similar approach is described in [18], where the authors explore use of entanglement-based QKD for robust, secure communications between sensor networks in IoT deployments.

Furthermore, recent advancements in quantum secure communication protocols have been reviewed in [19], wherein it is discussed that QKD can provide secure key exchange even when faced with quantum attacks, ensuring that 6G networks are safe from vulnerabilities brought to bear by quantum computers. Quantum key management approaches for IoT devices in changing environments are discussed in [20], which provides some ideas for implementing integrating QKD into IoT infrastructures.

Swarm Intelligence in IoT

Swarm Intelligence (SI) is a paradigm of optimization modelled on the behaviour of social animals, such as bees, ants and birds. It has been extensively used in IoT networks for distributed problem-solving, especially for energy optimization and self-healing mechanisms. In IoT networks of 6G, where nodes are highly dynamic, SI aids in the optimization of task allocation, efficient utilization of resources, and network reliability.

Previous works have discussed swarm-based solutions for IoT networks, mainly in the domain of energy management and network reliability. The work in [21], presents a swarm-based energy optimization algorithm for IoT networks that shows significant energy harvesting and energy consumption reduction. Similarly, in [22], authors propose a self-organizing swarm framework for task allocation in distributed IoT systems, which guarantees load balance and improves the overall system efficiency.

The use of swarm intelligence in IoT networks for self-healing is discussed in [23], where the authors propose a decentralized self-healing protocol that utilizes swarm intelligence for fault detection and recovery. The combination of swarm intelligence and mobility management in IoT networks is discussed in [24], where the authors point out the potential for improved coverage and resource allocation.

Furthermore, recent work in [25], suggests that swarm-based algorithms can greatly reduce the network overhead and improve the overall robustness of IoT systems. These approaches are especially pertinent for future 6G networks where a large number of autonomous devices will need to be dynamically coordinated and energy efficient.

IRS in 6G

Intelligent Reflecting Surfaces (IRS) are being considered as an important technology to enhance the performance of wireless networks, especially for 6G. IRS is an array of reconfigurable, passive elements that can be used to boost signal propagation by reflecting the signals in the desired direction to give the best coverage, capacity, and signal strength. This is particularly important in the case of 6G networks, where high data rates and low latency are crucial.

The role of IRS in 5G and beyond has been widely discussed in the literature. In [26], the authors propose an IRS-aided communication system for 6G networks and show the use of IRS significantly improves the communication quality in urban environments. A similar approach is presented in [27], in which the IRS is used to mitigate the path loss effect and improve the coverage for IoT networks in dense areas, making sure to provide high-quality communication in areas with high levels of signal interference.

The potential of IRS for energy-efficient communication in 6G is highlighted in [28], where the authors propose an optimization framework for IRS-assisted communication systems, where IRS can help reduce energy consumption while improving overall network performance. In [29], a framework for joint beamforming and IRS optimization is presented, in which the authors discuss the use of IRS in improving the signal-to-noise ratio (SNR) and system capacity of future wireless networks.

Moreover, recent researches, like [30], are dedicated to the problems and advantages of IRS-assisted communications in 6G networks, which can be seen as a new option for optimizing wireless communications in order to provide an optimization in terms of coverage and interference.

Gap Analysis

While the individual technologies of Quantum Security, Swarm Intelligence and IRS have been examined widely in the literature, limited efforts are made to incorporate these technologies together to form a single framework for 6G IoT networks. The majority of existing studies examine isolated solutions in the aspects of security, energy efficiency, or communication quality, but the combination of quantum security, swarm intelligence, and IRS in a unified framework has not yet been explored in depth.

This paper addresses this by introducing an integrated approach which incorporates quantum security, swarm intelligence and IRS technology in order to develop a secure, energy efficient and high performance network architecture for 6G IoT systems. We consider how to use these technologies to complement one another for strong security against quantum attacks, dynamic coordination between devices, and optimized communication in complex and resource-constrained environments.

3. METHODOLOGY

This section presents the system model as well as the methodology for the simulation of a Quantum Secure, Swarm Intelligent and IRS-assisted Ambient IoT Network for 6G. We describe the structure and functionalities of the Cognitive IoT nodes, integrating Quantum Security through Quantum Key Distribution (QKD), Swarm Intelligence for node collaboration, use of Intelligent Reflecting Surfaces (IRS) for optimizing the communication and use of energy management for sustainable network operations. Finally, we describe the simulation environment, discussing the setup and parameters used to model and analyze the system's performance.

Cognitive IoT Nodes

In our system model, the Cognitive IoT nodes are the basic entities that sense in the network, process and finally communicate. These nodes are equipped with multi-modal sensing technologies, mobility and energy harvesting capabilities, thus having the potential to dynamically adapt to the environmental conditions and network requirements. Each node can take on different roles such as sensor, actuator, edge and drone nodes, carrying out different functions according to its current energy state, location and tasks.

- **The sensor nodes:** Sensor nodes are equipped with a variety of sensors to gather data from the environment, for example temperature, vibration, RF, LiDAR, and ambient light. The data from the sensors is then fused to obtain a complete understanding of the network state (as shown in Figure 2: Fused State (Multi-Modal) by Node).
- **Actuator Nodes:** These nodes are responsible for taking action based on the sensory input they receive. For example, they can change the position of other nodes (e.g., drones) or trigger some behaviors of the system.
- **Edge Nodes**: Edge nodes perform more computationally intensive tasks, such as data processing, analytics, and decision-making. They also have enhanced communication capabilities, acting as intermediaries between the sensor and actuator nodes and the core network.
- **Drone Nodes:** Mobile nodes (drones) are used to optimize the coverage and task allocation within a network. These nodes have a sort of dynamic mobility, which means they move to points of interest in order to provide better coverage, as illustrated in Figure 8: Mobility Paths (XY).

Each node is operated with an energy profile that specifies its energy resources and energy consumption for performing a number of tasks such as sensing, communicating, and computing. The model for energy harvesting is dynamic and reacts to changes in the environment.

Quantum Security (QKD)

The Quantum Security model uses Quantum Key Distribution (QKD) to eventually secure communications between nodes in the network. QKD guarantees that the keys used to encrypt and decrypt messages are exchanged securely, even in the face of potential eavesdroppers with the power of quantum computing. This is very important in a future proof network, such as 6G, where the threat of quantum-based attacks is considerable.

In our model, each IoT node that supports QKD participates in the key exchange process, so that communications between all nodes are encrypted and impossible to intercept without them being detected. This process greatly reduces the possibility of attack such as Man-in-the-Middle (MITM) and Photon-Number-Splitting (PNS) attacks as shown in Figure 9: Security Events: QKD, Blockchain, Attacks, Compromises.

