

Retrofitted IoT Based Communication Network with Hot Standby Router Protocol and Advanced Features for Smart Buildings

G. Pradeep Reddy^{ID}, Y. V. Pavan Kumar^{ID}

School of Electronics Engineering, VIT-AP University, Amaravati-522237, Andhra Pradesh, INDIA

(pradeep.19phd7025@vitap.ac.in, pavankumar.yv@vitap.ac.in)

[‡]Corresponding Author; Y. V. Pavan Kumar, VIT-AP University, Amaravati-522237, Andhra Pradesh, INDIA

Tel: +91863-2370155, pavankumar.yv@vitap.ac.in

Received: 15.07.2021 Accepted: 18.08.2021

Abstract - The use of renewable energy sources near the load centres brought the concept of building power systems. Further, the modern smart buildings increase operational efficiency, safety, and consumer comfort, where, all the operations are monitored/controlled by central monitoring and control unit (CMCU). For reliable communication between the components of smart building and the CMCU, a well-established network with advanced features such as user alerts, usage details, remote control, link failure handling, security, etc., is essential. However, the conventional IoT network can't provide all these features, especially the fault tolerance, where, communication failure is usually observed in remote control operations when there exists any link failure. This is the major drawback of conventional networks. To overcome this issue, this paper proposes a retrofitted IoT based communication network with Hot Standby Router Protocol (HSRP) for remote monitoring and control of smart building devices. This proposed network provides a redundant path during the link failures, thereby ensures reliable communication in the network. This is the major contribution of this paper. Besides, this network possesses advanced features viz., Adaptive Security Appliance (ASA) firewall to provide intrusion prevention (blocking unauthorized packets), Message Queuing Telemetry Transport (MQTT) protocol to enable the broker for broadcasting messages to all the subscribers of a particular topic, and email alert to provide communication between different users. Altogether, this proposed communication network enhances the reliability of smart buildings, which is simulated and verified using Cisco Packet Tracer 7.3.1. The results show that the proposed HSRP based network performance is better than the conventional network.

Keywords Smart Buildings, Internet of Things (IoT), Hot Standby Router Protocol (HSRP), Adaptive Security Appliance (ASA) firewall, Message Queuing Telemetry Transport (MQTT), Central Monitoring and Control Unit (CMCU).

1. Introduction

In the present-day scenario, with the growing population and their electricity needs/expectations, the power consumption is also growing rapidly. Thus, an imbalance has been created in the power generation and consumption parity which is a major cause of power grid outages. In the traditional fossil fuel-based macrogrid scenario, the power flow is unidirectional, i.e., from the grid to load, which makes the metering process easy. Whereas, with the evolution of renewable/alternative sources of energy, the scenario is moving towards localized energy generation through the formation of microgrids at the customer premises

(domestic, industrial, etc., buildings). In such buildings, the power flow is bidirectional, which requires smart metering infrastructure to record the bidirectional data. This makes the system smarter and helps to optimally utilize the energy availability while providing superior benefits and features to the consumers. Further, the use of information and communication technology (ICT) establishes effective communication between various components of the smart building [1]. In line with this, a detailed review of the major issues with the ICT application to smart grids was presented in [2] and a discussion on the challenges faced by communication networks and information security were given in [3].

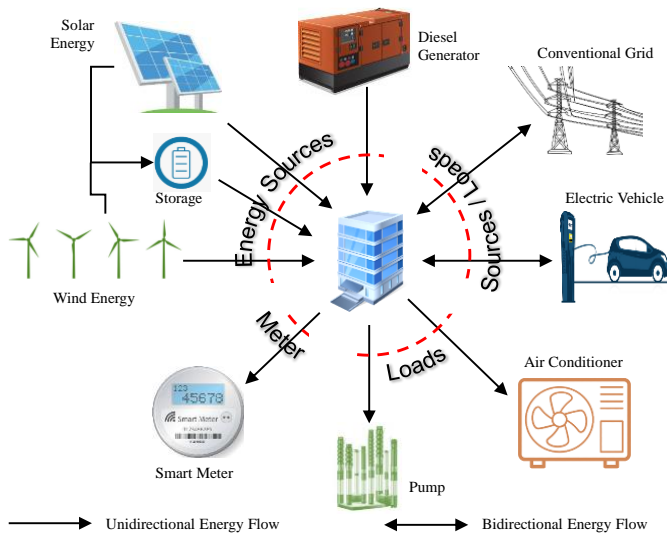


Fig. 1. Typical elements connected to a smart building.

The typical elements of any such smart building are loads, generating units (renewable energy, conventional grid, diesel generator, etc.), metering infrastructure, etc., as shown in Fig. 1. All these elements are communicated with the central monitoring and control unit (CMCU) to record the timely data of the demand and supply. The CMCU monitors the energy consumption details of each appliance/equipment of the building and executes the informed decisions to optimize the energy consumption of the building. These smart building microgrids can operate in standalone mode or integrated mode with respect to the utility grid based on the availability and requirement of the energy to serve the building load [4]. As the power generation capacity of these microgrids depends on environmental conditions, a storage facility is used to serve the building loads during uncertainties. This way, these microgrids can help in reducing the burden on the utility grids. However, the effective operations of such smart buildings depend on the establishment of a reliable communication network [5, 6]. In this view, various attempts were made in the literature as discussed follows.

Several network architectures and standards used for the information exchange are detailed in [7-10]. Important IEEE and IEC standards that are needed for smart grid communication and networking are discussed in [11]. These networks consist of various sensors, controllers/processors and actuators which collect and process the data to make decisions [12]. Microgrid uses network components like a gateway, switches, etc., to transfer the data between various components [13]. Further, to manage all the assets of the microgrid, an asset management system was recommended in [14]. Home automation can be achieved by integrating all the appliances, embedded controllers such as Raspberry Pi, NodeMCU, etc., using an internet facility [15, 16]. This IoT feature facilitates the user to control various appliances present in the home [17]. Zigbee can also be used for establishing communication between various components in wireless sensor networks. Further, a received signal strength indicator (RSSI) based indoor localization was discussed in [18]. The energy requirement of the home is not constant all the time, so, to manage the supply and need, AI techniques








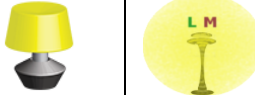

















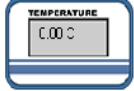
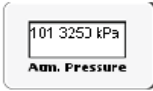










were used to predict the energy requirement and price of the energy [19, 20]. Similarly, a dynamic distributed energy storage strategy was discussed in [21], which enables the optimal utilization of the stored energy during peak hours. Also, it is identified that the game theory approach helps in achieving competitive prices, where, various users can participate in the energy market [22]. Various challenges faced during the connectivity of different components of the smart home were discussed in [23]. A special mention to energy thieves by proposing a smart energy theft detection system was presented in [24].

The advent of various simulation tools encourages researchers to study various aspects to support smart building deployments. Among all such tools, Cisco Packet Tracer is one of the simple and effective tools. The new IoT feature in this tool enabled the researchers to work on various simulations related to smart homes. The tool is equipped with various components (sources, loads, etc.) with the registration server capability. The environment can be changed in the tool based on the user requirement. Numerous IoE (Internet of Everything) devices are connected to the microcontroller unit (MCU) to achieve smart home operation [25]. This MCU can be programmed using Python or Java [26]. DSL Modem can be used to have the connection between the cloud and the home gateway [27]. The smart home operation by considering the four places (living room, kitchen, incoming door, and garage) was discussed in [28]. A similar analysis by connecting all the IoE devices of smart homes to derive the optimal control operations were discussed in [29-32].

Though there were few works exist in the literature for the communication establishment in the building power systems, some of the key features such as reliability, optimization, security, etc., were not addressed. These are continuously posing challenges in the implementation of smart building microgrids. With this motivation, this paper proposes a retrofitted IoT based communication network with Hot Standby Router Protocol (HSRP) and advanced features (intrusion prevention, broadcasting messages, and email alerts) for smart buildings. The HSRP based proposed network provides a redundant path during the link failures, thus provides reliable communication for remote monitoring and control of smart buildings. All the abovementioned desired features are achieved through Adaptive Security Appliance (ASA) firewall, Message Queuing Telemetry Transport (MQTT) protocol, and Email services respectively. Altogether, this is a novel contribution discussed in this paper towards the smart buildings' research to establish an effective communication network for local and remote load management.

The rest of the paper is organized as follows to explain the proposed concept and its implementation. Section.2 describes the case study of a smart building. Section.3 describes the implementation of the proposed system with its features such as remote control operations through HSRP, security through ASA firewall, MQTT protocol, email alerts, etc. Section.4 presents the analysis of simulation results observed with the proposed system. Finally, Section.5 gives the salient achievements of the paper. It also provides key limitations of the work and suggests possible future scope.

Table 1. Various components used for the implementation of smart building

Sources			
			
Solar Panel	Wind Turbine	Battery	Power Meter
Essential Equipment			
			
Air Conditioner	Fan	Door	Smart Lights
			
Garage Door	Window	Appliance	Smart LED
Accessory Equipment			
			
Home Speaker	Bluetooth Music Player	Humidifier	Blower
			
Lawn Sprinkler	Water Drainer	Water Level Monitor	
Safety and Protection Equipment			
			
Carbon Dioxide Detector	Carbon Monoxide Detector	Smoke Detector	Siren (Works in on/off modes)
			
RFID Reader	Humidity Monitor	Temperature Monitor	Atmospheric Pressure Monitor
			
Fire Monitor	Motion Detector	Webcam	Fire Sprinkler
Testing Equipment			
			
Old Car (releases smoke-CO ₂ , CO)	RFID Card	Push Button Toggle Switch	Heating Element
			
Push Button	Rocker (On/Off) Switch		

2. Case Study Description

To implement the proposed system, a case study of a multi-floored building is considered. The components of this building are connected to the CMCU as shown in Fig. 2. The list of all such components considered in this case study to implement the proposed network is given in Table 1. All these components are divided into five categories as mentioned follows.

