ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

A RESEARCH TO IMPROVE PERFORMANCE ACCURACY BY CONNECTING OPNETS TO IOT WITH HYBRID TECHNIQUES

[1]M.Anjaneyulu, Research Scholar, School of Computational Sciences, SRTM University, Nanded-M.H., India & Asst. Prof. of Computers, S.R.R. Govt. Arts & Science College (A), Karimnagar-TS, , anjan.lingam1@gmail.com

[2]Dr.S.B.Thorat, Director, Shri Sharda Bhavan Education Society's, Institute of Technology and Management, Nanded-M.H., India, , suryakantthorat63@gmail.com

[3]Dr.Pritam Rajendra Patil, Asst. Prof., SSBES Institute of Technology & Management, Nanded-M.H., India, , pritam.itm@gmail.com

[4]Mr. Amol V.Suryawanshi, Asst. Prof. SSBES Institute of Technology & Management, Nanded-M.H., India, suryawanshiamolv@gmail.com

[5]Smt. M. Krishnaveni, Lecturer in Computers, S.R.R. Govt. Arts & Science College (A), Karimnagar-TS, , krishnaveni.meka@gmail.com

Abstract

The quick ascent of the Internet of things has made it workable for different upgrades to be acquainted into our day-with day lives as well as the items and administrations that we enjoy. The plan of the "Internet of Things" (IoT) organization might be gainful to a wide assortment of things, including gadgets, hardware, cars, houses, and structures that have implicit sensors and actuators. It's possible that you've worked with this framework before when it was known as the "Internet of Things." It makes it feasible for the numerous electronic gadgets to speak with each other and share data with each other. As the utilization of area based versatile showcasing applications for the Internet of Things fills in notoriety, it is crucial for offer an excellent of administration for the administration of media information gushing over remote and portable organizations. This is due to the fact that managing multimedia data streaming over mobile and wireless networks requires a high-quality service. OPNETs are placed into operation in areas where there is a lack of existing infrastructure and where it would be impractical to attempt to repair the current infrastructure. Integration of OPNET with the Internet of Things to allow for ad hoc connections between OPNET and WSN the formation of an OPNET cluster will enable the OPNET nodes to be organized into small groups, hence avoiding the routing challenges that are present in large OPNETs. Integration between OPNET and IoT will be carried out. Be that as it may, to empower area based portable promoting applications inside the Internet of Things, the issue of dealing with the spilling of information bundles over remote and versatile organizations must be settled first. This is a crucial hindrance.

Keyword: IoT, Multimedia, WSN, OPNETs, and performance.

INTRODUCTION

ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

The Internet of Things (IoT) can be defined in a number of different ways, and different writers have presented it in a number of different contexts. This variation is due to the fact that the meaning of the word shifts depending not only on the situation in which it is spoken but also on the objective served by the product. According to Patel and Patel (2016), the Internet of Things has expanded beyond being merely a network of computers to include not only these but also digital cameras, autos, smartphones, appliances, medical devices, industrial systems, humans, and structures. Previously, the IoT was simply a network of computers. In addition to this, the Internet of Things has developed into a network. Because all of these interconnected devices are able to speak with one another and share data, it is now possible to implement intelligent relocations, placements, online updates, process management, and administrative tasks.

In order to be functional, mobile marketing apps need to make use of wireless networks, mobile devices (such as personal digital assistants, smartphones, and navigation devices), geo-information systems, and location or positioning identification technologies. It is essential to have efficient mobility management among mobile devices if these apps are to achieve the level of precision in location criteria that is required.

It is essential to have a strong command of QoS in the management of multimedia data streaming within an IoT environment if you want your location-based mobile marketing apps to be effective. The mobility management plays an essential part in this process. The transmission of multimedia data packets will, as a result, place a significant emphasis on IoT convergence networks and mobility management. As IoT settings continue to develop, mobile devices will increasingly connect to networks that are located in other countries. Because people are constantly moving about with their mobile devices, there will be a substantial increase in the volume of multimedia traffic. As a result, there is a chance that packets will be lost, and there may be issues with the sequencing of packets. Mobility management systems have been presented by the research community in order to create a mobile network that is smooth and satisfies the routing needs of location-based mobile marketing apps in the Internet of Things (IoT).

Figure 1.1 Things Connected to the Internet

Deepak Kulhare (2019) investigated that a mobile ad hoc network, or MANET, was a wireless mobile network that does not have centralised administration over the mobile nodes. Instead, the nodes in the network are free to move about without the oversight of a centralised administrator. The DSR protocol was a type of dynamic routing that was employed on the manet. In this study, the throughput for both the original DSR and the UPDATED DSR was analysed so that both may be compared to one another. The opnet simulator was used to run the simulation, which was carried out on 100 mobile nodes. Research has also been conducted on the dsr manet routing protocol in order to do research on the routing traffic that has been received and that which has been transmitted.

ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

Kumar and Vidyarthi (2018) developed an innovative concept for an algorithm by making use of a tool called Fork and Join Adaptive Particle Swarm Optimization (FJAPSO). Green routing is a novel concept that has the potential to make sensor networks more useful for a longer period of time. The use of this FJAPSO allows for the determination of the ideal number of control nodes as well as the optimal clustering of those control nodes, which is of tremendous assistance to the process of auto-optimization. If you want the very best outcomes, you are going to have to accomplish both of these things. When compared to other strategies, including those that are now considered to be state-of-the-art, it was shown that the FJAPSO is better in terms of its ability to prolong the lifetime of sensor networks.