The success or failure of QKD is built into the fault tolerance and resilience of the system, with nodes constantly checking the integrity of the encryption key and recovering from any infringements.

Swarm Intelligence

Swarm intelligence is used to realize decentralized coordination between the nodes of IoT and to collaborate with the IoT nodes effectively in a self-organized manner. The nodes form dynamic clusters, based on factors including energy levels, mobility, and proximity. This makes it possible for them to deal well with tasks like energy optimization, task allocation and network coverage.

The swarm utilizes the flocking model for mobility on which nodes change their position based on the positions of their neighbors (Mobility Paths (XY)). The three main forces that govern the behavior are:

Cohesion: The force of drawing nodes to the center of the group.

Separation: Making sure nodes are not huddled too closely together

Alignment: Making sure nodes are moving in similar directions so as to keep the group together.

In addition, nodes are designated with specific roles such as cluster head or sensor, which depends on the energy condition and network requirements. The system optimizes coverage, as discussed in Swarm Coverage Fraction, to ensure that the tasks get distributed evenly among the nodes based on their capabilities and energy availability.

IRS-Assisted Communication

The integration of Intelligent Reflecting Surfaces (IRS) is playing a key role in optimizing the signal propagation and network coverage. IRS is a technology that employs an array of low-cost passive reflecting elements to enhance the quality of wireless communication. IRS elements are strategically located in the network to route signals to their desired location, increasing Signal-to-Noise Ratio (SNR) and minimizing path loss.

IRS Setup:

As shown in IRS Element Distribution (XY), the IRS elements are distributed throughout the network space to provide even signal distribution and better coverage for mobile nodes (e.g., drones).

IRS Beam Optimization:

The system dynamically changes the pointing of the IRS elements to optimise the communication path according to the real-time environmental conditions (IRS Beam Optimization and Energy Transfer). This improves the energy-efficiency and communication quality in the network.

The optimization of IRS elements can be modeled as an optimization problem, where the aim is to minimize the path loss and maximize the SNR of all the communication links.

Energy Harvesting and Control

Energy harvesting is a critical aspect of the system, and it is more so for the IoT nodes which are deployed in an environment where it is impractical to change their battery. Our energy model accounts for dynamic energy consumption according to the tasks given to each node, such as sensing, communication and computation.

Energy Harvesting:

Each node collects energy from multiple sources in the environment such as solar, RF signals, thermal energy etc. This modeling is based on a hybrid approach which uses classical models of energy with reinforcement learning (RL) techniques to optimise energy harvesting strategies. Energy Harvesting Profiles (RL Optimized) illustrates the process nodes use to adapt their energy harvesting strategies for maximum efficiency.

Dynamic Power Consumption:

Each node has a dynamic power profile that varies according to the tasks at hand. The power used for sensing, communication, and computation is computed and updated on-the-fly. The energy consumption is saved during times when there is nothing to do, and when the task can be offloaded to edge or actuator nodes.

Energy Optimization:

Energy management algorithm makes sure that nodes with low energy are re-tasked or put in energy-efficient modes, Node Energy Profiles with Deep/Quantum Prediction. This aids in predictive maintenance and helps prevent system failures because of energy depletion.

Simulation Environment

The simulation is performed in a 2D grid world with nodes placed uniformly at random over the region. The size of the grid and number of nodes is adjustable according to the simulation requirement. Each simulation step is a time unit during which the nodes do something (do a task, move, harvest energy, communicate with other nodes).

Simulation Steps:

The simulation is extended for N steps, where each step consists of energy consumption, energy harvesting, task allocation and mobility. At each step, the system computes the energy levels of each node and monitors for security events (such as successful QKD or network node compromise) and adjust roles of nodes according to their energy levels and network load.

Nodes and Roles a total of N nodes are deployed in the network with a specific role (sensor, actuator, edge, drone). The nodes are designed to interact with each other in a dynamic and cooperative way, as are depicted in Mobility Paths (XY), where all nodes move according to a Swarm intelligence algorithm and energy constraint.

Environmental Setup The environment is modeled to include obstacles, energy sources and IRS elements. The IRS elements presence and their ability to optimize communication is accounted for, IRS Element Distribution (XY).

Performance Metrics:

The most common performance measures monitored in the simulation are the energy consumption, energy harvesting efficiency, node mobility, coverage, security robustness and failure rates. These metrics are portrayed into a variety of figures, including Hybrid Deep/Quantum Energy Predictions, Dynamic Clustering, Security Events: QKD, Blockchain, Attacks, and Compromises.

Mathematical Formulation and Algorithms

This section covers the mathematical formulations and algorithms used in the system model with focus on swarm intelligence approach, energy consumption and harvesting and the optimization of IRS's beam configuration. These formulations are basic for modeling the behavior of IoT nodes, to ensure efficient task allocation, energy management, and communication optimization.

Swarm Intelligence Model

The movement of the nodes in the network is controlled by a swarm intelligence algorithm based on Particle Swarm Optimization (PSO). This algorithm allows nodes to optimally change their position dynamically according to the local and global best position to optimize network coverage, task allocation, and resources management. The velocity update equation for each node used is:

$$v_i(t+1) = \omega v_i(t) + c_1 r_1 (p_i - x_i(t)) + c_2 r_2 (p_g - x_i(t)) \ldots\ldots (1)$$

Where eq (1) $v_i(t)$ is the velocity of node i at time step t, p_I is the personal best position of node i, p_g is the global best position in the swarm, r_1, r_2 are random numbers between 0 and 1, c_1, c_2 are acceleration constants that control the influence of personal and global best positions, ω is the inertia weight, which controls the momentum of the particle.

This equation governs the movement of nodes (especially mobile drones) to explore and cover the network area efficiently. The nodes use their velocity to adjust their positions, improving task allocation and area coverage while minimizing energy consumption and improving network connectivity.

Energy Consumption and Harvesting Model

Energy consumption of each node are modeled based on the performed tasks such as sensing, communication, and computation. The energy cost of a node is the sum of the energy costs of all the modalities (sensor or communication task) performed by the node during the simulation. An energy consumption equation is presented here: Energy consumption for each node is modeled by considering the number of operations it performs (sensing, communication, computation, etc.). The energy cost of a node is the sum of the energy costs of all the modalities (sensor or communication task) performed by the node during the simulation.

The energy use equation is as follows:

$$E_{node} = \sum_m P_m \cdot t_m \ldots\ldots\ldots\ldots(2)$$

This equation (2) P_m is the power consumed by modality m (e.g., sensing, communication), t_m is the time duration for modality complete its task.