- i) Sources (solar panel, wind turbine, battery, and power meter).
- ii) Essential equipment (air conditioner, fan, door, smart lights, garage door, window, appliance, and smart LED).
- iii) Accessory equipment (home speaker, Bluetooth music player, humidifier, blower, lawn sprinkler, water drainer, and water level monitor).
- iv) Safety and protection equipment (carbon dioxide detector, carbon monoxide detector, smoke detector, siren, RFID reader, Humidity monitor, temperature monitor, atm pressure monitor, fire monitor, motion detector, webcam, and fire sprinkler).
- v) Testing equipment (old car, RFID card, heating element, push-button toggle switch, push-button, and rocker switch).

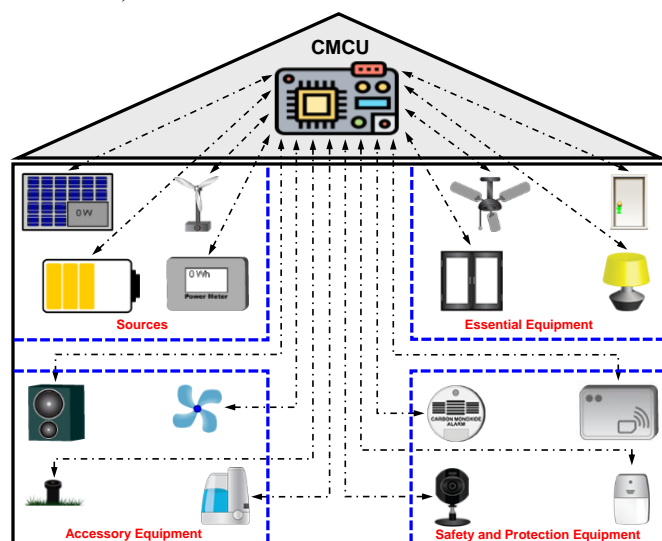


Fig. 2. Information exchange between various sources and loads in a smart building.

3. Proposed System Implementation

The proposed system implementation is carried out through Cisco Packet Tracer 7.3.1 simulation tool. This tool is equipped with various IP based components as given in Table 1, that can be used for establishing any network scenario. Out of all these components, routers, switches, and gateways are the key components for communication network studies related to smart building research. Besides, the performance of the network depends on selection of suitable interconnection cables. So, this tool provides various types of connection cables such as console, copper straight-through, copper cross-over, optical fiber, phone, coaxial, serial DCE, serial DTE, octal, IoT custom cable, and USB

cable. All these have specific application and purpose. Further, the logical and physical workspaces are available in the tool, where customized scenarios can be built.

The communication network is established with all the proposed features using the abovementioned components for the smart building. The implemented simulation network is shown in Fig. 3 with respect to implementation steps described in Table 2. As shown in Fig. 3, all the components are connected to the home gateway through a wireless interface. These components can be operated locally or remotely. The local operation of all these components can be done using a smartphone (which is connected to the home gateway) and also data is stored in a local server for further operations. All the proposed features are explained in the following subsections. Besides, various conditions given in Fig. 4 were implemented in the system to understand the efficacy of proposed concepts.

Table 2. Implementation steps for system simulation

- Step-1: Consider the home gateway in the simulation tool, and set SSID and Authentication key (Default IP assigned is 192.168.25.1/24).
- Step-2: Place all the other required components in the logical space as shown in Fig. 3.
- Step-3: Enable the wireless facility to all the components by changing the network adaptor settings.
- Step-4: Connect all the components to the home gateway by following the navigation "Component > Advanced > Config > IoT Server > Home gateway".
- Step-5: Enter the SSID and Authentication key in all the components by following the navigation "Component > Advanced > Config > Wireless". Thus, all the components are connected to the home gateway and get assigned with IPs.
- Step-6: Once the connection establishment of all the components to the home gateway gets over, place the smartphone in the logical space and enter SSID and Authentication key to get connected.
- Step-7: Connect the server to the home gateway wirelessly by entering the SSID and Authentication key.
- Step-8: Open the smartphone by following the navigation "Smartphone > IoT Monitor > Enter IP".
- Step-9: Enter the login credentials of the home gateway to access the components connected in the logical space.
- Step-10: The conditions (ex: turning on/off the devices based on set threshold levels, as given in Fig. 4) can be written in the smartphone based on the requirement.

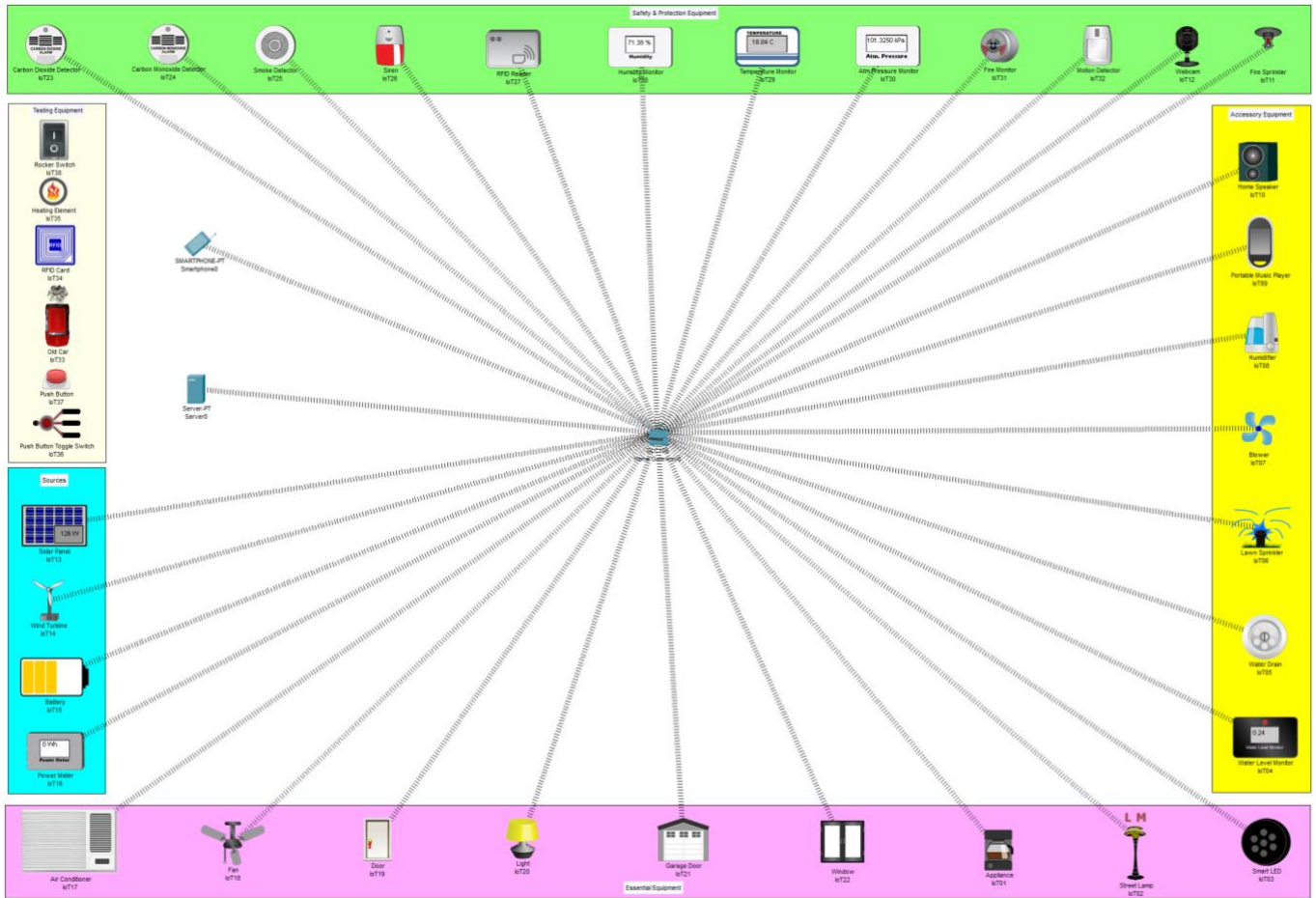


Fig. 3. Simulation model of the proposed smart building network.

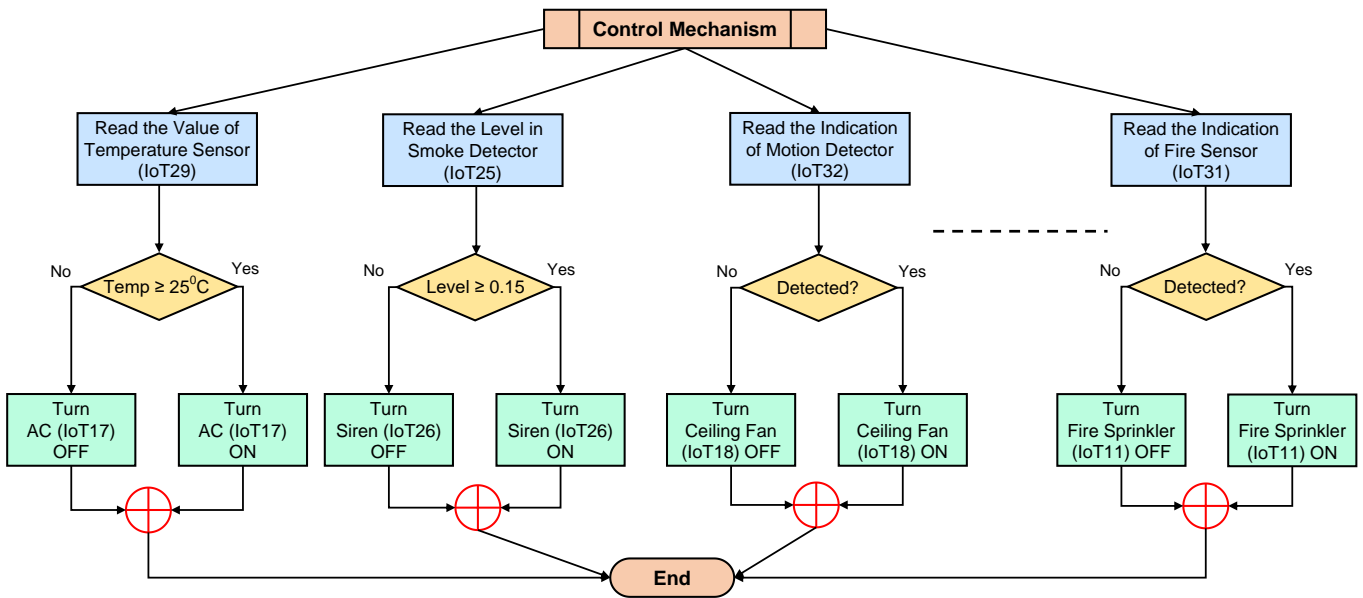


Fig. 4. Various test conditions implemented in the system.

