SMART SENSING SCHEME FOR ENERGY MONITORING IN HOME AREA NETWORK

Manimuthu ARUNMOZHI Ramesh RAMADOSS
Department of Electrical & Electronics Engineering, CEG Campus, Anna University, Chennai, India, 600025,
maniasaldhinesh@gmail.com

Abstract: *Sensors with IoT assistance boost the communication, monitoring, and security in Grid-connected home network unit. Segmenting of different operational units, testing and validating of grid operations in real time is difficult and requires specific network design and power monitoring framework is essential. Need for connection establishment, power loss mitigation and secure data transfer give the path for developing this framework. Internet of Things helps in making a home network to perform smarter by accessing, controlling and monitoring every electronic device operations from remote places. The primary objective of this proposed research work is to develop cost-effective adaptive IoT-HAN connected with grid and establishing energy aware routing and power management scheme. The developed design possesses state of art network design where all the home appliances are connected to central control gateway and users are authorized using a three-way security check for power data access. This design scheme helps to place network nodes, sensors, and control gateway in a predefined boundary which consumes less energy for data transfer and data processing. This proposed framework is tested in both simulation and real-time and it is compared with the existing home network systems. The test results are detailed in this paper which proves the proposed system gives very less error% in data delivery and packet loss is also very much reduced. A hardware prototype is also developed to test the developed system and it also provided better results and improved performances.*

Keywords: *Automation, Control system, Gateway, Network route, Power monitoring, Security.*

1. Introduction

In HAN, the framework is developed using IoT which is defined and structured based on the NIST (National Institute of Standards and Technology) conceptual model. It uses radial concentrators and gateway for sensor placements. NIST also defined several domains for meter design and communication standards for the full load network connection and information exchange between the centralized control unit and the HAN equipment inside the gateway boundary region. Network standard used in defining the gateway boundary depends on the communication protocol. Using the NIST conceptual model of smart grids as a reference the energy routing scheme is developed for home and industrial unit based on the power usage and demand. This helps to maintain the load balance between generation and distribution unit. It also helps to accommodate renewable energy resources as an energy source to meet up with the customer needs at the time of emergency in the system [1]. The system is developed in such a way to meet up the energy demands of the customers both at peak load and no-load conditions. Local generation unit must be equipped with centralized as well as sectional control. Sufficient gateway must be provided for continuous monitoring of power usage by the consumers and other utilities. This helps in optimizing the energy generation and distribution without disturbing the demand response. Smart home automation with network connectivity helps in monitoring and diagnosing the power usage of a different load at a different time interval [2]. The customer can trace the power usage from any remote area if HAN is connected to the internet and made online. With IoT as a service provider, HAN gets connected with central control gateway and made the data accessible from any remote place. Smart intelligence system embedded with the HAN helps to trace the best route for the data delivery to the customer on a request basis [1] [3]. This smart system includes a network design, sensor placement algorithm, and energy aware routing framework. This developed system helps to keep the grid connected HAN with proper security and maintenance. This proposed system can help in power sharing with the neighborhood HAN connected with the same gateway. Self-generating power units like solar panels, wind turbines etc can also be incorporated into the system without altering the basic design scheme and structure. In this paper, we present an architecture and design framework for setting up gateway and concentrators with IoT devices. The developed design has an algorithm which has elements of novelty and state of art, where each design code helps to provide easy access to HAN and helps in sensor deployments. Sensors act as embedded agents with IoT helps in full automation, monitoring and establishing secure HAN throughout the network ranges. Apart from framework design, this paper concentrates on various problems related to the power system and communication

networks both inside the HAN boundary and also within the gateway perimeter.

2. IoT in Smart Grid Network

In smart grid, a central control unit for communication network interface is provided which helps in system automation and performance improvement [4-6]. The existing framework in power system lacks data storage network and consumes excess power for indigenous system operations. Thus a proper network gateway and structured protocol must be employed for the power utility monitoring in the power grid. For establishing secure data exchange and continuous proper power usage monitoring inside the gateway boundary region of HAN, IoT is employed. IoT gets combined with the sensors which are available at different electronic devices inside HAN and helps in proper connection and power usage monitoring and control. Here, a central server and the gateway are embedded with programmed IoT devices and sensors [7]. It also involves the following sections for 24X7 online data supports to HAN:

IoT at the Gateway provides*:*

- Smart routing and specific protocol usage.
- Distributed computing for a sequence of data for the different time interval.
- I/O performance monitoring of connected devices.
- Integrated communication capability (to sensors and to the cloud).

IoT-enabled sensor and device manageability:

- Simple, generic and fast installation and configuration of network devices.
- Structured placement of sensors within the connectivity boundary limit.
- Remote administration of gateways.

IoT Security Management:

- Electronics equipped with sensors are made online for continuous monitoring and control.
- Smart and secure sensing for a variety of network devices (wireless LAN, PLC).
- End-To-End Security from a different type of sensors with the IoT devices and provision for cloud service is available.

IoT Data Scalability*:*

- Data processing and decision making from remote to local system using network protocols and standards.
- Data storage at the central server and cloud database for future reference and analysis.
- Hierarchical clouds (fogs) assistance.

Thus, IoT in the grid-connected home requires skilled operating units and advanced networking scheme.

3. Challenges in Smart Grid Employing IoT in India

India faces a number of challenges in using IoT and network-connected devices in a smart grid. It also creates issues in existing power grid which is explained as follows:

Absence of skilled manpower

IoT is a new concept that involves in-depth knowledge of various distinct domains: Power system, generation control and automation, IT and telecommunications. The Distribution Companies of India (DISCOM) is well versed in the electrical technologies of the electricity grid, but when it comes to telecommunications and IT, their expertise is limited. The practical difficulty is the fact that IoT-HAN in smart grid is an evolving technology where limited awareness of usage and benefits are available.

Limited Awareness

As IoT is an emerging technique in India, manufacturer, developers, suppliers, regulators and DISCOMs are still trying to understand its operations, benefits and other nuances. As a result, they often find it hard to justify investments in IoT-HAN in the grid. Also, limited availability of success rate in IoT system leads to its poor development.

Weak procurement framework

In most government tenders in India, the lowest bidder is awarded the contract. This often leads to the poor testing, partially development and improper deployment of unproven technologies and systems by inexperienced parties. Often the lifecycle cost of such poor systems without any through study and research results leads to much higher cost.

Lack of universal standards

DISCOMs in India tend to choose different technical specifications, independent of each other, for the smart meters in their design of IoT-HAN. This leads to increased costs and unnecessarily inflated time-to-market. In the case of Europe, several large, quasi-national, rollouts went this route and have suffered delays after creating additional burdens for vendors.

