energies

MDPI

Article

Multi-Controller Model for Improving the Performance of IoT Networks

Ganesh Davanam [1], Suresh Kallam [1], Ninni Singh [2], Vinit Kumar Gunjan [2], Sudipta Roy [3], Javad Rahebi [4], Ali Farzamnia [5,*] and Ismail Saad [5]

[1] Department of CSE, Sree Vidyanikethan Engineering College (Autonomous), Tirupati 517102, Andhra Pradesh, India
[2] Department of Computer Science & Engineering, CMR Institute of Technology, Hyderabad 501401, Telengana, India
[3] Department of Artificial Intelligence & Data Science, Jio Institute, Navi Mumbai 410206, Maharastra, India
[4] Software Engineering Department, Istanbul Topkapi University, 34087 Istanbul, Turkey
[5] Faculty of Engineering, Universiti Malaysia Sabah, Kota Kinabalu 88400, Malaysia
* Correspondence: alifarzamnia@ums.edu.my

Abstract: Internet of Things (IoT), a strong integration of radio frequency identifier (RFID), wireless devices, and sensors, has provided a difficult yet strong chance to shape existing systems into intelligent ones. Many new applications have been created in the last few years. As many as a million objects are anticipated to be linked together to form a network that can infer meaningful conclusions based on raw data. This means any IoT system is heterogeneous when it comes to the types of devices that are used in the system and how they communicate with each other. In most cases, an IoT network can be described as a layered network, with multiple tiers stacked on top of each other. IoT network performance improvement typically focuses on a single layer. As a result, effectiveness in one layer may rise while that of another may fall. Ultimately, the achievement issue must be addressed by considering improvements in all layers of an IoT network, or at the very least, by considering contiguous hierarchical levels. Using a parallel and clustered architecture in the device layer, this paper examines how to improve the performance of an IoT network's controller layer. A particular clustered architecture at the device level has been shown to increase the performance of an IoT network by 16% percent. Using a clustered architecture at the device layer in conjunction with a parallel architecture at the controller layer boosts performance by 24% overall.

Keywords: internet of things; radio-frequency identification; device level clustering; layered networking; parallel architectures; performance optimization; topology binding

Citation: Davanam, G.; Kallam, S.; Singh, N.; Gunjan, V.K.; Roy, S.; Rahebi, J.; Farzamnia, A.; Saad, I. Multi-Controller Model for Improving the Performance of IoT Networks. *Energies* **2022**, *15*, 8738. https://doi.org/10.3390/en15228738

Academic Editor: Antonio Cano-Ortega

Received: 26 September 2022
Accepted: 2 November 2022
Published: 21 November 2022

1. Introduction

As of today, over two billion people use the internet to transmit and receive e-mails, to obtain the Web's material, to use social networking, and to engage in a wide range of other tasks. Eventually, more people can have access to the large amounts of information that is accessible on the Internet, pushing the Web to another height where devices and connected gadgets will interact, communicate, compute, and cooperate with each other. Within a few years, the Web will have developed into a large range of connected and networked devices. Newer methods of working, communication, and entertainment will always be possible because useful access to data will always be available. This will allow for newer ways of living [1,2].

Globalization of information has been largely realized thanks to the ongoing development of the Internet, and the entire world is becoming an interconnected whole. People can now communicate with each other more easily and frequently. Although, despite this, the rapid growth of information helps make people realize that most information exchange remains in communication with people. The world will be a more beautiful

place when we can tear down this barrier and allow people and things to communicate with each other normally. The Internet of Things (IoT) was born as a result of this concept. The Internet of Things (IoT) is the latest era of Internet-based network technology that is changing people's lives. An interconnected world is created by the Internet of Things. As a result of the abundance of amenities equipped with sensors, it is possible to connect any ordinary physical object [3]. There are a number of components that make up the Internet of Things (IoT), including sensors, which collect data and transmit them via wired or wireless interaction. In this manner, information acquisition, transmission, and processing can be effectively integrated, resulting in an increase in the utilization rate of various resources and an increase in the efficiency of users.

The IoT system, on the other hand, necessitates the integration of a wide range of sensors and objects. These perception devices or objects transmit most of their information wirelessly. Criminals may use wireless information to their own ends by misusing it. As a result, IoT system security is an urgent issue that must be addressed. In addition, despite the fact that the IoT devices are built on top of the existing Web, there are many strong security solutions that can be used as a reference. While conventional Internet security solutions can be useful in the IoT [4], we cannot expect them to solve all of the system's security issues. Sensor networks, node gateways, communication base stations, and background systems make up an IoT wireless sensor network. Sensors communicate with gateway nodes, gateway nodes communicate with background systems, and so on. When it comes to cyber-attacks, IoT devices and communications networks can become targets [5,6].

In order for the IoT networks to be successful, many different layers of networking must be implemented, and those layers must be implemented while taking into account a wide range of different devices. A wide range of factors must be taken into account when attempting to gauge and improve the IoT networks' performance. One of most important factors is the availability of numerous alternative communication links with the goal of utilizing the least amount of power possible. There are many tiers in an Internet of Things network because of the interconnectivity between low-bandwidth devices and high-bandwidth devices. When interconnecting networks at different layers, performance optimization must take into account the topology of the network used in each layer.

Computation of performance in each layer and logging the performance in a remote server is equally important. Determining a specific topology in each layer, considering different types of things in each layer, and achieving the most appropriate interconnection between different networks is challenging. Just focusing on mere power dissipation for extending all devices' longevity in the network is not sufficient [7].

The issue of heterogeneity is one of the critical issues to be considered so that the time delays caused due to frequent protocol conversions are kept at a minimum [8]. Thus, the problem is to enhance IoT network performance due to numerous heterogeneous things and considering different layers existing in an IoT network by choosing appropriate networking topologies and internetworking the networks contained in different layers of an IoT network. The solution to figure out the network's overall performance is that the IoT network's performance comprises the performance of the individual devices, the controllers, the services, the gateways, and the cloud.

An IoT layer must be evaluated separately from and in tandem with its predecessors, and this is clearly the case. Connectivity topologies and software can be used to improve the performance of an IoT network at each layer, interconnecting various topologies in each. The key advantages of this paper are to describe in detail the experiments and data analysis conducted on the prototype network, as well as the performance improvements made in the device layer and the controller layer, which are both connected to the device layer's network.

2. Related Work

For the purposes of this section, we summarize the current research in the Internet of Things (IoT) field. Currently, there are a number of experts in the field of Internet of Things security. Even though IoT has just begun, many theorical frameworks are still far from ideal, and there is no complete security design for IoT. As of right now, the vast majority of Internet of Things security research is focused on various technological branches and various industry applications that are built on the Web of Things. For academic purposes, social IoTis a type of Internet of Things. The data unloading method proposed by the writers of literature [9] can help people from different social networks communicate and complete their communication. In order to better serve users on the socioeconomic Internet of things, the authors of reference [10] rationally use software defined networks (SDN) virtualization characteristics to classify facilities. Data coolant leaks and transmission congestion are common when problems with the inter-cell drilling interface arise in a network. The authors of regard [11] proposed a next-generation network solution based on SDN to address this issue, and it was a successful solution.

Researchers have proposed a variety of approaches to handle the data generated by the Internet of Things. One of the authors of literature [12] proposed a framework that combined the IoT with block chain technology for managing data. Blockchain mining is also applied to the Web of Things by the authors of literary work [13], who use multi commander and multi supporter game theory to overcome the difficulties of blockchain mining. Writings [14,15] investigate public blockchain consensus protocols and find solutions to various problems using various consensus protocols. Internet of Vehicles users are concerned about its security and overall quality as a component of the Web of Things. Using the blockchain, the writers of literature [16] recommend a technical solution for the Vehicular networks based on the blockchain technology. Use the reputation mechanism in the blockchain, and then pertain it in the Vehicular networks, and suggest a car network security based on the blockchain, as suggested by the authors of the literature [17].