3.1. Remote Control Operations Over HSRP Configuration

To access the components remotely, an additional network is required to be connected to the building given in Fig.3. Conventionally, this additional network has been implemented as shown in Fig. 5, which is formed with ASA

firewall, Internet Service Provider (ISP) router, central-office-server, cell-tower, and the user (with a smartphone). The smartphone (connected via 3G/4G to the cell tower) that is present in the remote location can access the components present in the building. The network operations are simulated as per the implementation steps described in Table 3. In this

conventional network, if there is a link failure between the building server and the ISP router, then the last mile communication is lost. This is the major issue with conventional remote monitoring networks.

To avoid the abovementioned problem, this paper proposes retrofitting the conventional network with HSRP. The HSRP is a Cisco proprietary redundancy protocol that is useful when link failures occur in the network. It creates a virtual router (which physically doesn't exist) among the physically existing routers by sharing an IP address and MAC address. This virtual router helps in altering the communication paths (which are established with individual physical routers) during link failures.

Among all the communication paths, the user sets a priority path that always establishes the primary communication in the network. This priority path can be decided based on user convenience, cost-effectiveness, the distance between nodes, etc. Usually, the router corresponding to the priority path is set as active and the routers of all other paths are set as standby. Based on the requirement, some of the standby routers can also be turned as active to make the corresponding communication path as the priority.

If there is any link failure in the priority path (active router path), it automatically becomes standby and the next priority router becomes active, thereby, the packet loss can be avoided. Further, once the link is recovered, the communication paths are reset to the primary configuration (i.e., the present standby router becomes active and the active router becomes standby). This way, the HSRP provides successful communication in the network all the time.

In the proposed network shown in Fig. 6, the building server is connected to the ISP router via a network switch, priority path (with active router R1), secondary path (with standby router R2), and router R3 (to connect R1 or R2 to ISP router). Besides, a virtual router is established to alter the paths during link failures as discussed above. If there is a link failure in the priority path (i.e., network switch-to-R1-to-R3), the network shifts to the secondary path (i.e., network switch-to-R2-to-R3) for the communication establishment without any manual intervention. In this case, the active router R1 becomes standby and the standby router R2 becomes active until the priority path is restored. Thus, this approach ensures communication reliability in the network.

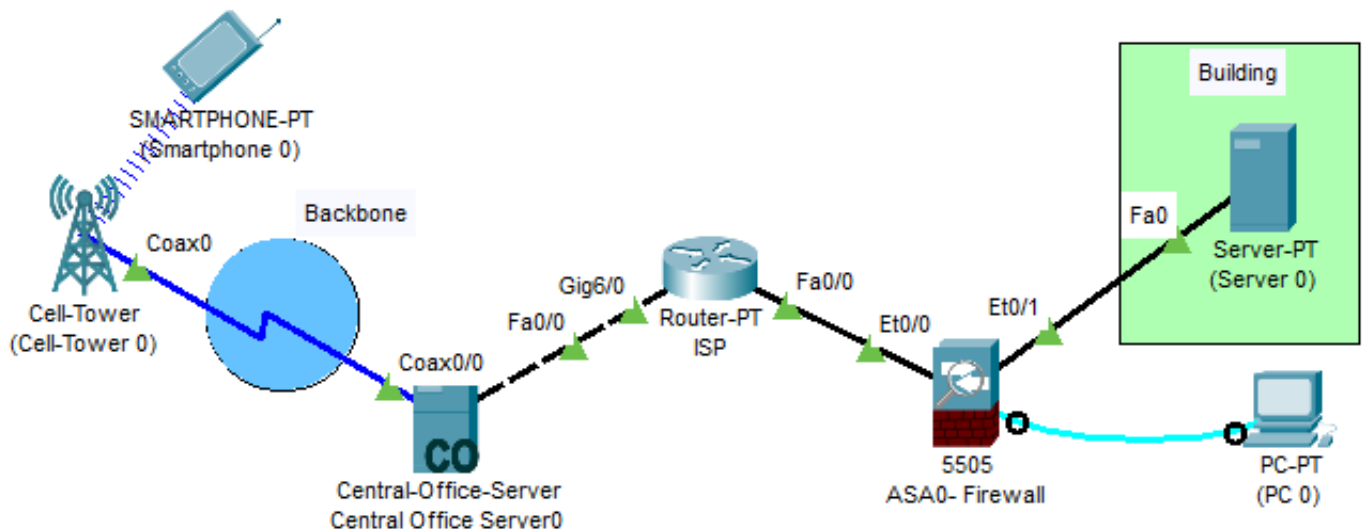


Fig. 5. Smart building's remote-control operations using the conventional network.

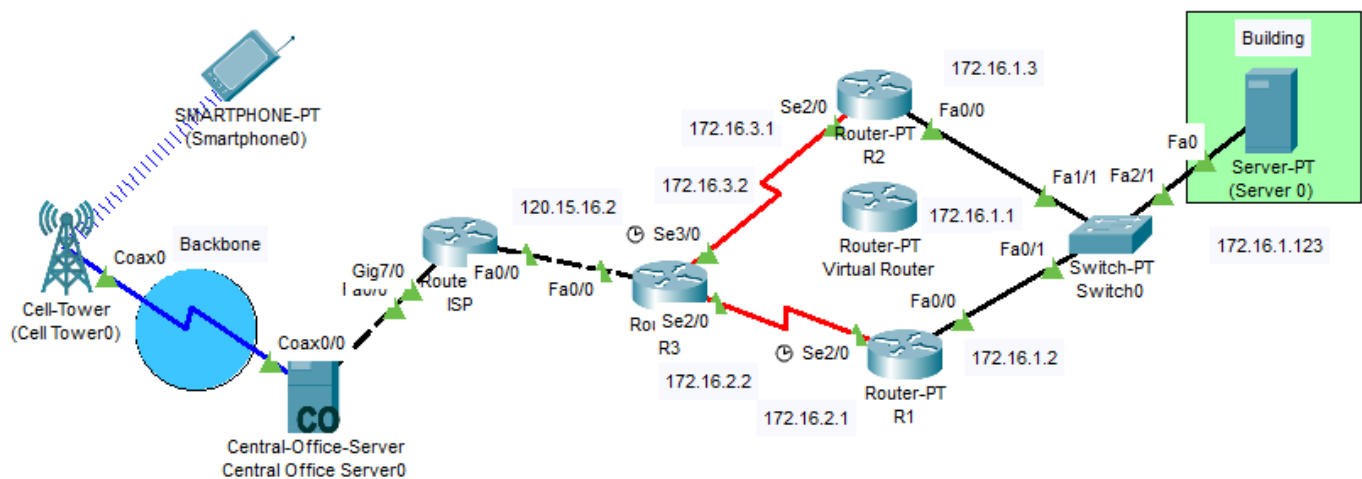


Fig. 6. Smart building's remote-control operations using the proposed HSRP based network.

Table 3. Implementation steps for remote control operations

Step-1:	Consider all the network components as shown in Fig. 5.
Step-2:	Connect Smartphone to the cell tower via 3G/4G.
Step-3:	Connect the cell tower to the central office server (backbone) using a coaxial cable.
Step-4:	Connect the server to the ISP router using a copper crossover cable.
Step-5:	Connect the ISP router to the server present in the building via the ASA firewall.
Step-6:	Configure the following network constituents i) The firewall via a PC console. ii) The components by assigning the IPs as required.
Step-7:	Access the building server remotely through the smartphone.

3.2. Security Through ASA Firewall

A firewall is a network security system that monitors the incoming and outgoing packets through it. It works based on the set of predefined rules, thereby, drops a suspicious packet. Generally, firewalls are deployed whenever there is a communication establishment required with the unknown network/outside network.

In the proposed system, the Cisco ASA 5505 firewall is used to implement an Intrusion Prevention System (IPS) as shown in Fig. 7. This controls the unauthorized user who is trying to enter into the building network. The firewall is connected between the ISP router and the building network and acts as a safety barrier between them. After configuring the vlan1 and vlan2 of the firewall, the security level has to be configured. The level of security is varied from 0 to 100, where 0 stands for high-level security and 100 stands for low-level security. Generally, low-level security is used for

inside networks and high-level security is used for the unknown network/outside network.

3.3. MQTT Protocol

Message Queuing Telemetry Transport (MQTT) is a lightweight protocol that works on publish and subscribe commands. It’s a simple way to communicate between devices with low bandwidth. The publisher can publish a message on a particular topic, where it will be broadcasted by a broker to all the subscribers who are subscribed to that particular topic. As shown in Fig. 8, the MQTT protocol is implemented in this paper to send messages to users present on different floors of the building. (e.g., topic: maintenance, publisher: engineer, subscriber: agent in each floor).