Customer engagement

Many potential benefits of an IoT-HAN project rely on robust customer engagement. In India, this is an often overlook aspect by most DISCOMs. Customers will take part in fully controlled automation, smart sensing and demand response initiatives only when they understand the importance and benefits to them.

4. Structural Design Framework and Elements Involved in IoT

For any IoT network, sensors and actuators are the two important components (Table 1). The data acquisition system, central server, and connectivity devices are some other IoT areas which help in proper and secure connection setup and smart sensing security control [8]. Sensor and actuator in the devices support full duplex communication with the IoT server. Since the system is open and wireless, it is prone to vulnerabilities like hacking, security breach, bug etc. So IoT services must be provided in an encrypted format to all users inside the HAN. For this, TCP/IP client-server and master control model is used. All data request and services are made using secured gateway and it is node to node encrypted. Sensors deliver data in raw data format [9-12].

It has to be decrypted and handled at the control unit for easy access to the customer. Sensor nodes and concentrators at the gateway help in gathering the power usage data from different HAN devices. All this information are scripted into a standard message format which must have data, payload, timestamp, position coordinates and error checking codes (client-server).

Signature data without any error is manipulated easily and made available online to the customer 24X 7 accordingly. The sensor used in this data scheduling, collection, and processing at the gateway boundary must be monitored continuously for vulnerabilities.

Table 1
Essential Components of Internet of Things (IoT) Platform

Components	Functions and Features
Sensors	Detecting and Sensing
Actuators	Control and Command
IoT Sever	Decision making and Central Control
Concentrator	Region lookup and boundary perimeter monitoring
Connecting Devices	Connection establishment, data transfer, and path selection
AMI (Advanced Metering Infrastructure)	Data collection, encryption, transfer, and storage

The entire IoT integrated system is wireless accessible and allows users to communicate with the installed nodes via the sensors and the actuators. The data about the power usage of different end devices is obtained from central control unit using embedded agents [5] [12] [14]. Details of real-time geographical coordinates, device operation and power consumption are delivered instantly to the customer on request. Ease of access through different application programming interfaces (API) based on network device operating systems (Android, IOS, etc.) and the software embedded into it. A web-based Graphical User Interface (GUI) developed helps the users to access both real-time sensitive and confidential data. This type of layered architecture ensures adequate security and safety.

From the technical aspect of security and safety, customer data should be hidden and encrypted from external malware and vulnerabilities [7] [11-13]. To ensure safety, users need to be authenticated before they can access their own licensed IoT platform and through HTTPS (Hyper Text Transfer Protocol-Secured), data can be obtained from any specific sensor using sensor ID provided to all sensors connected within the HAN. The IoT server supports multiple encryption protocols. There was a direct and indirect link of communication from all home nodes and control center. The information from one node must not be traced from any other node connected through the same gateway to the central control unit. So safety and security about the power usage and connectivity from each node must be ensured. Communication from another node must be mirrored and hidden from each another. In the developed topology, every node is provided with three-layered security and protection as shown in Fig. 1. On successful connection establishment, the users can avoid all types of communication overlap, data mismatch and corrupted power usage value from the sensors.

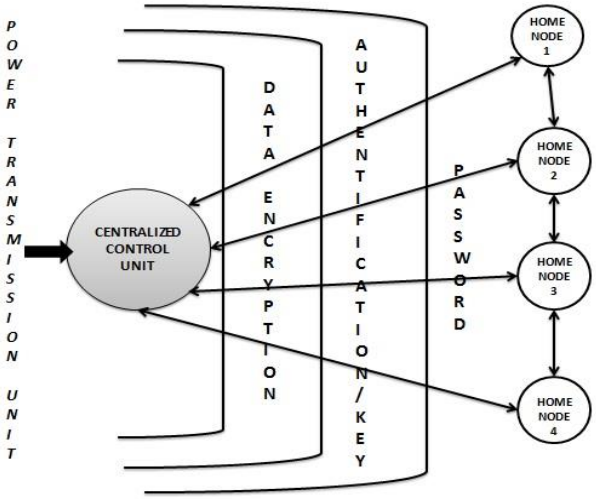

Fig. 1. 3-layered security scheme for secured data delivery to customer

This secured architecture supports two-way data encryption and single-handed user authentication between the control unit and HAN devices [13-15]. The IoT platform consists of several hardware and software components, GUI tools and connectivity devices where each can get revamped, altered, and adjusted with minimum impact on other connected nodes in the system. Without IoT AMI and smart sensors, control center must send personnel to

customer premises to manually read the meter data. Implementation of AMI inside HAN enables remote metering both regularly and on-demand. Data entry and processing is performed automatically at a reduced cost relative to traditional meter reading [16-18].

Sensors installed at every HAN automatically detect meter tampering and enable real-time energy accounting. This reduces theft through by-passing the meter, thereby substantially reducing aggregate technical and commercial losses. AMI will also streamline online billing, or meter-to-cash, payment process considerably [18-20].

5. Gateway Design and Data Exchange

In the proposed HAN-IoT system, it is the IoT server that performs connection establishment and data exchange. Central Gateway Unit (CGU) monitors the operations of sensors and concentrators as explained in Fig. 2. Therefore, the gateway sends network packets over TCP/IP in segmented partitions. Both the CGU and central concentrator are transparent in HAN between device sensors and IoT server [21].

In this developed framework, certain additional features are implemented based on location, sensor boundary range, smart meter capacity and gateway connectivity [22-24].

Some of them include

- Provision for cloud assistance for individual HAN connected consumers.
- Physical Ethernet data logistic facility.
- Choice of data delivery based on time, date and position coordinates.
- Manual versatility check of concentrators, gateway, and sensors.
- Smart Digi lock data backup to IoT clients on request.

These features will have the following advantages in improving the performance of IoT-HAN:

- The hardware requirements are less at the home unit and also at the CGU.
- Different Application Programming Interfaces (API) with new and different functionality can be developed and added without modifying the gateway.

The user side GUI platform can communicate with API and directly with network nodes.

6. Communication Protocol and Connectivity

After setting up the sensors and the concentrator based on position and gateway index, set up the connection between all the network devices using suitable protocols and network devices [5] [17] [24-27]. The range, signal strength, and the boundary play a major role in choosing the best route and link for data packet delivery from node to node and to CGU and IoT server (vice-versa). The standard which is chosen must be reliable, cost-efficient and also robust ensuring energy saving and best route data delivery [28-30].

