A Framework of Smart Homes Connected Devices Using Internet of Things

M. Bala Krishna
University School of Information & Communication Tech.
Guru Gobind Singh Indraprastha University
New Delhi, India
E-Mail: mbalakrishna@ipu.ac.in

Anudit Verma
University School of Information & Communication Tech.
Guru Gobind Singh Indraprastha University
New Delhi, India
E-Mail: verma.anudit@gmail.com

Abstract - Internet **of Things (IoT) is an extensive network of connected components working in unison by coordinating, acknowledging and sharing the resources in the network. Smart frameworks provide an optimal ambient environment for the occupants in smart homes, offices and surrounding environment. The proposed smart home framework incorporates multiple heterogeneous devices that communicate with each other and establish a collaborative network. In this framework, the server accepts incoming requests from connected devices and support interoperability across the connected devices. Simulation for IoT Smart Home includes components such as the centralized server, home security, smart phones, smart thermostat, centralized air condition, connected lights, windows and ventilation control, smart TV and smart fridge. Smart home simulations based device initialization (between server and device), data exchange sequence, module log and event log are given in the proposed framework.**

Keywords - Smart Home, Energy efficient smart buildings, secure smart home, Multi-device smart home, smart locks, smart office

I. INTRODUCTION

Internet of Things (IoT) connects sensors, smart devices, actuators, RFIDs, laptops, PDAs and mobile phones to share the network resources and work in conjunction with each other. The device collaboration and synchronization is based on physical network, virtual networks via the internet (Web of Things) and coordinated cloud database servers. Software defined architectures [1, 2] configures the devices such as smart phones, iPads, refrigerators, ACs, TVs, lighting facilities, traffic monitoring systems, and home security systems across the virtual networks and cloud database servers. Software defined smart IoT architectures avoid design prototype and widen the network platform for developers, operators and end-users. This technology helps in energy management systems [3] for real-world applications. Multi-layer IoT architecture supports lightweight access to smart devices, a high degree of device usability, bidirectional channels for better connectivity, remote monitoring of embedded devices and smart IoT network management. Evolutionary and smart IoT frameworks extend the idea of context-awareness and social group network paradigms to coordinate with multi-utility users, share the resources and reduce the energy consumption in large-scale networks. The operational aspects of context-awareness include (i) categorizing the smart devices as user-dedicated service (such as health, security, etc.) and generic service (such as internet browsing, group messaging, etc.) and (ii) applying the business rules based on user services. Smart healthcare applications extend the IoT features to physical sensors attached to patients and thus provide a continuous monitoring system to avoid health hazards. Multi-stage verification in internet-based services permit the authentic users to enable the services and minimize the intrusion levels in the system. The smart framework ensures high-level functionality that monitors the user mobility patterns and preserves the privacy and integrity of user data.

Cognitive impaired and non-intrusive expert system for smart home [4] considers a proactive approach for real-time scenarios and guides the users based on preferences and operational constraints. This feature incurs errors in multi-utility operations of the smart home environment. Visual-based tracking systems such as cameras can monitor the status of occupants in the smart home. Artificial Intelligence (AI) based IoT framework [5] applies vision and sensory based tracking system to identify the user based on facial expression and emotion recognition. Context-awareness allow the users to prioritize their services and reveal their location to local cloud servers. Cognitive sensing systems support elderly and blind persons by providing timely alerts of surrounding areas and obstacles in the pedestrian path. The transmission alert signals are sent to the monitoring system. Intelligent-based traffic monitoring system update the vehicle and commuter paths, identify congestion paths, traffic diversions and accident prone areas.

IoT integration in smart home framework [6] is a process of incorporating sensors with image processing and decision making units. This further considers a new cooperative living and device synchronization with family members of the house. The role of smart sensors embedded in smart home environment enhance the framework features and resource sharing directed by the centralized controller. AI methods are embedded in device layer and network layer, and adaptive application layer protocol monitor and coordinate the surrounding environments. This

978-1-5090-5256-1/16/$31.00 ©2016 IEEE

approach enables the devices to coordinate with each other and share their network resources.