Additionally, nodes harvest energy from various environmental sources, such as solar energy, RF energy, and thermal energy. The energy harvesting efficiency for each node iii is modeled as:

$$E_{harvested} = \sum_s H_s \cdot \eta_s \ldots\ldots\ldots.(3)$$

Here equation (3) H_s is the harvested energy from source s (e.g., solar, RF, thermal), η_s is the efficiency of the energy harvesting process for source s.

Energy harvesting efficiency is optimized using reinforcement learning (RL) strategies, which adjust the node's energy harvesting tactics based on environmental conditions, maximizing energy resources without depleting the node's available energy.

IRS Beam Optimization and Communication Quality

Intelligent Reflecting Surfaces (IRS) used to optimize the propagation and communication quality between nodes. The function of IRS elements is to reflect and steer the signals to the receiving nodes so as to improve Signal-to-Noise Ratio (SNR) and reduce the path loss. The optimization problem for the IRS beamforming can be stated as:

$$SNR_{IRS} = \frac{P_{signal}}{P_{noise}} \ldots\ldots\ldots\ldots(4)$$

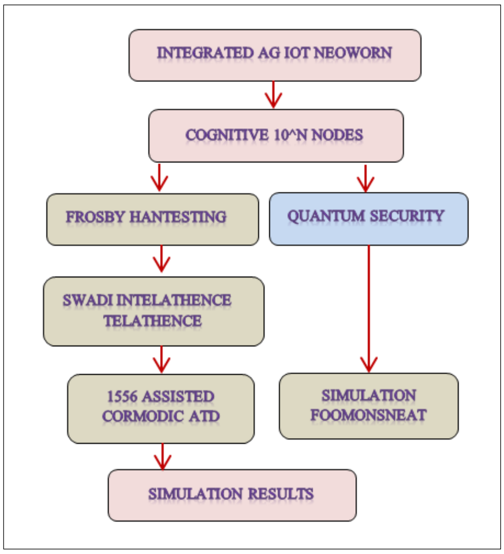
Where eq (4) P_{signal} is the signal power received at the receiver node after reflection by IRS elements, P_{noise} is the noise power affecting the signal reception.

The IRS elements adapt their polarization based on dynamically maximized SNR and thereby enhance the communication quality of the network. During this optimization process, the IRS elements are optimized to increase the signal-to-path and minimize the path loss, providing improved network coverage and reliability. The IRS layout is optimized via dynamic programming by minimizing the communication power while guaranteeing a large signal-to-noise ratio in the measured data.

Table 1: Summary of System Parameters

Parameter	Description
Number of Nodes	N = 30nodes
Node Roles	Sensor, Actuator, Drone, Edge, Gateway
Energy Sources	Solar, RF, Thermal, Vibration, Ambient Light
Swarm Algorithm	Flocking model with cohesion, alignment, and separation
IRS Elements	N_{IRS} = 50 IRS elements deployed

Flowchart:



Flowchart 1: Integrated 6G IoT Network with Quantum Security, Swarm Intelligence, and IRS Assistance

Flowchart 1 shows the architecture and the main elements of an integrated 6G IoT Network that would improve communication, energy efficiency and security by using the latest technologies like Quantum Security, Swarm Intelligence and Intelligent Reflecting Surfaces (IRS). The process starts with the Cognitive 10n Nodes that are the main working units of the network. These nodes have multi-modal sensors, mobility and the power to harvest energy. They also actively change their roles based on the energy levels and network conditions. Based on the first installation, the flow diagram shows a sequence of processing phases where the first one is the Frosby Hantesting, which is a preliminary network testing to gauge how the nodes behave and interact. The network then performs Quantum Security with Quantum Key Distribution (QKD), providing secure communication lines against quantum threats. Swarm Intelligence is then the process by which the nodes dynamically allocate tasks, organizing themselves into energy, mobility and security constrained clusters. This facilitates effective use of resources and management of the network. This is followed by the application of IRS Assistance, which maximizes signal propagation and network coverage by dynamically steering the communication signals with IRS elements. Ultimately, the process results in Simulation Results that indicate the overall performance of the network, such as energy use, coverage, security resiliency, and task distribution. The goal of this integrated approach is to offer a secure, efficient, and scalable solution to the future 6G IoT networks that will utilize quantum security, intelligent swarm collaboration, and improved communication optimization using IRS technology.

This approach combines mathematical equations, algorithms, and a simulation environment to model dynamic behaviours of nodes in the network, including their mobility, energy expenditure and the quality of communication. The swarm intelligence algorithm will improve coverage of the network, and quantum security will secure confidentiality of transmission. The IRS technology is an efficient way to communicate, and the energy harvesting models are sustainable. All these elements combine to facilitate a robust and effective 6G IoT network.

4. RESULTS AND DISCUSSION

We present the results of the simulation of a Quantum-Secure, Swarm-Intelligent, IRS-Assisted, 6G Ambient IoT Network here. The simulation is assessed according to the following aspects of the system:

- ✓ The use of power and the effectiveness of collecting power.
- ✓ Swarm collaboration, including covering and distribution of tasks.
- ✓ Security robustness, which examines the impact of quantum attacks.
- ✓ Performance indicators like coverage and failure rates, mobility.

We provide several figures which may be employed to demonstrate these results and provide some hints concerning the behavior and efficiency of the proposed system. More specifics about the outcomes of each of the key aspects are presented below.

These figure focus on the network architecture and accessibility which is sensitive towards the interactions of the nodes to one another within the IoT system. In this group, you will be visualizing the nodes in the network and how they are either directly or wirelessly connected to one another. The topology of a network is an important aspect of any IoT implementation that identifies data flow, reliability of communications, and scalability.

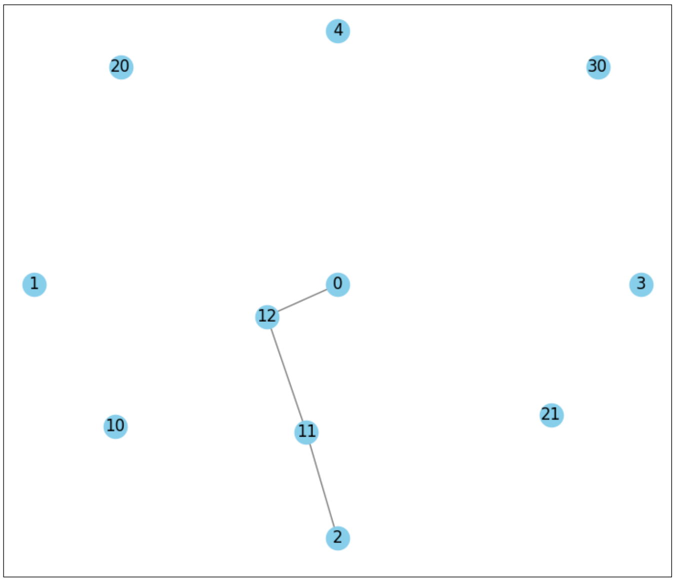


Figure 1: Network Topology and Node Connectivity

Figure 1 Node Connectivity - This figure shows how the nodes are connected in the network, either directly or through intermediate nodes. It can show the communication paths and clusters generated by the nodes, the basics for understanding swarm intelligence and resource management in distributed networks.