Many researchers are currently using deep learning to fix the Internet of Things problem, which is in full swing at the moment. There are even more people using 4G networks, which makes it difficult to assure the quality of the service. In order to address the Internet of Things' local decision-making issues, the authors of reference [18] use deep reinforcement learning technology. There has never been a proposal like this before in the field of advanced wireless networks using deep learning, as described in the literature [19,20]. The performance of the IoT network has been the subject of numerous studies in the literature [21]. This section contains a summary of the contributions.

Most of the literature as shown in the Table 1 focuses on improving performance in the cluster layer of the IoT, rather than the other layers. There is little attention paid to networking and topology issues even when devices are clustered in the smallest IoT networks. Even though heterogeneity is a problem, it has not been addressed [22]. Until now, no one has explained how each one of the IoT link layer can be used to compute the overall response time of an IoT network [23].

Table 1. Summary table of the related research findings.

Reference No.	Article Title	Focused Investigated Method
[9]	IoT-enabled helmetto safeguard the health of mine workers	Data unloading method proposed by the authors can help people from different social networks communicate and complete their communication
[10]	Deep reinforcement learning for mobile 5G and beyond: fundamentals, applications, and challenges	Users on the socioeconomic Internet of Things rationally use SDN's virtualization characteristics to classify facilities
[11]	IoT-based automatic plant-watering system through soil moisture sensing—a technique to support farmers	Next-generation network solution based on SDN to address congestion problem

Table 1. *Cont.*

Reference No.	Article Title	Focused Investigated Method
[12]	Cloud/fog computing resource management and pricing for blockchain networks	Designed a framework that combined the IoT with blockchain technology for managing data
[13]	Rating-based recommender system based on textual reviews using IoT smart devices	A novel recommender system based on IoT for reviews
[14]	Cloud/edge computing service management in blockchain networks: multi-leader multi-follower game-based ADMM for pricing	Multi-commander and multi-supporter game theory to overcome the difficulties of blockchain mining
[15]	Efficient privacy-aware authentication scheme for mobile cloud computing services	Public blockchain consensus protocols to find solutions to various problems by using various consensus protocols
[16]	Toward secure blockchain-enabled Internet of Vehicles: optimizing consensus management using reputation and contract theory	Technical solution for Vehicular networks based on blockchain technology
[17]	Contract mechanism and performance analysis for data transaction in mobile social networks	Applied deep reinforcement learning technology for mobile social networks
[18]	Machine learning paradigms for next-generation wireless networks	Machine learning solution to improve the performance of IoT network
[9]	IoT-enabled helmetto safeguard the health of mine workers	Data unloading method proposed by the authors can help people from different social networks communicate and complete their communication
[10]	Deep reinforcement learning for mobile 5G and beyond: fundamentals, applications, and challenges	Users on the socioeconomic Internet of Things rationally use SDN's virtualization characteristics to classify facilities
[11]	IoT-based automatic plant-watering system through soil moisture sensing—a technique to support farmers	Next-generation network solution based on SDN to address congestion problem
[12]	Cloud/fog computing resource management and pricing for blockchain networks	Designed a framework that combined the IoT with blockchain technology for managing data
[13]	Rating-based recommender system based on textual reviews using IoT smart devices	A novel recommender system based on IoT for reviews
[14]	Cloud/edge computing service management in blockchain networks: multi-leader multi-follower game-based ADMM for pricing	Multi-commander and multi-supporter game theory to overcome the difficulties of blockchain mining
[15]	Efficient privacy-aware authentication scheme for mobile cloud computing services	Public blockchain consensus protocols to find solutions to various problems by using various consensus protocols
[16]	Toward secure blockchain-enabled Internet of Vehicles: optimizing consensus management using reputation and contract theory	Technical solution for Vehicular networks based on blockchain technology
[17]	Contract mechanism and performance analysis for data transaction in mobile social networks	Applied deep reinforcement learning technology for mobile social networks
[18]	Machine learning paradigms for next-generation wireless networks	Machine learning solution to improve the performance of IoT network

The remaining paper is organized as follows. Section 3 provides the problem statement. Section 4 discusses the system model and data analysis of the entire prototypical network. Section 5 discusses performance evaluation, and performance improvement measures are provided in Section 6. Section 7 compares our work with existing works, and, finally, Section 8 concludes the paper.

3. Problem Statement

Performance difficulties affect several layers of the IoT environment. A previous study revealed that introducing crossbar connectivity and employing separate base station equipment for communication increased performance by 18% [15]. It is feasible to enhance the performance of each layer by utilizing diverse network topologies. The problem for an IoT network as it expands is combining the different networking technologies used for different layers. The most essential issue addressed is the employment of a multi-stage system implemented at the device level to connect a control layer architecture utilized to improve the quantity of transmission between base stations and controllers. Integration must consider expanding the number of alternate channels to boost data transmission rates while also improving network fault resilience.

4. Typical Prototypical System Model and Data Analysis

Figure 1 shows a sample Internet of Things (IoT) network designed specifically for this project. An IoT network typically comprises a device level, control system layer, social and health layer, hub layer, and processing layer. These levels were considered when designing the IoT network. At the device layer, there is a cluster of devices.

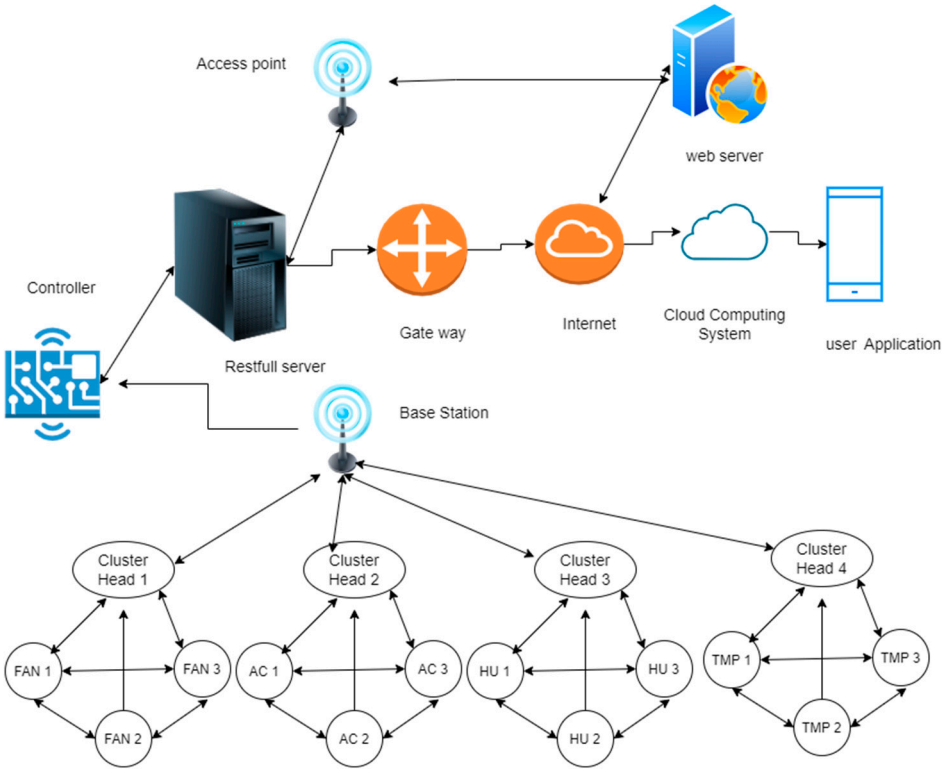

Figure 1. Typical prototype network.

