SURVEY ON SMART HOME TECHNOLOGIES AND THEIR SCALING CHALLENGES: INTEROPERABILITY, SECURITY, AND HEALTHCARE INTEGRATION ISSUES IN AMBIENT ASSISTED LIVING SYSTEMS

Dr. Hana kim[1]
prof. Giulia conti[1]
[1] university of copenhagen, department of smart environments and biomedical iot systems, copenhagen, denmark

ABSTRACT

A perfect smart home technology is like an interface between humans and systems. It can detect the human feelings and situations. Then it automatically control the home appliances according to their needs. Home appliances can use various type of technologies for communication. In this paper characteristics of different wireless communication techniques like Wi-Fi, ZigBee, Bluetooth, EnOcean, Z-Wave, WiMax, Thread and GSM are studied and their working principles are compared with each other. From this users can choose their own choice of technologies. In SH-IoT the key requirements are channel security, handover support, consistent data rates and mobility management. Proxy mobile IPv6(PMIPv6) is one of the core solutions to handle extreme mobility. The default PMIPv6 using SH-IoT cannot ensure performance enhancement, that is Route Optimization(RO). The existing protocols for RO in PMIPv6 based home automation systems cannot support security. So in this survey, security of route optimization in home automation systems are also discussed, their advantages and disadvantages are highlighted. Proposed system is a combination of refined smart home technology with secure route optimization.

KEYWORDS: component; Smart Home technologies, Proxy mobile IPv6, Route Optimization.

1. INTRODUCTION

Smart city movement make massive influences in people, from both local areas and crowded cities. As a part, availability of money changes the lifestyle, then they depend more up on machines. Primary aim of people is make living more comfortable, convenient, entertaining, sustainable provide security, here the relevance of smart home technology was arrived.

A smart home is a working environment, it control the device or systems automatically using technologies. A Home with techniques to automatically adjust the temperature, provide security and allow effective communications to all over the world are benefit to all. Especially for elderly and disabled people. But they do not go too far and affect the freedom of choice of the person living within them [1]. In brief smart home is a integrated version of safety (for example alarms generated when an intruder enters into a home), Environmental control systems (for example remote control or programmed controlled doors, windows and lights, now automatic control lights are also available), communication (linked to the telephone or the Internet) energy control systems (for example adjusting the heat generated during electronic devices are working) and entertainment (for example television, film and music)[1].

The rest of the paper is organized as follows. Section II briefly review some smart home technology. In section III,various current and proposed RO mechanism are discussed.

2. SMART HOME TECHNOLOGIES

A. IEEE 802.15.1 Bluetooth LE

It is introduced by R.Piyare and M.Tazi. Hardware components are used in this type of home automation system is smartphone and Arduino board and is communicated through wireless Bluetooth technology, it is low cost and provide security. Data rate is 3Mbps and bandwidth is 2.4 GHz.

B. Voice Recognition Based Home Automation

It is one of the most user friendly home automation system. Hardware architecture of this automation system are Arduino UNO and a cell phone. Communication between these components are taken by wirelesses using

Bluetooth technology. Range of Arduino BT board is around 10 to 100 meters, data rate is 3Mbps and bandwidth is 2.4 GHz. Operating system (OS) of smartphone detect the voice of user with the help of built-in voice recognizing feature of that OS [2]. Then convert this voice command to text message, and the text message is transmit to Bluetooth module HC-05. It is connect to the Arduino UNO. Then the smart phone application control the home appliances.

C. ZigBee Based Wireless Home Automation System

It consists of three modules, microphone module (it use ZigBee protocol), central controller module(based on PC) and appliance controller module. Voice recognised by microphone module is using Microsoft speech API and are communicating through RF ZigBee(wireless communication technology). It consume low power and cost effective.

D. GSM Based Home Automation System

Hardware components contains in Global System for Mobile communication (GSM) based home automation system is GSM modem, PIC16F887 microcontroller and smartphone. Electric appliances are controlled through SMS request and GSM it is handled by GSM module. This received message is read and decode with the help of microcontroller. It is connected to the home appliances.

E. EnOcean Based Home Automation System

Hardware components contains in Global System for Mobile communication (GSM) based home automation system is GSM modem, PIC16F887 microcontroller and smartphone. Electric appliances are controlled through SMS request and GSM it is handled by GSM module. This received message is read and decode with the help of microcontroller PIC16F887 and execute the command. It is connected to the home appliances.

F. Internet Of Things (IoT) Based Home Automation System

Various components are used to design the system such as embedded micro web server, controlling devices, smartphone and a software application. And its controlling also done using the same. Now it is the most widely used technique for home automation. The system architecture consists of three important sections, they are home environment, home gateway and remote environment.