LEACH-EECHS, which stands for "Energy Efficient Cluster Head Selection," is a method that was proposed by Wang (2019). This provides more alternatives for nodes that are physically close to the cluster's epicenter, which is a huge boon to the CH selection process and contributes significantly to its overall improvement. As a result, it is possible to demonstrate that LEACH-AEC is superior in terms of reducing the amount of energy required and speeding the process. The overall number of nodes in a network as well as their typical amount of energy consumption are both factors that are considered throughout the decision-making process at CH. We are able to show, via the use of simulation, that our protocol is superior than the LEACH protocol in terms of its ability to keep a network connection for a much longer period of time.

G. Liu (2015) designed a mobile RFID system that has discrete network, node, and process domains in order to investigate the influence that anti-collision algorithms and other environmental factors have on the tag recognition rate. This system is built upon the OPNET three-layer modeling method, which serves as its basis. In terms of accuracy, the findings of the simulation indicate that the CFDSE method (also known as the Coarse-Fine Double Searching-based tag Estimation) works better than the other three conventional approaches (which each had tag recognition rates of 3.5 percent, 5.1 percent, and 7.2 percent, respectively). According to the findings of this research project, tag density has a bigger influence on the rate of tag recognition than tag speed does when tag speed is relatively low. This is the case regardless of whether or not there is a shift in the identification intensity. In order to achieve a high recognition rate in real-world applications, it is necessary to pick the appropriate tag movement speed and density, which may be done with the use of a recognition rate curve.

Kosunalp (2019) looked on a possible method for developing the MAC protocol for WSNs that collect energy from the environment. Energy-Harvesting Receiver-Initiated Medium Access Control (ERI-MAC) is one of the protocols studied alongside On-Demand Medium Access Control (OD-MAC), Energy-Harvesting Medium Access Control (EH-MAC), QoS-Aware Energy Efficient Medium Access Control (QAEE-MAC), and a few others. Our analysis led us to conclude that the receiver-initiated architecture provided some novel insights that aided greatly in the design of these protocols. Despite this, every protocol implementation has its own quirks, guiding principles, and compromises.

Fu et al. (2019) in order to maintain a stable level of energy usage. Two CHs are chosen at random at the beginning of each game. The first CH may be switched out for the second CH in the event that the first CH does not have sufficient energy or if the distance between it and the base station is too great. It has been demonstrated that the LEACH-TLCH has a higher energy efficiency and a longer network lifetime than the original LEACH. This was accomplished via the use of a simulation.

OBJECTIVE OF THE STUDY

1. To conduct simulation-based analysis in order to evaluate the suggested models' performance and confirm its efficacy and efficiency.

ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

2. Using a hybrid technique that combines identity-based signatures and encryption to improve performance accuracy.

Information Security

Organizations and individuals who rely on information technology are required to take safeguards on a consistent basis to ensure the confidentiality of their data. These systems transmit and store a significant amount of data, which necessitates the implementation of a wide range of security precautions to guard against a number of threats. The storage and transmission of this data is handled by these networks. Because of this, ensuring the systems' safety is absolutely necessary. It is of the utmost importance to ensure that unauthorized individuals are unable to get access to these systems and make unlawful modifications to the data that they contain. According to the findings of study conducted by Vashi et al. (2017), the number of vulnerabilities and security threats linked with the Internet of Things is expanding along with the expansion of its use. According to research conducted by Burg, Chattopadhyay, and Lam (2018), an extensive wireless and wired infrastructure connects the various gadgets that make up the internet of things, hence facilitating communication and ensuring users' safety. The network makes it possible for the various devices to communicate with one another.

There are vulnerabilities in the traditional internet as well as in the internet of things with regard to the protection of individual consumers. The Internet of Things cannot work independently of the current Internet infrastructure. The Internet of Things is supported by three distinct layers: the perception layer, the transport layer, and the application layer. The process of maintaining security is already challenging enough without adding each of these extra degrees of complexity on top of it.

Security threats of IoT

If you ask different people, you'll get different answers, but it's possible that the Internet of Things has anywhere from three to five unique levels of structure. The first three levels are comprised of several layers, including the perception layer, the network layer, and the application layer. After the operating system layer comes the network layer, followed by the middleware layer, the business layer, and finally the application layer. Every layer is susceptible to the same sorts of threats and attacks when it comes to security. These can operate in either an active or a passive capacity, depending on the context. These threats may have originated from an external source or an inside network. Either one is a possibility (Yousuf, Mahmoud, Aloul and Zualkernan, 2015). To begin, an assault on the perception layer can include the revelation of private information, a denial-of-service attack (also known as a DoS attack), or something else of a similar nature. Second, attacks directed against the network layer can take the form of a man-in-the-middle attack, a sinkhole attack, a Sybil attack, or an attack of a similar nature. Attacks against the application layer may include, but are not limited to, activities such as sniffing attach, inserting malicious code, and other similar activities.

IoT security implementation

Each of the levels, as was discussed in the section that came before this one, is vulnerable to a different form of security breach. Several different security processes, such as encrypting the data, authenticating users, keeping the information secret, and regulating who may access it, are implemented so that the data can be kept secure.

ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

The Internet of Things, also known as IoT, is not a single piece of technology but rather an ecosystem of interconnected hardware and software systems. The solutions that are made available by the Internet of Things are founded on information technology, which encompasses the different instruments that are used to gather, organize, and analyze data. According to Patel and Patel (2016), the capability of the internet to connect a large number of devices is one of the factors that contributes the most to the efficacy of these strategies. The Internet of Things cannot be successful without the use of a wide variety of different electronic communication technologies. The Internet of Things makes use of a wide variety of wireless networking protocols, some of which include Bluetooth, RFID, Near Field Communication (NFC), and Wi-Fi. These are only few of the acronyms. Bluetooth, RFID, and Near Field Communication (NFC) are a few of them. If communication systems are going to be able to satisfy the requirements of the Internet of Things, then they need to be dependable, secure, and effective.

Concerns about Internet of Things Security

The bulk of the devices that are part of the Internet of Things have a plain design, which is founded on the idea that they may be utilized in a quick and uncomplicated manner, or that regular equipment can be changed into IoT devices by adding Internet connectivity. It is not uncommon for non-visible aspects of a product, such as its reliability and security, to be disregarded in the process of meeting the expectations of providing a product in a timely manner.

It should not come as a surprise that concerns regarding security are not always taken into consideration as part of the manufacturing cycle for Internet of Things devices, from the hardware/software applications to the frameworks. This applies to all aspects of the manufacturing process, including the frameworks. The great majority of newly developed Internet of Things devices rely on cloud computing in order to fulfill their connectivity requirements. According to the findings of researchers working in the field of information security. Cloud infrastructures already have documented security issues, which may make it easier for Internet of Things devices to become targets of cyber attacks. The bulk of Internet of Things devices run on new development platforms that are still in their infancy and may have security problems. One of these operating systems is used in the great majority of internet-enabled devices today. Because the firmware and software that runs on many Internets of Things devices cannot be updated, these devices will be especially vulnerable to attacks and exploits in the future. Many Internets of Things devices will be affected by this. This adds another layer of complexity to a situation that was already complex.

The attacks that are launched against the Internet of Things may be divided into two basic categories: those that aim to compromise the architect levels, and those that want to compromise the data stages. A further contrast that can be drawn between the conventional Internet and the Internet of Things is that the content and data on the traditional Internet are generated by the actions of people, whereas the content and data on the Internet of Things are produced by the activities of machines. It is not unusual for data to be captured and created by intelligent devices in the world of the Internet of Things (IoT) (sensors, actuators). It is possible to influence machines in such a way that they send or receive misleading information, despite the fact that machines do not intentionally lie. The OWASP Internet of Things Project conducted research in 2018 and determined the following to be the top 10 security flaws connected with Internet of Things (IoT) devices:

1. Passwords that are either simple to decipher or are hardcoded;
2. Insecure services for computer networks;

ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

3. Connections that cut across different ecosystems that are unsafe
4. The lack of a dependable method for keeping the information up to date;
5. The utilisation of components that are either vulnerable or obsolete;
6. Inadequate protection of personal privacy;
7. Unsecure data transport and storage;
8. Insufficient administration of the devices;
9. Insecure settings that are the default;
10. Insecure settings that are the default;

In order to protect the privacy of our sensitive information, we need to ensure that the data that is collected and the data that is traded are both in accordance with the regulations outlined in the following paragraphs: I confidentiality, which means that the data that is transmitted as well as the communication that takes place between endpoints, sensors, and readers is encrypted; ii integrity, which means that the data that is transmitted is accurate and complete; and iii authenticity, which means that the data that is transmitted has been verified and originates from authorized sensors, endpoints, and readers. I confidentiality, integrity, and authenticity are the three pillars of a secure network. I confidentiality means that the data that is transmitted is accurate and complete.

Networking defined by software (SDN)

Software-defined networking, or SDN for short, is a type of network design that allows for greater control and flexibility in the manner in which data is forwarded by inserting programmable switches between the data plane and the control plane of a network.

Software-defined networking, often known as SDN, has the potential to supplant traditional computer networks in a variety of different ways. Conventional networks are hardware-based, which implies that their architecture must consist of physical equipment such as switches and routers. This is because software-based networking is becoming increasingly obsolete. As a direct consequence of this, conventional networks are limited in terms of both their speed and the degree to which users may exert control over them. On the other hand, Software-Defined Networking (SDN) is software-based; as a consequence, it may be virtually managed through the control plane. In contrast to having functionality that is predetermined, the software that is used in an SDN may be easily and quickly modified in order to meet shifting requirements. Second, the implementation of higher-level algorithms is necessary for routers that are used in traditional networks in order for those routers to be able to determine the destination of data packets. In software-defined networking (SDN), the SDN controller is the component that communicates with the devices that make up the network in order to centrally govern the flow of packets in accordance with the configuration. This is accomplished by connecting with the devices that make up the network.

System Model

Every single day, brand-new Internet of Things (IoT) devices are brought to market, despite the fact that this industry is one of the most quickly increasing ones in the field of technology in the contemporary period.

ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

These electronic devices are able to communicate with one another and share information and data thanks to their internet connection. Because of the fluidity of their operating settings, conventional networks are not ideally suited to fulfill the requirements of the Internet of Things (IoT). For activities related to the Internet of Things to function as intended, a network architecture that is not only more dynamic but also more secure is required. Software-defined networking, more often known as SDN, is a cutting-edge technology that gives users the ability to control and manage network congestion. In the field of networking, "software-defined networking," abbreviated as "SDN," is an invention that is at the leading edge of what's possible. With the assistance of the debugging tools supplied by the SDN controller, the level of security within the IoT ecosystem may be increased. It's possible that the controller may act as a gateway to these instruments.

