ANALYSIS OF SIP'S APPLICABILITY IN SMART GRID ENVIRONMENT

Rohan Mukkamala
B.Tech., Jawaharlal Nehru Technological University, India, 2008

PROJECT

Submitted in partial satisfaction of
the requirements for the degree of

MASTER OF SCIENCE

in

COMPUTER SCIENCE

at

CALIFORNIA STATE UNIVERSITY, SACRAMENTO

SPRING
2011

ANALYSIS OF SIP'S APPLICABILITY IN SMART GRID ENVIRONMENT

A Project

by

Rohan Mukkamala

Approved by:

______________________________________, Committee Chair
Isaac Ghansah, Ph.D.

______________________________________, Second Reader
Ying Jin, Ph.D.

____
Date

Student: Rohan Mukkamala

I certify that this student has met the requirements for format contained in the University format manual, and that this project is suitable for shelving in the Library and credit is to be awarded for the Project.

___ __________________________, Graduate Coordinator __________________

Nikoruz Faroughi, Ph.D. Date

Department of Computer Science

Abstract

of

ANALYSIS OF SIP'S APPLICABILITY IN SMART GRID ENVIRONMENT

by

Rohan Mukkamala

Smart Grid is the modernization of the existing power grid, which utilizes the digital technology for the two-way exchange of information and electricity between the utilities and consumers. It requires a 'communication overlay' network, which facilitates intelligent communication between various nodes of the heterogeneous Smart Grid network. SIP is widely used in similar 'communication overlay' networks for the IP telephony as an established de-facto protocol for 'session management'. This project discusses the use of SIP in the Smart Grid environment.

This project gives a detailed analysis on the appropriateness of using SIP (Session Initiation Protocol) in the Smart Grid environment. The project mainly investigates the role of SIP in HAN (Home Area Network) and Demand Response System. In HAN, one of the network segments of the Smart Grid network, the interaction of the residential or commercial devices (such as TV, washing machine, surveillance camera, etc.) with the smart meter/energy management system and vice-versa is analyzed. An observation of the proposed SIP-Zigbee interworking architecture involving the SIP presence framework is done. The Event-service model of SIP is analyzed which makes it an effective protocol and architecture to realize open automated demand response system in the smart grid.

In this report, SIP's support for mobile metering, the realization of an efficient SIP-Zigbee Internetworking architecture and an Open-ADR system based on SIP's Presence Framework and Event Service model respectively strengthens the candidacy of SIP for deployment in various components of the Smart Grid infrastructure.

__________________________, Committee Chair
Isaac Ghansah, Ph.D.

____
Date

ACKNOWLEDGMENTS

I would like to thank my project advisor, Dr. Isaac Ghansah for his guidance and constant support throughout the project. His suggestions have been of great value for the project.

Words alone cannot express the gratitude, I owe to my loving parents for their constant support throughout my life.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Page

Chapter 1

INTRODUCTION

1.1 Background

1.1.1 Smart Grid

There is an urgent need to address the problem of a steady increase in the demand for energy. A smart grid can address this problem by the improvement and modernization of the existing power grid [1]. Smart grid uses information technology in order to provide a two-way exchange of information as well as electricity. It is a paradigm shift in the electricity system. It can be said as a transition from a traditional power grid, which is a one-way system of disconnected power suppliers to an intelligent two-way interoperable digital network [2]. The essential concept of a smart grid can be observed in figure 1.

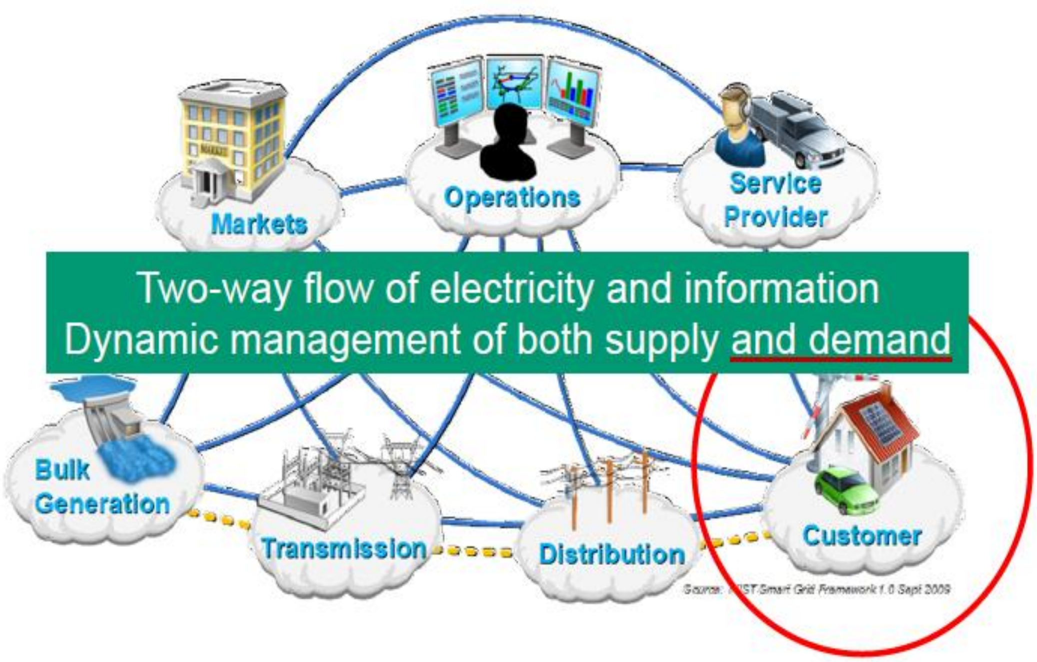

Figure 1: The Concept of Smart Grid [5].

The following areas are benefits of having a smart grid [3]:

a) Reliability: By minimizing the power outages and improving the quality of power.
b) Economics: As the operation of the grid is based on the basic laws of supply and demand, it will result in adequate supplies and fair pricing.
c) Efficiency: Brings down the production, transmission, consumption costs, transmission and distribution losses. The demand response program of Smart grid plays a major role in this.
d) Environmental: Reducing the air pollution (greenhouse gas emissions) by supporting the Plug in electric vehicles (PEV's) and renewable sources of energy.
e) Security: Minimizes the possibility of manmade errors, reduces vulnerabilities and fast recovery to natural disasters. The improvement of cyber security helps to provide resilience to physical and cyber attacks without suffering massive blackouts.
f) Safety: Reducing the scope of accidents in grid related events.

The components of the Smart Grid infrastructure such as the Demand management, smart appliances, Generators etc, can be seen in figure 2.

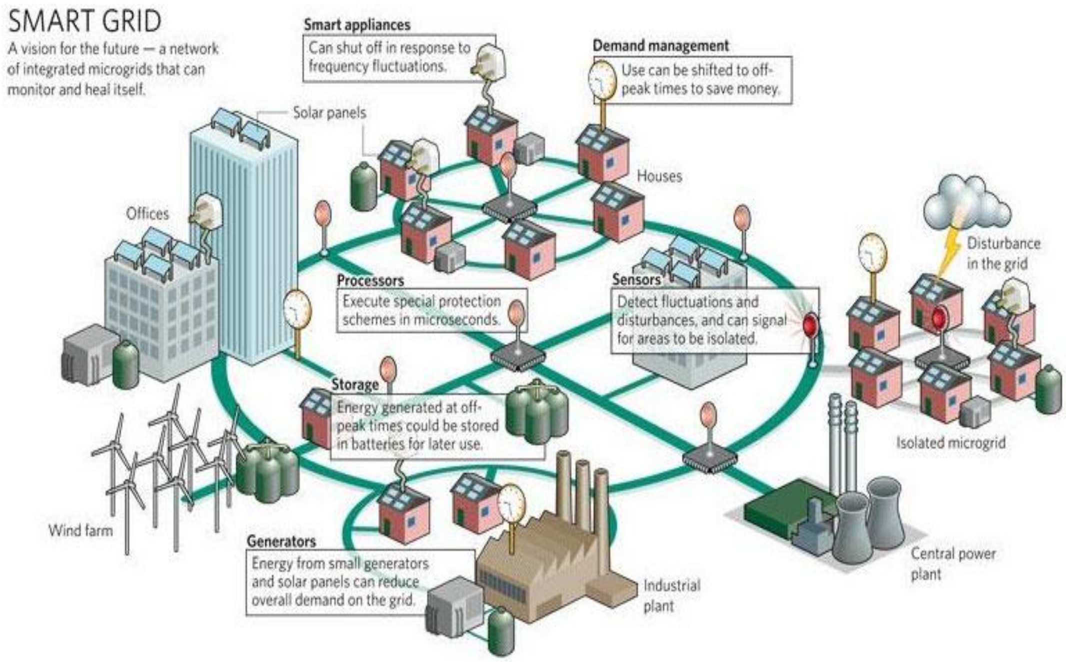

Figure 2: Smart Grid Infrastructure [6].

One of the key roles in the growth of the Smart Grid is to bring manufacturers, consumers, energy providers, and regulators together to develop interoperable standards [4]. NIST, the national institute of standards and technology is a measurement standards agency, which makes sure that these pieces of "the world's largest and most complex machine" are able to work together [7]. Organizations which are as diverse as Electric Utilities, US Department Of Energy (DOE), NIST, Google, Microsoft, General Electric, IEEE, NERC, FERC, IEC, and ANSI have published documents about Smart Grid. This in a way proves the importance given for the Smart Grid [7].

1.1.2 SIP (Session Initiation Protocol):

In the mid-1990s, SIP first emerged in the Columbia University as the result of a research project which prevailed as the facilitator for VoIP and instant messaging [8]. Currently many hardware devices, PC applications like Skype, applications for smart phone and online services have SIP installations embedded in them. In 1997, Multiparty Multimedia Session Control (MMUSIC) submitted SIP Version 1.0 to the IETF as an internet draft which later advanced to proposed status and was then shortly published as RFC2543 which eventually was replaced with a revised standard, RFC3261 [14].

As stated in the IETF draft, RFC3261 describes Session Initiation Protocol (SIP) as "an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia, distribution, and multimedia conferences [9]."

