THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Relative Study of Home Automation Technologies

Renu Sharma
Research Scholar
School of Computer Application ,Lovely Professional University
Phagwara, India
renusharma1978@yahoo.com

Dr. Anil Sharma Professor
School of Computer Application ,Lovely Professional University
Phagwara, India
anil.19656@lpu.co.in

Abstract—Home automation is a technology based on IoT. It is focused on three layer architecture (sensors and actuators, network layer, application layer). Network layer can be configured by many available technologies like Zigbee, Z-Wave, Insteon, X10, Bluetooth etc. Every technology has its own trade-offs. Every technology has its own architecture and functionality of that decides about security provided, interoperability possibility, its range, support of number nodes and their communication. Many other characteristics are also their which decides suitability of a particular protocol. Depending upon need (ease, security, low energy, integration etc.) a protocol could be selected. This paper has compared various parameters of these home automation protocols and their suitability for the application.

Keywords—IoT, Smart Home, ZigBee, Z-wave, Insteon, X10

I. INTRODUCTION

Smart Home (IoTenabled devices) is an abode having interconnection of many appliances that can communicate within the network or with outer domain through internet. Due to possibility of this communication a person can manage a home remotely. Smart Home refers to a structure in which sensors assemble statistics from the network, and then share that statistics on the Internet, where it can be exploited for various applications [1]. Smart Home means devices linked through internet to exchange their information and to facilitate modern living. Future of computing will not be centered on computers itself but it will be based on smart devices.[2]. Smart home is facing many challenges like interoperability and integration[3], security[4], privacy[5], constrained resources, data storage and data analysis. These areas are still bottlenecks in its widespread usage.

A. Interoperability and integration

Sensors are backbone of smart home. Sensors do have diverse architectures and their integration is a major test. Smart home engineering lacks in regulation. In another words we can say everybody is following their own rule. When it is on integration, this diversity creates technical problems. Issues of Integration can arise at two levels: hardware and software level. To add new device, its hardware specifications has to be harmonious with the existing devices and its software specification should counterpart with the current solution. If compatibility issues are there then many solutions suggested in the literature.

B. Security

Security is another major test for smart home. Smart home is built upon connected system and that is exposed to threats. Threats could be at many levels: starting from entry, changing of data or misusing data. In home automation system uniqueness of user could be based on RFID card. Duplicatecard is very

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

much possible. A burglar can use this access in many ways. If we check smart health devices, impostor can create major issues. A. Jacobsson et al. [6] have discussed various risks involved in smart home applications. Total 32 risks have been examined. For psychological satisfaction of the user, area of security is of foremost concern.

C. ***Privacy***

Privacy is also a big hurdle. All patterns of someone can be intercepted just by analyzing data of sensors. Studied information could become base for unlawful activities. Data collected form smart devicescan become a base to intercept into privacy of a life[7].Noah Apthorpe et al. [8] have demonstrated by taking some devices of smart home (Amazon Echo, camera, switch and a sleep monitor), how privacy is at threat even if the data is encrypted. Passive fragment of a network like internet service providers can easily analyze the data of the sensors and can tell pattern of the activities of home dwellers. So privacy is a major issue in the implementation of smart home.

D. ***Storage of Data***

In a smart home gigantic information is delivered. To process this immense information, conventional information handling systems can't be utilized or at the end of the day they are not skilled enough to process that colossal information. To beat this test there is a need of information preparing procedures competent to deal with data high in volume and speed. Information mining techniques are to be revised to satisfy changing needs.

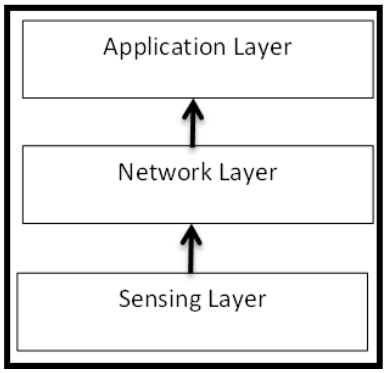
E. ***Constrained Resources***

In smart homeappliances principle segments are sensors. These sensors are truly compelled in computing power , battery life and memory. Numerous remote conventions are accessible (IEEE 802.11, 802.15, Zigbee, Zwave and so on.), yet on obliged assets it isn't possible to apply any convention. In the writing new conventions have been proposed, able to deal with less assets like Constrained Application Protocol (CoAP). Each sensor is distinctive to the extent its computational ability is concerned, so to have same arrangement is unimaginable. To beat these imperatives are additionally a major test.