The proposed framework for IoT small home comprises of the centralized database server that verifies the authenticity of smart devices, monitors, and coordinates the devices by applying intelligent based rules. The centralized server defines the functional attributes of each device based on device specifications, priority, and energy resource. The proposed model represents a collaborative environment in which the smart home devices interact with each other using scheduling and synchronization methods.

The rest of the article is organized as follows. Section II gives the literature survey of existing smart home IoT framework and their applications in detail. Section III explains the proposed smart home IoT framework and the device specifications. Section IV highlights the details of intelligent based rules used by the centralized server that monitors the status of smart devices in the smart home. Section V gives the smart home simulations based device initialization (between server and device), data exchange sequence, module log and event log for the proposed framework. Section VI concludes the proposed framework and gives the direction for future extension.

II. Related Work

The primary aspects of IoT include object connectivity, platform independence, resource management, data integrity and privacy preservation. Control and management unit of IoT access the disjoint network services and provide services for remotely operated smart objects. Multi-agent alert generation, controlled and coordinated local and global managers [7] process the user requests. IoT test-beds [8] are modified to suit the social acceptance factor, service quantification and device security. Multi-tier test-bed model separates the scope of technology and application domains with respect to structural aspects such as network composition consisting of indoor and outdoor services. SNMP distributed architecture helps to manage the devices in IoT network. Smart environment models [9] consider a well-coordinated sensor node set deployed at multiple locations, analyze the periodic data and address the issues of remote management and services in the network. Centralized controller manage the devices (Sensors, surveillance camera and RFIDs (active and passive tags)) with a wide range of data transmission. The manager in smart home environment handles the issues of remote management for systems such as pressure and temperature monitoring in power management. The devices in smart home environment provide precise data based on current time and device location to the centralized.

Failure monitoring system in the smart home [10] architecture monitors the device connectivity at physical layer and the execution of complex functions in application layer. Behavior monitoring and image processing models support scalability and reusability for heterogeneous IoT objects. Visible light communication [11] based on line-of-sight transmission from LED units of sensor node provide reliable services for indoor environments. Orthogonal code for light transmission uses multi-objective functions. Information management model [12] improves the device interoperability by classifying the context of user services and define the rules of data exchange with external database. Rule matrix addresses specific functions such as controlling automated device and monitor device status. The central management system monitors the physical parameters such as gas pressure, electrical overload, operational delay tolerance, energy levels and scheduler operations. 3D-based user interface for complex IoT smart environment [13] considers associated cognitive rules to control and coordinate the IoT devices. Further, Wi-Fi and Bluetooth technologies enhance the performance of a smart home network. The smart lock system [14, 15] have advantages over traditional deadbolts that consist of electronic control kits and communicate with user smartphones/manufacturer servers. The security and threat models in smart lock system mitigate the comprehensive list of state attacks. Smart home activity recognition [16] considers active and passive tasks performed by IoT devices.

Risk tolerant system [17] communicates with primary services, end users, and third party services. Risk tolerant system analyzes the input flow information from various databases and further, the risk models evaluate the system risk, application failure risk, and resource security risk. Historical and current data measures the frequency of operations, number of operational stages, failure levels (in terms of time and repeatability) and define sustainable levels to mitigate the failures.

III. Proposed Framework for IoT Smart Homes Components

The proposed framework comprises of a centralized server that monitors and controls the heterogeneous smart devices such as biometric sensors, temperature monitors, motion controllers, indoor lights (that use weather data and change the intensity), windows and ventilation control system, smart television and smart refrigerator units. The functions of each component as explained as follows:

A. Components of Smart Home

Server - A central monitoring and coordinating system with a local database. The server (external entity) provides remote access to connected smart devices. Smartphone sends the request (to access/configure the smart home devices) to the server that further authenticates the source node and forwards the message to the destination node. The server applies encryption rules to ensure system security and rejects unauthorized access to IoT framework.