There were several additional standards published later on such as the reliability of provisional responses was discussed in RFC3262; on locating of SIP servers in RFC3263; the offer/answer model in RFC3264; and on specific event notification in RFC3265 [8]. Simple Mail Transfer Protocol (SMTP) and Hypertext Transfer Protocol (HTTP) are the two other relatively new application protocols at the time, which played an influential role in the design of SIP. SIP is a session management protocol commonly used for VoIP signalling.SIP replaced H.323 protocol standard, which was formerly used for signaling [10]. The calling features of a traditional telephone system are supported in SIP but its usage is not limited to just voice applications. It is also used as a general purpose protocol for multimedia communications.

SIP supports the following functionality [10]:

a) User Location: This determines the addresses of both the end parties without knowing the details of each other's device addresses or physical locations.
b) User Availability: This determines whether the called party is willing to communicate with the caller at that point of time.

c) User Capabilities and Session Setup: Handles negotiations that enable all participants in a session to agree on common media and the technology details involved—including voice, video, audio, instant messaging, applications data exchange so that at both the called and calling party the session parameters are established.

d) Session management: Manages the adding, dropping of participants and allows for media change while a session is in progress.

SIP Protocols:

Call setup and termination part of the SIP uses the Session Description Protocol (SDP) to describe the configuration of the call. Real-time Transport Protocol (RTP) is used for the data transfer and Real-time Transport Control Protocol (RTCP) is used for data stream management. SIP can run over User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Asynchronous Transfer Mode (ATM) or any datagram or stream protocol [11]. The audio and video streams are transmitted over the Real-time Transport Protocol over UDP. SIP is commonly run over TCP/IP because of its widespread connectivity [11]. But UDP will be the preferred method due to its better performance and scalability. 5060 is the default port for SIP although any available port may be used. In figure 3, we can observe the SIP protocol stack.

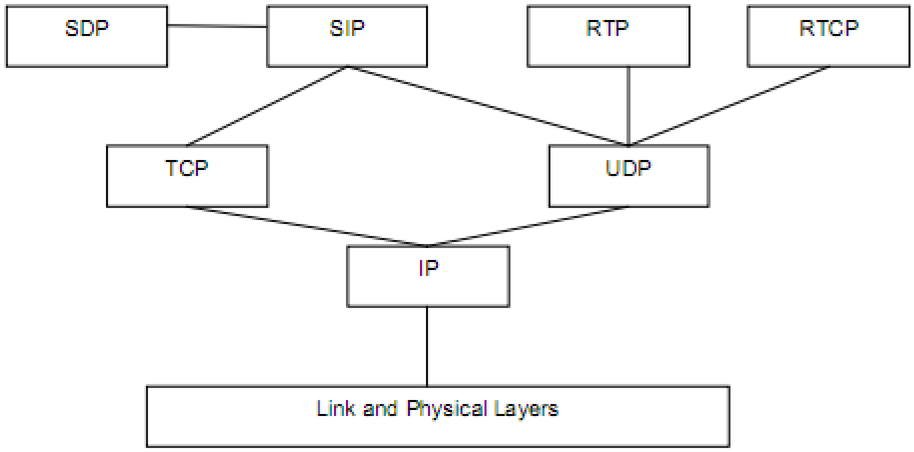

Figure 3: SIP Protocol Stack [11].

SIP Addressing:

Addressing in SIP uses URLs (Uniform Resource Locators) which supports both internet and PSTN addresses. The general form is name@domain and in order to complete a call, it needs to be resolved down to user@host.User name or a telephone number comprises of the user part and the host part may be a domain name, a host name or a numeric network address.

Some typical SIP URLs are:

a) sip: land@emphis.com (host independent)

b) sip:clinton@whitehouse.gov (host specific)

c) sip:+1-800-555-1212@information.att.net

SIP is regarded as a text based and highly extensible as it borrows many concepts from HTTP and SMTP. Features like mobility, call control and interoperability with many standards can be accommodated in SIP.

SIP Entities:

As seen in figure 4, an SIP network comprises of four types of logical SIP entities. They are as follows [12]:

a) User Agent: In SIP, user agents are the endpoint entities who initiate or terminate a session. User Agent is defined as an application in RFC2543, which contains both a User Agent client and User Agent server, as follows:

User Agent Client (UAC) – It is a client application that originates the call or SIP requests. User Agent Server (UAS) – It is a server application that listens to the request or call and returns SIP responses to the client. Workstations, IP-phones, telephony gateways, call agents are examples of devices having a UA function in SIP network.

b) Proxy Server: A proxy server is an intermediate stateless server, which decides the next hop and forwards for the purpose of making requests on behalf of other clients. It relays call signaling and operates in a transactional manner.

c) Redirect Server: A redirect server is a server, which accepts a SIP request and sends address of the next hop back to the client. It directs the client to an alternate set of URIs.

d) Registrar: A registrar is a server, which maintains the users contact information in a database at a location server and accepts clients request for the purpose of updating the information.

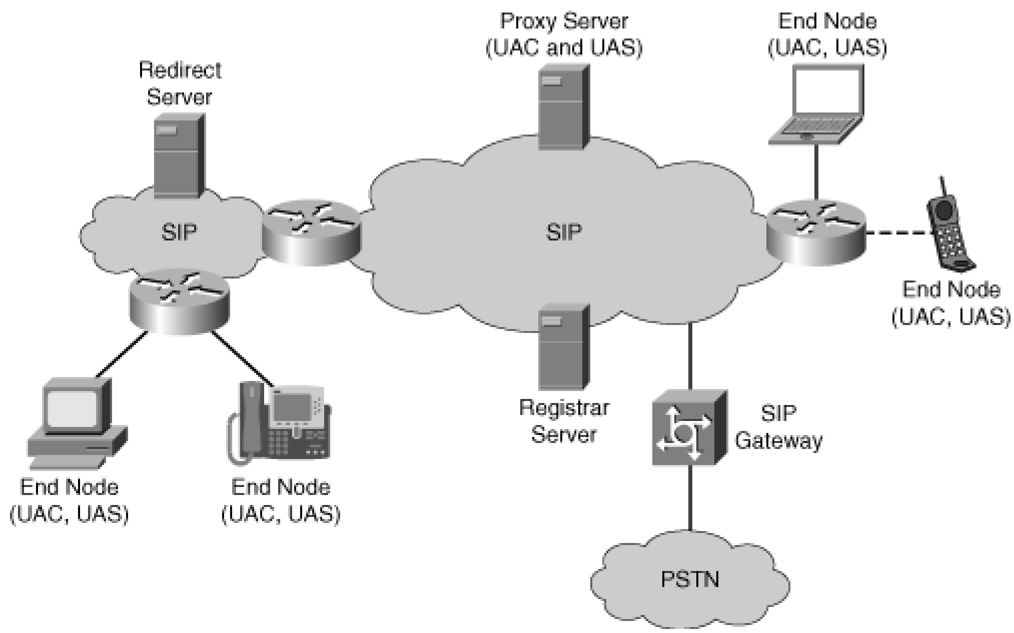

Figure 4: SIP Network [55].

An SIP session between two end points can be seen in figure 5.The request methods in SIP are as follows [12]:

a) REGISTER: Used by a UA to bind a permanent address to current location and may convey user data.

b) INVITE: Initiates a session and the message body includes the session.

c) ACK: Acknowledges, confirms session establishment and final response for INVITE.

d) CANCEL: Terminates or cancels a pending request or INVITE.

e) BYE: Terminates a session (hanging up).

f) OPTIONS: Inquires for information about the capabilities of a caller or client.

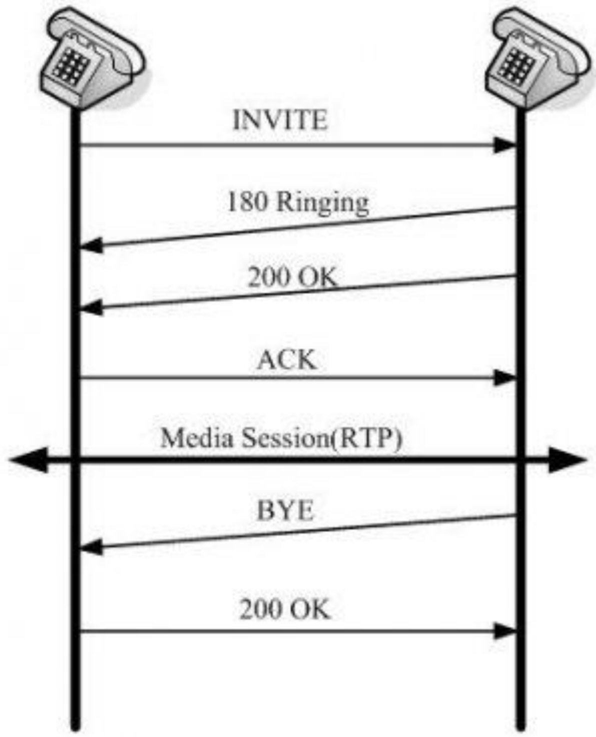

Figure 5: SIP Session between Two Entities [56].

Response messages in SIP contain numeric response-codes, which are partly based on HTTP response codes. They are as follows [9]:

a) 1xx = provisional, searching, ringing, queuing etc (being processed).

b) 2xx = success

c) 3xx = redirection, forwarding

d) 4xx = request failure (client error)

e) 5xx = server failures

f) 6xx = global failure (busy, refusal, not available anywhere and cannot be fulfilled at any server)

An Internet-based architecture is enabled by SIP to manage communication sessions over IP networks, resulting in converged multimedia sessions [13]. In this way, the communications landscape is reshaped by SIP.

1.2. Reason for considering SIP in Smart Grid

The Smart grid uses an intelligent communication system where the IP-based networks will play a crucial role. The IETF was given the task of submitting a document that identifies the structure of the internet protocol suite and also the key protocols which are considered critical to integrate the smart grid devices into an IP based infrastructure [16]. IETF responded by publishing the following draft:

http://tools.ietf.org/html/draft-baker-ietf-core

This draft mentioned SIP as the suitable protocol for the multi-media session management in the internet [16]. This interested many organizations like Avaya, Cisco and many groups, forums etc. to research on the potential aspects of SIP in Smart grid.