F. ***Data Analysis***

Utilizing sensors, tremendous information is produced. It is a test to deal with such an enormous information. Existing information preparing systems can not be utilized on this piece of information. So look into is required to have new calculations which could be founded on AI, man-made brainpower or some different systems. For examination of information created by IoT sensors, M. Mohammadi et al.[9] have utilized profound learning procedure of AI. Information created is sorted in two classes: quick information and huge information. Requirement for examination is diverse for two. First classification needs expedient investigation and second classification needs approaches to bargain immense measure of information.

Smart home has layered architecture comprising of three layers: (a) Sensing Layer, (b) Network Layer and (c) Application Layer [10] as shown in Fig.



ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Fig.1 Smart Home Architecture[10]

This engineering has three layers: sensors layer, network layer and application layer[10]. By utilizing innovation, brilliant home gives another degree of control to the property holders. Brilliant home idea is for the most part to elevate level of extravagance. However, it has given numerous included preferences, other than extravagance. A portion of the advantages of Smart Homes are: (a) Remote checking, (b) (c) Assisted living for old [11], (d) Energy efficiency [12], (e) Comfort and so on. Many platforms are available to create smart home. Some of them are: Zigbee, Z-Wave, X10, Insteon etc. This paper has comprehensive information regarding characteristics of these protocols.

II. LITERATURE REVIEW

A. Zigbee

Zigbee is based on IEEE 802.15 standard and it is similar to with Bluetooth and wi-fi [13]. Zigbee has a layered architecture comprising of four layers: (a) Physical layer, (b) Medium AccessControl Layer, (c) network layer, (d) application layer. It uses mesh topology, so it is useful only for low range devices. Its operating range is from 10-100 meters. It is a low power stack. Nodes of Zigbee can be characterized as: coordinator, router and end device[14]. Zigbee uses highly secure 128 bit AES encryption system [15]. It provides security but level has to be checked as per the requirement. Versions of Zigbee are backward compatible and to provide that compatibility some compromises are to be done. Network size could be of 64000 [16]. Three possible data rates are there (20 Kb/s, 40 Kb/s, 250 Kb/s) [16]. Interoperability is a hurdle for this, before integrating a new device its compatibility has to be checked. This can work with three frequency bands (2.4 GHz, 915 MHz, 868 MHz) [16]. Reliability features are also added into this, but 100% reliability is hard to achieve.

B. Z-Wave

Z-wave is a wireless, mesh based, low cost protocol which is primarily used for home automation. Its layered architecture has four layers: transfer layer, MAC layer, Routing Layer and Application Layer[17]. Its layered structure is described in Fig. 2s

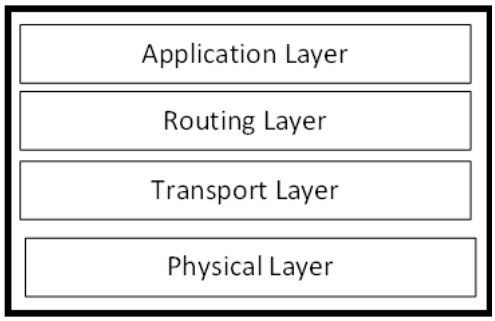


Fig 2. Layered Structure of Z-Wave[18]

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Network of Z-wave is comprising of two types of nodes controllers and slaves. Possible data rates are 9.6 Kbps, 40 Kbps and 200Kbps[16]. It is providing security by 128 bit AES encryption. Eight bit CRC is also provided for reliability[17]. For providing interoperability special version has been introduced. A smart home network can have 232 different devices in this network[19]. Its range is around 100 meters. Main advantage is low cost and lesser energy is required. Home automation is its main area.