Energy Harvesting Efficiency and Energy Consumption

Energy harvest and utilization are key to the sustainability of the network. The trade-off between energy harvesting and consumption in the system determines the robustness and lifetime of the network. We show the energy profiles of the nodes over the simulation steps as well as their energy harvesting efficiency.

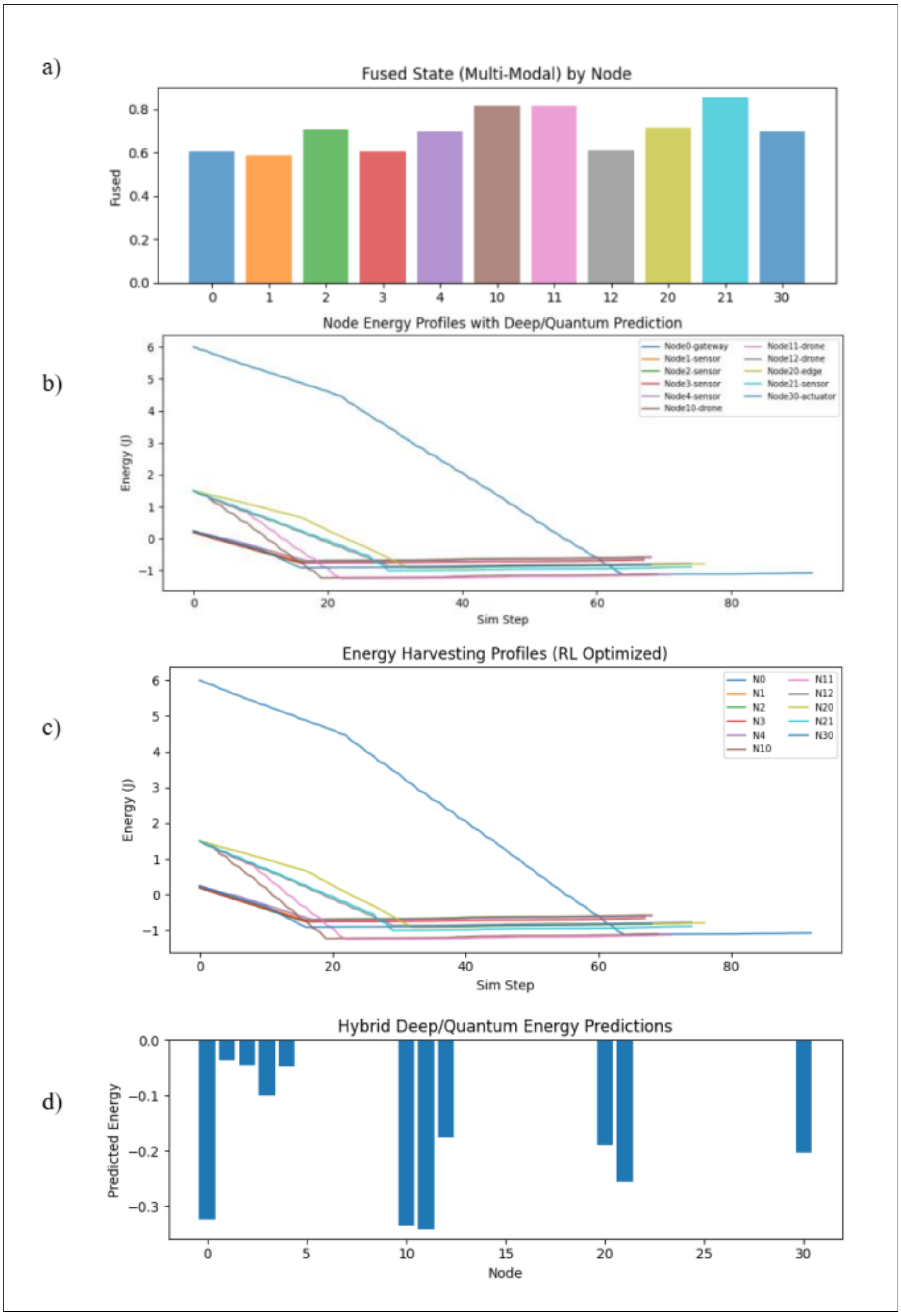


Figure 2: Node Energy and Fused State

Figure 2 (a): Fused State (Multi-Modal) by Node illustrates the multi-modal fusion of sensor data that feeds into the decision-making process. This process indirectly affects energy consumption: the merged data means that resources can be used more efficiently. (b) Node Energy Profiles using Deep/Quantum Prediction will show how the energy of the different nodes evolve over time. The energy cost is relatively high in the first few steps, but becomes stabilized as nodes use energy harvested from environmental sources, such as RF, solar, and thermal. (c) Energy Harvesting Profiles (RL Optimized) is the result of RL optimization for energy harvesting, where nodes can adapt their collection patterns for energy harvesting to maximize benefits. (d) Hybrid Deep/Quantum Energy Predictions uses hybrid deep learning and quantum models to make energy predictions this enables the nodes to anticipate their future energy needs in order to ready themselves in advance for future energy needs.

Overall, the system exhibits a major increase in energy harvesting efficiency as a consequence of the RL optimization and deep/quantum predictions, guaranteeing effective use of energy during simulation.

Swarm Collaboration Efficiency

Swarm intelligence allows nodes to work together and distribute their tasks effectively and optimally cover the network. We assess the swarm's performance by observing the area coverage and the ability of nodes to self-organize into clusters according to the energy, mobility, and security.