Many consider that SIP is only a VOIP/telephony protocol. This is a common misconception as SIP supports MIME type of payload and supports multi-media sessions, which may contain voice, video, instant messaging, shared data, and subscriptions of events.

As seen in Figure 6, SIP is an application level protocol, which runs over TCP or UDP. SIP offers maturity, extensibility, reliability, scalability and the interoperability to work with other protocols. These features help SIP to leverage much of the functionality from the IP networks based on the TCP/UDP etc [15]. SIP also supports next generation networks through the ubiquitous connectivity. The research paper by Konnetic on SIP states the following:

“Session Initiation Protocol (SIP) has emerged as the strongest candidate to provide the signaling backbone for the next generation networks and the future of ubiquitous connectivity [8].” SIP supports mobile metering which is useful for PEVs and it brings in a robust unified communication capability to the Smart Grid infrastructure [15].

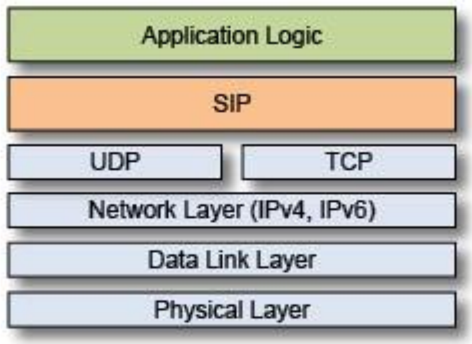

Figure 6: SIP in OSI Model [15].

1.3. Scope of the Project

The main focus would be to investigate the role of SIP in HAN (Home Area Network) particularly with the Zigbee specification and Demand Response System. This report attempts to explore the various features and concepts that SIP brings in such as the presence framework, offer-answer model, event service model etc and their role in the influencing the HANs and demand response systems of the smart grid environment. It also discusses security threats and the countermeasures for SIP.

1.4. Report Organization

This report is organized as follows:

- Chapter 1: Introduction

  This chapter gives an introduction to to the concepts of Smart grid and SIP. It also discusses the reason for considering SIP in Smart grid and the scope of the project.

- Chapter 2: Review of HAN, ZigBee, PEV and DR

  In this chapter, an overview is given for the understanding of Home area networks, ZigBee wireless networking standard, Plug in electric vehicles and the Demand Response system as a part of the Smart grid infrastructure.

- Chapter 3: Analysis of SIP

  This chapter analyzes the role of SIP in the Smart Grid Infrastructure (HAN, ZigBee, PEV and DR) and evaluates the appropriateness of using SIP.

- Chapter 4: Security Considerations

  This chapter identifies the security threats faced by an SIP based architecture in the Smart grid environment and the countermeasures involved in securing the environment.

- Chapter 5: Conclusion

  This chapter comprises of brief summary of the project report, the conclusion arrived and the scope for future work.

- Glossary

- References

Chapter 2

REVIEW OF HAN, ZIGBEE, PEV AND DR

2.1. Home Area Networks (HAN)

HAN is considered as one of the important network segments of the smart grid network where emphasis is given on how the residential or commercial devices like TV, washing machine etc. interact with the smart meter or energy management system and vice-versa [17].

It is a challenging task for the utilities to manage the energy consumption at the consumer side. This is achieved through the intelligent control of in-home devices, which can guarantee an automated home environment while maintaining the consumer costs. HAN is considered as an essential tool that allows multiple devices in a home to interact with the smart grid applications in an intelligent way [21]. A two-way communication between the devices, users and utilities is facilitated by the HAN, which is made possible by the deployment of the Advanced Metering Infrastructure (AMI), which combines the HAN and NAN (Neighborhood Area Network) [21]. NAN is responsible for connecting the homes for the utility network. The ultra low-power IEEE 802.15.4-based wireless networking standard is considered as the key to robust, reliable and secure HAN deployments and Zigbee based on IEEE 802.15.4 is considered as the most popular open standards for HANs [20]. A typical HAN can be seen in figure 7.

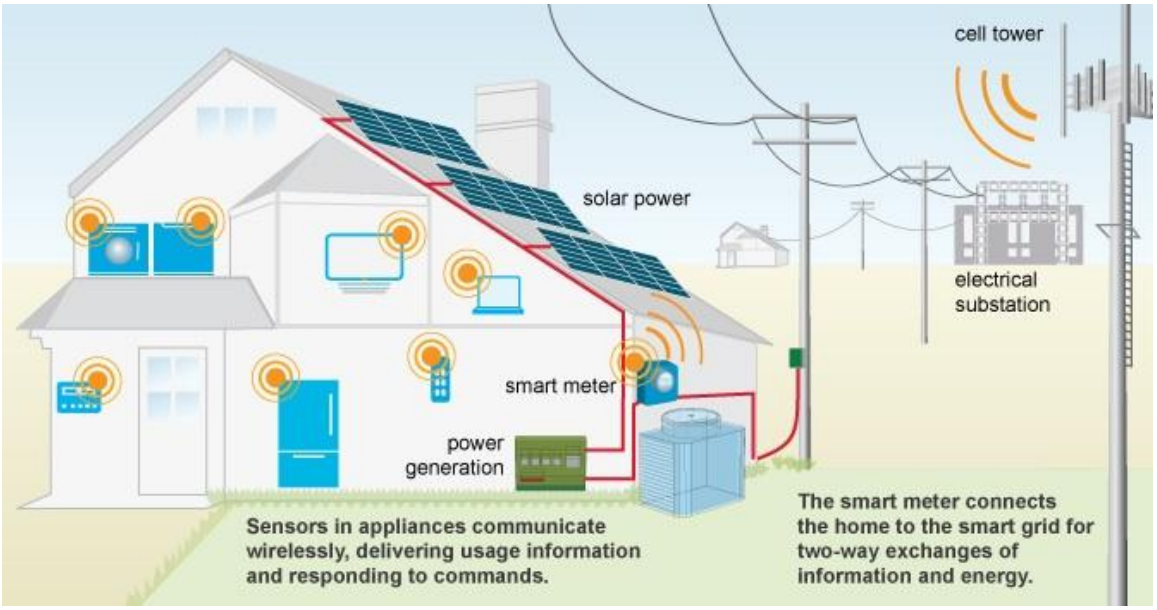

Figure 7: Home Area Network [21].

The following is an excerpt as stated in the Green Tech Media (GTM) report:

"GTM Research forecasts the HAN and home energy management market to grow nearly 90% from $400 million in 2011 to over $750 million in 2015. The market's scaling potential is buoyed by the need for utilities to provide compelling consumer energy services in parallel with their projected $16.7 billion smart meter rollout over the next five years [19]."

The above excerpt gives us an insight into the huge market scope for the HAN and the energy management system.

The introduction of the smart grid infrastructure like the in-home display units etc. into the HAN will empower the consumer to participate in energy management programs, which will help in maintaining the peak energy demand for the utilities. Some of the benefits achieved through this approach are as follows [18]:

a) Maintaining a centralized access to multiple devices in a HAN.

b) Receiving the price alerts sent by the utilities.

c) Controlling and monitoring of real time data.

d) Real-time information on the energy consumption.

e) Enabling a proactive role for the consumer in the energy savings.

f) Optimization of energy usage.

2.2. Zigbee

Zigbee is a very popular wireless networking technology built on top of IEEE 802.15.4 standard for implementing low-cost, low-power wireless monitoring and control networks which are used to automate the home through the HAN appliances and devices like wireless light switches with lamps, electrical meters with in-home-displays, consumer electronics equipment via short-range radio [22]. In comparison to other Wireless Personal Area Networks (WPANs) such as Bluetooth, Zigbee is considered much simpler and less expensive [25]. The applications which require low data rate, secure networking and long battery life are targeted by Zigbee. A Zigbee-based HAN can be seen in figure 8.

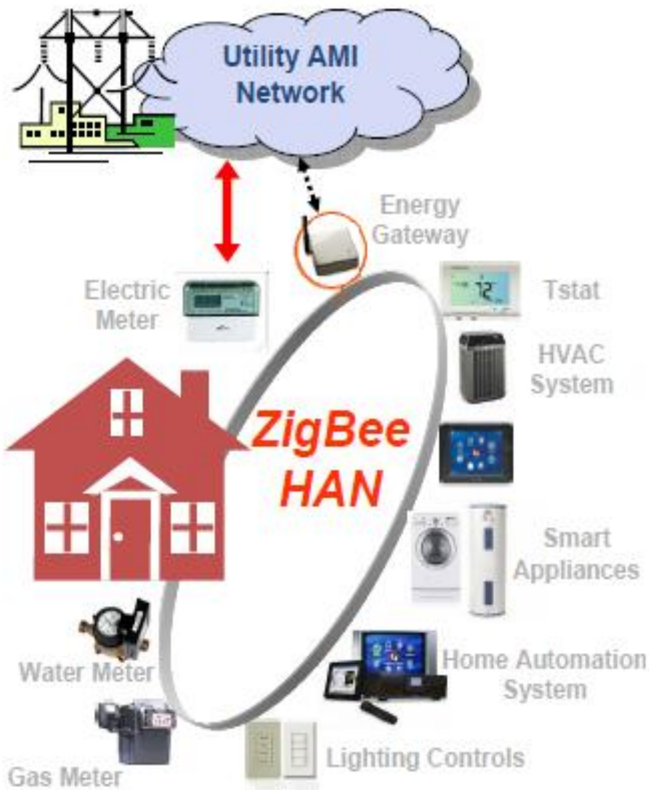

Figure 8: Zigbee-Based HAN [27].

The IEEE 802.15.4 Working Group defines the lower layers of protocol stack (See Figure 8) which are Medium Access Control Layer (MAC) and Physical layer (PHY) [24]. The Zigbee alliance can be said as a consortium of 50+ companies with a goal to define a complete open global standard for Zigbee. This Alliance takes the responsibility to define upper layers of protocol stack: from network to application, including application profiles and also provides compliance, certification testing and branding [25]. The Zigbee platform can be seen in figure 9.