Structured data networks, also known as SDNs, are used to describe the underlying architecture of the Internet of Things (IoT), and the SDN controller makes it possible for users to set up a large number of separate networks, known as subnets, inside the larger network. The Northbound Application Programming Interface (API) is a specific form of the application programming interface (API) that facilitates communication between the Internet of Things application and the SDN Controller. The latter responds by taking action in accordance with predefined rules that are arrived at via an analysis of network data. However, in order to connect with the network switches in a manner that is compliant with the laws that have been set, this particular application programming interface (API) is known as the Southbound API, and it is used by the controller. This API is not shared with the rest of the system. Integrating IoT with SDN is beneficial for IoT operations and network security because it enables complete remote administration of the network configuration without requiring direct connections to be made with the IoT devices themselves. This eliminates the requirement to create direct connections with the IoT devices.

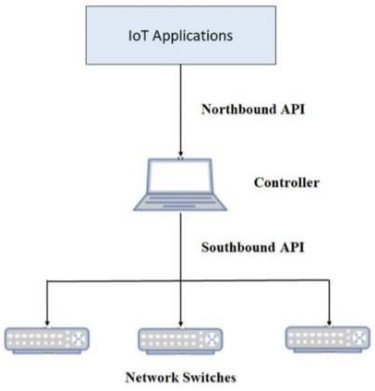

Figure 1.2 SDN and IoT Structure

In the system that we described, SDN was realized through the utilization of Open flow Protocol as the protocol of choice for data transfer. The functioning of the SDN switch makes use of a flow table, which is comparable to the routing table that is utilized in the operation of traditional routers. However, it does support chaining and makes it possible to match a broader range of fields, along with actions that follow each flow. Once a packet has been received by a switch, it is compared to the flow table, and the relevant actions are conducted based on whether or not a match is discovered. In the event that there is no match, the switch will go on with the processing of the packet as it would normally. In the event that there is no match, the package is thrown away. If there is no match detected, which is something that is

ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

likely to occur whenever a new device is added to the network, the received packet is delivered to the SDN controller using the Southbound Application Programming Interface (API). After the controller has completed its examination of the packet, the further steps will be carried out in accordance with the results of the investigation. It is likely that it would do some action such as adding a new flow to the switch so that future packets might be routed independently of the controller's involvement. In the future, this would be done in order to simplify the process of routing packets. By making use of the Northbound API, the SDN application will have the ability to receive alerts.

CONNECTING OPNETS TO IoT

A network of mobile nodes that is infrastructure-less and self-configurable is known as the Mobile Ad hoc Network (OPNET), which is another name for this network. In most situations, OPNETs are placed into operation in areas where there is a lack of existing infrastructure and where it would be impractical to attempt to repair the current infrastructure. Attempting to repair the existing infrastructure would be impractical because of the absence of existing infrastructure. It has been shown that OPNET is of tremendous service in areas of conflict as well as other contexts where natural disasters have taken place. Multi-hop communication and extremely cheap implementation costs are two of the most compelling elements of OPNET, both of which contribute to the application of the technology in the places stated above. OPNET was developed by Open Protocol Networks (OPNET). In an OPNET, each individual node performs the duties of a router by passing on data packets to the subsequent node in the network. Recent research trends including Green Communication, Machine-To-Machine Networks (M2M), Device-to-Device (D2D) communication and the Internet of Things (IoT), imply that ad hoc network must be implemented in their design to minimize the cost of deployment and communication (Abduljalil et al. 2007). Green communication, M2M networks, D2D communication, and IoT are all examples of recent research trends. Green communication, often known as environmentally friendly wireless communication, is a kind of wireless communication.

In the research that has been done, a wide variety of possible technologies that may be utilized to connect the OPNET to the Internet have been discussed. The individual nodes that comprise an OPNET are often provided with IP addresses in order to facilitate the routing of data packets between them. As a direct consequence of this, creating a link between the OPNET and the Internet is always an option. Nevertheless, there are primarily two roadblocks that need to be conquered:

1. Each node in the OPNET network needs an efficient way in order to determine whether or not a certain address in the network is present. This is due to the fact that OPNET nodes are continually moving across the network.
2. It should be plainly clear that in order to connect to the Internet, it is essential to make use of either a gateway or an access point. This fact should be brought to everyone's attention.

OPNET – IoT INTEGRATION PROTOCOL

We will talk about our protocol, which clusters OPNET nodes in order to integrate OPNET with the Internet of Things.

An outline of the basic plan for the construction of the protocol

The following are two of the most important functions that are included in our proposed protocol:

ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

Integration of OPNET with the Internet of Things to allow for ad hoc connections between OPNET and WSN The formation of an OPNET cluster will enable the OPNET nodes to be organized into small groups, hence avoiding the routing challenges that are present in large OPNETs. Integration between OPNET and IoT will be carried out.

While the OPNET is being integrated with the Internet of Things and the WSN backbone, the OPNET will be required to provide two services, which are as follows: (i) the finding, and (ii) the announcement Through the process of discovery, OPNET nodes are able to analyze the topology of the WSN and select a node from the WSN to use as an entry point. The process of announcing relays information about recently discovered data to other nodes in the WSN. It is necessary to tell the nodes that comprise a WSN that there are OPNET access points present in order to fulfil the function of the announcing process. IT needs to cut down on the number of packet swaps that take place between OPNET and WSN in order to minimize an excessive quantity of power usage. This may be accomplished by keeping the OPNET nodes inactive in usual settings and encouraging them to participate in active communication instead. Additionally, this can be accomplished by coordinating with WSN packets to guarantee that higher priority packets are transmitted.