To use this model, we could examine how the performance of the IoT show has improved after implementing the suggested adjustments. Figure 1 depicts how IoT networks are made up of various strategies such as sensors, controllers, and service-rendered devices, as well as heterogeneous communication. Total reaction time must be calculated by adding the time spent by all network devices and layers during the different phases of sensing, processing, protocol conversion, receiving, and transmitting. The key problem before improving the performance of the IoT network is calculating the reaction time. Every layer has a procedure for logging performance statistics, such as when data are received, how long it takes to process, and how long it takes to broadcast. To begin arriving at the real processing time necessary for a layer's data handling, time spent computing response times should be subtracted from total processing times.

tpLi = the time it would take to handle one layer of data
ttLi = length of time it takes to send the data
tcLi = how much time it takes a converter to process the data
ttcLi = the amount of time it takes for the data to be transferred from the converter
tRLi = received computational moment at tile i + 1
tPLi = following the receipt of the data, processing time for i + 1
tTLi = tSLi = calculations are stored on a web computer, which takes time
totLi = the amount of time it took to send and receive the data.

$$totLi = tpLi + ttLi + tcLi + ttcLi + tRLi + tPLi + tTLi \quad (1)$$

TT—sending data from one place of an IoT network to another takes a lot of time

$$TT = \sum_{1}^{7totLi} \quad (2)$$

Data Analysis of a Prototype Model

The achievement of the prototype model was computed based on the transfer of three data packets among components positioned in different layers of an architecture. As the system is operational, response time estimations are obtained and attempted to log into a web computer. To collect and transfer the data, four categories are used. Each cluster has three paths that connect each of the three devices. Any can communicate with another device via any of the paths as long as the link is operational. Wi-Fi-based communication is a popular option for internet communication due to its 11 Mbps speed. There was no thought given to the network's heterogeneity. A power loss of 0.001 watts is caused by the transmission of 36 bytes. The data rate of each layer has been calculated and stored in a database. The performance of the prototype model has been summarized based on numerous parameters. Power reserve in the devices, data size, transmission and conversion power consumption, data reception power consumption, post-transmission power depletion, estimated number of packets to be transmitted before devices enter initial state, number of routes used for broadcast, and overall time it takes to send data are all considered.

The behavior of the networks has been researched through data analysis to determine how the parameters affect them. The data were analyzed by comparing reaction times to the typical response time. Response time vs. network communication volume (Figure 2). Figure 3 depicts the sent data size, as well as the link between response data and information size. Figure 4 depicts a number of packets transmitted when power was at its lowest. The file size of the material being transferred (Figure 5).

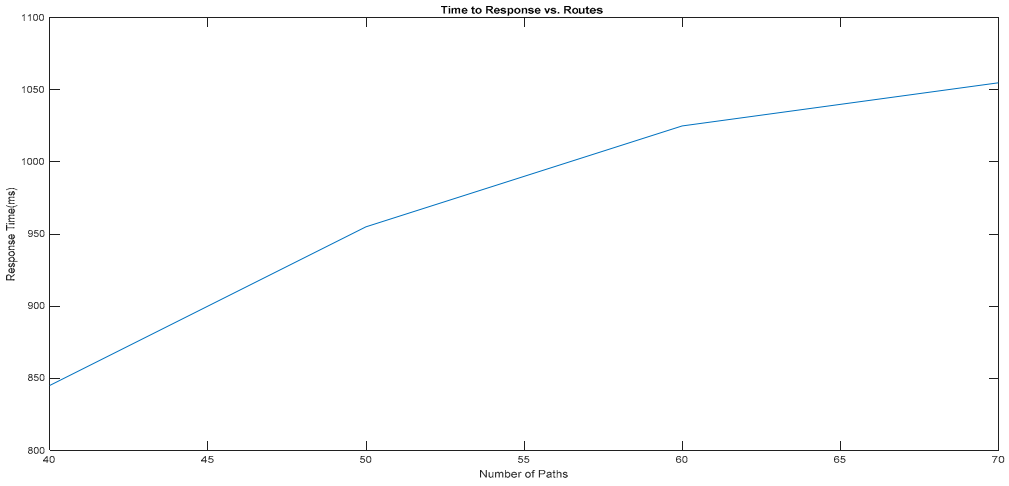

Figure 2. Time to response vs. routes.

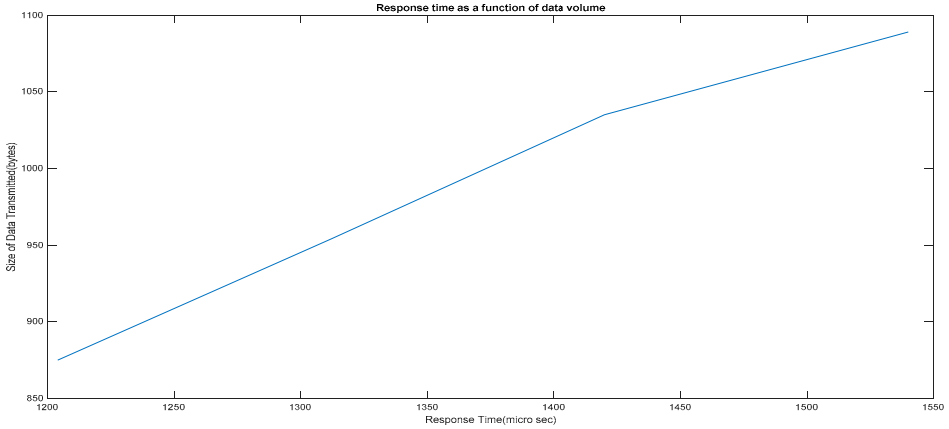

Figure 3. Response time as a function of data volume.

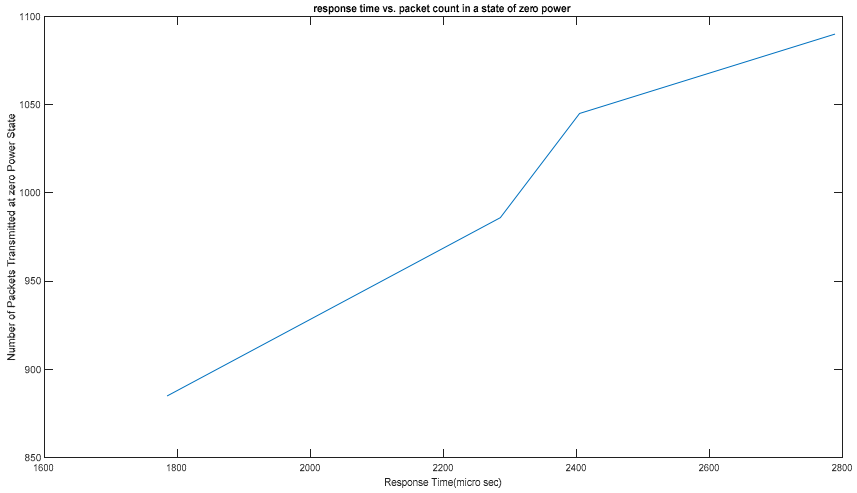

Figure 4. A graph of response time vs. packet count in a state of zero power.