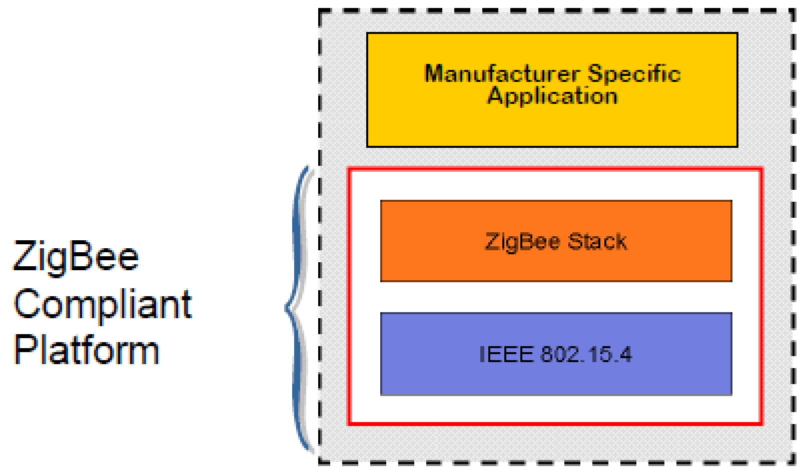

Figure 9: Zigbee Platform [22].

The Zigbee standard is built on top of IEEE 802.15.4 specification for the PHY and MAC layers. ZigBee defines the network layer and the application layer framework that provide services such as security and multihop routing [26]. Then the network (NWK) layer and the application support (APS) sub-layer, the Zigbee device object (ZDO) and the manufacturer-defined application objects which form the framework for the application layer are provided by the Zigbee Alliance [26]. These layers are built on the foundation laid by the 802.15.4 standard. All the layers of the Zigbee stack can be observed in figure 10.

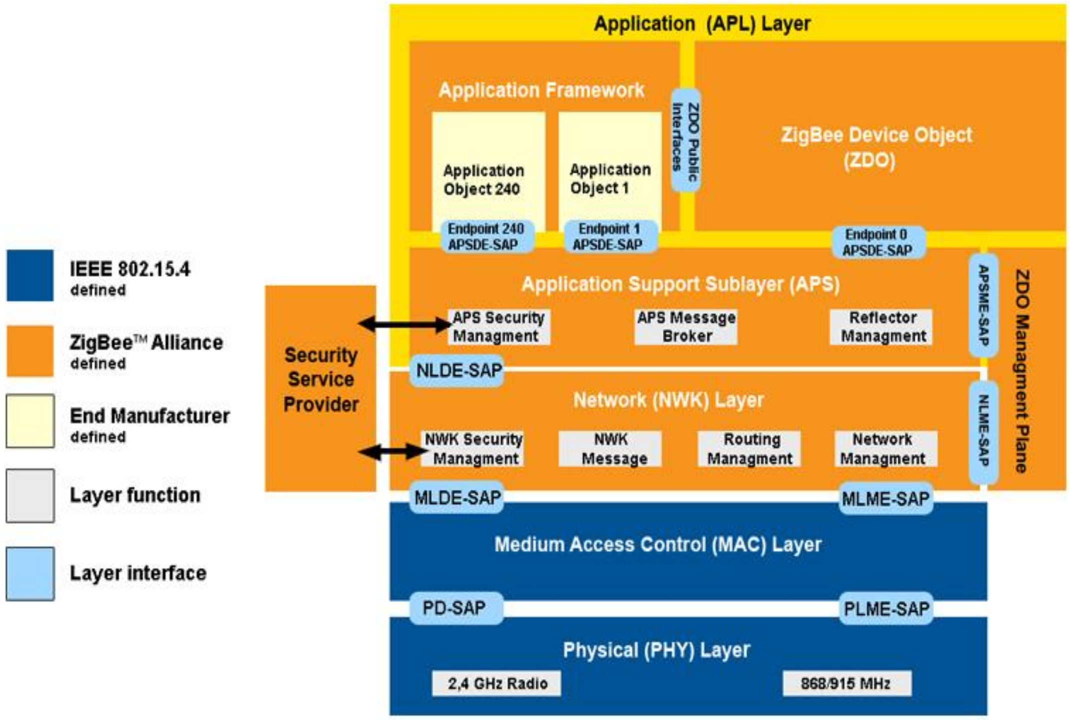

Figure 10: Zigbee Stack Architecture [23].

The types of Zigbee devices are as follows:

a) Zigbee Coordinator (ZC)

b) Zigbee Router (ZR)

c) Zigbee end device (ZED)

- Zigbee Coordinator (ZC) is a fully functional device (FFD), which is used to initiate network formation and stores information about the network. It has routing functionality and acts as a bridge to other networks. Only one ZC is required in a network.
- Zigbee router (ZR) is a reduced functional device (RFD) which routes between nodes and extends the network coverage.

- Zigbee end device (ZED) is a reduced functional device which is optimised for low power consumption and does not participate in the routing. It is the cheapest device type [26].

The following are the network topologies available for Zigbee (See Figure 11):

a) Star
b) Mesh
c) Cluster Tree

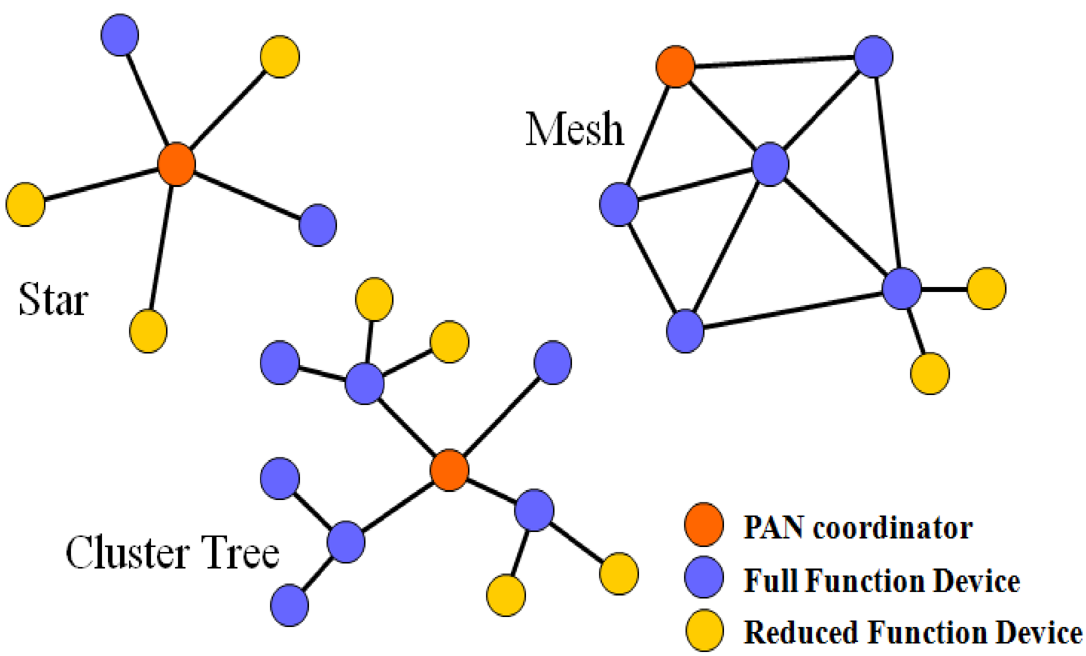

Figure 11: Zigbee Network Topologies [23].

The mesh network topology is a preferable choice for the design of ZigBee as mesh topology offers many advantages in HAN with multiple devices, including higher data reliability due to multiple transmission paths [23]. The following are few of the important terminology used in Zigbee [23]:

a) Node and Subunits: There can be a number of nodes in a Zigbee network. A node can be defined as a piece of hardware, which shares a single radio. A node can have many subunits like switches, bulbs, thermostats etc. So, the subunits in a node share the same radio. There can be a maximum of 240 subunits per node and each subunit is identified by a unique endpoint which is numbered from 1 to 240.

b) Zigbee Application: A group of application objects present on the same or different nodes is called a Zigbee application. Take the example of a lighting system application which consists of lighting controls, bulbs, switches, light sensors etc.

c) Zigbee Device Descriptors: A device descriptor comprises of an input and output data attributes in relation to the description of the functionality of the device. For example, the temperature attribute of the thermostat represents the temperature of the room.

d) Zigbee Device Objects (ZDO): The functionality or role of the devices within a network like the Zigbee coordinator, Zigbee end device etc. are given by the ZDO. The ZDO resides between the Application layer (APL) and Application Support Sub layer (APS).

e) Clusters, Zigbee Binding and Binding Table: A cluster can be referred to as a "group of of attributes" in a profile. Each cluster is identified by a unique cluster ID with respect to a profile. A binding can be said as a point to point logical link between Input/Output ClusterIDs belonging to one Application Object and Input/Output ClusterIDs of another Application Object. The information about the bindings between nodes is stored in a Binding Table.