The need for better design helps to avoid various issues and emergency situations like system failure, security outages, gateway control and network boundary coverage. Network in which all connections are setup is flexible and adapting to all the worst-case routing issues present in the communication as well as smart grid environment [8] [12] [24] [27] [29-30].

Developed topological setup should possess the following:

- Active and passive control units.
- Sectionalized communication medium.
- Path tracing segments for power line communication.
- Data packet security and authenticity.

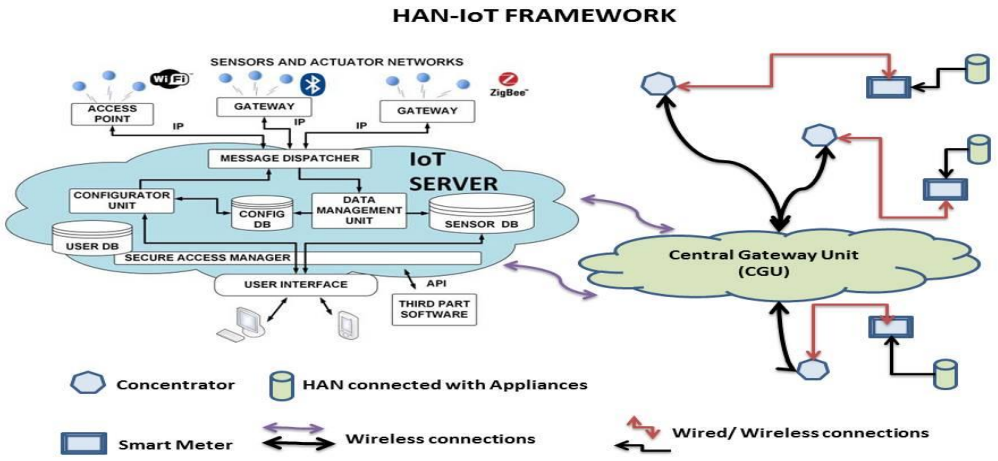

Fig. 2. Proposed HAN-IoT design framework

Table 2.
Wireless Technology Comparison

Wireless Technology	Area Coverage	Number of Nodes	Frequency	Topology	Power Consumption
Infrared	1m (max)	2	470-698 MHz	Bus	Low
Bluetooth	10m	8	2.4 GHz	Star	Low
Zigbee	10-300m	25400	2.4 GHz	Mesh, Star, Tree	Very Low
Wi-Fi	10-100m	32	10.6 GHz	Star	High
Li-Fi	3-8m	8	430-770 THz	Star, Bus, Tree	Low

Network band analysis is the common way through which power usage and area coverage can be easily compared and installed at suitable positions. Table 2 shows the comparison between various wireless technologies available and helps in selecting the best choice and energy saving scheme in developing HAN [12] [18] [31].

Apart from communication strategies, system schematic must be designed and developed for proper control over the devices involved in the network. Broader the area, larger will be node concentrator and gateway complexity. Sectionalized partition of network based on smart grid -HAN helps IoT in monitoring the power usage and network adaptability. Control unit design should hold good for all time power system diagnosis and load demand estimate. The mobility of network nodes in mesh network helps in load balancing and data packet delivery continuously over the IoT server and cloud but continuous mobility increases the gateway complexity in data exchange [4] [7] [31-33].

7. M Design Framework for enhancing IoT-HAN

Abnormalities like sudden transience, power failure, power theft, load imbalance, peak overshoot, voltage drop, power lines sag and signal outages, node failure, communication backhaul, poor data transfer, improper message concatenation can cause severe and catastrophic damages to the entire network setup. To secure the system from damages and improve the performance, a novel design framework is proposed (Fig. 3). The state of art design is termed as Manimuthu (M) design frame.

The proposed design can be divided and distributed in four different sections based on the

- Boundary limit and area coverage
- Sensor and connectivity protocol
- Concentrator and Gateway setup
- Communication and Power

Table 3 explains the various terms and equipment involved in the sections of M design topology.

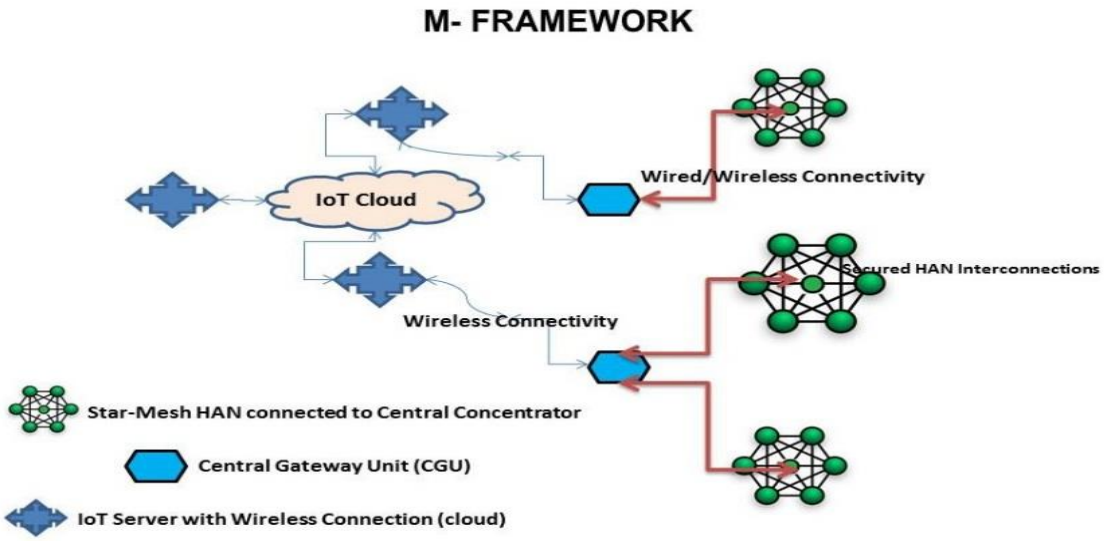

Fig. 3. Developed M design framework

Table 3.
Elements, Connectivity, and Networks Involved in each section of M Design

Elements of each section	Connectivity Type	Network Devices/ Medium
At HAN 1. Sensors 2. Actuators	1. Star 2. Mesh	1. Zigbee 2. Bluetooth 3. Wi-Fi 4. Li-Fi
At IoT-Smart Grid 1. Transmission Network 2. Domestic feeders 3. Industrial feeders	1. Star 2. Ring 3. Mesh	1. WAN 2. BAN 3. HAN 4. Cloud 5. Fog
Additional Elements 1. Generation Unit 2. Power Source 3. Renewable Energy Resources	1. Star 2. Mesh	1. WAN 2. MAN 3. Cloud

M-setup provides a continuous wireless link from all the connected nodes in the network via the hybrid sensors and IoT employed at all the critical nodes in the network. Situations like connection link failure lead to segregation of entire home node from the communication line. In such cases, the information and status of the fault node will be obtained from the centralized control unit. Elements and the nodes in every section were connected both via a direct link and indirect link to the centralized concentrator arrangement. It exchanges the information about the status of all HAN appliances with CGU and IoT with remote customer end in real time.