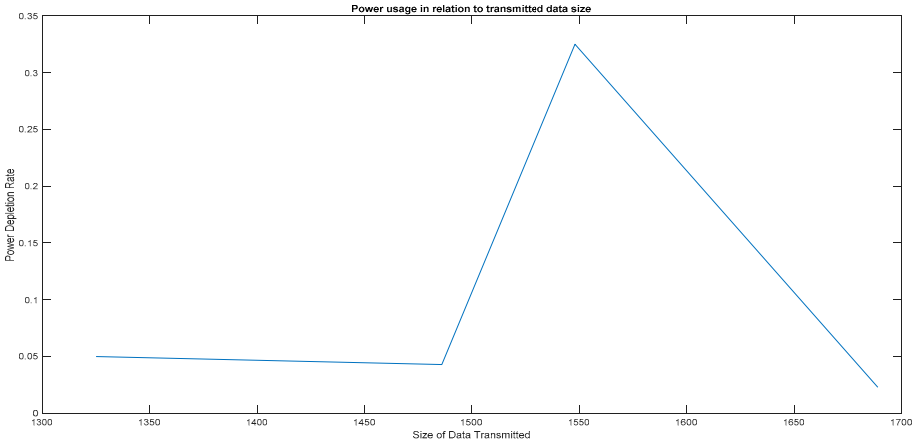

Figure 5. Power usage in relation to transmitted data size.

When the quantity of data to be transferred increases, electricity quickly depletes, yet response time does not alter if the number of transmission possibilities is not changed. Data size has a significant impact on power usage but has the opposite effect on response time.

5. Performance Evaluation

Due to increased connectivity, a multi-stage network has indeed been added to the test vehicle IoT network, with separate nodes acting as cluster heads, the base station

being linked to the ground station through a single controller, as well as the cluster heads being connected to the base station via the network. Each switching device that connects a multi-stage network is packed with clever software. The pace of power depletion of a gadget is a significant aspect in determining how long it may be expected to last. The revised network is seen in Figure 6.

Heterogeneity is addressed by a converter on the input side, and the complete multi-stage network operates utilizing Wi-Fi as a consistent communication paradigm. The path with the least amount of power utilized is picked for communication. The algorithm keeps a record of how much energy is utilized and how much data are transferred at each node. Three data packets travelling between devices in separate tiers were considered in the new model's achievement estimates. As the system is operational, response time estimations are obtained and attempted to log into a web computer. To collect and transfer the data, four categories are used. Each cluster contains three systems connected by 15 distinct pathways. If the link is active, each system interacts via any one of the trails. Wi-Fi-based communication is a popular option for internet communication due to its 11 Mbps speed. Since Wi-Fi packets are the major communication mode in this system, the diversity issue was considered when it was designed. An energy dissipation of 0.001 watts is caused by the transfer of 36 bytes. The processing and logging time for each layer was computed and documented in a database. The performance of the prototype model has been summarized based on numerous parameters. The magnitude of the data communicated, the power consumed during transmission, conversion and reception, and total power depletion after data transmission are all taken into account. Estimates for how many packets will be transmitted when devices enter the zero state, as well as the total time it takes to broadcast in nanoseconds and the number of transmission channels, are provided. The behavior of the networks has been researched using information analysis to see how the parameters affect them. The data were analyzed by comparing reaction times to the typical response time. As illustrated in Figure 7, there are numerous methods for sending and receiving information. Figure 8 depicts the number of messages delivered as a consequence of the total number of data packets transmitted. Figure 9: power loss vs. the file size of the data being supplied (Figure 10). This comparative study features the redesigned prototype model.

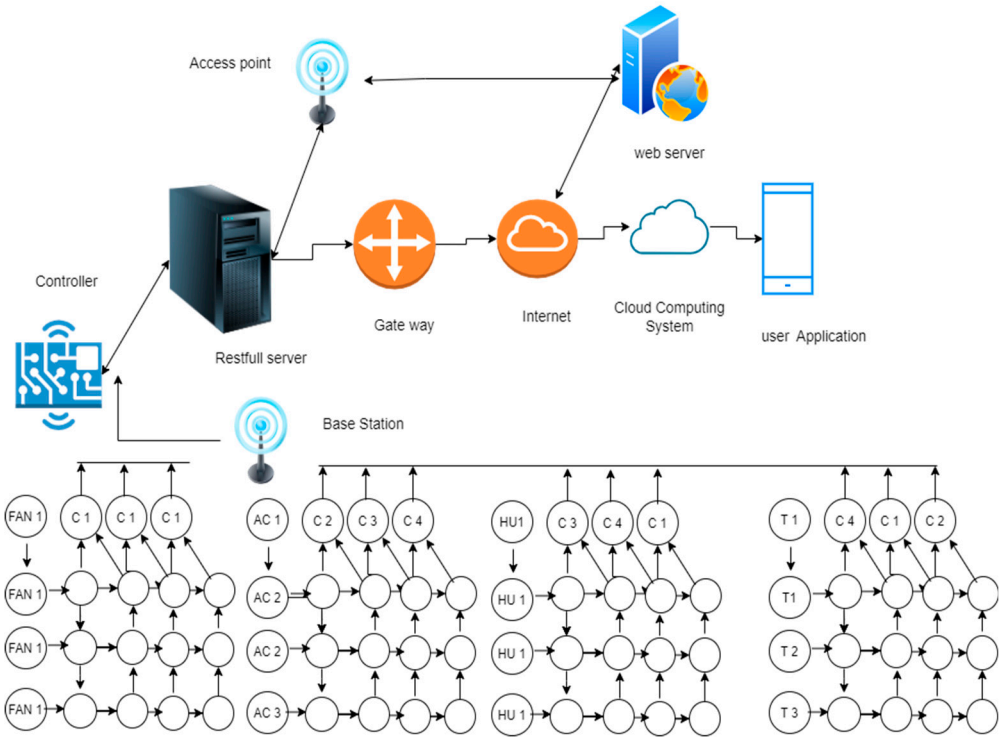

Figure 6. Revised IoT model through clustering in the device layer.

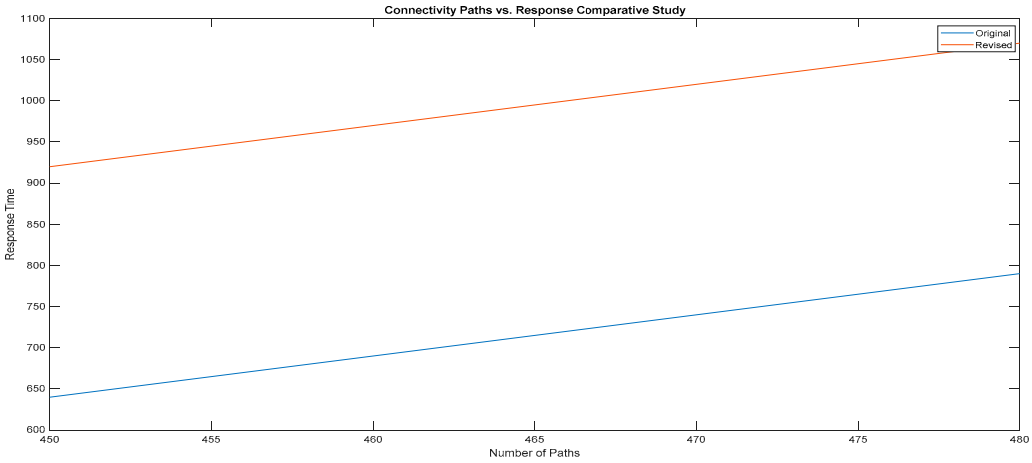

Figure 7. Connectivity paths vs. response comparative study.