Consider figure 12, where we can observe two nodes, a switch unit and a lamp unit where binding of their cluster IDs takes place as per the binding table and a logical link is established between the nodes which results in the control of lamps by the switches as shown below:

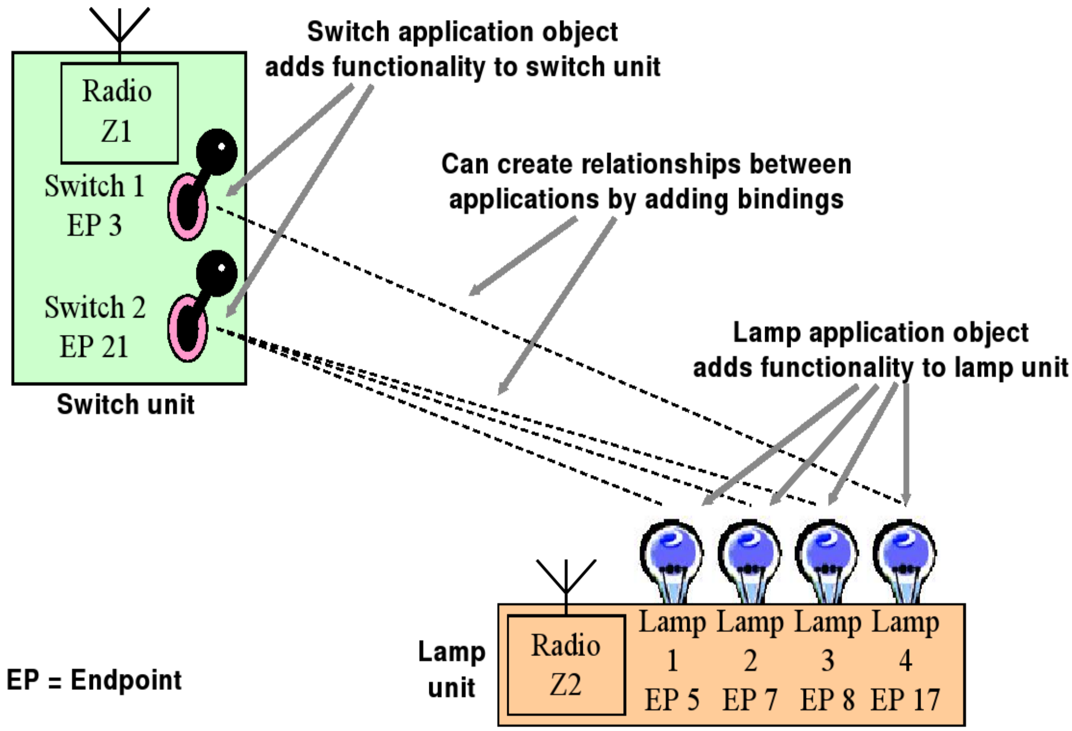

Figure 12: Zigbee Binding [23].

1) Zigbee network Gateway (See Figure 11): The responsibilities of the gateway would be to interface a Zigbee network into an external system, and to provide inter-network communications for the possibility of a global network that unites a number of underlying Zigbee networks as well as other solutions and information systems. Providing an interface between Zigbee and IP devices is an important aspect.

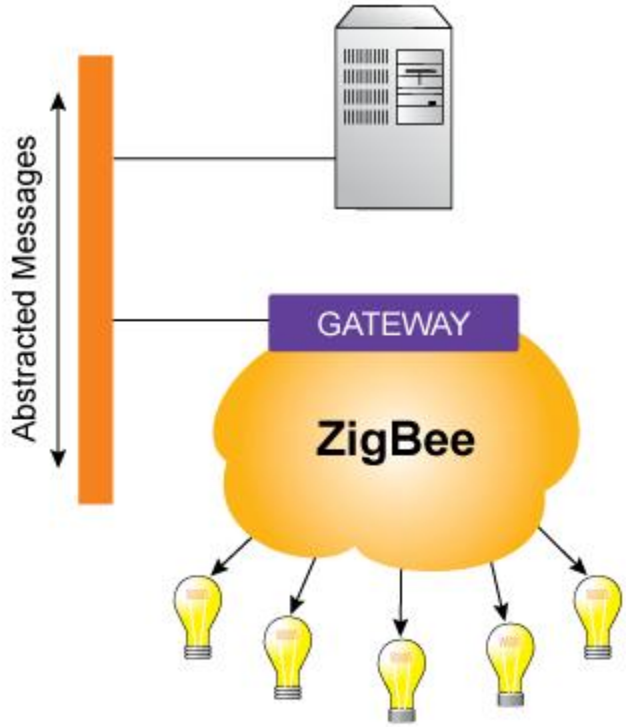

Figure 13: Gateway [23].

The characteristics of Zigbee can be summarized as follows [26]:

a) Reliable and self healing

b) Supports large number of nodes

c) Easy to deploy

d) Very long battery life

e) Secure

f) Low cost

g) Can be used globally

2.3. PEV (Plug in electric vehicle)

PEVs are being encouraged in the market presently as they are not dependent on the oil resources which have always been a fluctuating market. The emission of green house gases is very low in PEVs which will reduce the effect of global warming. In order to make the continued use of PEVs more prevalent, a massive deployment of the battery technology and the infrastructure is required which comprises of the grid and the charge stations [28].

Vehicle to grid (V2G) is a vital technology utilized by smart grid as V2G allows both vehicle owners and the energy providers to draw power from each other as needed thus making it an important prospect for both the parties [29].

Some of the motives for PEVs are as follows:

a) Energy flexibility.
b) Energy efficiency.
c) Reduced emissions.
d) Cleaner, quieter cars without performance changes. For electric cars, the ultimate fuel source is hydro, wind, nuclear, or any electricity source.
e) Overcome energy storage (range) and power (fuel rate) problems.

Secure Payment and Privacy, Smart Metering, and the Critical Infrastructure and Physical Security can be grouped under potential security concerns for PEVs [28]. Mobile metering is considered as one of the challenging hurdles for the PEVs to overcome. This challenge can be addressed by the use of SIP in smart grid [30].

2.4. Demand Response

Demand response (See Figure 14) is an important component offered and managed by the utilities. Demand response (DR) has been defined as "…action taken to reduce electricity demand in response to price, monetary incentives, or utility directives so as to maintain reliable electric service or avoid high electricity prices [31]."

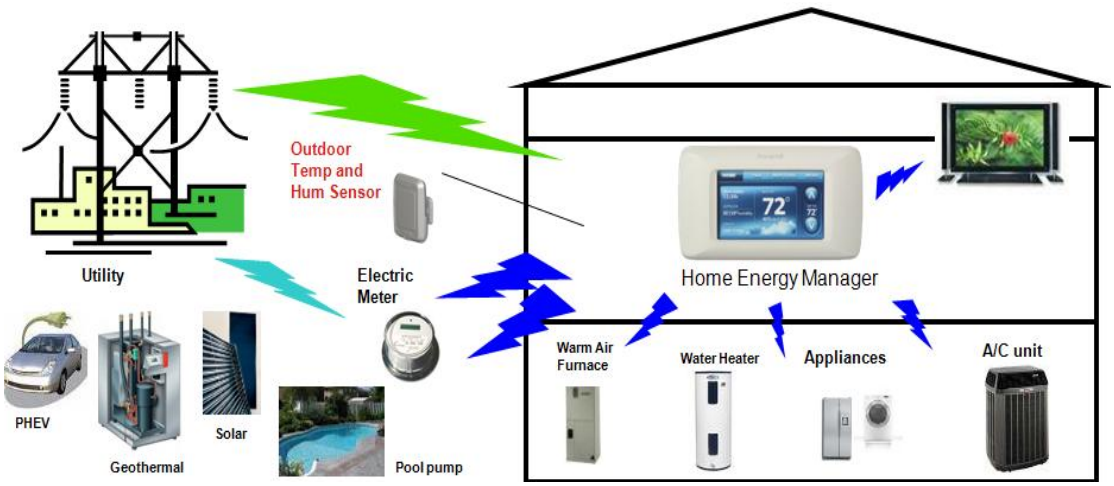

Figure 14: Overview of Demand Response [32].

Open Automated Demand Response (ADR) is one of the many communications technologies that are being developed to improve the efficiency between electric supply and demand in smart grid [33]. A dynamic pricing scheme is introduced with the demand response program based on the supply conditions and various other factors like time of the day etc. The automation of the demand response program is very useful as it annuls the scope for human intervention and also improves the efficiency and accuracy of the program [34].

Both the utilities and the consumers benefit from this program as the consumers can reduce their bill expenses on electricity and the utilities can bring down their production costs. From the utilities point of view, reducing the peak load and increasing the reliability would be the end goals for a demand response program [34]. Incentives are provided by the utilities to consumers (homes and businesses) to reduce or shift the power usage during critical times like peak summer days etc. The utilities can enforce the consumer participation as compulsory or optional. The consumers will have no choice to opt out of the program if it is compulsory. The utilities issue remote commands using demand load control (DLC) to ON and OFF the home appliances in order to reduce the peak load [34]. Open ADR can be said as a data communication model which ensures the information exchange with the transmission of demand response (DR) signals between the utilities or independent system operator (ISO) and the end users [33].

Chapter 3

ANALYSIS OF SIP

3.1. Home Area Network

SIP has brought in the possibility of achieving a ubiquitous computing with the convergence of telecommunications and the computer networks [35]. Ubiquitous computing refers to a "human-interaction model in which information processing has been thoroughly integrated into everyday objects and activities" [35]. In figure 15, we can observe the possibilities of ubiquitous computing with SIP. SIP meets all the requirements to access and reuse the infrastructure that has already been there for SIP.

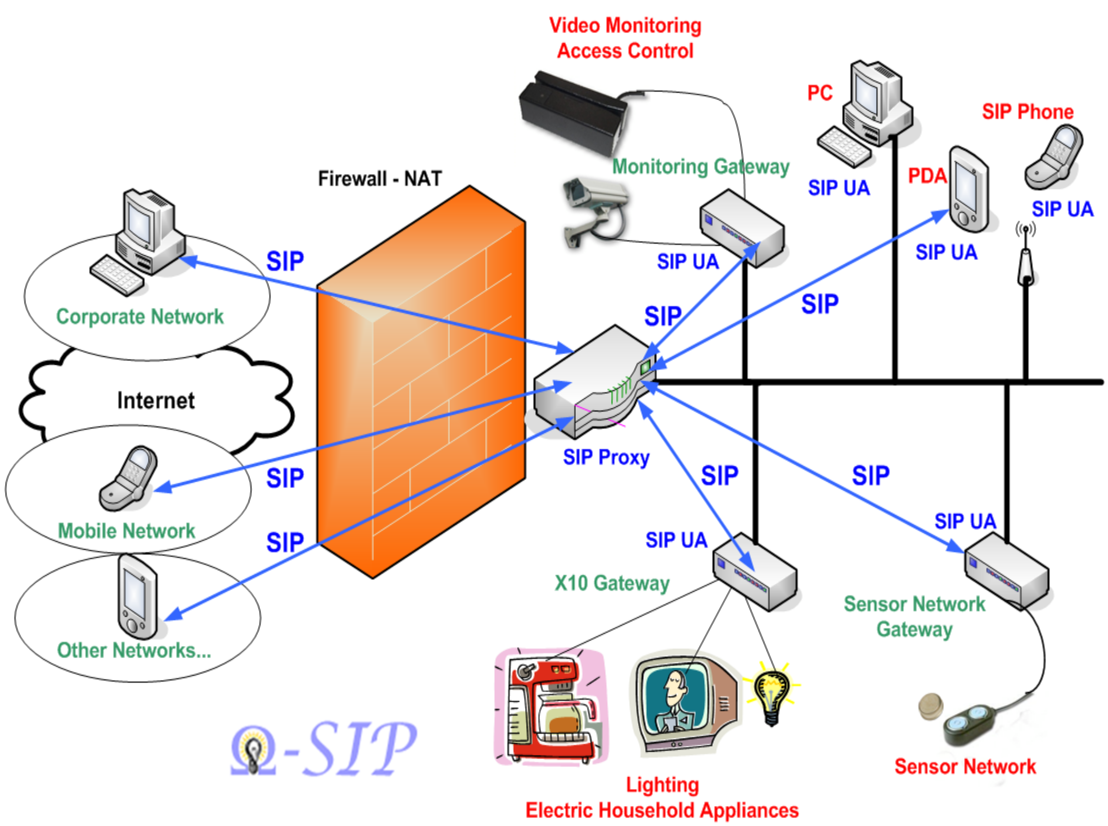

Figure 15: Envisioning the Possibilities of a Ubiquitous Computing with SIP [35].