8. Design Testing and Evaluation

The developed M design is implemented within an in-home prototype. The entire setup has customized and dedicated hardware and software. The prototype uses Wi-Fi and Bluetooth to get connected to the IoT server. The sensors such as motion sensors, current sensor and the temperature sensor etc., placed within every home appliances and smart meter collect process and deliver real-time energy consumption data from different devices connected to HAN. Customers can have a visual, text and also on request demand feedback of their energy consumption. And also, they can remotely control each load based on time, power schedule and operational efficiency.

The proposed M system is tested for different loads present inside the HAN-IoT boundary, also within the single metering gateway connection setup. The data obtained are sequential and without any time delay. The axial range of power consumption from different loads is obtained and formulated as a graphical array.

The voltage, current and power consumption by different loads present inside the HAN is shown in Fig. 4, 5, and 6. In this M-setup, every customer can access their own power consumption data from any remote location by sending customer ID and security codes to the CGU. The request will be processed in a timely manner. Data packets obtained with the same timestamp of a request from the user will get delivered to them. Remote access is provided through IoT server and access codes will be processed for security purpose by the CGU.

The proposed framework is tested in simulation using MATLAB Simulink and compared with the existing metering environment where IoT and gateway are not available. The test results obtained from testing and evaluation gives an improved data sets with very minimum error percentage in all aspects such as data packet delivery, packet transfer rate, and power consumption measurement.

In case of error correction, 0.8% is improved in every single packet reception from individual appliances installed inside HAN. This improved reception of data packets can be updated with the IoT gateway and made available to the authorized users for remote accessibility. As shown in Fig. 7. During the testing, 0.7 error coefficient was patched up for smooth operating frequency of appliances. Thus, it is the correction coefficient value for that particular operating frequency. From this experimental evaluation of the M framework with the existing metering system, an improved % error of 18% is obtained. It shows a greater advantage over the specific metering system.