Home Security System – The home security system of smart home framework includes the functionality to add new users, delete existing users and enable permissions to authorized users to access the services in smart home. Home security system (internal entity) is interconnected with main entrance door equipped with slow motion multi-directional UV and thermal camera. This feature identifies the stranger in neighborhood area, and unlocks the door if an authorized person rings the bell at the door. Home security system interacts with the server, updates the transaction and receives solution for the alert messages.

Smart Phone - An internal entity in smart home network that enables the occupants to send requests for services. Authentic users (via biometric, pin entry and password) controls the functionality of connected devices and enables the device options for other occupants of smart home. Centralized server monitors the events of smartphone.

Smart Thermostat - An internal entity in smart home network to controls the temperature. This component regulates the central AC system to optimal levels based on room temperature and weather outside the house. The user console interface monitors the temperature using intuitive based rules and controls the thermostat operations. This system ensures that if no user is present in the house, the connected smart devices are switched to low power mode. The server provides the weather updates to the thermostat.

Centralized Air Condition - An internal entity in smart home network that moderates the room temperature and regulates the air outflow in the house. For example, if the occupant wishes to have a cooler in living area, then AC vents would be open for that area of the house. This routes the cool air to required location and maintains optimal room temperature. Motion and infrared sensors embedded in smart home detects the presence of occupants in the house, and switch off the AC if an occupant is not present in the house. This method significantly saves the power in smart home network.

Connected Lights - The home lighting system provides artificial illumination inside the smart home. Smartphone application controls the illumination factor and sends the request to centralized server. The occupant's activity received by centralized server switches the lights as per occupant's movement in the room. Moreover, the lighting system also uses the weather data and adjusts the illumination factor in the house.

Windows and Ventilation Control - Standard windows are replaced by smart glass comprising of thin layers of thermochromic filters that are applied to the exterior layer of double sided glass windows. This layer activates the filters beyond the threshold temperature and enables the tinted window transitions. Smartphone application controls the movement of filters and room temperature. This regulates the intensity of solar rays penetrating the house and regulates the room temperature in the house.

Smart TV - An internal entity in smart home network connected to the server and internet support online video streaming and television programs. The occupants of smart home use the smartphone to control the playback, schedule favorite program recording and set the reminders for live TV channels.

Smart Refrigerator - An internal entity in smart home network that keeps track of stored food items, monitor the measure of grocery items and send reminders to the occupants of smart home. Smart camera embedded in refrigerator enables the occupant to view items in smart phone. The server sends alert messages to occupants of the house.

Intelligent-based sensing and controlling further enhance the performance of smart home IoT framework.

IV. Intelligent Control and Sensing For the Proposed Framework of IoT Smart Homes Connected Devices

The proposed smart home framework consists of a group of heterogeneous devices connected to the centralized server. The devices send requests to the server that are further verified and processed. This framework of IoT connected devices facilitate services to the occupants of smart home. The proposed IoT smart home framework is based on client-server model, where the client is an occupant of smart home accessing the services through smartphone, and the server as a centralized unit processes the requests of connected devices and executes the desired task.

A. Intelligent Control and Sensing

The client of IoT smart home framework controls the connected devices using smartphone. Since the proposed framework facilitates features of automated tasks, the connected devices support artificial intelligence techniques incorporated in the sensor units of smart home. Figure 1 indicates the state transition diagram for the proposed IoT Smart Home framework.