The connectivity provided by SIP in the wide area network makes it very useful in the home area network. Similar existing technologies like X.10, Jini etc., which are used for device communication can be replaced with SIP or it can co-exist with these protocols depending on the necessity in a HAN [36]. SIP can be used as a suitable protocol for intra-home as well as extra-home communications. The intra-home involves the communication between the devices and appliances within a home. The extra-home involves the use of techniques for access to the devices in the home from outside.

Before the communication, locating and identifying the device to talk with is essential for an inter-device communication in a HAN. These two issues are dealt separately in few methodologies where as few others tend to merge these two into a single solution [36]. In extra-home communications locating phase and identifying phase is merged into a single solution. An instruction message is sent by a requesting agent in order to perform the desired action. The name of the object and the action to be performed are sent in the message as the payload itself [36]. The name of the object will be resolved all along the routing path of the message as it goes along from agent to agent as seen in figure 16. For example, if the command is to turn the heater 'ON' in Jack's house, then the command is first routed to the server which is closer or knows the location of Jack's house and is routed to the firewall of the house where authorization and access checks are performed. If successful, the payload which contains the action is delivered to the named object in the message [36].

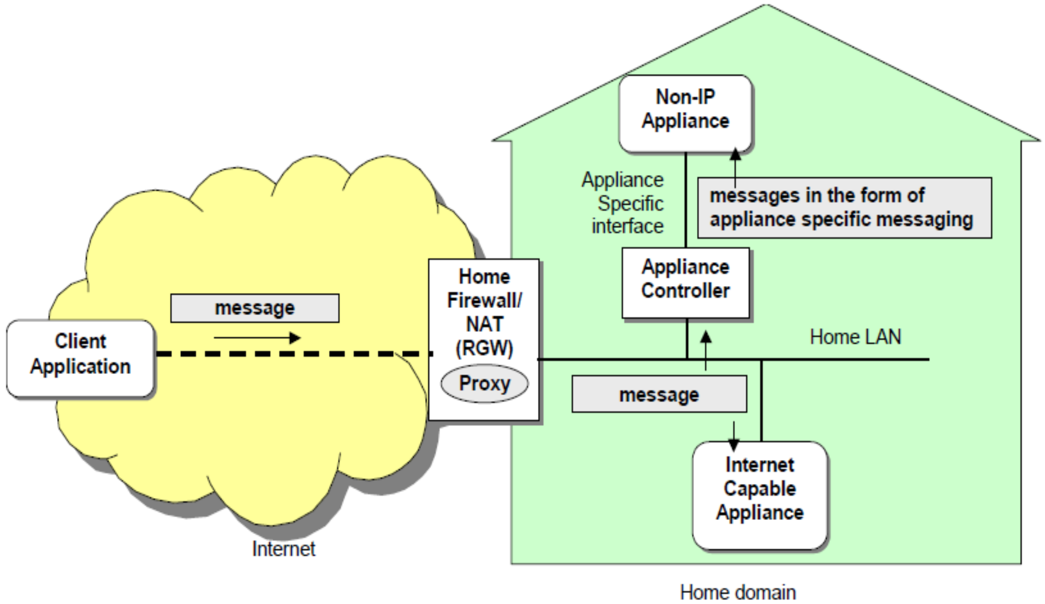

Figure 16: Networking Architecture [36].

SIP already has many of these similar mechanisms such the INVITE process which performs this type of routing by the name function. An INVITE can be sent to a proxy or an agent and the Proxy can rewrite the name and relay the INVITE which will eventually get it closer to the destination of the message. The payload will be described in the session description protocol (SDP) [38]. In SIP, the location and action process are used in the same procedure. SIP has the advantage of handling the Multipurpose Internet Mail Extension (MIME) type of payloads also. SIP has its own re-transmission logic, which works well on TCP as well as UDP. URIs, MIME, statelessness, proxy concepts etc. are supported in SIP, which makes it more suitable. SIP has the advantage of routing flexibility, which can be utilized by other protocols like the embedding of an SLP query inside an SIP request [40].

SIP can bring in a lot of interesting as well as efficient concepts for the devices in HAN. Some of them are as follows:

a) Addressing:

The SIP protocol supports abstract addressing for private IP addresses and non IP addresses. The contents of To: and From: fields are encoded as the Uniform Resource Locators (URL) [17]. The SIP devices which are addressed by this URL scheme can be reached independent of their IP address. The address of the SIP device can be resolved with the help of the routing mechanism as long as they are connected [17]. An example of the standard SIP URL syntax in plain text is "bulb@steve.home.net". "Heater.hall@steve.home.net" can be said as a more structured addressing scheme in SIP. The location will already be determined via the SIP routing. In order to avoid revealing information on the type of devices used within a HAN, encryption of the URL can be done with the help of base64 encoding [36].

"sip:56gh8trecsdvbk3z@steve.home.net" is an example of an encrypted URL in SIP.

<entity>@<location> is one of the simple formats which can be extended to accommodate the home appliances as well [17]. It also provides support for different modes of communication like media streaming, controlling, querying and asynchronous events.

For the purpose of carrying payloads other than SDP like the MIME type, a new method called 'DO' is introduced in the SIP. The 'DO' method can be used to carry any command with an MIME type that is targeted towards any device or appliance in a HAN such as 'Switch on the audio system" which will result in the triggering of a single response handled by the SIP response mechanisms [43]. A new payload MIME type named Device Messaging Protocol (DMP) based on the XML based specification is introduced in order to communicate with the devices. During the registering process of the device with the proxy through REGISTER message, a new protocol named Device Description Protocol (DDP) is used in order to convey the description of the device [43]. The exact details of the DMP and DDP are still under investigation.

- Establishing a Session with a HAN Appliance:

The establishment of a session is an important functionality of SIP and it usually is necessary to establish sessions with networked appliances. We can take the example where Alex wakes up to an alarm clock where the alarm is set dependent on the weather condition, traffic, news, emergency etc. So, depending on these factors the alarm service provider needs to set the alarm and as the provider also needs to send the reason he will have to set up and establish an audio session with the clock and play the message. In figure 17, we can observe the SIP message flow for this particular scenario:

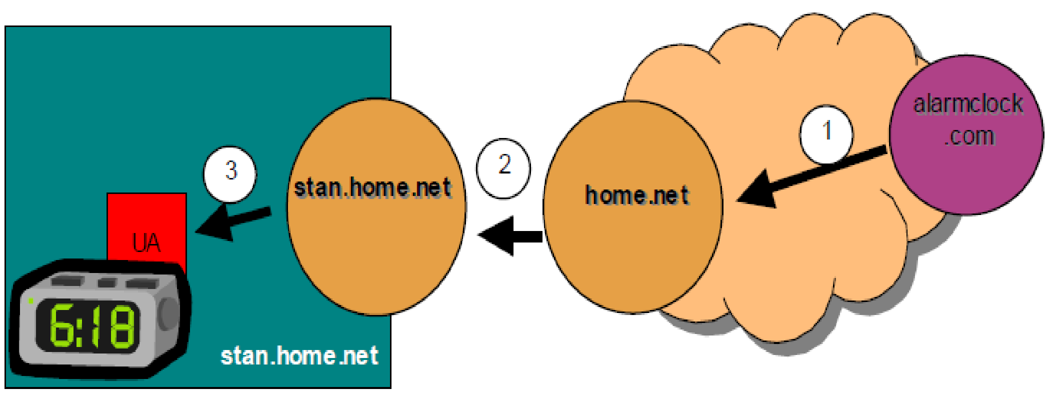

Figure 17: SIP Message Flows in a Network-Based Alarm Clock Service [36].

The structure of the message flows observed in figure 15 are as follows [36]:

1. INVITE sip:[d=alarmclock, r=bedroom]@home.net SIP/2.0

From: sip:announcement@alarmclock.com

To: sip:[d=lamp,r=bedroom]@stan.home.net

Via: SIP/2.0/UDP alarmclock.com

Content-type: application/sdp

[SDP Parameters for uni-directional RTP stream]

2. INVITE sip:[d=alarmclock,r=bedroom]@stan.home.net SIP/2.0

From: sip:announcement@alarmclock.com

To: sip:[d=lamp,r=bedroom]@stan.home.net

Via: SIP/2.0/UDP home.net

Via: SIP/2.0/UDP alarmclock.com

Content-type: application/sdp

[SDP Parameters for uni-directional RTP stream]

3. INVITE sip:[d=alarmclock,r=bedroom]@ua.stan.home.net SIP/2.0

From: sip: announcement@alarmclock.com

To: sip: sip:[d=lamp,r=bedroom]@stan.home.net

Via: SIP/2.0/UDP stan.home.net

Via: SIP/2.0/UDP home.net

Via: SIP/2.0/UDP alarmclock.com

Content-type: application/sdp

[SDP Parameters for uni-directional RTP stream]

RTP parameters are sent back as a response to the service provider and an audio RTP stream is initiated which is sent to the alarm clock.

b) Forking and Grouping

In the HAN, the architecture of SIP can be used to allow personal group device identification. The concept of Grouping allows multiple devices to be addressable using a single ID. SIP is also be used to send one command in parallel to multiple devices at the same time [17]. This is called forking. For example, the command 'set time on' to "clocks@Alanhome.net" will send the message to all the clocks in Alan's home.