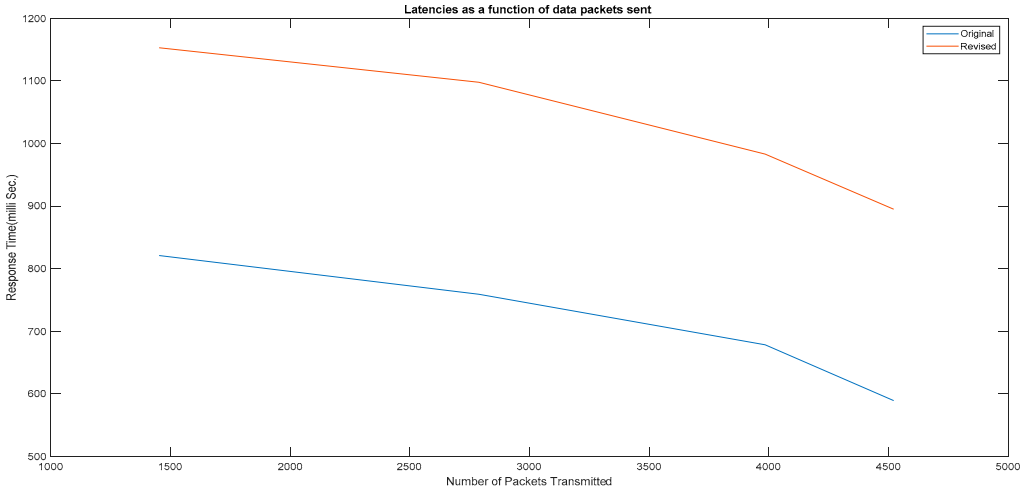

Figure 8. Latencies as a function of data packets sent.

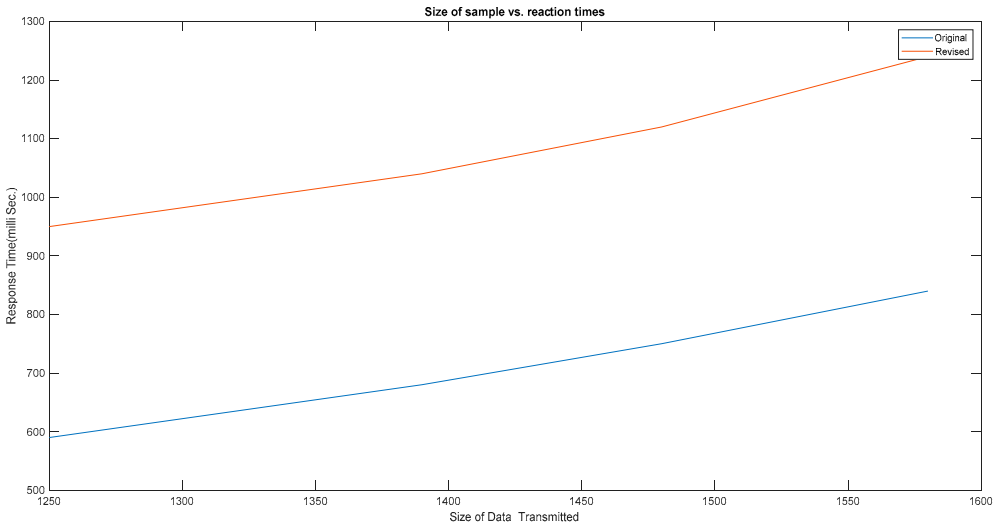

Figure 9. Size of sample vs. reaction times is compared in this study.

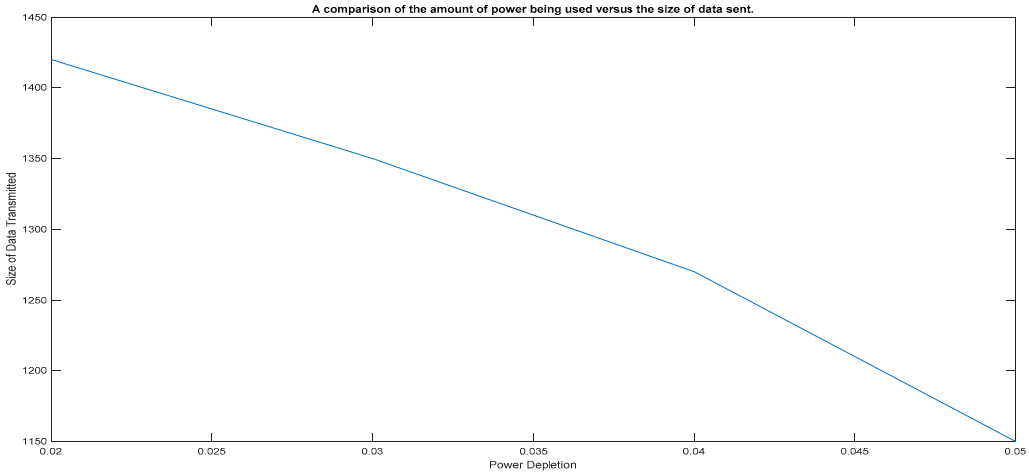

Figure 10. A comparison of the amount of power being used versus the size of data sent.

A comparison of IoT prototypes with upgraded models reveals that the latter outperforms its predecessor significantly. Fault-tolerant IoT networks have increased performance by 13%. Power depletion occurs quickly as the amount of information broadcast increases, but it has less of an impact on response time when the variety of options for transmitting packets remains constant. Although total power usage decreases drastically as data size grows, response time increases.

6. Performance Improvement Measure

The use of a multi-stage network at the cluster layer can boost controller layer efficiency by 13%. The system suffers because all contact is routed through a centralized base station or a simple controller. Because each of these elements has the potential to fail, the system is more vulnerable to failure if it is overloaded, has just one base station, and is managed by a single controller. Despite the fact that the system is built with a highly powerful architecture in the device level, the whole system fails. Adding too many base stations to the IoT network is inconvenient and contributes to network growth. The proportion of ground stations and controllers should be as high as feasible while keeping total costs to a minimum. A basic rule of thumb is that the proportion of ground stations and control systems ought to be equal to the total number of cluster devices. Figure 11 depicts updated IoT network performance calculations. As depicted in the picture, four stations and control systems connect the cluster heads. Each controller has two routes to each base station. In this situation, two threads in each terminal will manage traffic, allowing for parallel conversation. As a result of these configurations, the pace is enhanced by eight times using four controllers. To avoid overloading the rest servers, data produced by controllers are multiplexed and provided as a single message across various communication channels to the restful counterparts of those servers. Table 2 presents the findings of performance computations using the multi-ground station—multi-controller and parallel computing system. Figures 12–15 depict the performance of IoT networks in terms of reaction time, proportion of transmission paths, data volume, number of packets sent, and rate of electricity depletion. The figures show that, even though that more information is delivered as a result of much more transmission paths, response time has been considerably reduced.