C. *X10*

X10 had been developed as wired network which is further developed as wireless. It is a slow protocol as compared to its counterparts. Its functionality is limited. No security measures has been taken. Major problem with this signal interferenceand rapid loss in signal strength. Nothing is provided for security and privacy. The shortcomingsof this has been covered in later developed protocols.

D. *Insteon*

Insteon is a dual mesh topology based protocol. Each node in this act as peers. And any node can send and receive data. Data rate is 38.4 Kbps[20]. It works with a limited range. Number of nodes supported by 256.Reliability mechanisms has been employed in it as eight bit checksum. Public key encryption is being supported, so while deploying a automation system security requirements are to be scrutinized properly[21]. It is based on radio frequency as well as existing wired system. It works on 904 MHz.

Interoperability of above protocols can be summarized as : (a) Zigbee is not interoperable with other protocols.[22] , (b) Z-wave is interoperable only with Z-wave based Devices.[23] , (c) X10 is interoperable with insteon and X10, (d) Insteon based devices are interoperable with insteon based devices.

E. *Bluetooth*

Bluetooth is IEEE 802.15.1, radio frequency based protocol. It works on 2.4 GHz[24]. Range of Bluetooth is of 10 m. Bluetooth provides security with authorization. Latest version of Bluetooth like BLE (Bluetooth low energy) needs lesser power to operate. Even enhanced security features like AES has been included[25].

In Table I these protocols (Zigbee, Z-Wave, Insteon, X10, Bluetooth) has been compared on the parameters of security, interoperability, power requirement, range and no of node supported. Currently Z-wave and Zigbee is widely used for home automation.

III. COMPARISON OF VARIOUS TECHNOLOGIES

	Security	Interoperability	Nodes	Range	Power Requirement
Zigbee	AES	Backward compatibility is there but not fully interoperable	64000	10-100 mtrs	Low
Z-Wave	128 bit AES	For interoperability, measures has	232	100 mtrs	Low

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

		been taken			
Insteon	Public Key	Yes	256	45	Low
X10	No	No	limited	limited	More
Bluetooth	Yes	Yes	8	10	Low of BLE

TABLE I

IV. CONCLUSION

Authors have apprisedthe interoperability, security, power requirements in home automation and what is being provided by market vendors.Literature review of this paper, highlights the various works done on communication platforms available for smart home. If our main concern is of security, than we can check the comparative analysis of the protocols from Table I. Similarly depending upon need (easy installation, integration, security, power requirement) a particular technology can be picked. No technology has complete characteristics. Some is good in security but require more power. It is always a trade off between pros and cons. Smart home is facing challenges in terms of privacy& security, energy efficiency and interoperability and integration. Introduction to all these challenges have been covered to whet the appetite of the researchersand comprehensive information is given about communication protocols (Zigbee, Z-wave, insteon, Bluetooth, X10) on the parameters of security, interoperability, power consumption etc). For future work their hardware specifications can be compared.

REFERENCES

[1] K. Kaur, A. Sharma,"Interoperability Among Internet of Things (IoT) Components Using Model-Driven Architecture Approach", In : Fong, S., Akashe S., Mahalle, P.(eds) Information and Communication Technology for Competitive Strategies, ICTCS-2017, pp. 519-534 . Springer, Singapore (2019).

[2] G. Jayavardhana, R. Buyya, S. Marusic and M. Palaniswami.,"Internet of Things(IoT): a vision, architectural elements and future directions " , Journal of Future Generation Computer Systems, Vol. 29, Issue 2, pp. 1645-1660, September 2013.

[3] Raggett, D.: The Web of Things: Challenges and Opportunities. IEEE Computer 48(5), 26-32 (2015).

[4] M. Elkhodr, S. Shahrestani and H. Cheung., "The internet of things: new interoperability, management and security challenges", International Journal of Network Security & Its Applications, Vol. 8, No. 2, March 2016.

[5] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman and R. Boreli, "An experimental study of security and privacy risks with emerging house-hold appliances", In Proc. IEEE Conference on Communications and Network Security, 2014, pp. 79-84.

[6] A. Jacobsson M. Boldt and B. Carlsson, " Arisk analysis of smart home automation system", Future Generation Computer Systems", Vol. 56, pp. 719-733, 2016.