A detailed example on forking in SIP is seen in figure 18. In the example, John wants to print a document in the office, which has 3 printers. In order to print the copy John has to contact the default proxy server which then forks the request to the 3 different printers. Let us assume John has to establish the session with an available printer to which he will send the data once the confirmation is received.

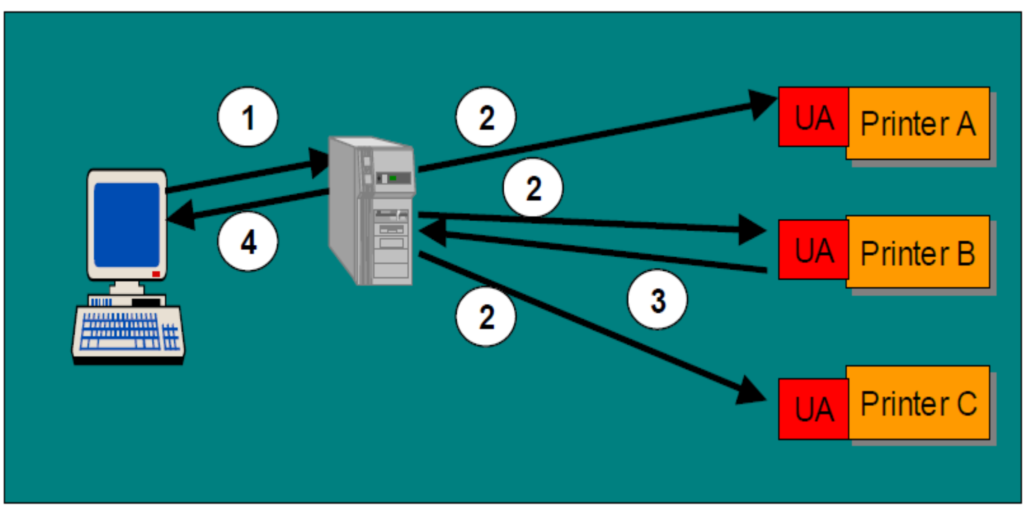

Figure 18: Forking of Service Requests [36].

The structure of the message flows observed in figure 16 are as follows:

1. INVITE sip:anyprinter@office.com SIP/2.0

From: sip:john@office.com

To: sip:anyprinter@office.com

Via: SIP/2.0/UDP calvin.office.com

2. Proxy forks the following messages:

INVITE sip:printerb@office.com SIP/2.0

From: sip:john@office.com

To: sip:anyprinter@office.com

Via: SIP/2.0/UDP hobbesproxy.office.com

Via: SIP/2.0/UDP calvin.office.com

INVITE sip:printerb@office.com SIP/2.0

From: sip:john@office.com

To: sip:anyprinter@office.com

Via: SIP/2.0/UDP hobbesproxy.office.com; branch=a1234

Via: SIP/2.0/UDP calvin.office.com

INVITE sip:printerc@office.com SIP/2.0

From: sip:john@office.com

To: sip:anyprinter@office.com

Via: SIP/2.0/UDP hobbesproxy.office.com; branch=a1234

Via: SIP/2.0/UDP calvin.office.com

3. Printer B responds with OK

SIP/2.0 200 OK

From: sip:john@office.com

To: sip:anyprinter@office.com

Via: SIP/2.0/UDP hobbesproxy.office.com; branch=a1234

Via: SIP/2.0/UDP calvin.office.com

4. SIP/2.0 200 OK

From: sip:john@office.com

To: sip:anyprinter@office.com

Via: SIP/2.0/UDP calvin.office.com

Proxy now proceeds to CANCEL all other pending requests.

Now, we will consider an example for device grouping and personal identification in HAN. Using SIP, an appliance like a heater can be nicknamed "coolboy" for instance and also can be grouped under category of heaters at the same time [36]. So, this allows the user to select from a two-fold concept as the device can be addressed either by personal name or a group name.

To set the temperature of "coolboy" to 25 degrees C, Hagar can send the following messages [36]:

1. DO sip:[d=coolboy,r=room,u=hagar]@hagar.home.net SIP/2.0

From: sip:hagar@vacation.com

To: sip:[d=coolboy,r=room,u=hagar]@hagar.home.net

Via: SIP/2.0/UDP vacation.com

Content-type: application/dmp

<command>

Temperature

<set> 25C </set>

</command>

A multicast or a broadcast of the switch off command by the user can power off all the heater devices at the same time.

2. DO sip:[*group=heater*, *u=hagar*]@hagar.home.net SIP/2.0

From: sip:hagar@vacation.com

To: sip:[*group=heater*, *u=hagar*]@hagar.home.net

Via: SIP/2.0/UDP vacation.com

Content-type: application/dmp

<command>

Off

</command>

c) Offer-Answer Model

As described in RFC3264, SIP offers a mechanism named ‘offer/answer’ model which makes use of the session description protocol (SDP) in order to reach a common view for establishing a multimedia session between two entities. This model ensures that the session is established using capabilities that both the endpoints support. In this model, one entity in the session sends an SDP message which contains the media capabilities and the port number to which the offerer prefers to receive the data [38]. Then, the other entity which is answerer responds to the offer by sending an answer consisting of its media capabilities whether a matching one with offerer or not and the preferred port numbers in a SDP message [38]. For example, if Alice wants to monitor his security camera with his desk phone, then the offer-answer mechanism will automatically detect the inability of the phone to support video and an audio session is only established with the camera.

- Querying the capabilities of a HAN Appliance:

In the following scenario, a person named Wally tries to use his workstation at office to query the capability set of a VCR at Dilbert's house. Here as shown in the figure, we observe that the response message to Wally consists of the entire capability set of the VCR at Dilbert's house like the codecs supported and other media features etc. This example can be seen in figure 19.

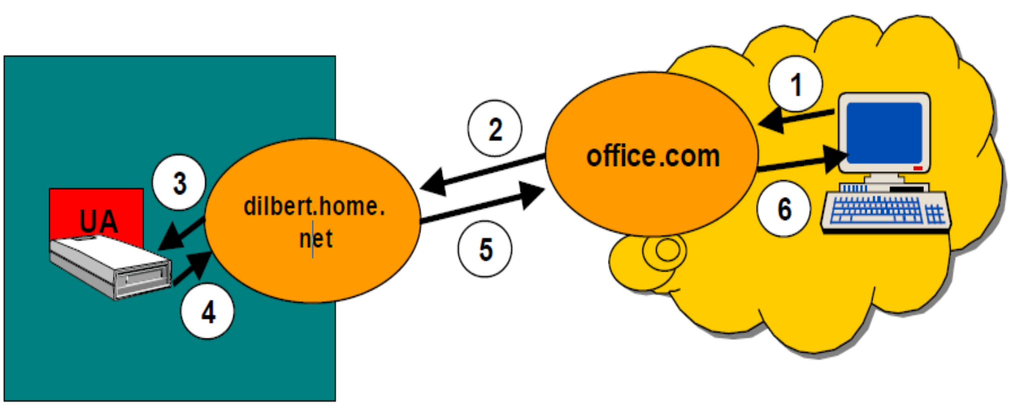

Figure 19: Querying the Capabilities of Devices in a HAN [36].

The structure of the message flows observed in figure 17 are as follows [36]:

1. OPTIONS sip:[*d=vcr,r=den*]@office.net SIP/2.0

From: sip:wally@office.com

To: sip:[*d=vcr*,*r=den*@dilbert.home.net

Via: SIP/2.0/UDP wallyville.office.com

2. OPTIONS sip:[*d=vcr*,*r=den*]@dilbert.home.net SIP/2.0

From: sip:wally@office.com

To: sip:[*d=vcr*,*r=den*@dilbert.home.net

Via: SIP/2.0/UDP office.com

Via: SIP/2.0/UDP wallyville.office.com

3. OPTIONS sip:[*d=vcr*,*r=den*]@dilbert.home.net SIP/2.0

From: sip:wally@office.com

To: sip:[*d=vcr*,*r=den*@dilbert.home.net

Via: SIP/2.0/UDP dilbert.home.net

Via: SIP/2.0/UDP office.com

Via: SIP/2.0/UDP wallyville.office.com

4. SIP/2.0 200 OK

From: sip:wally@office.com

To: sip:[*d=vcr*,*r=den*@dilbert.home.net

Via: SIP/2.0/UDP dilbert.home.net

Via: SIP/2.0/UDP office.com

Via: SIP/2.0/UDP wallyville.office.com

Supported: com.sony.videopack.mm-extensions

Content-Type:application/ddp

<XML tagged body describing the video control package downloaded in this VCR in more details>

5. SIP/2.0 200 OK

From: sip:wally@office.com

To: sip:[*d=vcr,r=den*@dilbert.home.net

Via: SIP/2.0/UDP office.com

Via: SIP/2.0/UDP wallyville.office.com

Supported: com.sony.videopack.mm-extensions

Content-Type:application/ddp

<XML tagged body describing the video control package downloaded

in this VCR in more details>

6. SIP/2.0 200 OK

From: sip:wally@office.com

To: sip:[*d=vcr,r=den*@dilbert.home.net

Via: SIP/2.0/UDP wallyville.office.com

Supported: com.sony.videopack.mm-extensions

Content-Type:application/ddp

<XML tagged body describing the video control package downloaded

in this VCR in more details>

d) The Event Service:

The RFC3265 document describes the capability of SIP to provide event notification mechanism which enables any entity in the network to request for notifications from remote entities indicating that certain events have occurred [17]. In order to provide this kind of an asynchronous communication, the SIP event notification draft defines the SUBSCRIBE and NOTIFY primitives. This mechanism is very useful in many SIP services, which require cooperation between two endpoints [17].