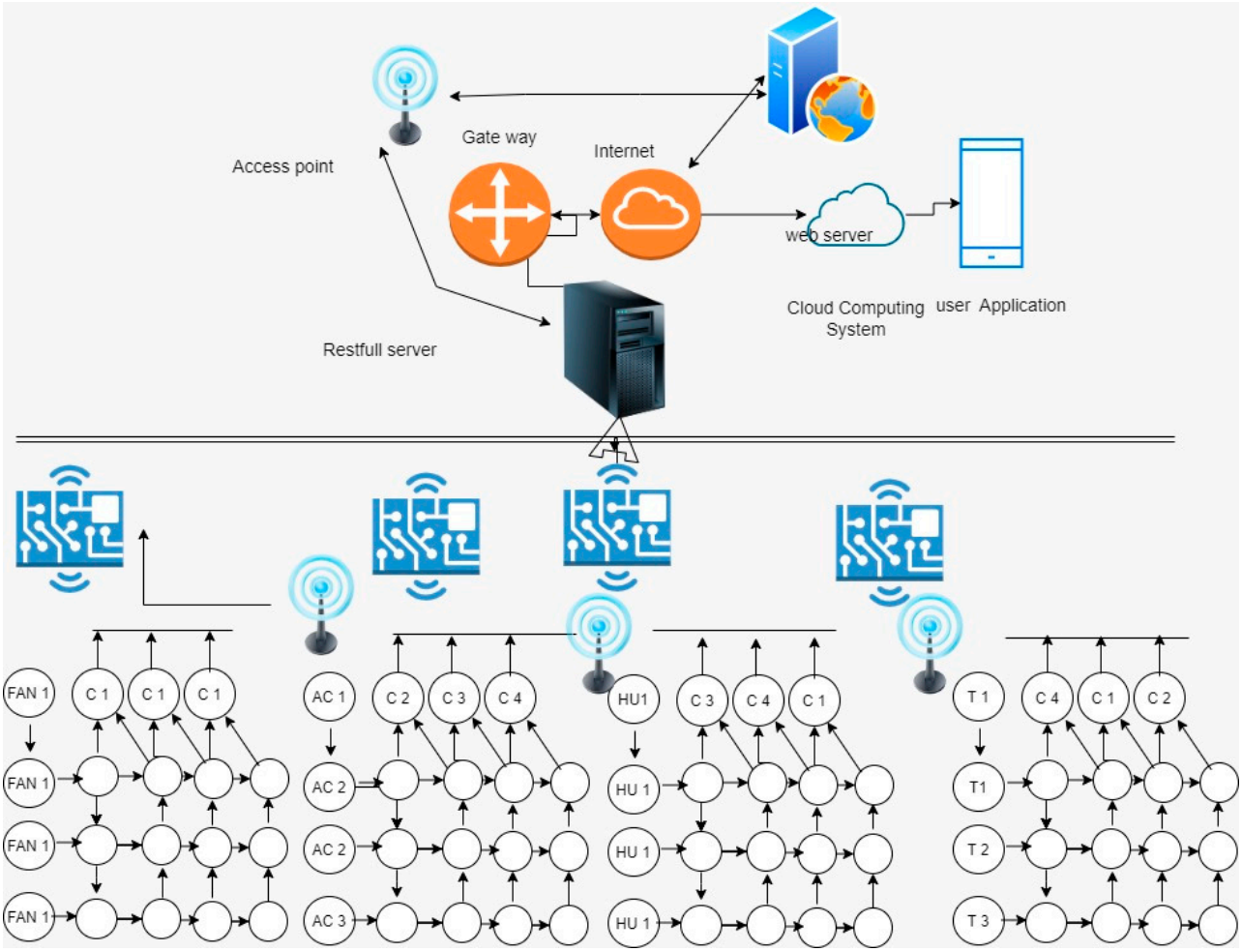

Figure 11. Revised IoT with parallel computing initiated in the controller layer.

Table 2. Summary of performance of cluster devices + multi-controller model.

Packet Number	Original Total Power of the Devices in the Clusters	Size of the Data Transmitted	Total Power Consumed	Power Gained due to Cluster Head Rotation	Actual Power Consumed	Power Depletion	Estimated Packets Transmitted before the Power Goes to 0 Stage	Number of Paths Used for Transmission	Number of Conversions Used for Handling Heterogeneity	Response Time
1	2288.000	1452	49.111	0.015	49.126	0.300	7627	1892	4	367.428
2	2238.889	1596	47.954	0.015	47.939	0.300	7463	1892	4	341.590
3	2190.935	1596	47.936	0.015	47.921	0.300	7303	1892	4	341.530

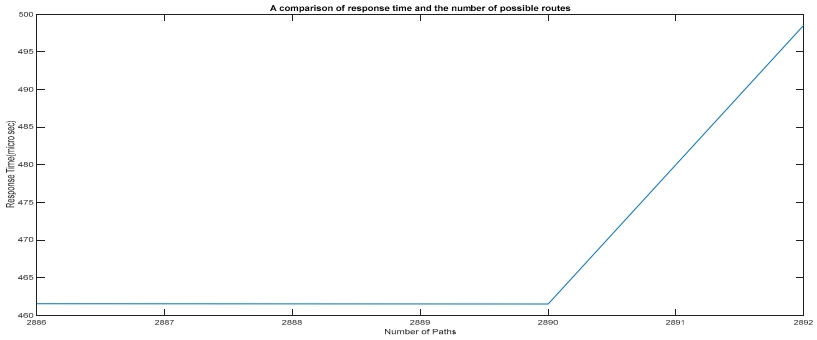

Figure 12. A comparison of response time and the number of possible routes.

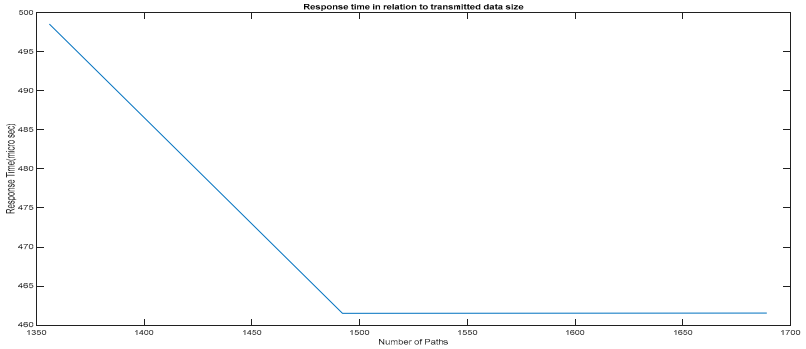

Figure 13. Response time in relation to transmitted data size.

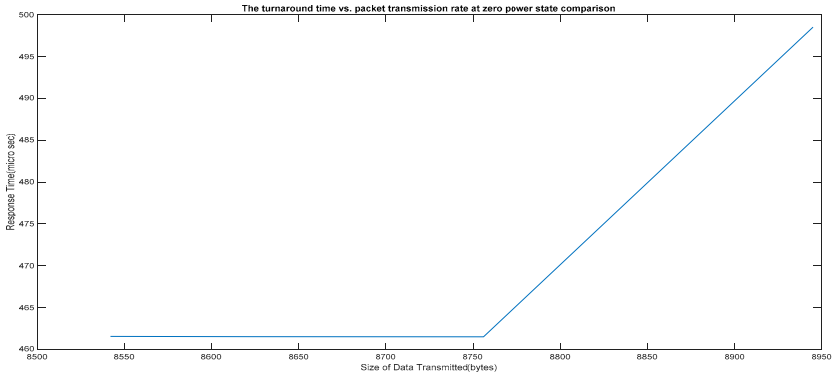

Figure 14. Turnaround time vs. packet transmission rate at zero power state comparison.

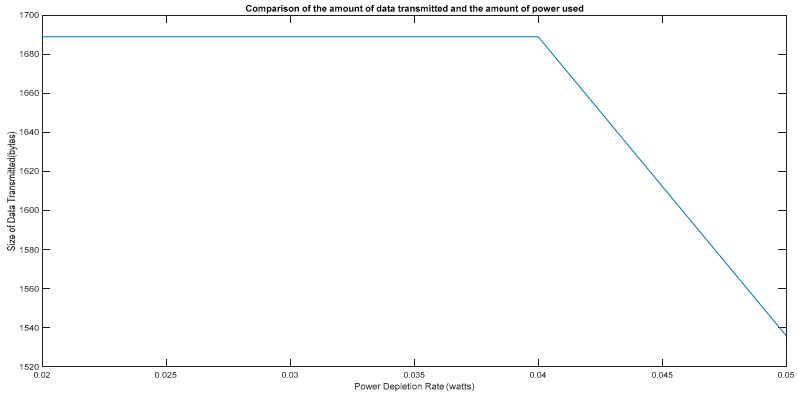

Figure 15. Comparison of the amount of data transmitted and the amount of power used.