3.4. Email Alerts

A local Email server is established to send the emails to different users of the building with the domain extension. For example, in the proposed system, the domain name created for the implementation is “mybuilding.com”. This email service can be used in the building whenever a low priority communication is to be sent. The admin can assign the users by turning the Email server ‘on’. The steps for implementing the Email service in the building are given in Table 4.

Table 4. Implementation steps for enabling the email alerts

Step-1:	Get the server into the logical space and connect the users.
Step-2:	Assign IPs to all the components.
Step-3:	Turn the Email server ‘on’ by setting the domain name (mybuilding.com) and assign users with passwords as shown in Fig. 9(a).
Step-4:	At the user location, configure the emails by entering the server information (incoming and outgoing) as shown in Fig. 9(b).
Step-5:	Once the configuration is done, users can send emails to each other.

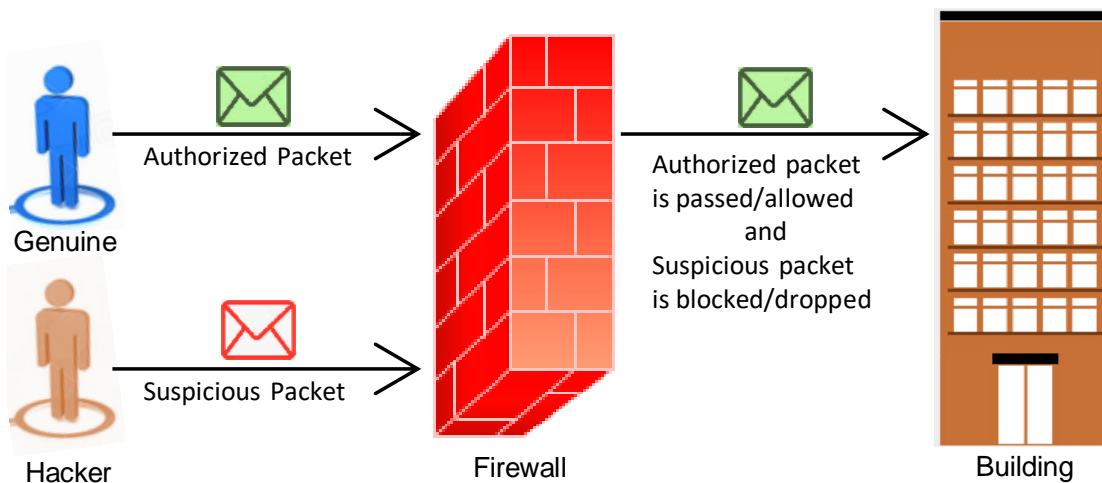
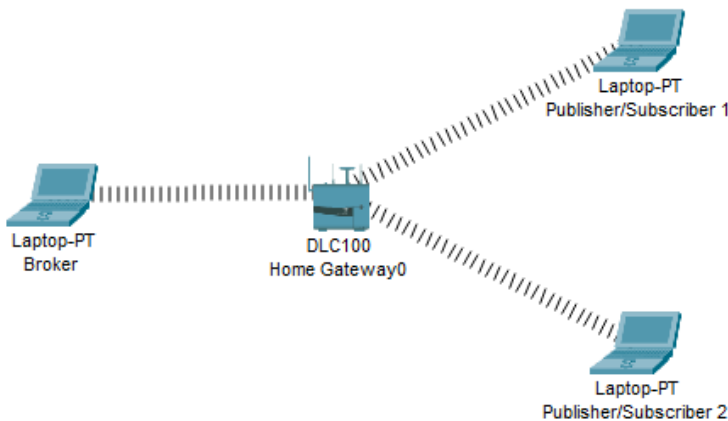
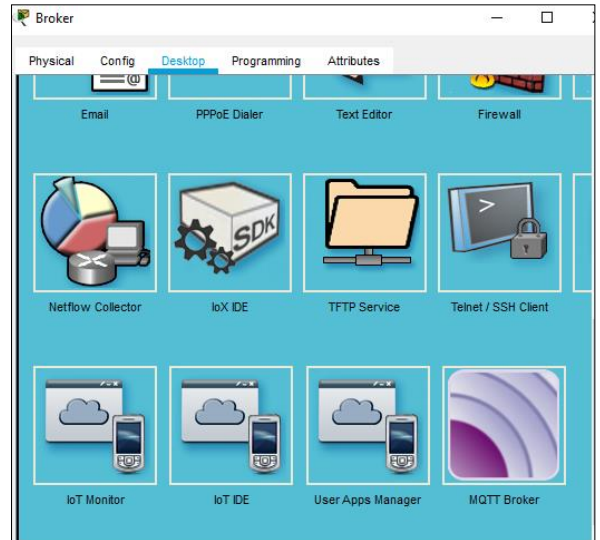


Fig. 7. Firewall connectivity scenario.

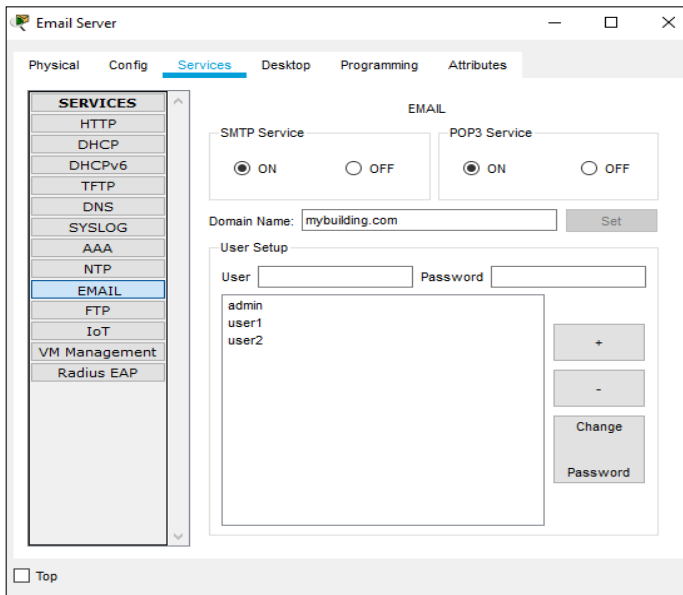


(a) Broker and publisher/subscriber connectivity

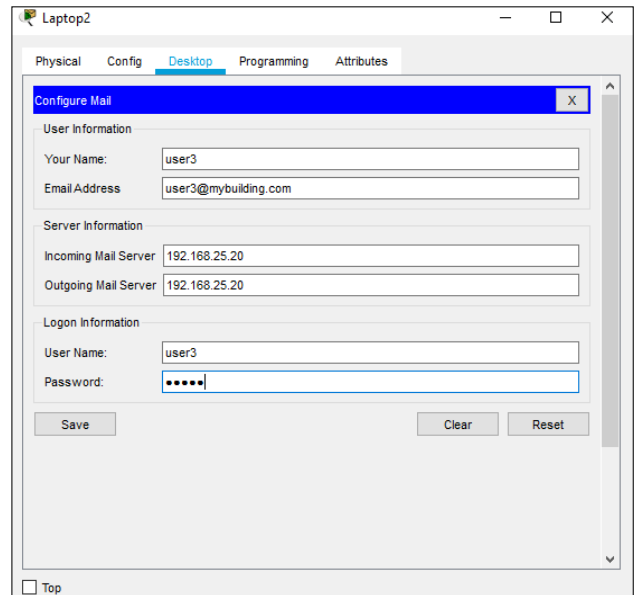


(b) MQTT broker application

Fig. 8. Implementation of MQTT protocol scenario.



(a) Assigning users at the email server



(b) Configuring the emails

Fig. 9. Implementation of Email alert.

4. Results and Analysis

To emphasize the advantage of the proposed method over the conventional method, the simulation results are segregated into two subsections described as follows. Through the detailed simulation results, these local and remote operations of the smart building are studied.

4.1. Results Pertaining to Local Operations

The objective of the local operations is to manage various components of the building using a local server. For this local management, the communication between the components is done via the home gateway. All the

components are accessed through a smartphone that is connected to this same network via SSID and Key. Fig. 10 indicates the local access of various loads and sources. Once this access is established, various conditions that are mentioned in Section.3 (Fig. 4) are tested to validate the proposed concept. The implementation of these conditions for the local operations is shown in Fig. 11 and is explained as follows.

- **Condition 1 - Turning the A.C on/off:** It works based on the temperature values monitored by the temperature monitor. The AC is turned ‘on’ if the temperature is greater than or equal to 25° C and ‘off’ if the temperature is less than 25° C.

- *Condition 2 - Turning the Siren on/off:* It works based on the smoke detector level. The siren is set to ‘on’ if the smoke detector level is greater than or equal to 0.15 and ‘off’ if the smoke detector level is less than 0.15.
- *Condition 3 - Using the RFID card and Reader:* It works for the open/close of the entry door for authorized and unauthorized user access. For this purpose, the RFID card id is assigned with a user-defined number (e.g., for the implementation, it is considered as 1001). With respect to user access, if the reader reads card id number as 1001, then the reader status is set to valid, thereby, the door will be given access (open). Similarly, if the reader reads an id number other than 1001, then the reader status is set to invalid, thereby, the door will not be given access (remains closed).
- *Condition 4 - Turning the Fan on/off:* It works based on the input from the motion detector. The Fan is turned ‘on’ if the motion detector status goes to “true” and ‘off’ if the motion detector status goes to “false”.
- *Condition 5 - Turning the Fire Sprinkler on/off:* It works based on the status read by the fire sensor. The Sprinkler is turned ‘on’ if the fire sensor detects the fire and ‘off’ if there is no fire detected.
- *Condition 6 - Turning the Water Drain on/off:* It works based on the water level measured by the water level monitor. The Water Drain is turned ‘on’ if the water level is greater than or equal to 20cm and ‘off’ if the water level is less than 20cm.