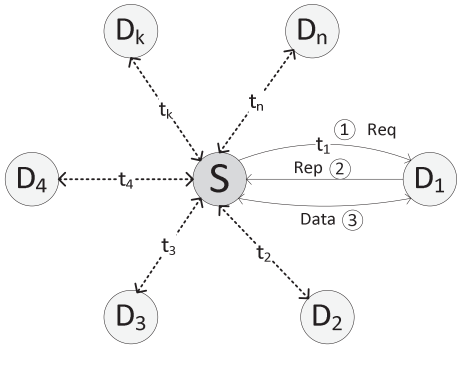


Figure 1. State transition diagram for the proposed IoT Smart Home framework

Smart thermostat with built-in temperature sensor records the temperature, intelligently sends the request to central AC unit and adjusts the surrounding temperature. This system tracks the weather condition and regulates the temperature to optimal levels. Smart fridge equipped with camera identifies the food items and sends the notification to occupants of smart house. Smart AC and ceiling fans communicate with motion and infrared sensors to regulate the speed based on occupants present in the room. If a person enters a room, fans and connected lights would automatically get switched on. The lighting system controlled by sensors intelligently maintain the illumination in smart house. The cameras in each room identify the presence of occupants and activate the smart devices accordingly.

```
Algorithm : IoTSmartHome

IoTSmartHome (S, D)
Server: S, DeviceSet: D = {D1,…D8};
Signals: REQ, RESP,Data;
Begin
 // Initialize and configure the Server and Devices
   Initialize(S);
   Configure(D);
   For  (i = 1 to 8)
   // Establish Connection
   Begin
      Ser_Req_Conn(S, Di)
      Ser_Est_Conn(S, Di)
   EndFor
   Display(Module_Log)
   While (TRUE)  // server monitors the smart devices
   Begin
      For ( i= 1 to 8)  // server connects to 8 devices
      Begin
        If (User.Command == START)
            Usr_Send_Req(User, Di, S)
            Usr_Est_Conn(User, Di, S)
            Usr_Send_Data(User, Data, Di)
        Elseif (User.Command == EXIT)
            Usr_Close_Connec(User, Di, S)
        EndIf
        Display(Event_Log)
      EndFor
   EndWhile
EndFunction
```

The smart devices are configured based on specifications and requests from the occupants of smart home. The smart TV schedules the recording of favorite programs based on user requests and switches to the default mode in normal view conditions. The water heater is activated based on the user profile that takes a bath within specified time duration (morning or evening). Ambient lighting in smart house is a function of user profile and surrounding environmental conditions.

V. SIMULATION RESULTS

The proposed framework incorporates multiple heterogeneous devices that communicate with each other. The server hosts middleware services and support interoperability across the connected devices. In the proposed IoT framework, the server accepts requests from connected devices. The proposed IoT smart home framework is simulated using OmNet++. The simulation parameters are defined as follows: number of servers: 1, number of IoT devices: 8, simulation time: 100 sec, number of device events: #9, number of message event: #40

Figure 2 illustrates the deployment of smart IoT home components controlled and managed by the centralized server. Server middleware services establish the links with IoT smart home components. The occupant of smart home authenticates with server and the get connected (Connection.Open(Device_Type)) to the target smart device, and further exchange the data (CMessage(Msg,Device_Type)).

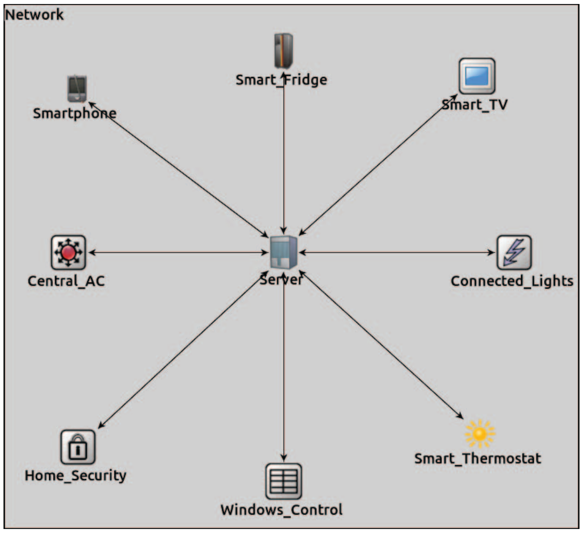
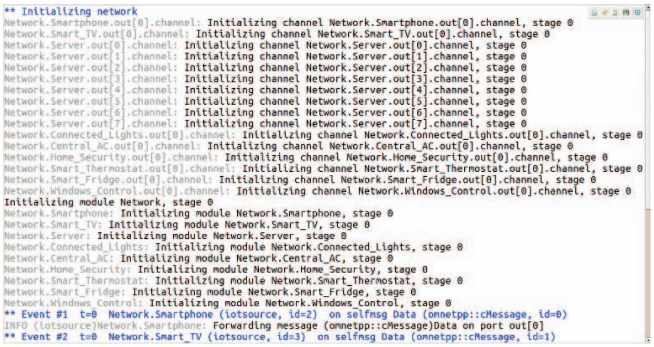