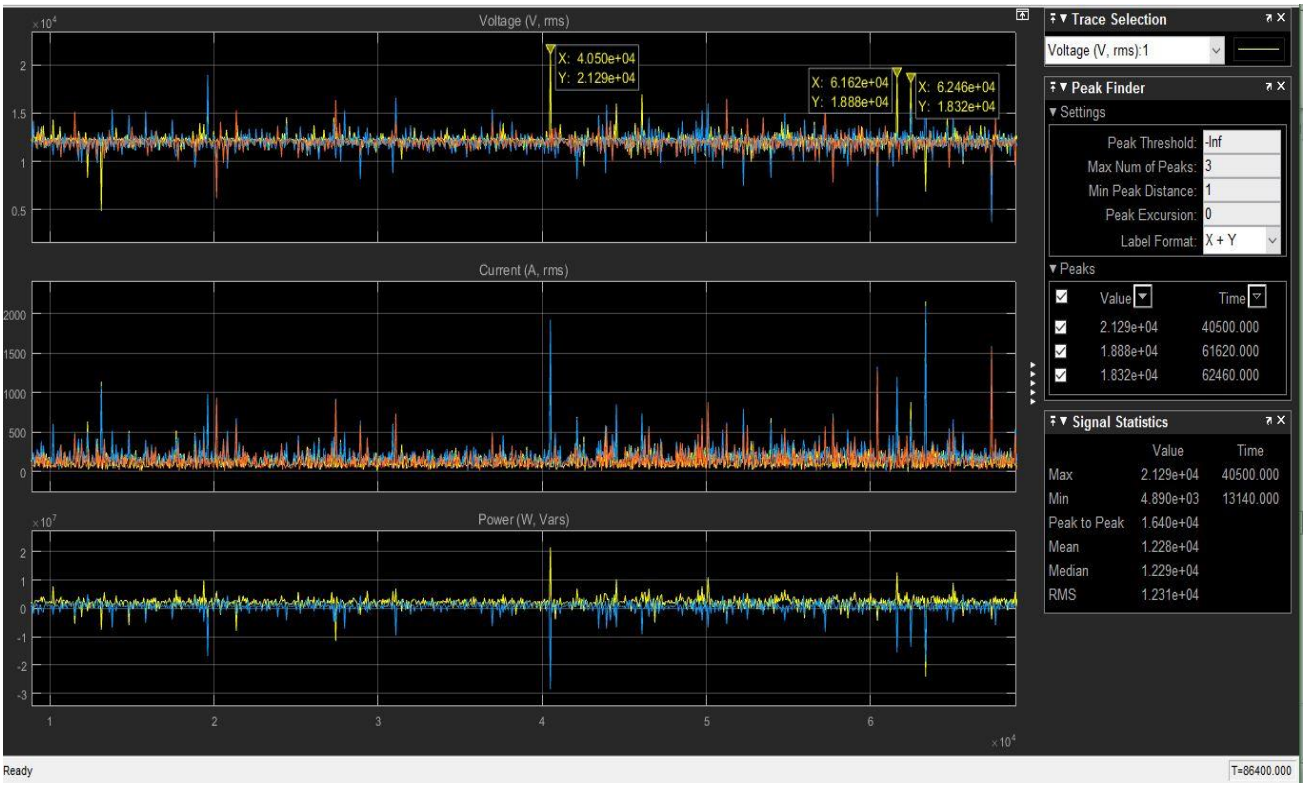

Fig. 4. Voltage Metering Data

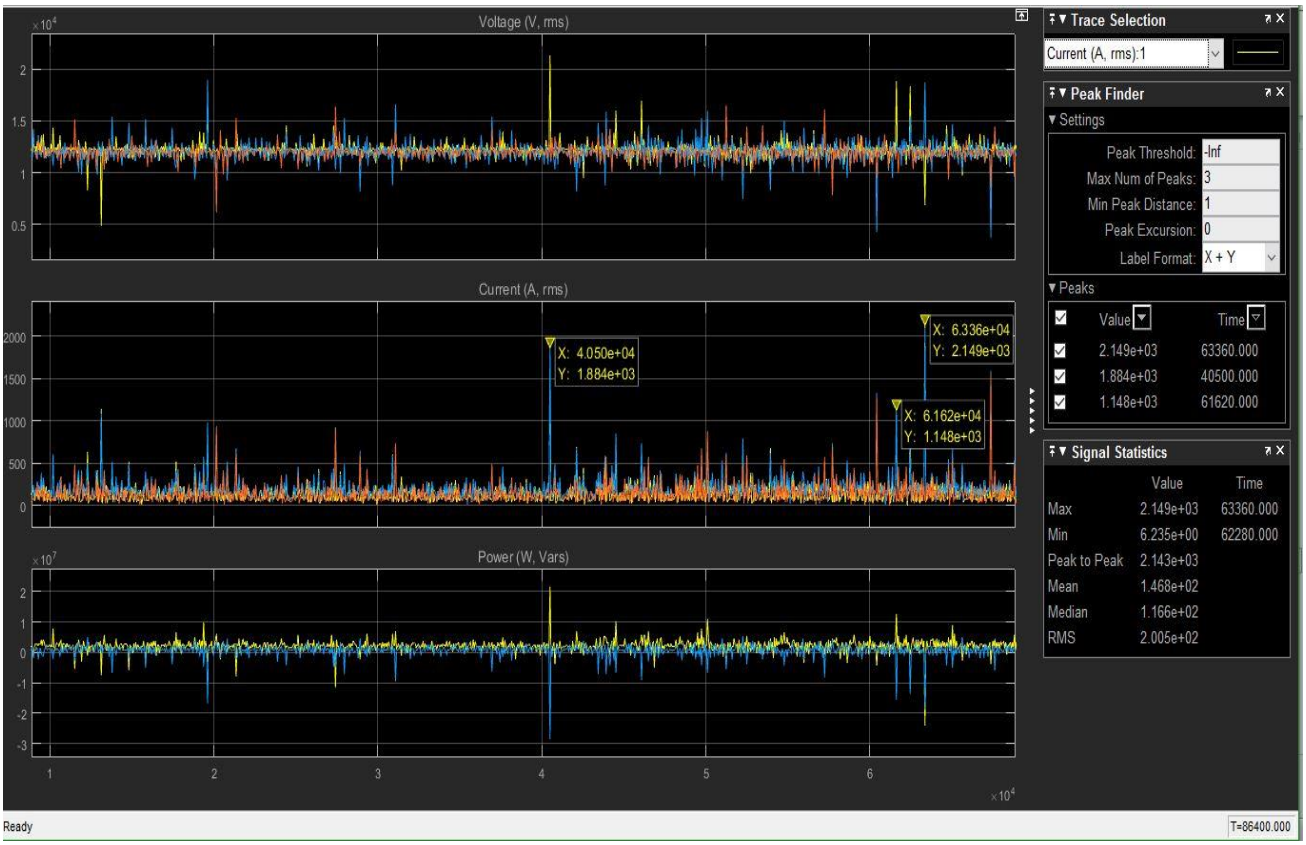

Fig. 5. Current Metering Data

Fig. 6. Power Metering Data

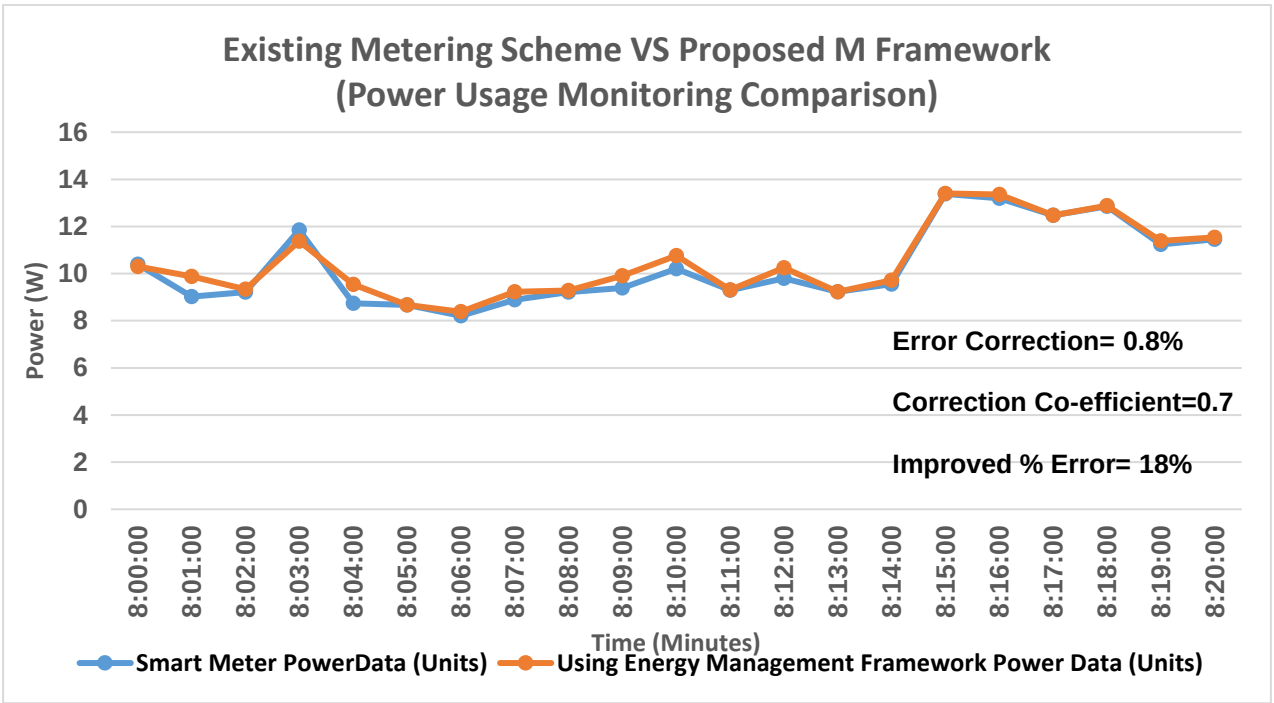

Fig. 7. Power Usage Monitoring Comparison

IoT server and CGU help in finding the shortest route for data delivery to customers in case of mobile nodes. By doing so, energy-aware routing and faster data delivery are achieved.