7. Performance Comparison

Figures 16–19 compare the power consumption, data size, quantity of pathways, and projected number of packets relocated before achieving the zero-power state of prototype, clustered, then clustered + multi-controller models. Figures 16–19: at the device level, inter-architectural style and clustered architecture were used to produce a 24% improvement.

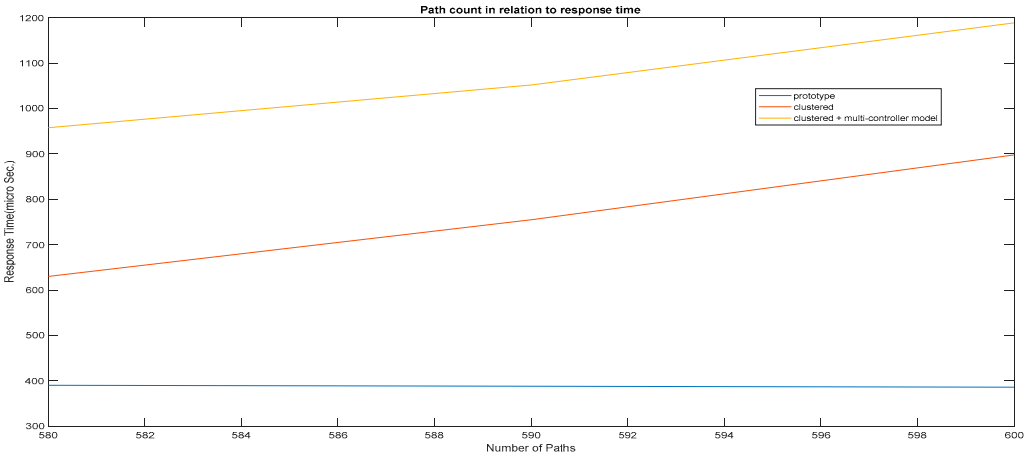

Figure 16. Path count in relation to response time.

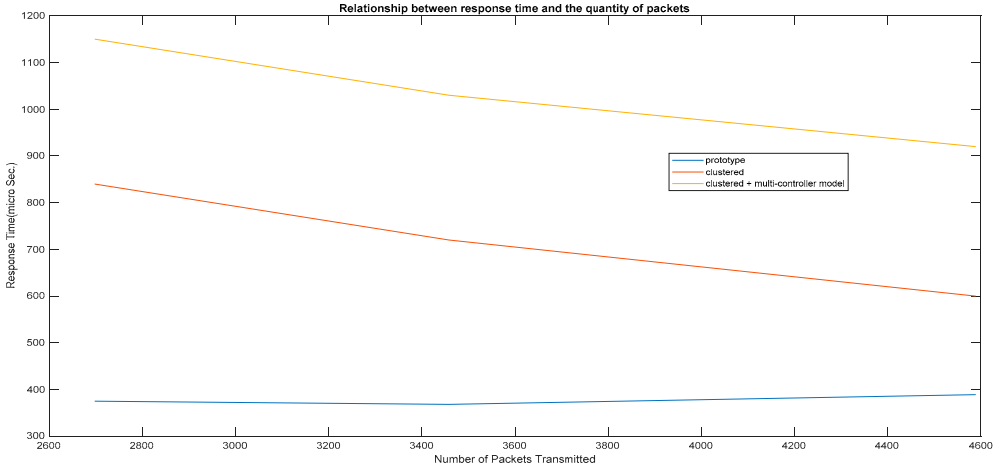

Figure 17. Relationship between response time and the quantity of packets.

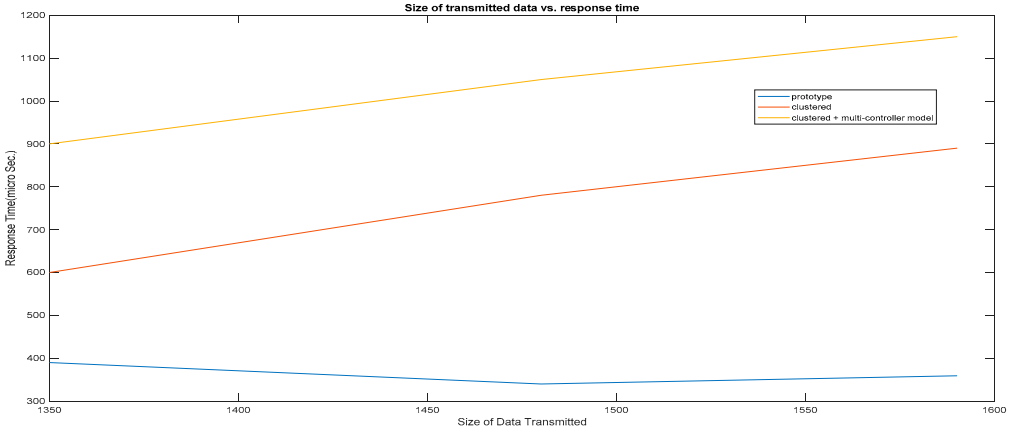

Figure 18. Size of transmitted data vs. response time.

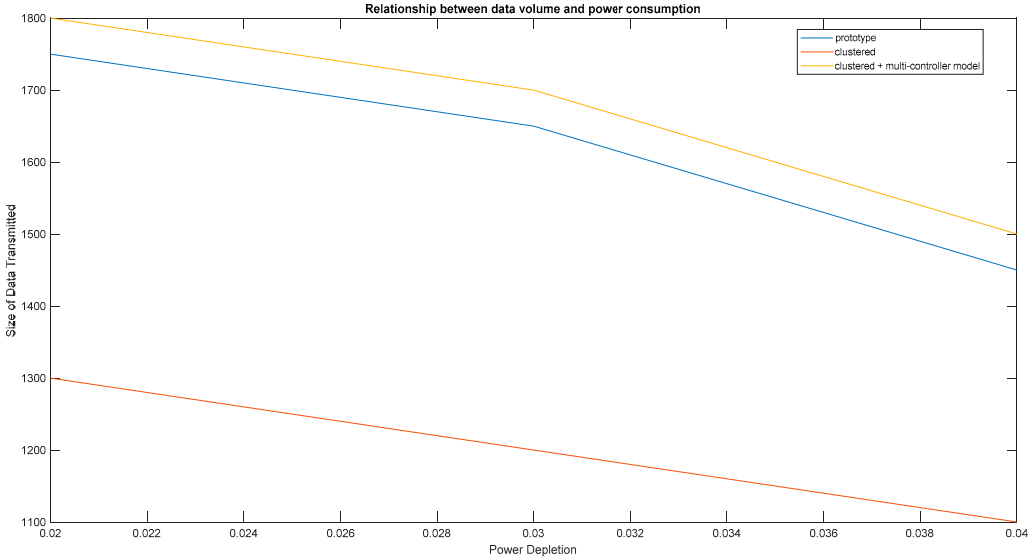

Figure 19. Relationship between data volume and power consumption.

The results displayed in Figures 16–19 are compared to the most recent state-of-the-art models, namely prototype, clustered, and clustered+ multi-controller suggested systems. Various parameters such as path count, response time, data size transferred, and power consumption are taken into account in all four outcomes. In all outcomes, the prototype model performs moderately, the clustered model performs well, and our suggested clustered+ multi-controller model works exceptionally well. When the overall performance of all models is considered, our recommended clustered+ multi-controller is 4% better than clustered and 24% better than the prototype model.