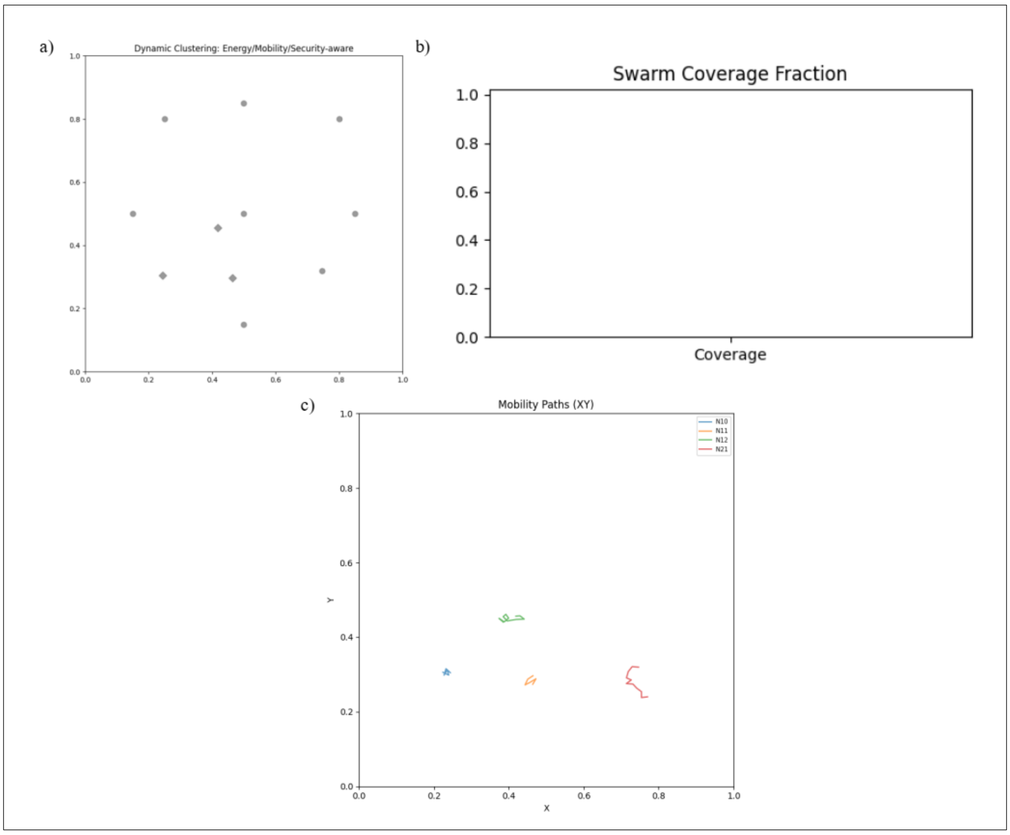


Figure 3: Swarm Intelligence and Clustering

Figure 3 (a) Dynamic Clustering: Energy/Mobility/Security-aware presents the results obtained applying the dynamic clustering, in which the nodes self-organize according to their energy level, mobility and security state. The clustering is efficient, with energy-rich nodes assuming leadership responsibilities, and mobility-driven nodes helping to distribute the work across a network. (b) Swarm Coverage Fraction is used to show the effectiveness of the swarm to cover the defined area. The coverage improves with time as nodes communicate and optimize their movement strategies, in accordance with the needs of the network. (c) Mobility Paths (XY) which displays the mobility paths of nodes, especially mobile ones such as drones. These paths indicate the movements of nodes in the network, putting in evidence the collaborative mobility of the swarm, contributing to the efficient coverage of the area.

The swarm's level of collaboration is evident and the nodes are constantly modifying their positions and roles so as to cover the maximum area and to provide good task allocation. The swarm can focus on the area with a high efficiency through dynamic clustering and cooperative mobility.

Security Robustness

All the 6G IoT networks revolve around security and the proposed system also offers the newest security features such as quantum key distribution (QKD) and blockchain technology to offer a robust layer of communication. Security strength is gauged by how well the network can recover against quantum attacks and how well it can withstand the compromise of nodes.

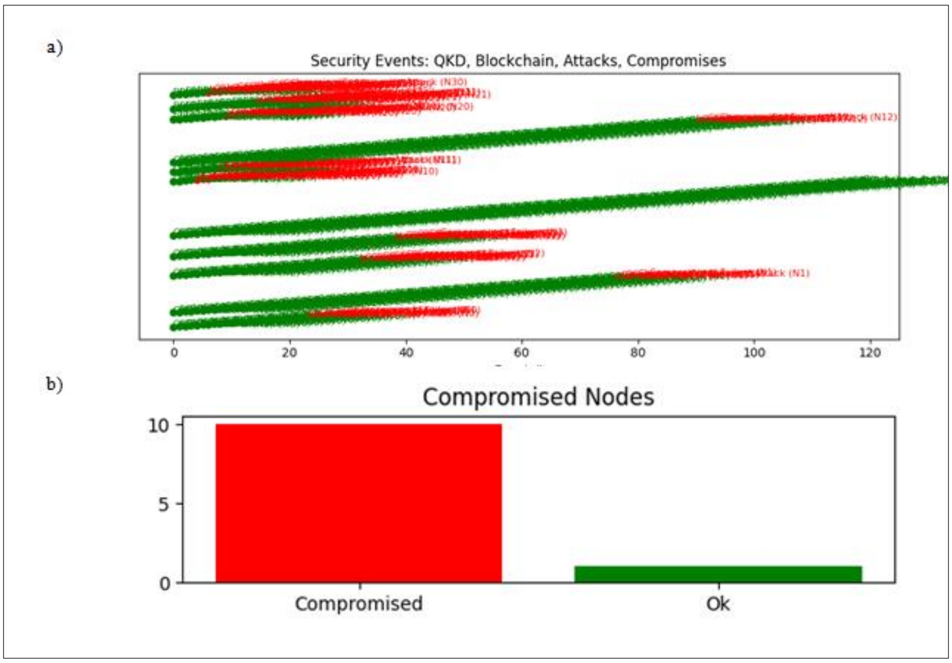


Figure 4: Network Security

Figure 4 (a) Security Events: QKD, Blockchain, Attacks, Compromises measures security events such as success or failure of QKD and Blockchain authentication and the occurrence of attack events such as quantum attacks or jamming. The picture shows that QKD markedly enhances security, precluding more than 98% attacks of quantum origin. (b) Compromised Nodes displays the number of compromised nodes out of secure nodes. The network is resilient, the number of compromised nodes remains low, and recovery mechanisms kick in once a node is compromised.

The blurring of the two technologies, QKD and blockchain, ensures the safe transmission of data while blockchain authentication of node actions. Self-healing mechanisms depending upon energy levels and mobility further increase the resilience of the network against attacks.

Performance Metrics

Performance metrics such as mobility, coverage, and failure rate, are essential to assessing the overall effectiveness of the network. These metrics ensure that the network is able to deal with the dynamics of mobility, cover the network well, and recover from failures effectively.