Figure 2. Deployment of IoT Smart Home Components with Centralized Server

Figure 3 illustrates the module log generated during the simulation process. The module log displays the event record (with stage), event number, source data and message ID. IoT smart home devices are configured based on the specification, and further the server initializes each device. Log file illustrates the trace of event sequence for IoT smart home network. The log file further helps to diagnose the network, trace a faulty device and identify the network failures in the smart home environment.



```
** Initializing network
Network.Smartphone.out[0].channel: Initializing channel Network.Smartphone.out[0].channel, stage 0
Network.Smart_TV.out[0].channel: Initializing channel Network.Smart_TV.out[0].channel, stage 0
Network.Server.out[0].channel: Initializing channel Network.Server.out[0].channel, stage 0
Network.Server.out[1].channel: Initializing channel Network.Server.out[1].channel, stage 0
Network.Server.out[2].channel: Initializing channel Network.Server.out[2].channel, stage 0
Network.Server.out[3].channel: Initializing channel Network.Server.out[3].channel, stage 0
Network.Server.out[4].channel: Initializing channel Network.Server.out[4].channel, stage 0
Network.Server.out[5].channel: Initializing channel Network.Server.out[5].channel, stage 0
Network.Server.out[6].channel: Initializing channel Network.Server.out[6].channel, stage 0
Network.Server.out[7].channel: Initializing channel Network.Server.out[7].channel, stage 0
Network.Connected_Lights.out[0].channel: Initializing channel Network.Connected_Lights.out[0].channel, stage 0
Network.Central_AC.out[0].channel: Initializing channel Network.Central_AC.out[0].channel, stage 0
Network.Home_Security.out[0].channel: Initializing channel Network.Home_Security.out[0].channel, stage 0
Network.Smart_Thermostat.out[0].channel: Initializing channel Network.Smart_Thermostat.out[0].channel, stage 0
Network.Smart_Fridge.out[0].channel: Initializing channel Network.Smart_Fridge.out[0].channel, stage 0
Network.Windows_Control.out[0].channel: Initializing channel Network.Windows_Control.out[0].channel, stage 0
Initializing module Network, stage 0
Network.Smartphone: Initializing module Network.Smartphone, stage 0
Network.Smart_TV: Initializing module Network.Smart_TV, stage 0
Network.Server: Initializing module Network.Server, stage 0
Network.Connected_Lights: Initializing module Network.Connected_Lights, stage 0
Network.Central_AC: Initializing module Network.Central_AC, stage 0
Network.Home_Security: Initializing module Network.Home_Security, stage 0
Network.Smart_Thermostat: Initializing module Network.Smart_Thermostat, stage 0
Network.Smart_Fridge: Initializing module Network.Smart_Fridge, stage 0
Network.Windows_Control: Initializing module Network.Windows_Control, stage 0
** Event #1  t=0  Network.Smartphone (iotsource, id=2)  on selfmsg Data (omnetpp::cMessage, id=0)
INFO (iotsource)Network.Smartphone: Forwarding message (omnetpp::cMessage)Data on port out[0]
** Event #2  t=0  Network.Smart_TV (iotsource, id=3)  on selfmsg Data (omnetpp::cMessage, id=1)
```

Figure 3. Module log of IoT Smart Home Network

Figure 4 illustrates the data flow between server and connected IoT smart home components. The sequence of events can be viewed in user's console (smartphone). The server monitors the device state (idle or busy) and schedules the events based on user profiles and smart home conditions. Smart home devices save energy and conserve the resources in smart home network.