Shorter the distance of data request faster will be the delivery. Since the host requesting the packet is within the gateway unit, M-setup process and delivers the packet within less delay of 2-5ms. Since all routes are meshed up to the concentrator unit, processing time will be very less. The design is tested for packet reception with the existing metering system. Transfer rate per node in the

system is checked for the spatial distribution of entire packet set along with cyclic error correction. In this operation, the error rate obtained is reduced by 28% per packet and correction coefficient of 2.8 is improved in the entire data transfer from every single equipment in the HAN.

The Fig. 8, 9 shows the results in a detailed way, where the developed system proves the best error correction results with an improved error rate of 28% per packet. Thus, data delivery happens very fast. And also, connectivity protocol helps in delivering data in much faster and better way. After error correction improvement, the data rate is checked for the better packet delivery along with the node density. Thus, a comparison is made for checking the data rate and node density of both the existing and proposed M framework as shown in Fig. 10. The result obtained shows drastic improvement in the data rate with node density of about 18.8% which is the highest ever achieved in the simulation environment. The gateway is routed for the best path data delivery and sort out the easiest and earliest way for packet reception from the meters and gateway installed in the M framework.

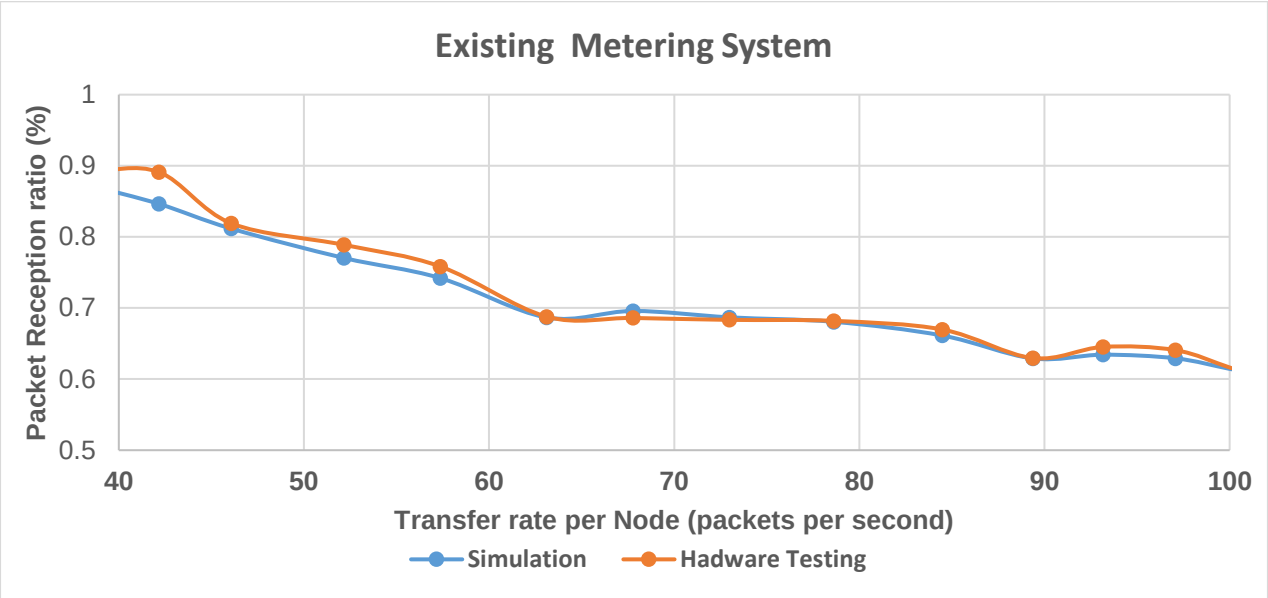

Fig. 8. Packet Reception and Transfer Rate (Existing)

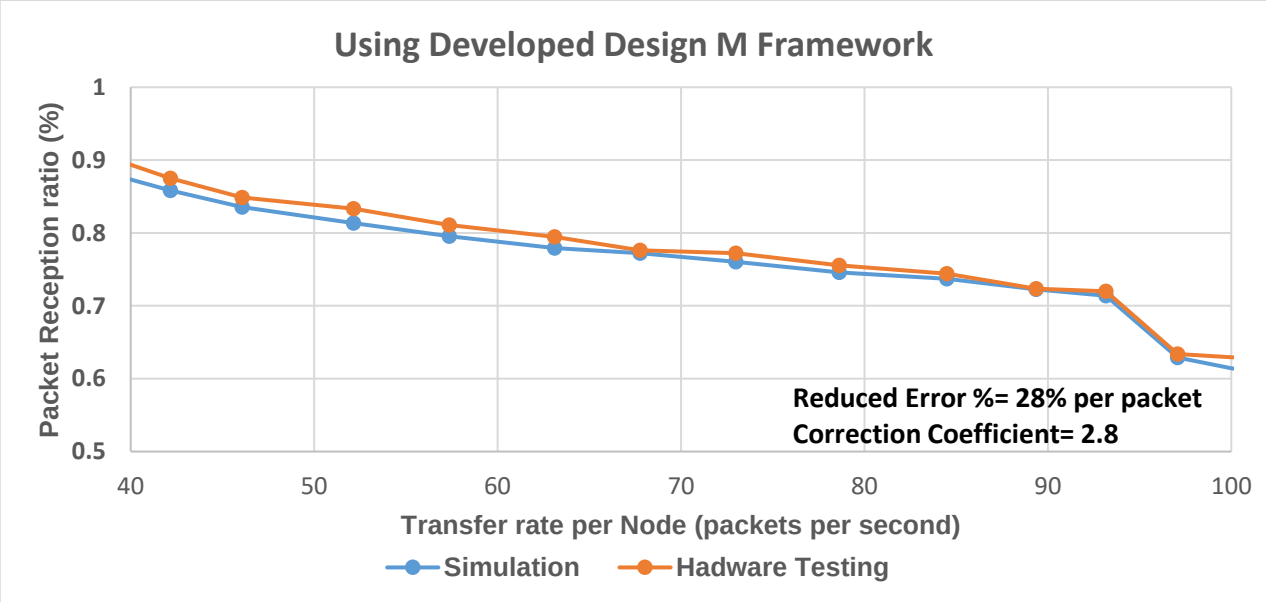

Fig. 9. Packet Reception and Transfer Rate (M Framework)