DATA ANALYSIS

During the process of developing test cases, the OPNET network layer's State Machine undergoes certain modifications and is simplified by the removal of the "default" and other interruptions that are deemed to be unimportant. This is how the whole apparatus of the state appears. This state machine model has the ability to provide network layer test cases, which may then be generated with the help of an appropriate tool for creating test cases.

ModelJUnit carried out a series of experiments in order to build test cases, and the results of the tests were averaged over the course of ten iterations.

Both the Random Walk and the Greedy Random Walk algorithms were used in order to produce test cases for the purpose of comparing them in the experiment. The Random Walk technique is able to put a system to the test quickly and simply by traveling randomly around its model of a State Machine. On the other hand, the Greedy Random Walk algorithm emphasizes new pathways throughout the system in order to find optimal solutions. The generation process itself is not nearly as important as the test case coverage, and ModelJUnit offers support for three unique coverage metrics: the state meter, the event metric, and the transition metric. This metric keeps track of the number of states that have been visited. The event metric will provide the total number of events that have occurred on at least one occasion. This study will focus on at least one transition measure due to the fact that it is essential to validate each state change in order to ensure that the network layer functions appropriately. The particulars of the experiments that were carried out in order to carry out the assessments are presented below.

Experiment 1: The original OPNET network model had the same number of states.

The following is the test time (number of test suites) that must be performed in order to get 100% coverage of all transitions when the state machine model in question has 16 states and 25 interruptions (events).

- 16 states and 25 events in a state machine model
- Walk at Random: 210
- Random Walk of Greed: 160

ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

The amount of time required to complete the test (Random Walk) increased dramatically once an arbitrary number of State Machine states were included.

Experiment 2: The original OPNET network model is made simpler, which reduces the number of states.

The similar set of states has been integrated in the following manner for the goal of making the state machine mode more straightforward.

- (ACK SEND, ACCEPT CONF) => ACCEPT
- PEND SEND => (PEND SEND, PEND CONF)
- (ACK RCV, RXDN) => RXDN
- (BRx, BRxON) => BRxRXON
- (BTxTXON) => (BTxTX, BTxTX, BTxCONF)

The following is a breakdown of how long the test ran for while the network was in each of its 10 states when there were 19 interruptions, also known as events (Figure 1.4).

- Model of State Machine: 10 States, 19 Events
- Walk at Random: 170
- Random Walk of Greed: 50

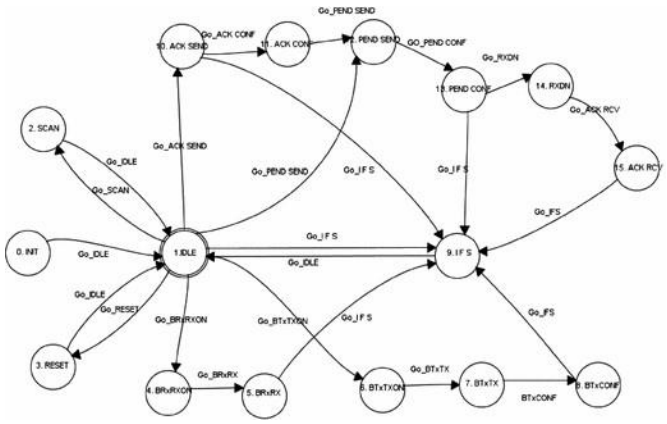

Figure 1.3 ModelJUnit's Network Layer State Machine

In an Internet of Things environment with limited resources, the length of time spent testing the network might be quite important. Experiment 2 illustrates how merging states may significantly cut down on the total number of test cases that need to be run. This is especially true for random walks that are motivated by greed. In order to reduce the total number of possible states, the OPNET state machine has to have its complexity reduced. In OPNET modeler, it is also feasible to verify that the state machine model has been simplified appropriately. The output of the OPNET simulation offers a means by which the effect of merged states may be tracked. It's possible that this might work very well as a two-way street between the generation of test cases and the simulation of networks.

ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

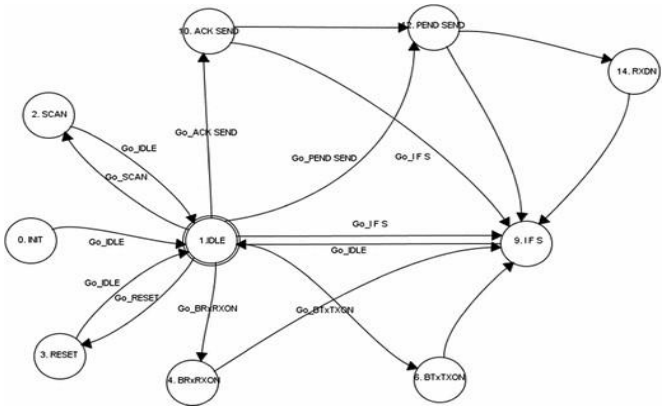

Figure 1.4 ModelJUnit's Simplified State Machine at the Network Layer

Discussion

Connecting OPNET (Optimized Network Engineering Tool) to IoT (Internet of Things) involves leveraging OPNET's capabilities to simulate and analyze IoT networks. Key aspects of this process include defining the IoT network topology, modeling traffic patterns, configuring OPNET to represent IoT devices and protocols accurately, specifying performance metrics, and evaluating network scalability. The benefits of using OPNET for IoT simulations include cost-effectiveness, rapid prototyping, the ability to model realistic scenarios, and network optimization. However, there are challenges to consider, such as achieving a balance between accuracy and simulation time, accurately simulating real-world variability, addressing protocol support limitations, and factoring in security considerations. Best practices include validation against real-world data, sensitivity analyses, comprehensive documentation, collaboration with domain experts, scaling up network size for performance assessment, and effective visualization of simulation results. This approach offers a valuable means of testing and optimizing IoT networks before deployment, ensuring their reliability and efficiency.