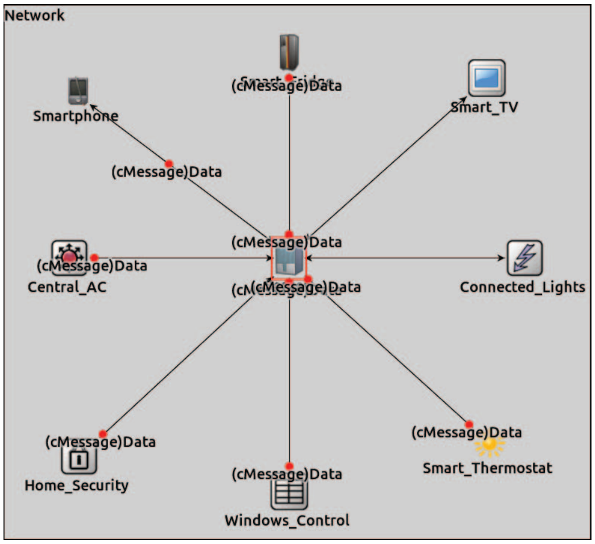
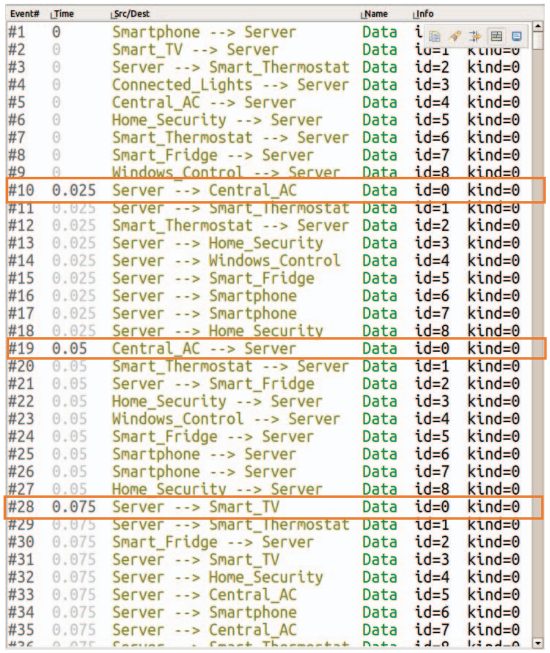


Figure 4. Data exchange between connected IoT Smart Home devices and Centralized Server

Figure 5 illustrates the event log table of IoT smart home environment. IoT smart home event log comprises of the following attributes: event number (#), time (ms), src->dest/dest->src, event type (data), message ID and kind (role, type, category and message identity). In the simulation, kind is configured to 0 (the default value). Initially, at event = 0 ms, the smartphone (occupant) sends a request to the server to grant access for the connected devices in network. The simulation is performed for every 9 cycles (IoT devices (8) + server (1)). Further at 0.025 ms, the server sends the response to Centralized AC based on user's specification.