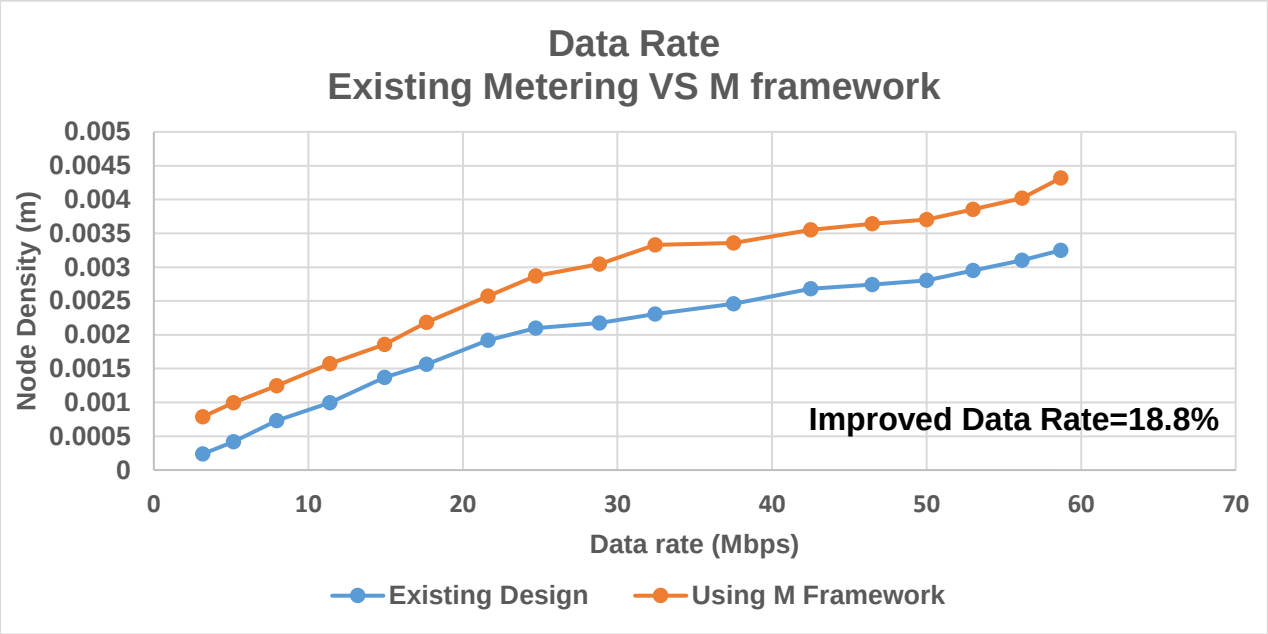

Fig. 10. Data Rate Calculation

9. Developed Hardware Prototype for Proposed Design

Higher the signal strength and bandwidth, greater is the resource output. The nodes involved in the network were under three-layered security continuously and the information from each node is getting transferred instantly and updated in real time. The rate of real value updating is 5ms-10ms. The data about the power usage from different nodes were continuously monitored and values get updated in the concentrator and CGU instantly. Hardware Prototype Model for the developed M-Architecture is shown in Fig. 11.

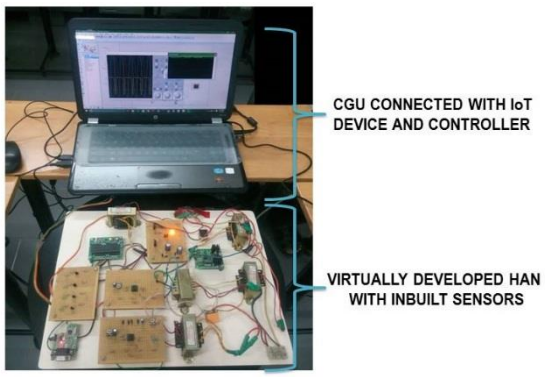

Fig. 11. Hardware Prototype Model for the developed M-Architecture

Discussions

There are always chances of human errors when meters are read manually or even via automatic hand-held devices. This is totally avoided in this proposed system. It is fully automated, wireless and has cloud assistance for remote access. This improves the efficiency by delivering data automatically over communication networks. By making the system available online, metering unit eliminates error for the remote access of the customers.

Quality improvement

Smart meters are capable of measuring power consumption data in near real-time, such as power factor, over or under voltage, and overcurrent. This helps utilities to enhance system power quality in conjunction with power quality data from other sources. Improved power quality also leads to lower power losses. M-setup assures the end-end power usage data delivery to customers in a scheduled aspect.

Asset Optimization

The developed HAN-IoT system supports granular monitoring of power flows on the distribution network which helps to avoid over- and under-loading, sensing issues, connectivity problems and also connection mesh. This helps to enhance design layout, planning, and optimizing network. CGU and concentrator also help to balance the load, which reduces power losses. Furthermore, network monitoring can decrease the failure rate of distribution transformers by identifying phase imbalances in advance which can be corrected without any delay.

Metering Advancements

Smart meters monitoring, collecting and transferring of power consumption data to HAN typically include remote switching, which allows

utilities to remotely disconnect or reconnect whenever necessary, in the case of non-payment, or when a customer moves. Additionally, utilities can monitor the health of the meter and dispatch maintenance when it is required and essential.

10. Conclusion

This research paper provides detailed information about IoT, challenges for IoT-HAN in smart metering in India. A novel M-framework is proposed, tested and validated with suitable test results and graphical expressions. The proposed system is deployed with suitable security architecture and assures maintenance free, cost-effective and energy saving routing of data packets to customers. Hardware developed for testing shows better response with indoor connectivity. But the prototype is not sufficient for outdoor implementation of the proposed system. Simulation results of the proposed system shows better results but improvements must be made for long-range connectivity with same energy efficiency and performance. Further, the M- framework may be tested with cluster computing and machine learning for cases like calibrations and data exchanges.

References

1. Lee, Y.T., Hsiao, W.H., Huang, C.M., Chou, S.C.T.: *An integrated cloud-based smart home management system with community hierarchy*. In: IEEE Trans. Consum. Electron., Vol. 62, No. 1, Feb. 2016, p. 1-9.

2. Kumar, P., Gurtov, A., Iinatti, J., Ylianttila, M., Sain, M.: *Lightweight and secure session-key establishment scheme in smart home environments*. In: IEEE Sensors J., Vol. 16, No. 1, Jan. 2016, p. 254-264.

3. Qingyu Yang, Jie Yang, Wei Yu, Dou An, Nan Zhang, Wei Zhao,: *On false data-injection attacks against power system state estimation: Modeling and countermeasures*. In: IEEE Trans. Parallel Distrib. Syst., Vol. 25, No. 3, Mar. 2014, p. 717-729.

4. Lin, J., Yu, W., Yang, X.: *Towards multistep electricity prices in smart grid electricity markets*. In: IEEE Trans. Parallel Distrib. Syst., Vol. 27, No. 1, Jan. 2016, p. 286-302.