CONCLUSION

The Internet of Things will include a wide range of technologies, including radio-frequency identification (RFID), wireless sensor networks (WSN), and mobile ad hoc networks (OPNET), amongst others. Even while it is possible to connect a large number of devices to the internet and the internet of things utilizing a variety of communication technologies, standards, and protocols, not all of the issues have been resolved. Problems with power management, inefficiencies in energy consumption, and assaults that exploit an energy component are some of the obstacles that need further exploration. When paired with OPNET and WSN, the Internet of Things will make an even greater contribution to the development of intelligent environments than it did on its own. This is as a result of the fact that the enabling services and applications of the Internet of Things are becoming an increasingly integral part of our everyday life. This is because the Internet of Things is becoming more integrated into our daily lives in more and more ways. The Internet of Things (IoT) has difficulties as a result of the constraints imposed by these technologies as well as their inherent complexity. In order to solve the problems that now exist and shield the Internet of Things (IoT) from the myriad of possible threats that exist, inventive technical solutions need to be devised.

ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

REFERENCE

[1] S. Seneviratne et al, "A survey of wearable devices and challenges," *IEEE COMM. surveys & tutorials,* vol. 19, no. 4, pp. 2573-2620, fourth quarter 2017.

[2] K. Hartman, "Make: Wearable Electronics: Design, Prototype, and Wear Your Own Interactive Garments," *Maker Media*, Sebastopol, CA, USA, 2014.

[3] E. Sazonov and M. R. Neuman, "Wearable Sensors: Fundamentals, Implementation and Applications," *Elsevier*, Amsterdam, Netherlands, 2014.

[4] C. Nave and O. Postolache, "Smart Walker based IoT Physical Rehabilitation System," *International Symposium in Sensing and Instrumentation in IoT Era (ISSI),* Shanghai, China, 2018.

[5] G. Yang, J. Deng, G. Pang, H. Zhang, J. Li, B. Deng, Z. Pang, et al., "An IoT-Enabled Stroke Rehabilitation System Based on Smart Wearable Armband and Machine Learning," *IEEE J. Transl. Eng. Health Med.* , pp.1-10, 2018.

[6] A. Ghorbel, S. Bouguerra, N. B. Amor, M. Jallouli, "Cloud based mobile application for remote control of intelligent wheelchair," *14th International Wireless Communications & Mobile Computing Conference (IWCMC),* Limassol, Cyprus, 2018.

[7] M. Opoku, A. Al-Mahmood, "Design and implimentation of a wearable device for motivating patients with upper and/or lower limb disability via gaming and home rehabiliation," *Fouth international conference on fog and mobile edge computing* , 2019.

[8] C. F. Pasluosta, H. Gassner, J. Winkler, J. Klucken and B. M. Eskofier, "An Emerging Era in the Management of Parkinson's Disease: Wearable Technologies and the Internet of Things," *Biomedical and Health Informatics,* vol. 19, pp. 1873-1881, 2015.

[9] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," *IEEE Access,* pp. 26521-26544, 2017.

[10]S. Jayanth, M. B. Poorvi, R. Shreyas, B. Padmaja and M. P. Sunil,, "Wearable device to measure heart beat using IoT," *International Conference on Inventive Systems and Control (ICISC),* Coimbatore, 2017.

[11]K. Majumder, Y. ElSaadany, R. Young, "An Energy Efficient Wearable Smart IoT System to Predict Cardiac Arrest," *Advances in Human- Computer Interaction,* vol. 2019, 2019.

[12]A. Brezulianu, "IoT Based Heart Activity Monitoring Using Inductive Sensors," *Journal of Sensors (Basel, Switzerland)* , vol. 19, 2019.

[13]S. Milici, J. Lorenzo, A. Lázaro, R. Villarino, and D. Girbau, "Wireless breathing sensor based on wearable modulated frequency selective surface," *IEEE sensors* , vol. 17, pp. 1285-1292, 2017.

[14]S. Syed Tauhid, B. Faizan, D. Faheem, A. Nouman, & A. Jan, "Cloud- Assisted IoT-Based Smart Respiratory Monitoring System for Asthma Patients", Applications of Intelligent Technologies in Healthcare, 2019.

[15]I. Mahbub et al., "A low-power wireless piezoelectric sensor-based respiration monitoring system realized in CMOS process," *IEEE sensors,* vol. 17, pp. 1858-1864, 2017.

[16]D. N. Hernández et al., "Smart Vest for Respiratory Rate Monitoring of COPD Patients Based on Non-Contact Capacitive Sensing," *Sensors (Basel, Switzerland),* vol. 18, 2018.

[17]J. Wan, M. Al-awlaqi, M. Li, et al, "Wearable IoT enabled real-time health monitoring system," *Wireless Communnication Network* , 2018.

[18]S. Yoshida, H. Miyaguchi, T. Nakamura, "DEvelopment of tablet-shaped ingestible core-body thermometer powered by gestric acid battery," *IEEEsensors,* vol. 18, pp. 9755-9762, 2018.

ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

[19]F. Lamonaca et al., "An Overview on Internet of Medical Things in Blood Pressure Monitoring," *IEEE International Symposium on Medical Measurements and Applications (MeMeA)*, Istanbul, Turkey, 2019.

[20]D. Murali, D. R. Rao, S. R. Rao and M. Ananda , "Pulse Oximetry and IOT based Cardiac Monitoring Integrated Alert System," *International Conference on Advances in Computing, Communications and Informatics (ICACCI)* , Bangalore, 2018.

[21]B. Sargunam, S. Anusha, "IoT based mobile medical application for smart insulin regulation," *IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, Coimbatore, India, 2019.

[22]S. Yang et al., "IoT Structured Long-Term Wearable Social Sensing for Mental Wellbeing," *IEEE Internet of Things Journal*, vol. 6, pp. 3652- 3662, 2019.

[23]J. Qi, P. Yang, M. Hanneghan, S. Tang and B. Zhou, "A Hybrid Hierarchical Framework for Gym Physical Activity Recognition and Measurement Using Wearable Sensors," *IEEE internet of things journal,* vol. 6, no. 2, April 2019.

[24]E. Mencarini, A. Rapp, Lia Tirabeni, and M. Zancanaro, "Designingwearable systems for sports: a review of trends and opportunities in Humman – computer interaction," *IEEE Trans. On human machine systems,*, vol. 49, no. 4, August 2019.

[25]D. Castro, W. Coral, C. Rodriguez, J. Cabra, and J. Colorado, "Wearable- Based Human Activity Recognition Using an IoT Approach," *Journal of sensor and actuators networks,* vol. 6, no. 28, 2017.

[26]H. Huang , X. Li, S. Liu, S. Hu, and Y. Sun, "TriboMotion: A Self- Powered Triboelectric Motion Sensor in Wearable Internet of Things for Human Activity Recognition and Energy Harvesting," *IEEE Internet of Things Journal*, vol. 5, no. 6, December 2018.

[27] W. Lu, F. Fan, J. Chu, P. Jing, and Y. Su, "Wearable Computing for Internet of Things: A Discriminant Approach for Human Activity
Recognition," *IEEE Internet of Things Journal*, vol. 6, no. 2, April 2019.

[28]L. Atallah, B. Lo, R. King, and G.-Z. Yang, "Sensor positioning for activity recognition using wearable accelerometers," *IEEE Trans. Biomed. Circuits Syst.*, vol. 5, no. 4, p. 320–329, Aug. 2011.

[29]M. Mathie, B. G. Celler, N. H. Lovell, and A. C. F. Coster, "Classification of basic daily movements using a triaxial accelerometer," *Med. Biol. Eng. Comput.*, vol. 42, no. 5, p. 679–687, 2004.

[30]A. Mannini and A. M. Sabatini, "Machine learning methods for classifying human physical activity from on-body accelerometers," *Sensors j.* , vol. 10, no. 2, p. 1154–1175, 2010.

[31]K. H. Walse, R. V. Dharaskar, and V. M. Thakare, "A study on the effect of adaptive boosting on performance of classifiers for human activity recognition," *Int. Conf. Data Eng. Commun. Technol., pp. 419–429*, 2017.

[32]Y. Chen and C. Shen, "Performance analysis of smartphone-sensor behavior for human activity recognition," *IEEE Access*, vol. 5, p. 3095– 3110, 2017.

[33]Z. He and L. Jin, "Activity recognition from acceleration data based on discrete cosine transform and SVM," *IEEE Int. Conf. Syst. Man Cybern., pp. 5041–5044.*, 2009.

[34]L. Liu, S. Wang, G. Su, Z.-G. Huang, and M. Liu, "Towards complex activity recognition using a Bayesian network-based probabilistic generative framework," *Pattern recognition*, vol. 68, p. 295–309, Aug. 2017.

[35]K.-C. Liu, C.-Y. Yen, L.-H. Chang, C.-Y. Hsieh, and C.-T. Chan, "Wearable sensor-based activity recognition for housekeeping task.," *IEEE Int. Conf. Wearable Implantable Body Sensor Netw., pp. 67–70,* 2017.

ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

[36]B. Logan, J. Healey, M. Philipose, E. M. Tapia, and S. Intille, "A longterm evaluation of sensing modalities for activity recognition," *UbiComp Ubiquitous Comput., vol. 4717., pp. 483–500*, Innsbruck, Austria, 2007.

[37]S. M. Lee, S. M. Yoon, and H. Cho, "Human activity recognition from accelerometer data using convolutional neural network," *IEEE Int. Conf. Big Data Smart Comput., pp. 131–134*, 2017.

[38]M. Ermes, J. PÄrkkÄ, J. MÄntyjÄrvi and I. Korhonen, "Detection of daily activities and sports with wearable sensors in controlled and uncontrolled conditions," *IEEE Trans. Inf. Technol. Biomed.* , vol. 12, no. 1, p. 20–26, Jan. 2008.

[39]M. Li et al., "Multimodal physical activity recognition by fusing temporal and cepstral information," *IEEE Trans. Neural Syst. Rehabil. Eng.*, vol. 18, no. 4, p. 369–380, Aug. 2010.

[40]S. Liu, R. X. Gao, D. John, J. W. Staudenmayer, and P. S. Freedson., "Multisensor data fusion for physical activity assessment," *IEEE Trans. Biomed. Eng.*, vol. 59, no. 3, p. 687–696, 2012.