Event#	Time	Src/Dest	Name	Info	
#1	0	Smartphone --> Server	Data	i	
#2	0	Smart_TV --> Server	Data	id=1	kind=0
#3	0	Server --> Smart_Thermostat	Data	id=2	kind=0
#4	0	Connected_Lights --> Server	Data	id=3	kind=0
#5	0	Central_AC --> Server	Data	id=4	kind=0
#6	0	Home_Security --> Server	Data	id=5	kind=0
#7	0	Smart_Thermostat --> Server	Data	id=6	kind=0
#8	0	Smart_Fridge --> Server	Data	id=7	kind=0
#9	0	Windows_Control --> Server	Data	id=8	kind=0
#10	0.025	Server --> Central_AC	Data	id=0	kind=0
#11	0.025	Server --> Smart_Thermostat	Data	id=1	kind=0
#12	0.025	Smart_Thermostat --> Server	Data	id=2	kind=0
#13	0.025	Server --> Home_Security	Data	id=3	kind=0
#14	0.025	Server --> Windows_Control	Data	id=4	kind=0
#15	0.025	Server --> Smart_Fridge	Data	id=5	kind=0
#16	0.025	Server --> Smartphone	Data	id=6	kind=0
#17	0.025	Server --> Smartphone	Data	id=7	kind=0
#18	0.025	Server --> Home_Security	Data	id=8	kind=0
#19	0.05	Central_AC --> Server	Data	id=0	kind=0
#20	0.05	Smart_Thermostat --> Server	Data	id=1	kind=0
#21	0.05	Server --> Smart_Fridge	Data	id=2	kind=0
#22	0.05	Home_Security --> Server	Data	id=3	kind=0
#23	0.05	Windows_Control --> Server	Data	id=4	kind=0
#24	0.05	Smart_Fridge --> Server	Data	id=5	kind=0
#25	0.05	Smartphone --> Server	Data	id=6	kind=0
#26	0.05	Smartphone --> Server	Data	id=7	kind=0
#27	0.05	Home_Security --> Server	Data	id=8	kind=0
#28	0.075	Server --> Smart_TV	Data	id=0	kind=0
#29	0.075	Server --> Smart_Thermostat	Data	id=1	kind=0
#30	0.075	Smart_Fridge --> Server	Data	id=2	kind=0
#31	0.075	Server --> Smart_TV	Data	id=3	kind=0
#32	0.075	Server --> Home_Security	Data	id=4	kind=0
#33	0.075	Server --> Central_AC	Data	id=5	kind=0
#34	0.075	Server --> Smartphone	Data	id=6	kind=0
#35	0.075	Server --> Central_AC	Data	id=7	kind=0
#36	0.075	Server --> Smart_Thermostat	Data	id=8	kind=0

Figure 5. Events log of IoT Smart Home Network

Figure 6 illustrates the sequence of events and data exchanged between the server and smart home components. The waiting time of each device (#1 to #8) to get connected is shown as green text. Data exchange (Data) between the server and IoT devices (#no) is indicated as red text in the sequence diagram.

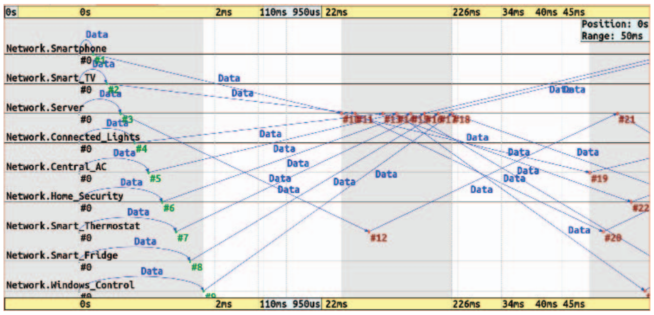


Figure 6. Time scale event sequence of data exchange between IoT Smart Home components and Centralized Server

VI. Conclusions

The proposed IoT framework for smart home incorporates multiple heterogeneous devices that communicate with each other. In this framework, the server accepts the incoming requests from authentic devices. The proposed IoT simulation for Smart Home includes components such as the centralized server, home security, smart phones, smart thermostat, centralized air condition, connected lights, windows and ventilation control, smart TV and smart fridge. IoT smart home simulations based on device initialization (by server), data exchange sequence and event log are explained in detail. Simulation results indicate the sequencing of events with respect to REQ-RESP (request and response) chart between the connected devices and the centralized server. This work can be further extended to include database modules at the server and multi-objective functions for smart IoT devices.

References

[1] Mainetti L., Mighali V., and Patrono L., "A Software Architecture Enabling the Web of Things", *IEEE Journal of Internet of Things,* Vol. 2(6), December 2015, pp. 445-454.