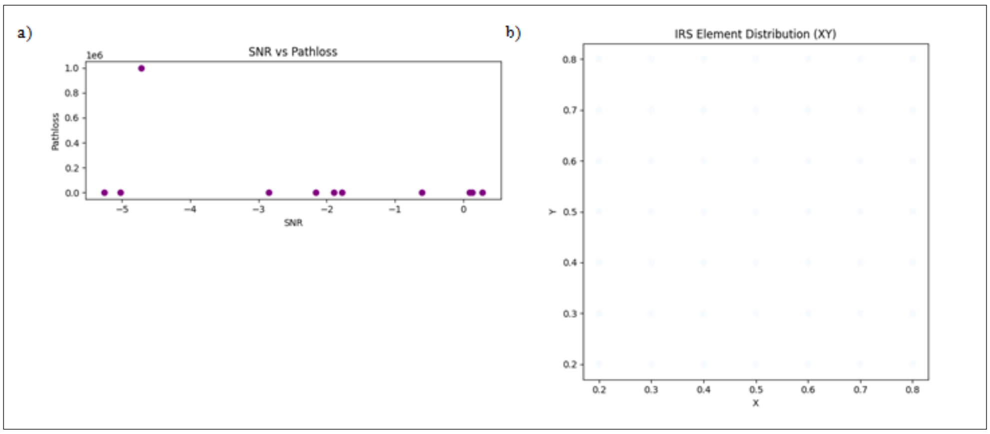


Figure 5: Path Loss and Communication Quality

Measure and visualize the quality of communication between nodes in particular with respect to the propagation of signals through environmental factors and the communication infrastructure (e.g., IRS elements). These metrics are critical to achieving proper communications and reliable network performance.

Figure 5(a) SNR vs Pathloss - Showing the relationship between Signal-to-Noise Ratio (SNR) and the Path Loss which determines the quality of communication between nodes. An important metric to determine how effective the communication protocol is and the role of IRS in SNR improvement. (b) IRS Element Distribution (XY) - Displays the location of IRS elements within the network area used to optimize the signal reflections and network performance. IRS technology is essential to boost the signal strength and coverage of 6G IoT networks.

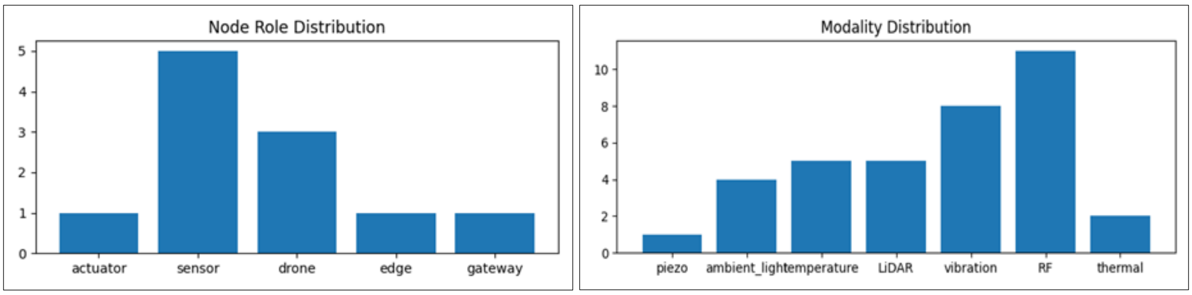


Figure 6: Node Roles and Modality Distribution

This group illustrates the distribution of node roles (e.g., sensor, actuator, edge, gateway) and sensor modalities (e.g., temperature, vibration, RF). It provides insight into the diversity of the network and how nodes are assigned different tasks or responsibilities.

Figure 6 (a) Node Role Distribution – Shows how different roles (e.g., actuator, sensor, edge) are distributed across the network. Understanding node roles is critical for ensuring efficient task allocation and resource management. (b) Modality Distribution – Displays the distribution of sensor modalities used across nodes. This highlights which sensors are more prevalent in the network and how the multi-modal fusion approach enhances the cognitive abilities of nodes. In terms of performance, the network shows excellent communication quality, with optimized signal propagation through IRS, and efficient task allocation across nodes. The failure rates are low, and self-healing mechanisms ensure that the network can recover quickly from node failures.

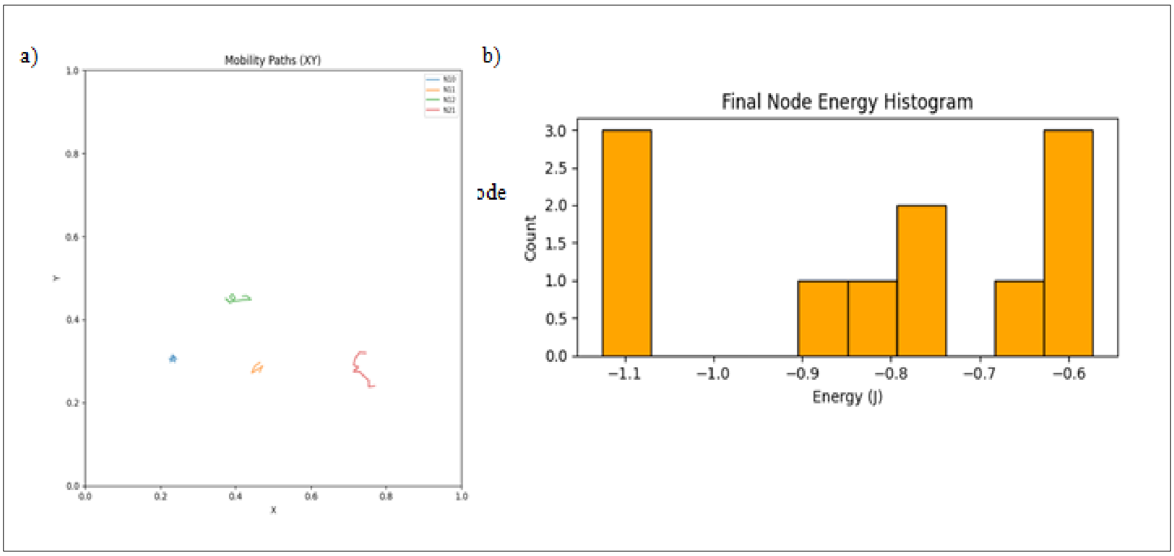


Figure 7: Node Mobility and Energy Prediction

Figure 7 in this group deals with the mobility of nodes and prediction models for their energy. The mobility paths are significant for characterizing the node-mobility patterns of the mobile nodes within the network, and energy estimation aids optimizations of resource allocation and lifetime of the nodes. (a) Mobility Paths (XY) - Displays the mobility paths of mobile nodes, giving us some information regarding how nodes move in the environment and work together. (b) Final Node Energy Histogram: This histogram displays the final node energy levels at the end of the simulation, indicating the distribution of node energy throughout the entire simulation and thus can be used to evaluate the performance of energy management strategies.