Further, to reduce the burden on the server, the MQTT protocol is implemented as part of the local management. It is a new feature added in the Cisco Packet Tracer, which can be installed from the user apps manager. The overall performance of the MQTT protocol service is measured by a parameter called “Quality of Service (QoS)”. The QoS indicates the guarantee of delivery. There are three QoS levels, which varies from 0 to 2, where, 0 indicates the lowest level of guarantee and 2 indicates the highest level of guarantee. The broker application is installed at the broker side by assigning the IP credentials. The MQTT client is installed on the users’ laptops who are located on different parts/floors of the building. Once the client is installed, it needs to establish a connection with the broker using the pre-defined credentials.

The MQTT protocol establishment is shown in Fig. 12, where, Fig. 12(a) represents the MQTT client application that is visible to publisher or subscriber, Fig. 12(b) represents the connection establishment between the broker and the publisher/subscriber, Fig. 12(c) and Fig. 12(d) represents the user screen of those who want to publish a message, Fig. 12(e) and Fig. 12(f) represents the user screen of those who subscribe to receive the messages on a particular topic (e.g., building maintenance). Besides, an email service to the users is created using the domain server name “mybuilding.com”.

The email composition and received messages (at various levels) are shown in Fig. 13.

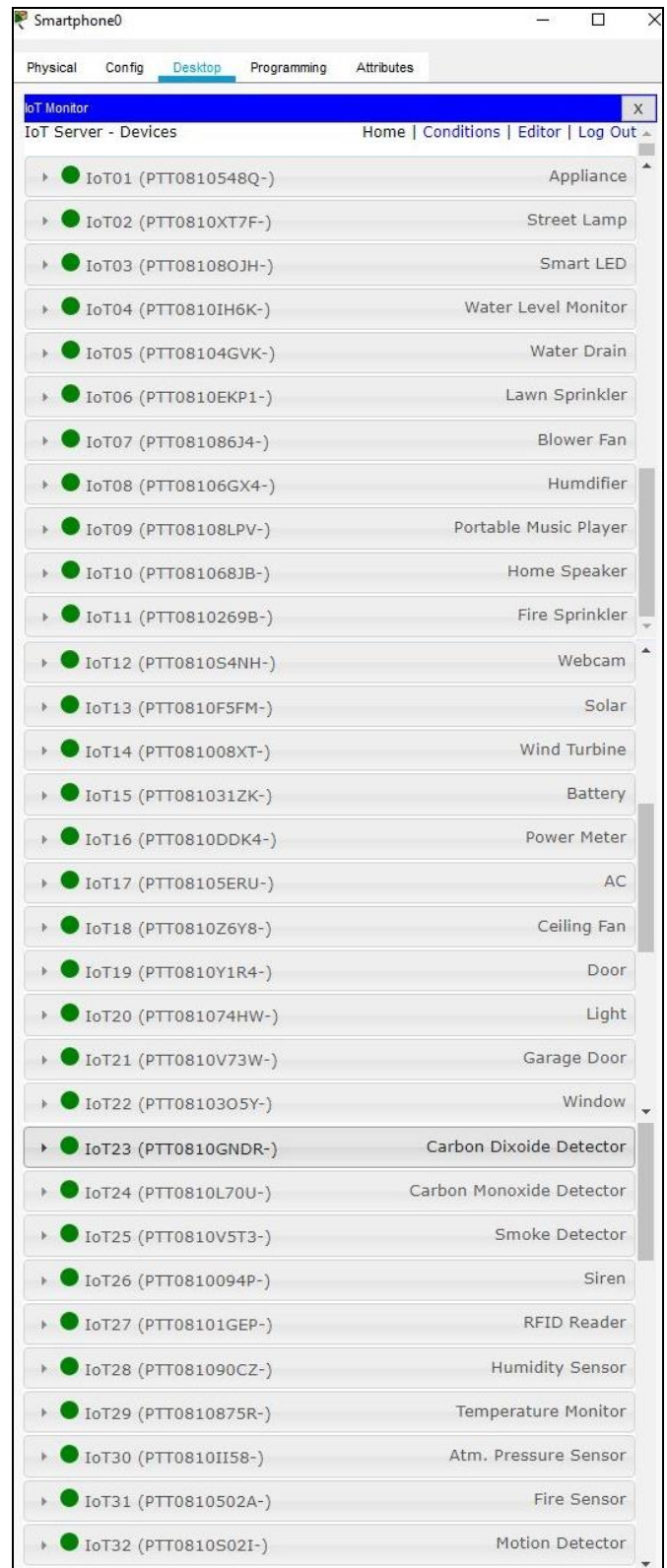
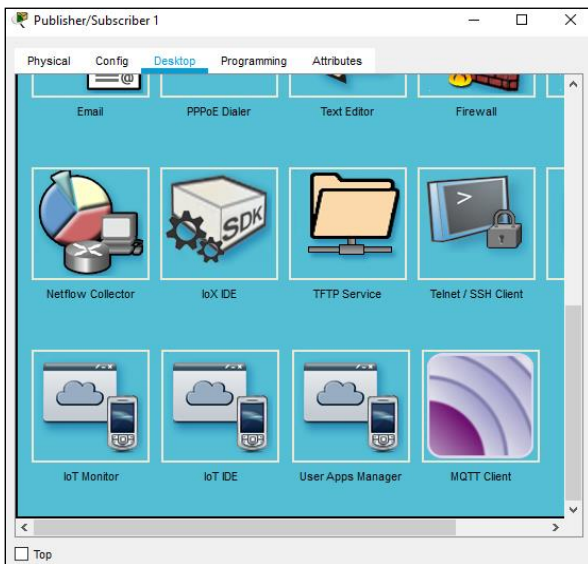


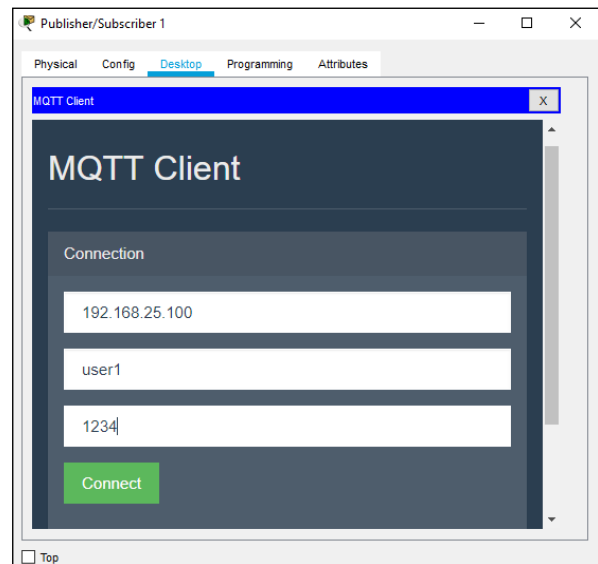
Fig. 10. Accessing the components from the smartphone for the local operations.

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	AC-on	IoT29 Temperature \geq 25.0 °C	Set IoT17 On to true
Edit Remove	Yes	AC-off	IoT29 Temperature $<$ 25.0 °C	Set IoT17 On to false
Edit Remove	Yes	Siren-on	IoT25 Level \geq 0.15	Set IoT26 On to true
Edit Remove	Yes	Siren-off	IoT25 Level $<$ 0.15	Set IoT26 On to false
Edit Remove	Yes	Reader-ok	IoT27 Card ID = 1001	Set IoT27 Status to Valid
Edit Remove	Yes	Door-open	IoT27 Status is Valid	Set IoT19 Lock to Unlock
Edit Remove	Yes	Door-close	IoT27 Status is Invalid	Set IoT19 Lock to Lock
Edit Remove	Yes	Reader-wrong entries	IoT27 Card ID \neq 1001	Set IoT27 Status to Invalid
Edit Remove	Yes	Fan-on	IoT32 On is true	Set IoT18 Status to High
Edit Remove	Yes	Fan-off	IoT32 On is false	Set IoT18 Status to Off
Edit Remove	Yes	Fire Sprinkler-on	IoT31 Fire Detected is true	Set IoT11 Status to true
Edit Remove	Yes	Fire Sprinkler-off	IoT31 Fire Detected is false	Set IoT11 Status to false
Edit Remove	Yes	Water drain-on	IoT04 Water Level \geq 20.0 cm	Set IoT05 Status to true
Edit Remove	Yes	Water drain-off	IoT04 Water Level $<$ 20.0 cm	Set IoT05 Status to false

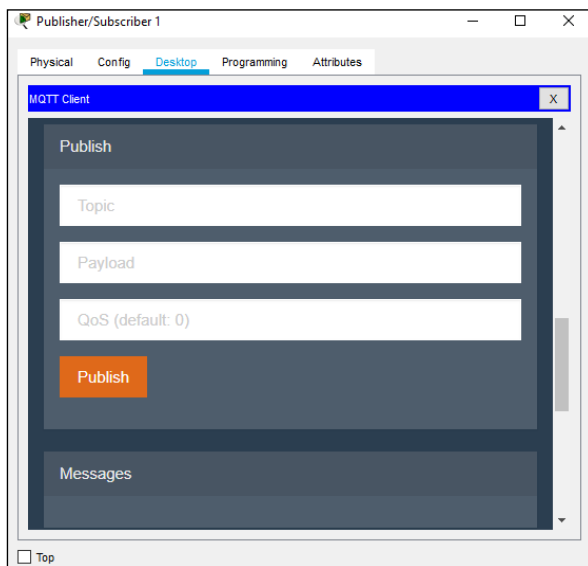
Fig. 11. Implementation of various test conditions for the local operations.