[41]I. C. Gyllensten and A. G. Bonomi, "Identifying types of physical activity with a single accelerometer: Evaluating laboratory-trained algorithms in daily life," *IEEE Trans. Biomed. Eng.*, vol. 58, no. 9, p. 2656–2663, 2012.

[42]Z. Wang, M. Guo and C. Zhao, "Badminton stroke recognition based on body sensor networks," *IEEE Trans. Hum.-Mach. Syst.,*, vol. 46, no. 5, p. 769–775, Oct. 2016.

[43]A. Raina, T. G. Lakshmi and S. Murthy, "CoMBaT:Wearable technology based training system for novice badminton players," *IEEE 17th Int. Conf. Adv. Learn. Technol., pp. 153–157*, 2017.

[44]J. C. Maglott, J. Xu and P. B. Shull, "Differences in arm motion timing characteristics for basketball free throwand jumpshooting via a body-worn sensorized sleeve," *IEEE 14th Int. Conf. Wearable Implantable Body Sensor Netw pp. 31–34*, 2017.

[45]S. Bogers, C. Megens, "Design for balanced engagement in mixed level sports teams," *SIGCHI Conf. Extended Abstr. Hum. Factors Comput. Syst., pp. 994–1002.*, 2017.

[46]Z. Wang, H. Zhao, S. Qiu and Q. Gao, "Stance phase detection for ZUPTaided foot-mounted pedestrian navigation system," *IEEE/ASME Trans. Mechatron*, vol. 20, no. 6, p. 3170–3181, Dec. 2018.

[47]Z. Wang, Jiaxin Wang, H. Zhao, Ning Yang and G. Fortino, "CanoeSense: Monitoring canoe sprint motion using wearable sensors," *IEEE Int. Conf. Syst., Man, Cybern., pp. 644–649*, Budapest,, 2016.

[48]J. Pansiot, B. Lo, and G. Z. Yang, "Swimming stroke kinematic analysis with BSN," *Int. Conf. Body Sensor Netw., , pp. 153–158*, Singapore, 2010.

[49]M. Bächlin, K. Förster, and G. Tröster, "SwimMaster: A wearable assistant for swimmer," *Int. Conf. Ubiquitous Comput., pp. 215–224.*, 2009.

[50] J. Häkkilä, M. Alhonsuo, L. Virtanen, J. Rantakari, A. Colley, and T. Koivumäki, "MyData approach for personal health - A service design case for young athletes," *49th Int. Conf. Syst. Sci., pp. 3493–3502*, Hawaii, 2016.

[51] Vadhwani, Diya & Singh, Megha; Kulhare, Deepak. (2019). Enhanced DSR with optimized throughput using opnet simulator. 1-4. 10.1109/NUiCONE.2013.6780100.

[52] Xu, C., & Wang, X. (2019). Transient content caching and updating with modified harmony search for Internet of Things. Digital Communications and Networks, 5(1), 24-33.

[53] Liu, G.; Cai, X. & Li, Y.. (2015). OPNET modeling and optimization simulation of mobile RFID system. Journal of Computational Information Systems. 11. 701-709. 10.12733/jcis13116.

ISSN: 2278-4632
Vol-14 Issue-02 Oct 2024

[54] Kosunalp, S. MAC Protocols for Energy Harvesting Wireless Sensor Networks: Survey. ETRI J. 2015, 37, 804–812.

[55] Fu, C.; Jiang, Z.; Wei, W.E.I.; Wei, 2019 A. An Energy Balanced Algorithm of LEACH Protocol in WSN. Int. J. Comput. Sci. Issues , 10, 354.

[56] Sreedevi, I.; Mankhand, S.; Chaudhury, S.; Bhattacharyya, 2013 A. Bio-Inspired Distributed Sensing Using a Self-Organizing Sensor Network. J. Eng. , 2013, 1–16.

[57] Srinidhi, N. N., Kumar, S. D., & Venugopal, K. R. (2018). Network optimizations in the Internet of Things: A review. Engineering Science and Technology, an International Journal.

[58] Tadayon, N.; Khoshroo, S.; Askari, E.; Wang, H.; Michel, H. 2018 Power management in SMAC-based energy-harvesting wireless sensor networks using queuing analysis. J. Netw. Comput. Appl. , 36, 1008–1017.

[59] Talavera JM, et al. 2017 Review of IoT applications in agro-industrial and environmental fields. Comput Electron Agric.;142(7):283–97.

[60] Wu, Y.; Wu, Y.; Guerrero, J.M.; Vasquez, J.C.; Palacios-García, E.J.; Guan, 2020 Y. IoT-enabled Microgrid for Intelligent Energy-aware Buildings: A Novel Hierarchical Self-consumption Scheme with Renewables. Electronics , 9, 550.

[61] Xu, C., & Wang, X. (2019). Transient content caching and updating with modified harmony search for Internet of Things. Digital Communications and Networks, 5(1), 24-33.

[62] Zhang, C., Zeng, G., Wang, H., & Tu, X. (2019). Hierarchical resource scheduling method using improved cuckoo search algorithm for internet of things. Peer-to-Peer Networking and Applications, 1-9.

[63] Zhu, Kai & Liu, Jia & Gao, Xue & An, Yong; Xiong, Qiang. (2021). Campus Network Upgrade and Optimization Based on OPNET. Applied Mechanics and Materials. 263-266. 1356-1359.10.4028/www.scientific.net/AMM.263-266.1356.