[2] Perera C., Liu C. H., Jayawardena S., and Chen M., "A Survey on Internet of Things From Industrial Market Perspective", *IEEE Access,* Vol. 2, 26 January 2015, pp. 1660-1679

[3] Chatzigiannakis I., Amaxilatis D., and Livathinos S., "A Collective Awareness Platform for Energy Efficient Smart Buildings," In *Proceedings of ACM 19th International Panhellenic Conference on Informatics (PCI)*, Athens, Greece, 1-3 October 2015, pp. 295-296.

[4] Belley C., Gaboury S., Bouchard B., and Bouzouane A., "Nonintrusive system for assistance and guidance in smart homes based on electrical devices identification", *Elsevier Journal of Expert Systems with Applications,* Vol. 42(19), 1 November 2015, pp. 6552–6577.

[5] Mano L. Y., Faiçal B. S., Nakamura L. H. V., Gomes P. H., Libralon G. L., Meneguete R. I*., et al.*, "Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition", *Elsevier Journal of Computer Communications,* Vol. 89-90, 1 September 2016, pp. 178–190.

[6] Moser K., Harder J., and Koo S. G. M., "Internet of things in home automation and energy efficient smart home technologies," In *Proceedings of IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, San Diego, CA, USA, 5-8 October 2014, pp. 1260-1265.

[7] Elkhodr M., Shahrestani S., and Cheung H., "A Smart Home Application Based on the Internet of Things Management Platform," In *Proceedings of IEEE International Conference on Data Science and Data Intensive Systems (DSDIS)*, Sydney, Australia, 11-13 December 2015, pp. 491-496.

[8] Gluhak A., Krco S., Nati M., Pfisterer D., Mitton N., and Razafindralambo T., "A survey on facilities for experimental internet of things research", *IEEE Communications Magazine,* Vol. 49(44), November 2011, pp. 58-67.

[9] Chana M., Estevea D., Escriba C., and Campo E., "A review of smart homes - Present state and future challenges", *Elsevier Journal of computer methods and programs in biomedicine,* Vol. 91(1), 2008, pp. 55–81.

[10] Kaldeli E., Warriach E. U., Lazovik A., and Aiello M., "Coordinating the Web of Services for a Smart Home", *ACM Transactions on the Web,* Vol. 7(2), May 2013, pp. 10:1-10:40.

[11] Tiwari S. V., Sewaiwar A., and Chung Y.-H., "Smart home multi-device bidirectional visible light communication", *Springer Journal of Photon Network Communication*, 13 January 2016 (Online), pp. 1-8.

[12] Capitanellia A., Papettia A., Peruzzinia M., and Germania M., "A smart home information management model for device interoperability simulation," In *Proceedings of Elsevier 24th Design Conference CIRP*, Milan, Italy, 14–16 Apr 2014, pp. 64-69.

[13] Shirehjini A. A. N. and Semsar A., "Human interaction with IoT-based smart environments", *Springer Journal of Multimedia Tools and Applications*, 14 July 2016 (Online), pp. 1-23.

[14] Ho G., Leung D., Mishra P., Hosseini A., Song D., and Wagner D., "Smart Locks: Lessons for Securing Commodity Internet of Things Devices," In *Proceedings of ACM 11th International Asia Conference on Computer and Communications Security (ASIACCS)* Xian, China, 30 May-3 June 2016, pp. 461-472.

[15] Granjal J., Monteiro E., and Silva J. S., "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", *IEEE Communication Surveys & Tutorials,* Vol. 17(3), Third Quarter 2015, pp. 1294-1312.

[16] Cicirelli F., Fortino G., Giordano A., Guerrieri A., Spezzano G., and Vinci A., "On the Design of Smart Homes: A Framework for Activity Recognition in Home Environment", *Springer Journal of Medical Systems,* Vol. 40(9), September 2016, pp. 1-17.

[17] Kirkham T., Armstrong D., Djemame K., and Jiang M., "Risk driven Smart Home resource management using cloud services", *Elsevier Journal of Future Generation Computer Systems,* Vol. 38, 2014, pp. 13–22.