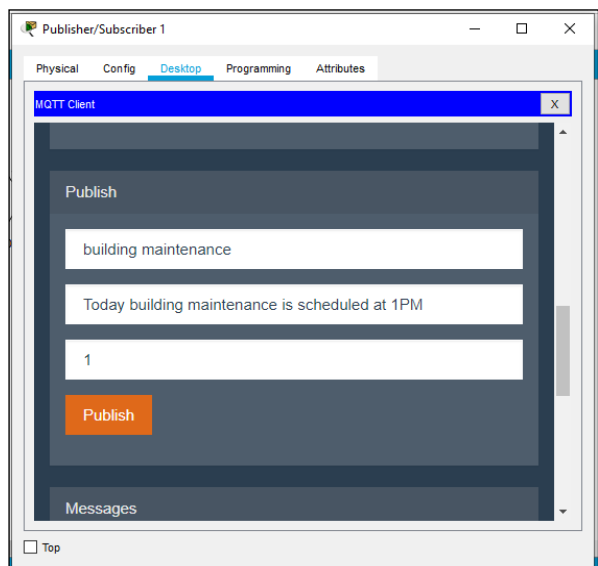
(a) MQTT client application



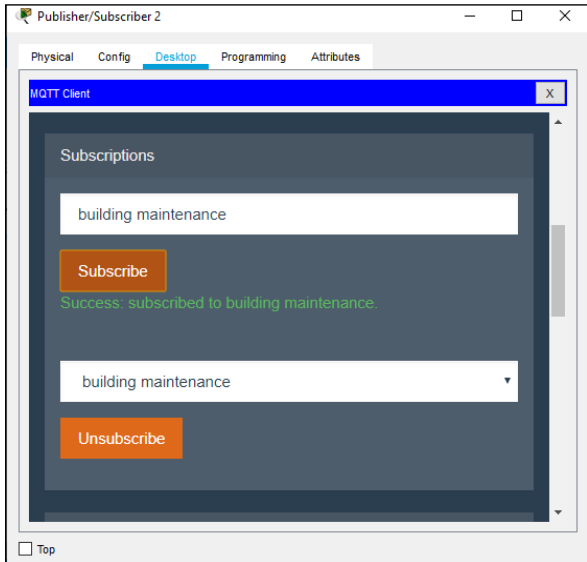
(b) Connection establishment



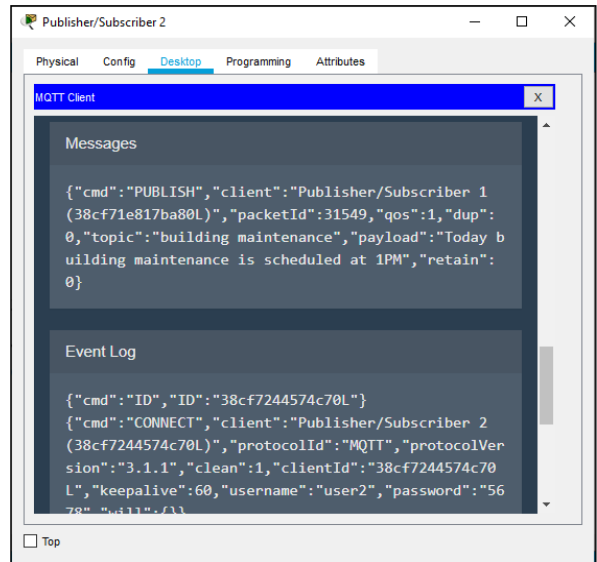
(c) Required credentials for publishing



(d) Credentials entered in the publisher

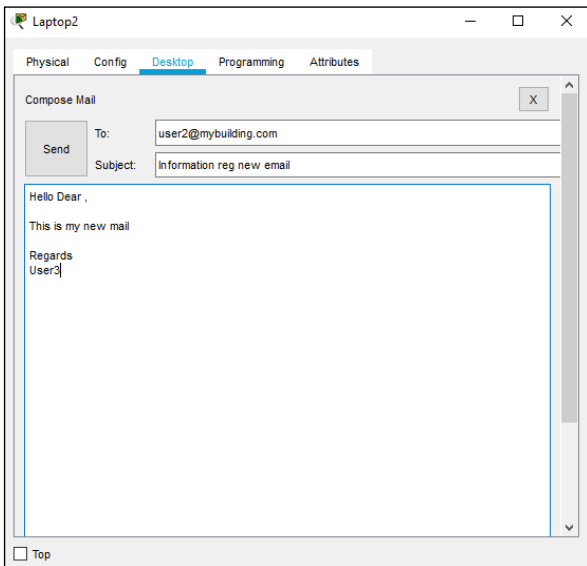


(e) Subscribing to the topic

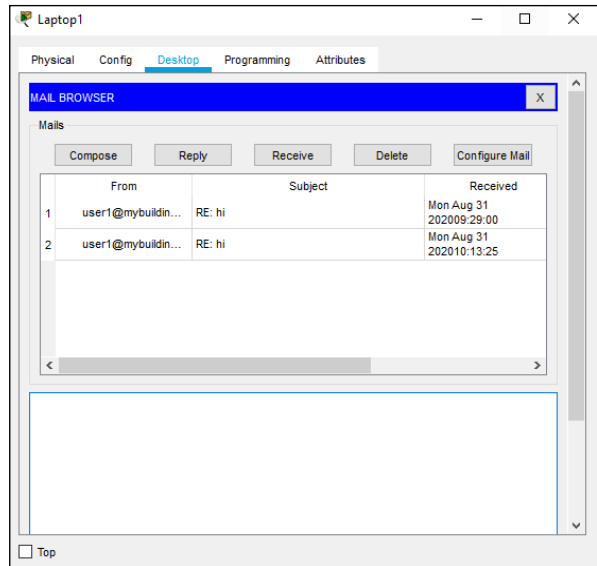


(f) Message received at the subscriber

Fig. 12. Various phases in the establishment of MQTT protocol.



(a) Email composition



(b) Received mails

Fig. 13. Various phases in the email service.

4.2. Results Pertaining to Remote Operations

The objective of the remote operations is to manage various components of the building from an external/remote location. Communication of the smart building with the remote control device is an important aspect of these networks. So, this section compares the conventional and proposed network scenarios with respect to this important aspect under various practical cases.

To validate the efficacy of the proposed HSRP network over the conventional IoT based network for remote management, the communication links are disabled and recovered at particular instants of time (e.g., a link failure is simulated at 3ms and link recovery is simulated at 5ms). The corresponding simulation results are shown in Fig. 14 to Fig.

16, where Fig. 14 shows the transmitted and received packets in the conventional network scenario, Fig. 15 shows the transmitted and received packets in the proposed HSRP based network scenario, and Fig. 16 shows the transmitted and received packets comparison in conventional and proposed networks.

In the case of a conventional network, the number of packets transmitted from sending node with respect to time is plotted as given in Fig. 14(a). From Fig. 14(b), it is seen that all these packets are lost when there is a link failure at 3ms. Further, the transmission of packets continues once the link is recovered at 5ms as shown in Fig. 14(c). Hence, from Fig. 14(d), it is understood that there is a missing of packets between the link failure and link recovery instants. This is the major issue with respect to the conventional smart building communication networks.

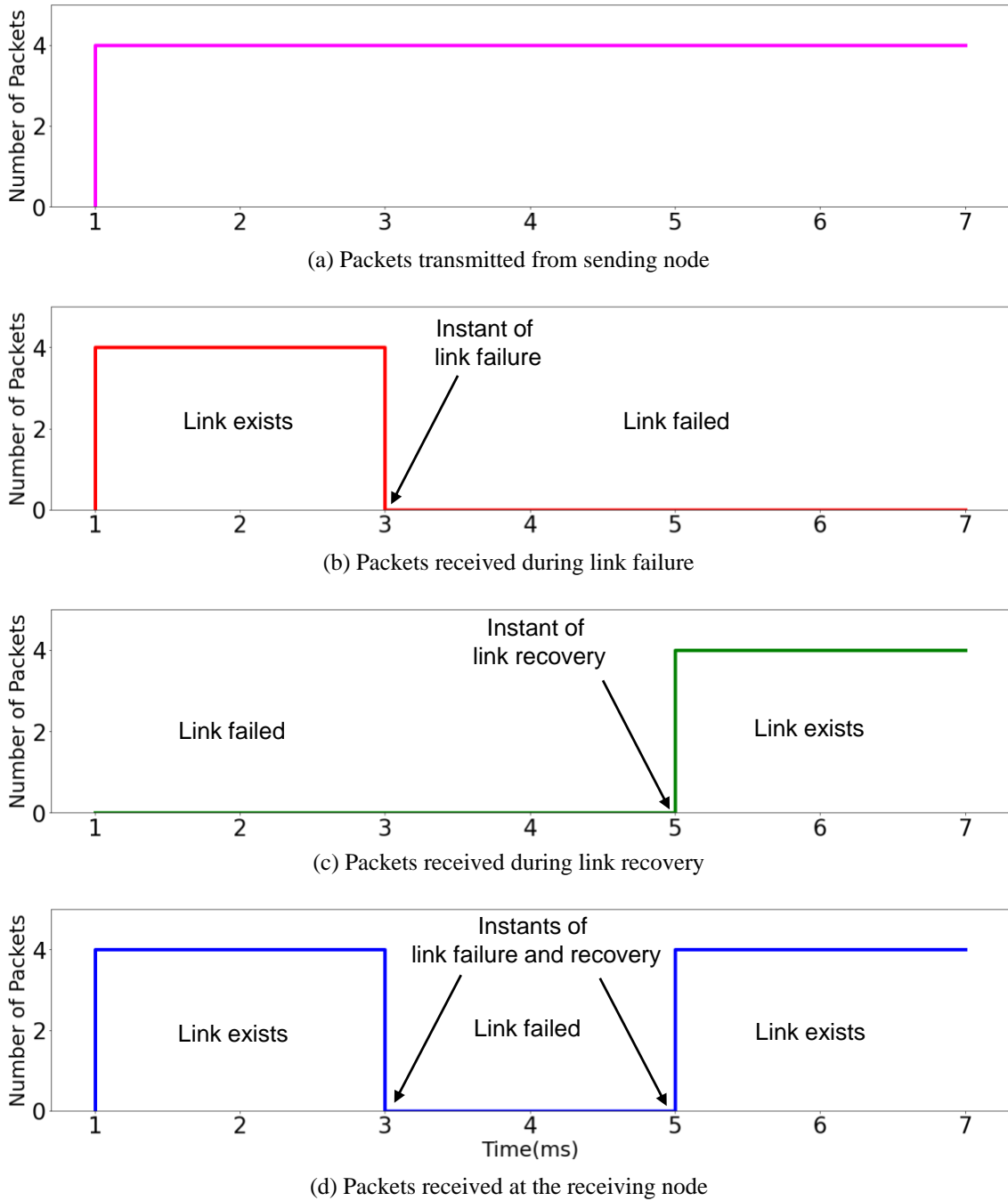


Fig. 14. Transmitted and received packets in the conventional network scenario.