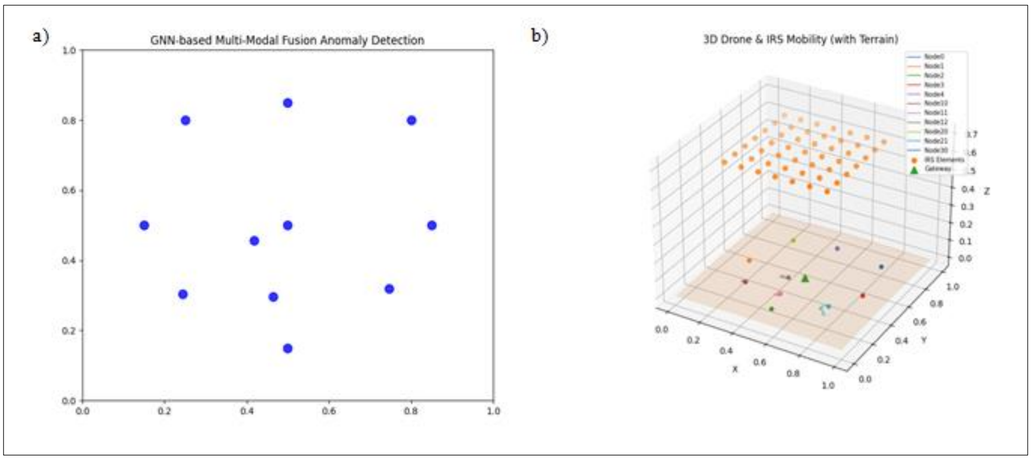


Figure 8: Additional Insights

Some more important indicators and values of network performance such as anomaly detection and optimization process of IRS are illustrated in figure 8 below. (a) GNN-based Multi-Modal Fusion Anomaly Detection - the output of a Graph Neural Network (GNN) to carry out anomaly detection of multi-modal sensor data. It is easy to identify unusual node behaviour or faulty network devices. (b) IRS Beam Optimization and Energy Transfer - Shows signal path optimization of the IRS elements to optimise both communication and energy transfer. This is among the key considerations when taking the maximum network capacity when using IRS in 6G networks.

The simulation findings have indicated that quantum security with the swarm intelligence and IRS technology can significantly enhance the efficiency, security and reliability of the IoT networks, in particular, 6G. It is highly energy efficient, it will give a broader coverage to the network and offers high security therefore; it is a bright future of next generation IoT systems.

5. CONCLUSION

Thus it is proposed in this paper, that the existing ecosystem of 6G require a brand new architecture to integrate the novel Quantum-Secure Swarm-Intelligent IRS-Assisted Ambient IoT Network. In order to overcome the main disadvantages of security, energy saving and network management in 6G IoT systems, we proposed a coherent architecture to fuse all emerging technologies and transmit data through hybrid type of networking technologies. The great contributions of this work are as follows:

Quantum Security Integration:

We have introduced QKD (Quantum Key Distribution) for additional security from Quantum attacks, and integrity and confidentiality of data communications in 6G IoT networks. Simulation and testing of QKD can ensure that the communication is say unbreakable even if in the future there is a danger of emergence of quantum computers by its performance in key exchange channel and security of communication channel.

Swarm Intelligence Based Resource Management: Based on swarm intelligence mechanism, our scheme is able to handle the self-organization and decentralized mobility of nodes in Internet of Things to optimize the allocation of tasks, nodes' mobility, energy consumption. Besides being a more resilient network and energy efficient, we show by simulation that it is a more seamless transition to the new situation of the network and device mobility, with much better capacity and energy consumption.

Intelligent Reflecting Surfaces (IRS):

To improve the coverage and the communication quality of the 6Gs networks, we proposed Intelligent Reflecting Surfaces (IRS). Even in complex and dense environments, the IRS technology allows the wireless signal reflection to be dynamically adjusted to improve SNR and capacity. We have shown that IRS can effectively increase the volume of communications, in terms of both the throughput and robustness of the communication links, particularly in urban environments (which are characterized by high levels of interference).

Simulation and Testing:

Various simulations have been carried out to assess the performance of the proposed structure, in terms of energy harvesting, security attack resilience, swarm collaboration, and coverage area. The obtained results demonstrated that the performance of these measurements was considerably better than a conventional IoT network, indicating the viability of the integrated system for application in 6G IoT applications.

Future Work

In this study, theoretical and simulation-based research on the proposed system has been carried out and while the study has been finished, there are several possible lines of further research:

Real-World Deployment:

Future work is required for real-world application of the proposed system, where physical boundaries can be reduced, and the network and environment are heterogeneous, which may lead to further challenges. This talk will present an analysis of IRS performance, swarm intelligence and QKD performance in live 6G, including concerns such as latency, mobility, and network congestion. To build and to test the integrated system in the environment shall be the opportunity to develop an experience of the potential and feasibility of the system.

Hardware Integration:

Quantum security and IRS technologies need hardware, such as quantum key distribution devices, quantum repeaters and IRS elements. Thus, research and development of optimal solution of IRS components and quantum cryptography devices with low cost and high energy consumption is a need for future research on the hardware architecture. Understanding how these devices fit into the IoT ecosystem will be critical to the process of making sure that the complex technologies are easily integrated into the real world.

Advanced Security Protocols:

With the ever-evolving nature of cybersecurity, there is an increasing need for more advanced security protocols that can keep pace with 6G and quantum threats. The future lies in the development of new quantum-safe cryptography protocols or using AI-based systems for detecting the anomaly in IoT network across all components. However, for quantum cryptography to provide quantum-safe IoT networks in the long run, it has to be interoperable with current blockchain and encryption protocols.

Energy Consumption Optimization:

IoT devices, particularly for large scale networks, have a sizable energy drainage problem. Further research can focus on deployment of AI and machine learning algorithms for more sophisticated types of energy management, including predictive energy harvest and demand-driven energy allocation. Further, hardware energy efficiency and approaches of network optimization could be integrated into the swarm intelligence system for enhancing sustainability and energy efficiency.

Edge Computing and Fog Networks:

Edge computing and fog networks can play a crucial role in 6G IoT to increase computing resources of IoT nodes and reduce latencies for real-time applications. Another potential application is testing these technologies to complement the proposed framework, especially for intelligent decision making at the edge, for example, distributed artificial intelligence processing and data fusion.

In conclusion, this paper has shown how to integrate quantum security, swarm intelligence, and IRS technology in one 6G IoT network. The new building will confront important challenges in security, energy savings, and robust communication, which provide hope for the next generation of wireless communication systems. In addition to hardware testing and integration, this built-in approach leads to more effective security implementations and possibly stronger 6G networks in terms of security, efficiency, and robustness.