[7] J. A. Martin,"10 things you need to know about the security risks of wearables", para. 4, March 24, 2017.[online]. Available: https://www.cio.com/article/3185946/wearable-technology/10-things-you-need-to-know-about-the-security-risks-of-wearables.html. [Accessed Feb. 12, 2018].

[8] N. Apthorpe, D. Resiman and N. Feamster," A Smart Home is No Castle : Privacy Vulnerabilities of Encrypted IoT Traffic", arXiv:1705.06805 (2017).

[9] M. Mohammadi, S. Sorour, "Deep learning for IoT Big Data and Streaming Analytics: A Survey", IEEE Communications Survey & Tutorials 20(4), 2923-2960(2018).

[10] Kang Bing, Liu Fu, Yun Zhuo, and Liang Yanlei, "Design of an Internet of Things-based Smart Home System", The 2nd International Conference on Intelligent Control and Information Processing, July 2011, pp. 921-924.

[11] S. J. Daraby,"Smart technology in the home : time for more clarity", Building Research & Information, Vol. 46, Issue 1, pp. 140-147, March 2017.

[12] S. T. Herrero, l. Nicholls and Y. Strengers," Smart home technologies in everday life :do they address key energy challenges in households?", Current Opinion in Environmental Sustainability, vol. 31, pp. 65-70, April 2018.

[13] C. Withanage, R. Ashok, C. Yuen, and K. Otto, "A comparison of the popular home automation technologies," *2014 IEEE Innov. Smart Grid Technol. - Asia, ISGT ASIA 2014*, pp. 600–605, 2014.

[14] NXP, "Maximizing security in zigbee networks," 2017.

[15] B. Fan, "Analysis on the Security Architecture of ZigBee Based on IEEE 802.15.4," *Proc. - 2017 IEEE 13th Int. Symp. Auton. Decentralized Syst. ISADS 2017*, pp. 241–246, 2017.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

[16] A. J. D. Rathnayaka, V. M. Podar, and S. J. Kuruppu, "Evaluation of wireless home automation technologies for smart mining camps in remote western Australia," *Smart Innov. Syst. Technol.*, vol. 12, no. June, pp. 109–118, 2012.

[17] M. B. Yassein, W. Mardini, and A. Khalil, "Smart homes automation using Z-wave protocol," *Proc. - 2016 Int. Conf. Eng. MIS, ICEMIS 2016*, 2016.

[18] B. Fouladi and S. Ghanoun, "Security Evaluation of the Z-Wave Wireless Protocol," *Black hat*, p. 6, 2013.

[19] B. Ray,"Z-wave Vs. Zigbee", para. 3,4, November 21, 2017. [online]. Available: https://www.link-labs.com/blog/z-wave-vs-zigbee [Accessed Feb. 13, 2018].

[20] C. M. Talbot, M. A. Temple, T. J. Carbino, and J. A. Betances, "Detecting rogue attacks on commercial wireless Insteon home automation systems," *Comput. Secur.*, vol. 74, pp. 296–307, 2018.

[21] C. Talbot, M. Temple, and T. Carbino, "Securing insteon home automation systems using radio frequency distinct native attribute (RF-DNA) fingerprints," *Proc. 12th Int. Conf. Cyber Warf. Secur. ICCWS 2017*, pp. 497–505, 2017.

[22] https://www.vesternet.com/pages/x10-or-z-wave

[23] O. Bello, S. Zeadlly and M. Badra," Network layer inter-operation of Device-to-Device communication technologies in Internet of Things(IoT)", Ad Hoc Networks, Vol. 57, pp. 52-62, March 2017.

[24] D. Naresh, B. Chakradhar, and S. Krishnaveni, "Bluetooth Based Home Automation and Security System Using ARM9," *Int. J. Eng. Trends Technol.*, vol. 4, no. 9, pp. 4052–4058, 2013.

[25] R. Piyare and M. Tazil, "Bluetooth based home automation system using cell phone," *Proc. Int. Symp. Consum. Electron. ISCE*, pp. 192–195, 2011.