The abovementioned problem of conventional networks is addressed with the proposed HSRP based communication network. In the proposed network, the number of packets transmitted from sending node with respect to time is plotted as given in Fig. 15(a). In this case, the packets are transmitted via the priority path as well as the secondary path based on the link status. Initially, when the link is active, all the packets are transmitted through the priority path set by the user (i.e., R1 is active). In this case, the other paths are deactivated (i.e., R2 is standby). However, when there is a link failure is observed in the network, the priority path will be deactivated (i.e., R1 becomes standby) and the secondary path will be activated (i.e., R2 becomes active).

The overall packets transmitted through the priority path (R1 path) and secondary path (R2 path) are shown by Fig. 15(b) and Fig. 15(c) respectively. From these plots, it is seen that the packet transmission path is automatically shifted from one path to another path during link failures, thereby, ensures the continuity of transmission to receiving node as shown in Fig. 15(d).

Finally, Fig. 16 shows the comparison of packets transmission in the conventional and proposed networks. From this, an uninterrupted transmission from sending node to receiving node has been seen using the proposed HSRP based communication network.

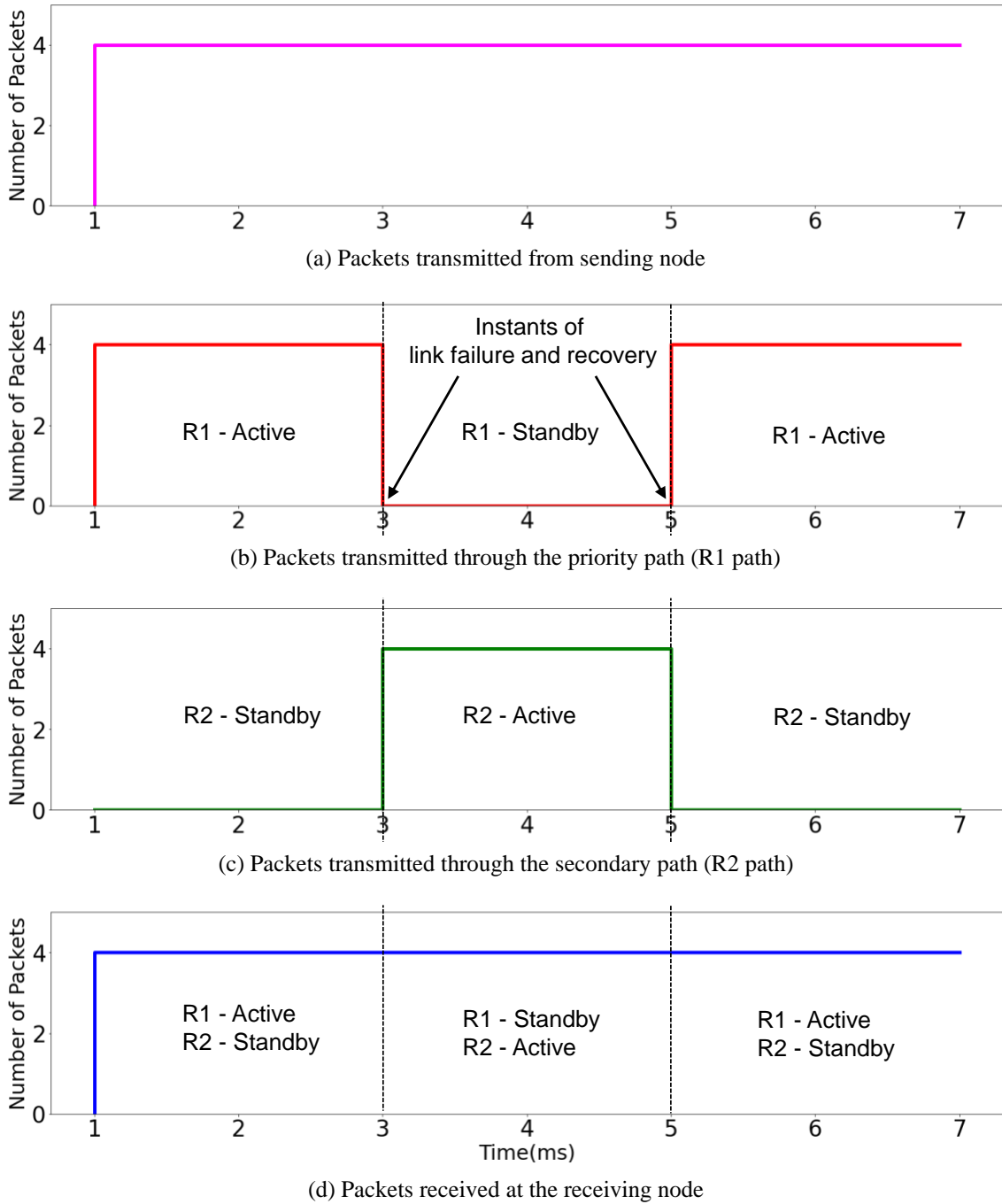


Fig. 15. Transmitted and received packets in the proposed HSRP based network scenario.

5. Conclusions

This paper proposes a reliable communication network with all the key added features that are essential for the smart building scenario. The proposed system is implemented using the Cisco Packet Tracer. The following are simulated and analyzed.

- Communication between all the components is established using a home gateway. These components are accessed through a smartphone that is connected to the home gateway (by entering SSID and key), thereby, local management is achieved.
- All the components are connected to the local server (in the building) which is connected to the external network via an ISP router, where the user from the remote location (using smartphone 3G/4G) can access the components, thereby, remote management is achieved.
- With the help of the proposed HSRP, during the link failures, the path is automatically shifted to the standby path, thereby, the last mile communication is effectively achieved.
- Cisco ASA firewall is connected between the public network (ISP) and the local network (building) which blocks unauthorized users, thereby, security is achieved.

- MQTT protocol is used in the smart building to broadcast the information to all the subscribers. This works on publish and subscribe commands. Authors successfully implemented the MQTT for publishing the maintenance of building information to all the subscribers.
- The email server is established with the domain name mybuilding.com, and emails were successfully composed and sent.

With all these abovementioned points, this paper concludes that the proposed objective is achieved, which can encourage more and more renewable energy based local and micro-power systems. This further helps in reducing the burden on the National central electric grid considerably.

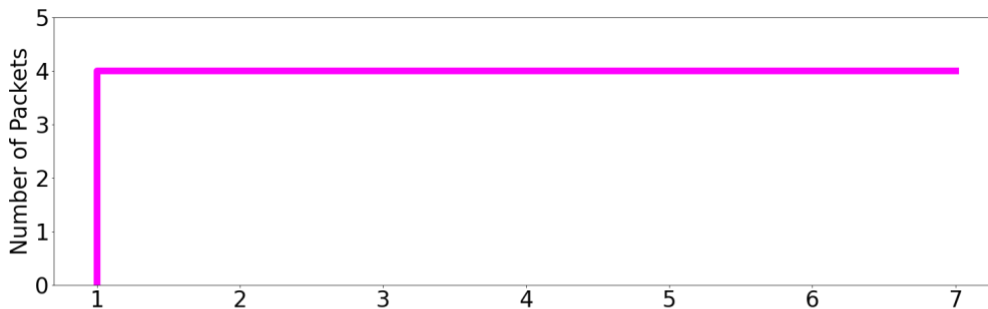
5.1. Limitations and Future Scope of the Proposed Research

The following are some of the limitations and suggested future directions for the proposed research.

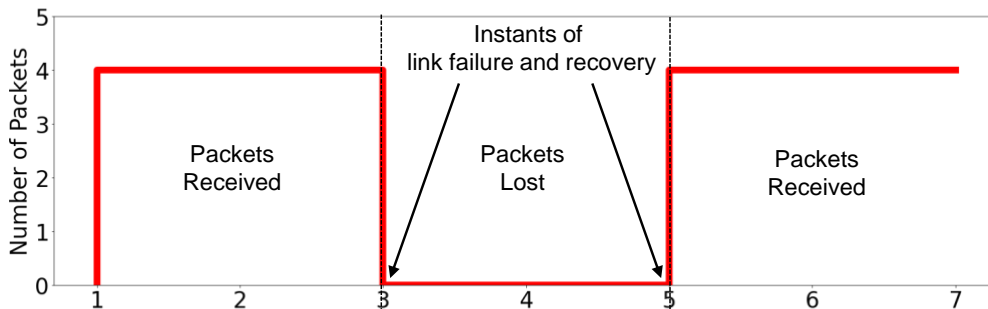
- If the number of components gets increased, it is difficult to manage with the existing gateway. So, use of high-performance gateways is required, which increases the

cost of the total system. So, in order to design a system with more components, instead of going for high-performance gateway, the whole scenario can be split into sub-scenarios and tested individually.