3. LITERATURE SURVEY

This literature survey mentioned three different papers for comparisons. These papers proposed different methods. Default Proxy Mobile IPv6 (PMIPv6) based SH-IoT networks[4] allow a Mobile Node (MN) to communicate with Corresponding Nodes (CNs). Corresponding Nodes is SH-IoT devices in home. Its location and movement are taken through two intermediate nodes. They are Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA). A smart home is composed in a PMIPv6 based SH-IoT networks by using Home Gateway (HGW) and SH-IoT devices. And each device on the HGW to communicate with external entities including MNs. It can be noticed that every message, which is to be transferred to/from the CN, follows a non-optimal path among the MAG, LMA, and HGW leading to excessive performance overheads. But the problem is that, whenever a handover decision is made, it must repeat the all procedure, through the MAG-LMA-HGW(path). It leads to increases the handover latency.Then it affects the entire network and decreases the performance. This problem arises due to there is no proper RO (Route optimization), and also problem is that, if RO is present it must be secure properly. If not secured it is attacked by various malicious attackers. In this approach there are three trusts are recognised. They are trust between MN and MAG, trust between MAG and LMA, and trust between HGW and CN. But it is not enough to secure the RO, if it is Available. Because using this techniques MAG cannot authenticate with HGW and exchange session keys. So triangle routing is a major issue of this paper.

In PMIPv6 Route Optimization Mechanism using the Routing Table of MAG [2] introduce a new mechanism to provide Route Optimisation. Here network has a hexagonal structure and contain n cells. It uses routing table of MAG for analyse the route. Here MN can move to another cell within the PMIPv6 domain and attach any MAGs except MAG2, in which the ON is attached where the ON is assumed as a wireless node. The ON-RO procedure follows by every hand off of the MN, because the optimized routing path is changed by MNs current location. The cost of ON-RO mechanism can be divided into a signaling cost and a packet delivery cost. In addition, the cost of MNs hand off is divided into a signaling cost and a packet delivery cost. We compare these costs with the PMIPv6 base specification (PMIPv6) and the ON-RO enabled PMIPv6 (PMIPv6-ON).

In Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks[4], the problem of secure RO is considered for a SH-IoT. The task of eliminating the excessive dependency over the LMA is handled on the basis of the pre-established trust between the HGW and the LMA, which can be

achieved by the smart home users with the help of smart home cloud services. That is the proposed approach counts on the pre-shared key between the LMA and the HGW to provide mutual authentication and secure session key exchanges among the established session keys, the first key, derived from the pre-shared key, and is used to protect the Diffie Hellman Key exchange for the second one, which is the master session key. Note that the master session key is established in a way for supporting Perfect Forward Secrecy (PFS) as well as is used to derive the last two session keys, which protect the confidentiality, authenticity, and privacy of the exchanged data between the MN and the CN. The key highlights of this paper is

- Secure transmission between the MN and the CN along with route optimization.
- Lower handover latency and high delivery ratio along with a high probability of handovers.
- Formal security analysis on the proposed security.

4. COMPARISON

Smart home technology very useful especially for disabled people.It reduces the energy consumption there by saving money and resources. So the main purpose of home automation is to provide improved convenience, comfort, and efficiency. For a good communication between controlling unit and home devices must have a well coordination between them.The lack of coordination during IoT expansion has resulted in a variety of communications protocols being developed. Communication between IoT devices/servers relies on underlying protocols. Which must be efficient and effective to establish and maintain reliability and integrity of data transfer.To a certain degree the Smart Home and Smart City share the same architecture, technologies and protocols, and therefore, are facing the same challenges.security goals for a smart home to meet are Integrity, Confidentiality and Availability. So the discussion on secure and reliable smart home technologies for communication and an effective communication protocols are discussed here.To identify best protocol and efficient security mechanism comparison is done on various parameters like architecture, protocols, methodology, mechanisms etc

5. CONCLUSION

A perfect smart home technology can act as a interface between humans and systems for detection of human intentions, feelings, and situations. In this paper many smart home techniques are discussed. Digi XBee Series-2 RF technology could help to minimize some problems occurring when the smart home technology is extend to wide campuses. Most of the networks are using triangle routing. It cause threats during hand-over and no security for routing. PMIPv6 route Optimization mechanism using routing table of MAG[2] uses triangle routing and thus cause threats during hand-over. In Secure and Efficient Protocol for Route Optimization in PMIPv6 Based Smart Home IoT Networks [4] method triangle routing is eliminated and provide optimal routes and security by introducing a new protocol. Building automation is an emerging application of smart home technology, proposed system is a combination of refined smart home technology with secure route optimization.

REFERENCES

[1] Muhammad Asadullah and Ahsan Raza. An overview of home automation systems. In 2016 2nd International Conference on Robotics and Artificial Intelligence (ICRAI), pages 27–31. IEEE, 2016.

[2] Byung-Jin Han, Jae-Min Lee, Jong-Hyouk Lee, and Tai-Myoung Chung.
Pmipv6 route optimization mechanism using the routing table of mag. In
2008 Third International Conference on Systems and Networks Communications, pages 274–279. IEEE, 2008.

[3] Toril Laberg. Smart home technology; technology supporting independent living-does it have an impact on health. In Tromsø Telemedicine and eHealth Conference, Tromsø, pages 23–24. Citeseer, 2005.

[4] Daemin Shin, Vishal Sharma, Jiyoon Kim, Soonhyun Kwon, and Ilsun

[5] You. Secure and efficient protocol for route optimization in pmipv6-based smart home iot networks. IEEE Access, 5:11100–11117, 2017.