8. Conclusions

The IoT show's performance is critical since long routes of travel are necessary when data are transported from a device to a cloud service. After using the clustered design, IoT network performance improves by 16%. According to the study, additional controllers, as well as a concurrent process among base stations and controllers, boost performance by 24%. The number of transmission paths and the rate at which data travel through a path both affect performance, as does the speed at which data flow through a path (Channel). When a machine requires fewer spins to transfer data, its life expectancy extends due to a reduction in power consumption. The drop in the power diffusion equation that happens when a device sends data using fewer turns causes this gain in life span. To achieve further improvements, various network topologies in the upper layers of the control layer, such as the subsidies and price or other layer-by-layer components of the IoT network, might be considered.

Author Contributions: Conceptualization, G.D., N.S. and S.K.; methodology, G.D., V.K.G. and N.S.; software, V.K.G.; validation, V.K.G., S.R. and J.R.; formal analysis, V.K.G., A.F. and I.S; investigation, V.K.G.; resources, N.S.; data curation, V.K.G. and N.S.; writing—original draft preparation, G.D., S.R., N.S. and V.K.G.; writing—review and editing, J.R., A.F. and I.S.; funding acquisition, A.F. and I.S. All authors have read and agreed to the published version of the manuscript.

Funding: This paper is supported by the Faculty of Engineering, and Research Management Center of Universiti Malaysia Sabah.

Data Availability Statement: The processed data are available upon request from the corresponding author.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Guan, Y.; Ge, X. Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks. *IEEE Trans. Signal Inf. Process. Netw.* **2018**, *4*, 48–59. [CrossRef]
2. Varadharajan, V.; Karmakar, K.; Tupakula, U.; Hitchens, M. A Policy-Based Security Architecture for Software-Defined Networks. *IEEE Trans. Inf. ForensicsSecur.* **2019**, *14*, 897–912. [CrossRef]
3. Das, T.; Mukherjee, S. Data Privacy in IoT Network Using Blockchain Technology. In *Intelligent Systems for Social Good*; Prasad, P.S., Beena Bethel, G.N., Singh, N., Kumar Gunjan, V., Basir, S., Miah, S., Eds.; Springer: Singapore, 2022; pp. 117–137.
4. Casellas, R.; Vilalta, R.; Martínez, R.; Muñoz, R. Highly Available SDN Control of Flexi-Grid Networks with Network Function Virtualization-Enabled Replication. *J. Opt. Commun. Netw.* **2017**, *9*, A207–A215. [CrossRef]
5. Kalbande, M.; Gaidhani, Y.; Panse, T.; Mahajan, M. Cloud Based Examination Hall Authentication System Using Fingerprint Module. In *Intelligent Systems for Social Good*; Sahu, H., Singh, N., Eds.; Springer: Singapore, 2022; pp. 185–192.
6. Xiong, Z.; Zhang, Y.; Luong, N.C.; Niyato, D.; Wang, P.; Guizani, N. The Best of Both Worlds: A General Architecture for Data Management in Blockchain-enabled Internet-of-Things. *IEEE Netw.* **2020**, *34*, 166–173. [CrossRef]
7. Roy, S.; Meena, T.; Lim, S.-J. Demystifying Supervised Learning in Healthcare 4.0: A New Reality of Transforming Diagnostic Medicine. *Diagnostics* **2022**, *12*, 2549. [CrossRef] [PubMed]
8. Xiong, Z.; Zhang, Y.; Niyato, D.; Deng, D.; Wang, P.; Wang, L. Deep reinforcement learning for mobile 5g and beyond: Fundamentals, applications, and challenges. *IEEE Veh. Technol. Mag.* **2019**, *14*, 44–52. [CrossRef]
9. Pramanik, M.; Manoj, K.; Man, S.; Singh, D.; Sudhishri, S.; Bhatia, A.; Ranjan, R. Automation of soil moisture sensor-based basin irrigation system. *Smart Agric. Technol.* **2022**, *2*, 100032. [CrossRef]
10. Xiong, Z.; Feng, S.; Wang, W.; Niyato, D.; Wang, P.; Han, Z. Cloud/Fog Computing Resource Management and Pricing for Blockchain Networks. *IEEE Internet Things J.* **2019**, *6*, 4585–4600. [CrossRef]
11. García, L.; Parra, L.; Jimenez, J.M.; Lloret, J.; Lorenz, P. IoT-Based Smart Irrigation Systems: An Overview on the Recent Trends on Sensors and IoT Systems for Irrigation in Precision Agriculture. *Sensors* **2020**, *20*, 1042. [CrossRef] [PubMed]
12. Xiong, Z.; Kang, J.; Niyato, D.; Wang, P.; Poor, V. Cloud/edge computing service management in blockchain networks: Multi-leader multi-follower game-based admm for pricing. *IEEE Trans. Serv. Comput.* **2020**, *13*, 356–367. [CrossRef]
13. He, D.; Kumar, N.; Khan, M.K.; Wang, L.; Shen, J. Efficient Privacy-Aware Authentication Scheme for Mobile Cloud Computing Services. *IEEE Syst. J.* **2021**, *12*, 1621–1631. [CrossRef]
14. Kang, J.; Xiong, Z.; Niyato, D.; Ye, D.; Kim, D.I.; Zhao, J. Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2906–2920. [CrossRef]
15. Du, J.; Jiang, C.; Han, Z.; Zhang, H.; Mumtaz, S.; Ren, Y. Contract Mechanism and Performance Analysis for Data Transaction in Mobile Social Networks. *IEEE Trans. Netw. Sci. Eng.* **2019**, *6*, 103–115. [CrossRef]
16. Jiang, C.; Zhang, H.; Ren, Y.; Han, Z.; Chen, K.; Hanzo, L. Machine learning paradigms for next-generation wireless networks. *IEEE Wirel. Commun.* **2019**, *24*, 98–105. [CrossRef]
17. Gunjan, V.K.; Singh, N.; Shaik, F.; Roy, S. Detection of lung cancer in CT scans using grey wolf optimization algorithm and recurrent neural network. *Health Technol.* **2022**, 1–14. [CrossRef]
18. Mukherjee, S.; Kumar, R.; Banerjee, S. Smart Healthcare Remote Monitoring System Using Internet of Things. In *Intelligent Systems for Social Good*; Springer: Singapore, 2022; pp. 99–115.
19. Palsodkar, P.; Palsodkar, P.; Dubey, Y.; Umate, R. Pandemic Surveillance Through Perspective Transformation Using YOLO and Mobile Net. In *Intelligent Systems for Social Good*; Springer: Singapore, 2022; pp. 193–205.
20. Kabiraj, A.; Pal, D.; Ganguly, D.; Chatterjee, K.; Roy, S. Number plate recognition from enhanced super-resolution using generative adversarial network. *Multimedia Tools Appl.* **2022**, 1–17. [CrossRef]
21. Sahoo, K.S.; Tiwary, M.; Luhach, A.K.; Nayyar, A.; Choo, K.-K.R.; Bilal, M. Demand–Supply-Based Economic Model for Resource Provisioning in Industrial IoT Traffic. *IEEE Internet Things J.* **2021**, *9*, 10529–10538. [CrossRef]
22. Mai, T.; Yao, H.; Zhang, N.; He, W.; Guo, D.; Guizani, M. Transfer Reinforcement Learning Aided Distributed Network Slicing Optimization in Industrial IoT. *IEEE Trans. Ind. Inform.* **2021**, *18*, 4308–4316. [CrossRef]
23. Li, Y.; Su, X.; Ding, A.Y.; Lindgren, A.; Liu, X.; Prehofer, C.; Riekki, J.; Rahmani, R.; Tarkoma, S.; Hui, P. Enhancing the Internet of Things with Knowledge-Driven Software-Defined Networking Technology: Future Perspectives. *Sensors* **2020**, *20*, 3459. [CrossRef] [PubMed]