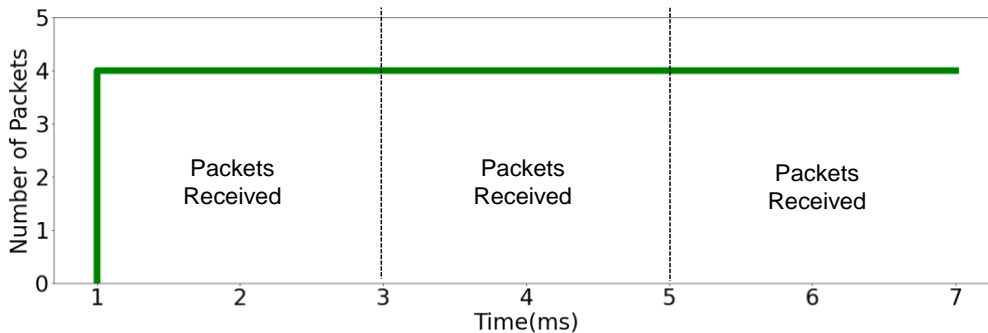
- To establish a highly reliable system, more redundant paths are usually required, which makes the network infrastructure as complex. So, optimal number of redundant paths have to be identified as a future work in this direction.
- In the real time scenario, the switch over speed during HSRP depends on the type of router. So, the real time scenario implementation can be done to understand more insights.
- More detailed packet level scenarios can be implemented with advanced network simulation tools.
- Machine learning algorithms can be used on the data collected from various appliances to estimate the power consumption of the building, to perform predictive maintenance, appliance health monitoring, etc.



(a) Packets transmitted from sending node



(b) Packets received at the receiving node in the conventional network scenario



(c) Packets received at the receiving node in the proposed network scenario

Fig. 16. Transmitted and received packets comparison in conventional and proposed networks.

Acknowledgements

This work was supported by Project Grant No: SRG/2019/000648, sponsored by the Start-up Research Grant (SRG) scheme of Science and Engineering Research Board (SERB), a statutory body under the Department of Science and Technology (DST), Government of INDIA.

References

- [1] Y. V. P. Kumar and R. Bhimasingu, "Key Aspects of Smart Grid Design for Distribution System Automation: Architecture and Responsibilities", *Procedia Technol.*, vol. 21, pp. 352–359, 2015.
- [2] I. Colak, S. Sagioglu, G. Fulli, M. Yesilbudak, and C. F. Covrig, "A Survey on the Critical Issues in Smart Grid Technologies," *Renew. Sustain. Energy Rev.*, vol. 54, pp. 396–405, 2016.
- [3] M. Yesilbudak and I. Colak, "Main Barriers and Solution Proposals for Communication Networks and Information Security in Smart Grids," 6th IEEE Int. Conf. Smart Grid, *icSmartGrids 2018*, pp. 58–63, 2019.
- [4] K. S. Rao and Y. V. P. Kumar, "Comprehensive Modelling of Renewable Energy Based Microgrid for System Level Control Studies," *Int. J. Renew. Energy Res.*, vol. 11, no. 1, pp. 223–234, 2021.
- [5] A. Bani-ahmed, A. Nasiri, and I. Stamenkovic, "Foundational Support Systems of the Smart Grid: State of the Art and Future Trends," *Int. J. SMART GRID(ijSmartGrid)*, vol. 2, no. 1, pp. 1–12, 2018..
- [6] V.J.kakeu, A. T. Boum and C. F. Mbey, "Optimal Reliability of a Smart Grid," *Int. J. SMART GRID(ijSmartGrid)*, vol. 5, no. 2, pp. 74-82, 2021.
- [7] S. M. S. Hussain, A. Tak, T. S. Ustun, and I. Ali, "Communication Modeling of Solar Home System and Smart Meter in Smart Grids", *IEEE Access*, vol. 6, pp. 16985–16996, 2018.
- [8] Y. V. P. Kumar and B. Ravikumar, "Review and Refined Architectures for Monitoring, Information Exchange, and Control of Interconnected Distributed Resources", *Progress in Systems Engineering. Advances in Intelligent Systems and Computing*, 2015, pp. 383–389.
- [9] Y. V. Pavan Kumar and R. Bhimasingu, "Review and Retrofitted Architectures to Form Reliable Smart Microgrid Networks for Urban Buildings", *IET Networks*, vol. 4, no. 6, pp. 338–349, Nov. 2015.
- [10] G. Chugulu, F. Simba, and S. Lujara, "Proposed Practical Communication Architecture for Automatic Fault Detection and Clearance in Secondary Distribution Power Network," *Int. J. SMART GRID(ijSmartGrid)*, vol. 4, no. 4, pp. 164–175, 2020.
- [11] G. P. Reddy and Y. V. Pavan Kumar, "Smart Grid Communication and Networking: Review of Standards," 2021 International Conference on Applied and Theoretical Electricity (ICATE), pp. 1-6, 2021.
- [12] U. Zafar, S. Bayhan, and A. Sanfilippo, "Home Energy Management System Concepts, Configurations, and Technologies for the Smart Grid," *IEEE Access*, vol. 8, pp. 119271–119286, 2020.
- [13] U. Ahsan and A. Bais, "Distributed Smart Home Architecture for Data Handling in Smart Grid," *Canadian Journal of Electrical and Computer Engineering*, vol. 41, no. 1, pp. 17-27, winter 2018.
- [14] Y. V. Pavan Kumar, "Overview on Role of Asset Management Systems for Smart Microgrids," *International Journal of Scientific & Technology Research*, vol. 8, no. 11, pp. 2082–2092, 2019.
- [15] W.A. Jabbar, T.K. Kiran, R.M. Ramli, S.N. Zubir, N.M. Zamrizaman, M. Balfaqih, V. Shepelev and S. Alharbi, "Design and Fabrication of Smart Home with Internet of Things Enabled Automation System," *IEEE Access*, vol. 7, pp. 144059-144074, 2019.
- [16] M.M Rafique, "Design and Economic Evaluation of a Solar Household Electrification System," *Int. J. SMART GRID(ijSmartGrid)*, vol. 2, no. 2, pp. 135–141, 2018.
- [17] A. Khan, A. Al-Zahrani, S. Al-Harbi, S. Al-Nashri and I. A. Khan, "Design of an IoT Smart Home System," 2018 15th Learning and Technology Conference (L&T), pp. 1-5, 2018.
- [18] V. Bianchi, P. Ciampolini, and I. De Munari, "RSSI-Based Indoor Localization and Identification for ZigBee Wireless Sensor Networks in Smart Homes," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 2, pp. 566–575, Feb. 2019.
- [19] C. M. Lin and M. T. Chen, "Design and Implementation of a Smart Home Energy Saving System with Active Loading Feature Identification and Power Management," 2017 IEEE 3rd International Future Energy Electronics Conference and ECCE Asia (IFEEC 2017 - ECCE Asia), pp. 739-742, 2017.
- [20] W. Li, T. Logenthiran, V. Phan and W. L. Woo, "Implemented IoT-Based Self-Learning Home Management System (SHMS) for Singapore," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2212-2219, June 2018.
- [21] N. T. Mbungu, R. C. Bansal, and R. M. Naidoo, "Smart Energy Coordination of Autonomous Residential Home," *IET Smart Grid*, vol. 2, no. 3, pp. 336–346, Sep. 2019.
- [22] H. R. Mansouri, B. Mozafari, S. Soleymani, and H. Mohammadnezhad, "Using Game-Theory to Implement an IoT re-Phasing Algorithm in Smart Grids," *Int. J. Renew. Energy Res.*, vol. 10, no. 1, pp. 425–437, 2020.
- [23] S. S. I. Samuel, "A Review of Connectivity Challenges in IoT-Smart Home," 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), pp. 1-4, 2016.
- [24] W. Li, T. Logenthiran, V. Phan and W. L. Woo, "A Novel Smart Energy Theft System (SETS) for IoT-Based Smart Home," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5531-5539, June 2019.
- [25] G. L. P. Ashok, P. Saleem Akram, M. Sai Neelima, J. Nagasaikumar and A. Vamshi, "A. Implementation of Smart Home by Using Packet Tracer," *International*

- Journal of Scientific & Technology Research, vol. 9, pp.678–685,2020.
- [26] I. Shemsi, “Implementing Smart Home Using Cisco Packet Tracer Simulator”, International Journal of Engineering Science Invention Research & Development, vol. IV, no. VII, pp.261-269, 2018.
- [27] Sk Tanvir Anjum, Md. Khalid Khan, Prosun Das, Md. Sabbir Hossain, and Tajul Islam, “Smart Home Design with DSL-Modem Using Cisco Packet Tracer Simulator,” 2019.
- [28] Rawan Kh. Flifel, “The Role of Packet Tracer in Learning Wireless Networks and Managing IoT Devices,” ISC International Journal of Information Security, vol. 11, no. 3, pp. 35–38, 2019.
- [29] M. Saleh, Y. Esa, N. Onuorah, and A. A. Mohamed, “Optimal microgrids placement in electric distribution systems using complex network framework,” 2017 6th Int. Conf. Renew. Energy Res. Appl. ICRERA 2017, pp. 1036–1040, 2017.
- [30] Pitcheri Praveen Kumar, Murali Krishna, and M.R Ramprakash, “Design and Implementation of Smart Home Using Cisco Packet Tracer Simulator 7.2,” International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 11S, pp. 107–111, 2019.
- [31] P. Praveen Kumar, and M. Murali Krishna, “Designing Smart Home Using Cisco Packet Tracer 7.2 Simulator,” International Journal of Research in Advent Technology, vol. 7, no. 4S, pp. 116-121, 2019.
- [32] <https://www.ciscopress.com/articles/article.asp?p=2164577&seqNum=5>, Cisco, last accessed on 05 Jul 2021.