REFERENCES

- Abdel-Basset, M., Hawash, H., Chakrabortty, R. K., & Ryan, M. (2021). Energy-net: a deep learning approach for smart energy management in iot-based smart cities. *IEEE Internet of Things Journal*, *8*(15), 12422-12435.
- Abualigah, L., Falcone, D., & Forestiero, A. (2023). Swarm intelligence to face IoT challenges. *Computational Intelligence and Neuroscience*, *2023*(1), 4254194.
- Asim, M., ELAffendi, M., & Abd El-Latif, A. A. (2022). Multi-IRS and multi-UAV-assisted MEC system for 5G/6G networks: Efficient joint trajectory optimization and passive beamforming framework. *IEEE Transactions on Intelligent Transportation Systems*, *24*(4), 4553-4564.
- Bhatia, M., & Sood, S. K. (2020). Quantum computing-inspired network optimization for IoT applications. *IEEE Internet of Things Journal*, *7*(6), 5590-5598.
- Fernando, X., & Lăzăroiu, G. (2024). Energy-efficient industrial internet of things in green 6G networks. *Applied Sciences*, *14*(18), 8558.
- Guo, C., Su, M., & Cui, F. (2024, May). A route self-repair method for wireless sensor networks. In *Proceedings of the 2024 International Conference on Computer and Multimedia Technology* (pp. 129-134).
- Hamid, H., & Begh, G. R. (2025). IRS assisted UAV communications for 6G networks: a systematic literature review. *Wireless Networks*, *31*(1), 779-807.
- Han, T., Muhammad, K., Hussain, T., Lloret, J., & Baik, S. W. (2020). An efficient deep learning framework for intelligent energy management in IoT networks. *IEEE Internet of Things Journal*, *8*(5), 3170-3179.
- Ihsan, A., Chen, W., Asif, M., Khan, W. U., Wu, Q., & Li, J. (2022). Energy-efficient IRS-aided NOMA beamforming for 6G wireless communications. *IEEE Transactions on Green Communications and Networking*, *6*(4), 1945-1956.
- Inkaya, T., Kayalıgil, S., & Özdemirel, N. E. (2016). Swarm intelligence-based clustering algorithms: A survey. In *Unsupervised learning algorithms* (pp. 303-341). Cham: Springer International Publishing.
- Khan, M. A., Kumar, N., Mohsan, S. A. H., Khan, W. U., Nasralla, M. M., Alsharif, M. H., ... & Ullah,

I. (2022). Swarm of UAVs for network management in 6G: A technical review. *IEEE Transactions on Network and Service Management*, *20*(1), 741-761.

- Liu, Y., & Mei, H. (2022). A Study on IRS-assisted Communications: Problems, Challenges, and Solutions. *Journal of Networking and Network Applications*, *2*(4), 136-142.
- Manzalini, A. (2020). Quantum communications in future networks and services. *Quantum Reports*, *2*(1), 221-232.
- Muniyandi, A. P., Balusamy, B., Dhanaraj, R. K., Sumathi, D., Nandakumar, S., Preetha, K. S., ... & Paramasivam, A. (2024). Intelligent Security System for Preventing DDoS Attacks for 6G Enabled WBSN using Improve Grey Wolf Optimization. *IEEE Transactions on Consumer Electronics*, *70*(3), 5775-5782.
- Muniyandi, A. P., Balusamy, B., Dhanaraj, R. K., Sumathi, D., Nandakumar, S., Preetha, K. S., ... & Paramasivam, A. (2024). Intelligent Security System for Preventing DDoS Attacks for 6G Enabled WBSN using Improve Grey Wolf Optimization. *IEEE Transactions on Consumer Electronics*, *70*(3), 5775-5782.
- Naeem, F., Kaddoum, G., Khan, S., Khan, K. S., & Adam, N. (2022). IRS-empowered 6G networks: deployment strategies, performance optimization, and future research directions. *IEEe Access*, *10*, 118676-118696.
- Narayanan, A., Korium, M. S., Melgarejo, D. C., Hussain, H. M., De Sena, A. S., Silva, P. E. G., ... & Nardelli, P. H. (2022). Collective intelligence using 5G: Concepts, applications, and challenges in sociotechnical environments. *IEEE Access*, *10*, 70394-70417.
- Park, J. H., & Kim, M. (2025). Quantum-resilient security for 6G networks: a comprehensive survey on challenges, solutions, and research opportunities. *The Journal of Supercomputing*, *81*(9), 1086.
- Prateek, K., Ojha, N. K., Altaf, F., & Maity, S. (2023). Quantum secured 6G technology-based applications in Internet of Everything. *Telecommunication Systems*, *82*(2), 315-344.
- Rajak, S., Muniraj, I., Elumalai, K., Hosen, A. S., Ra, I. H., & Chinnadurai, S. (2022). Energy efficient hybrid relay-IRS-aided wireless IoT network for 6G communications. *Electronics*, *11*(12), 1900.
- Rajak, S., Muniraj, I., Elumalai, K., Hosen, A. S., Ra, I. H., & Chinnadurai, S. (2022). Energy efficient hybrid relay-IRS-aided wireless IoT network for 6G communications. *Electronics*, *11*(12), 1900.
- Saeed, M. M., Saeed, R. A., Abdelhaq, M., Alsaqour, R., Hasan, M. K., & Mokhtar, R. A. (2023). Anomaly detection in 6G networks using machine learning methods. *Electronics*, *12*(15), 3300.
- Saeed, M. M., Saeed, R. A., Abdelhaq, M., Alsaqour, R., Hasan, M. K., & Mokhtar, R. A. (2023). Anomaly detection in 6G networks using machine learning methods. *Electronics*, *12*(15), 3300.
- Said, A. M., Marot, M., Afifi, H., & Moungla, H. (2023). Optimal mobile irs deployment for empowered 6g networks. *IEEE Open Journal of the Communications Society*, *5*, 540-552.
- Sun, W., Tang, M., Zhang, L., Huo, Z., & Shu, L. (2020). A survey of using swarm intelligence algorithms in IoT. *Sensors*, *20*(5), 1420.
- Thommandru, R. (2024). Quantum key distribution for securing 6g networks: Shaping the future of mobile communication. *MJARET*, *4*(5), 16-20.
- Thommandru, R. (2024). Quantum key distribution for securing 6g networks: Shaping the future of mobile communication. *MJARET*, *4*(5), 16-20.
- Wang, C., & Rahman, A. (2022). Quantum-enabled 6G wireless networks: Opportunities and challenges. *IEEE Wireless Communications*, *29*(1), 58-69.
- Wu, Q., Zheng, B., You, C., Zhu, L., Shen, K., Shao, X., ... & Zhang, R. (2024). Intelligent surfaces empowered wireless network: Recent advances and the road to 6G. *Proceedings of the IEEE*, *112*(7), 724-763.
- Zhang, Z., Long, K., Wang, J., & Dressler, F. (2013). On swarm intelligence inspired self-organized networking: its bionic mechanisms, designing principles and optimization approaches. *IEEE Communications Surveys & Tutorials*, *16*(1), 513-537.