5. Kumar, J.S., Patel, D.R.: *A survey on Internet of Things: Security and privacy issues*. In: Int. J. Comput. Appl., Vol. 90, No. 11, 2014, p. 20-26.

6. Premarathne, U.S.: *Reliable context-aware multi-attribute continuous authentication framework for secure energy utilization management in smart homes*. In: Energy, Vol. 93, No. 1, 2015, p. 1210-1221.

7. Gomez, C., Paradells, J.: *Wireless home automation networks: A survey of architectures and technologies*. In: IEEE Commun. Mag., Vol. 48, No. 6, Jun. 2010, p. 92-101.

8. Kailas, A., Cecchi, V., Mukherjee, A.: *A survey of communications and networking technologies for energy management in buildings and home automation*. In: J. Comput. Netw. Commun., Vol. 2012, Dec. 2011.

9. Oksman, V., Galli, S.: *G.hn: The new ITU-T home networking standard*. In: IEEE Commun. Mag., Vol. 47, No. 10, Oct. 2009, p. 138-145.

10. Chen, J.-L., Chen, M.-C., Chian, Y.-R.: *QoS management in heterogeneous home networks*. In: Comput. Netw., Vol. 51, No. 12, 2007, p. 3368-3379

11. Hwang, W.-J., Tung, Y.-C., Chen, Y.-L., Lai, P.-Y., Ho, C.-H.: *A novel user-oriented quality of service algorithm for home networks*. In: IEEE Syst. J.

12. Wang, Z., Zheng, G.: *Residential appliances identification and monitoring by a nonintrusive method*. In: IEEE Trans. Smart Grids, Vol. 3, No. 1, Mar. 2012, p. 80-92.

13. Das, M.L.: *Two-factor user authentication in wireless sensor networks*. In: IEEE Trans. Wireless Commun., Vol. 8, No. 3, Mar. 2009, p. 1086-1090.

14. Suh, C., Ko, Y.B.: *Design and implementation of intelligent home control systems based on active sensor networks*. In: IEEE Trans. Consum. Electron., Vol. 54, No. 3, Aug. 2008, p. 1177-1184.

15. Karlof, C., Wagner, D.: *Secure routing in wireless sensor networks: Attacks and countermeasures*. In: Ad Hoc Netw., Vol. 1, No. 2, Sep. 2003, p. 293-315.

16. Jose, A.C., Malekian, R.: *Smart home automation security: A literature review*. In: Smart Comput. Rev., Vol. 5, No. 4, Aug. 2015, p. 269-285.

17. Saponara, S., Bacchillone, T.: *Network architecture security issues and hardware implementation of a home area network for smart grid*. In: J. Comput. Netw. Commun., Vol. 12, Nov. 2012.

18. Namboodiri, V., Aravinthan, V., Mohapatra, S.N., Karimi, B., Jewell, W.: *Toward a secure wireless-based home area network for metering in smart grids*. In: IEEE Syst. J., Vol. 8, No. 2, Jun. 2014, p. 509-520.

19. Vardakas, J.S., Zorba, N., Verikoukis, C.V.: *A survey on demand response programs in smart grids: Pricing methods and optimization algorithms*. In: IEEE

Commun. Surveys Tuts., Vol. 17, No. 1, Mar. 2015, p. 152-178.

20. Gudi, N., Wang, L., Devabhaktuni, V.: *A demand side management based simulation platform incorporating heuristic optimization for management of household appliances*. In: Int. J. Elect. Power Energy Syst., Vol. 43, No. 1, Dec. 2012, p. 185-193.

21. Han, D.-M., Lim, J.-H.: *Design and implementation of smart home energy management systems based on ZigBee*. In: IEEE Trans. Consum. Electron., Vol. 56, No. 3, Aug. 2010, p. 1417-1425.

22. Schramm, P., Naroska, E., Resch, P., Platte, J., Linde, H., Stromberg, G., Sturm, T.: *A service gateway for networked sensor systems*. In: IEEE Pervasive Comput., Vol. 3, No. 1, Mar. 2004, p. 66-74.

23. Zoha, A., Gluhak, A., Imran, M.A., Rajasegarar, S.: *Non-intrusive load monitoring approaches for disaggregated energy sensing: A survey*. In: Sensors, Vol. 12, No. 12, Dec. 2012, p. 16 838-16 866.

24. Zhang, Y., Rong Yu, Shengli Xie, Wenqing Yao, Yang Xiao, Mohsen Guizani,: *Home M2M networks: Architectures standards and QoS improvement*. In: IEEE Commun. Mag., Vol. 49, No. 4, Apr. 2011, p. 44-52.

25. Gungor, V.C.: *Smart grid technologies: Communication technologies and standards*. In: IEEE Trans. Ind. Informat., Vol. 7, No. 4, Nov. 2011, p. 529-539.

26. Zhang, H., Cheng, P., Shi, L., Chen, J.: *Optimal DoS attack scheduling in wireless networked control system*. In: IEEE Trans. Control Syst. Technol., Vol. 24, No. 3, May 2016, p. 843-852.

27. Yuan, Y., Li, Z., Ren, K.: *Modeling load redistribution attacks in power systems*. In: IEEE Trans. Smart Grid, Vol. 2, No. 2, Jun. 2011, p. 382-390.

28. Kopetz, H.: *Internet of things in Real-Time Systems*, Springer, 2011, p. 307-323.

29. Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D.: *Security of the Internet of Things: perspectives and challenges*. In: Wireless Networks, Vol. 20, No. 1, 2014, p. 2481-2501.

30. Nicanfar, H., Okar, P.J., Beznosov, K., Leung, V.C.M.: *Efficient Authentication and Key Manage ment Mechanisms for Smart Grid Communications*. In: IEEE systems journal, 2013.

31. Murad Khan; Bhagya Nathali Silva; Kijun Han,: *Internet of Things Based Energy Aware Smart Home Control System*. In: IEEE Access, 2016, Vol. 4, 2016, p. 7556 - 7566 .

32. Son, J.-Y., Park, J.-H., Moon, K.-D., Lee, Y.-H.: *Resource-aware smart home management system by constructing resource relation graph*. In: IEEE Trans. Consum. Electron., Vol. 57, Aug. 2011, p. 1112-1119.

33. Zamora-Izquierdo, M., Santa, J., Gomez-Skarmeta, A.: *An integral and networked home automation solution for indoor ambient intelligence*. In: IEEE Pervasive Comput., Vol. 9, No. 4, Oct./Dec. 2011, p. 66-77.