As stated in the RFC3265, “The general concept is that entities in the network can subscribe to resource or call state for various resources or calls in the network, and those entities (or entities acting on their behalf) can send notifications when those states change [39].”

The following is a typical flow of messages in this mechanism [39]:

```
Subscriber         Notifier
 |-----SUBSCRIBE--->|     Request state subscription
 |<-------200-----------|     Acknowledge subscription
 |<------NOTIFY------|     Return current state information
 |--------200---------->|
 |<------NOTIFY-----|     Return current state information
 |--------200--------->|
```

For example, when a user wants to get notified when a certain event triggers like the ‘ringing of an alarm’ or ‘a door bell ring’ etc. A thermostat can subscribe to the energy rate event of the smart meter, which enables the thermostat to get notified when the reading for the energy rate exceeds the limit. Few of the important terms in the event notification are as follows [39]:

- Notification: It is the act of sending NOTIFY message by the notifier to the subscriber indicating the state of the resource.

- Subscription: This consists of the application state which has a pointer to the associated event package name and an identification token.
- Notifier: A user agent who generates NOTIFY requests in order to notify the subscribers.
- Sunscribers: A user agent who generates SUBSCRIBE requests on order to send them to the notifiers to create subscription.
- Event Package: This consists of state information to be reported by a notifier to a subscriber and it also defines syntax and semantics based on the framework.

e) SIP Presence Framework:

The RFC3586 document describes a Presence Event Package for the Session Initiation Protocol (SIP). This document proposes SIP to be used as a presence protocol, which provides a presence service over the internet or any IP network.

The presence information refers to the availability and willingness of the user for communication. This information is published to the subscribers or other system users called as the ‘watchers’ to indicate their current event state [37]. Many variety of presence states which indicate their communication status are published by the users. Some of the example presence states are idle, busy, away etc. The basic presence flow and functionality can be observed in figures 20 and 21.

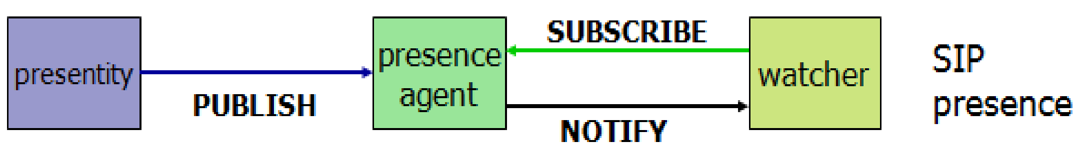

Figure 20: Presence Flow [44].

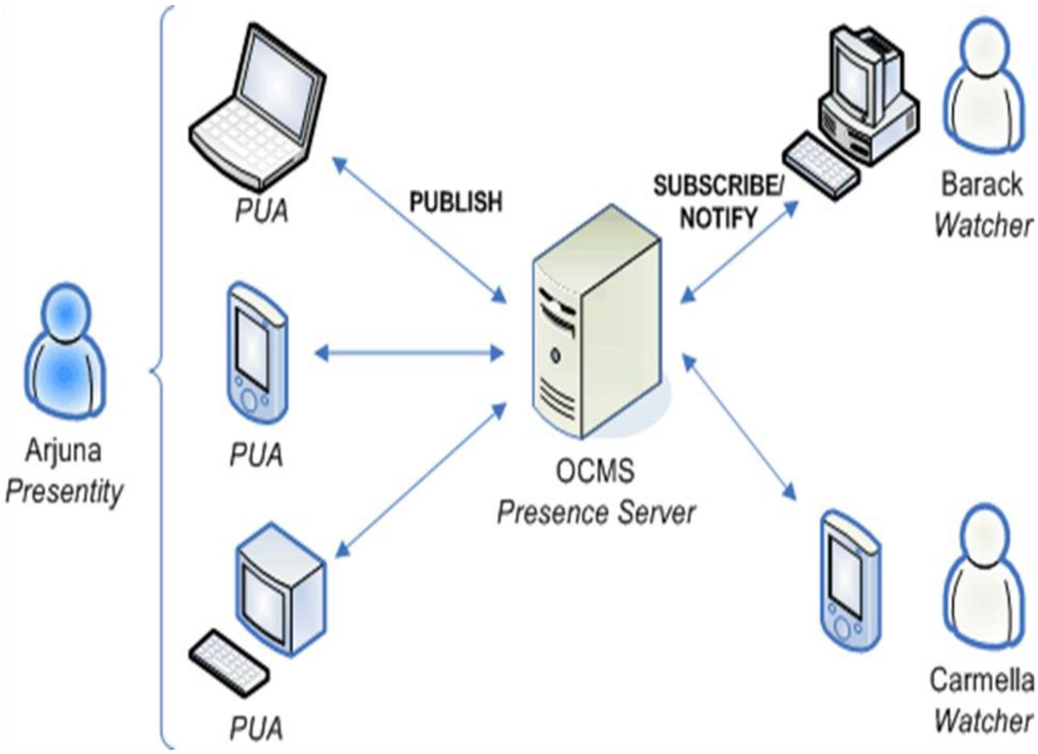

Figure 21: Basic Presence Functionality [45].

Some of the important terms in SIP presence are as follows [37]:

a) Presence User Agent (PUA): The PUA maintains and publishes the presence information of the user or entity to the PAs or presence server. The PUA is also known as the 'presentity'. The PUAs do not send SUBSCRIBE or send NOTIFY messages. The presence information is sent in SIP PUBLISH. For example, a user can have many devices like a cell phone and Personal Digital Assistant (PDA), each of which generates presence information for a presentity.

b) Presence Agent (PA): The PA is a physical entity that stores all the presence details of the agents in one document obtained through the PUBLISH messages from PUAs and allows the watchers to subscribe and get notified. The PA also acts as the presence server (PS) and sends the ‘presentitiy’ information in the SIP NOTIFY message.

c) Watchers: A watcher requests presence information about one or more presentities or about other watchers from the presence service. Some of the special types of watchers are:

- Subscriber: Asks the presence service to be immediately notified of any changes to more presentities.
- Fetcher: Makes a request for presence information, but has not requested a subscription to the presence service.
- Poller: Is a fetcher that makes regular request.

3.2 Zigbee

Zigbee is a widely used wireless standard in the HANs and the wireless sensor networks. SIP is considered to be the best suited protocol for ubiquitous computing in the future generation networks. In this chapter, an analysis of the proposed interworking architecture of Zigbee and SIP is given.

SIP- Zigbee Interworking Architecture:

The proposed SIP-Zigbee Interworking architecture is based on the unifying of the publish/subscribe/notify concepts of the SIP presence service and the Zigbee binding mechanisms [42]. This coupling of SIP and Zigbee will open up the possibility of remote access and control of Zigbee devices with common SIP enabled user devices [42]. For example, a user can remotely control the heating system through his SIP enabled phone.

Some of the key terms to be understood in this architecture are as follows:

a) Node and Subunits
b) ZigBee Application
c) ZigBee Device Descriptors
d) ZigBee Device Objects (ZDO)
e) Clusters, ZigBee Binding and Binding Table
f) Zigbee gateway
g) SIP Presence framework

All the above terms associated with Zigbee are explained in chapter 2.2 and the SIP presence framework along with the concepts of watchers, PA, PUA, PUBLISH, SUBSCRIBE are explained in chapter 3.1.

In Zigbee, a particular application is identified by an application profile ID. It can be further explained as a particular binding between the input clusters and output clusters of the attributes [42]. In figure 22, we can observe the establishment of a binding, where we assume that for a simple application (profile ID A) has an input cluster-c1 and is implemented at Device X, end-point 1, and an output clusterc1 implemented at Device Y, end-point 5.

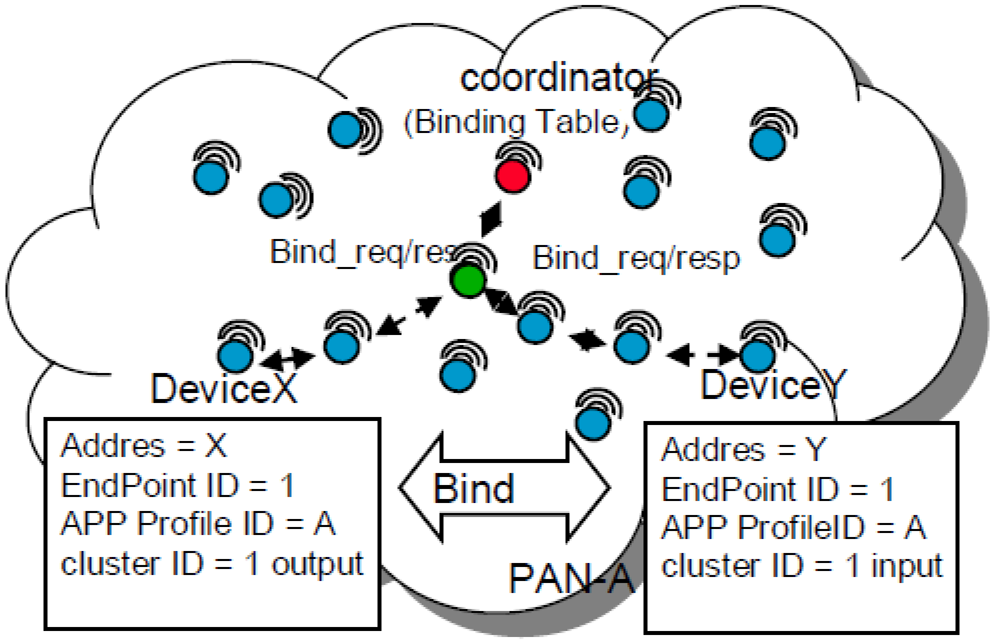

Figure 22: Zigbee Binding in Cluster Tree [42].

In order to visualize the SIP-Zigbee interworking scenario, a simple home automation application like a light control is used which is depicted in figure 23. Here, we consider two remote Zigbee Personal Area Networks PAN-A and PAN-B. The switches S1 and S2 can send messages to ON or OFF the light bulbs from B1-B4. In the PAN-A, the output cluster cl-1 is implemented at switch S2, which sends messages for switching on/off to bulbs B1 and B2 with the input clusters cl-1. The Zigbee binding table enables the implementation of the internal binding.

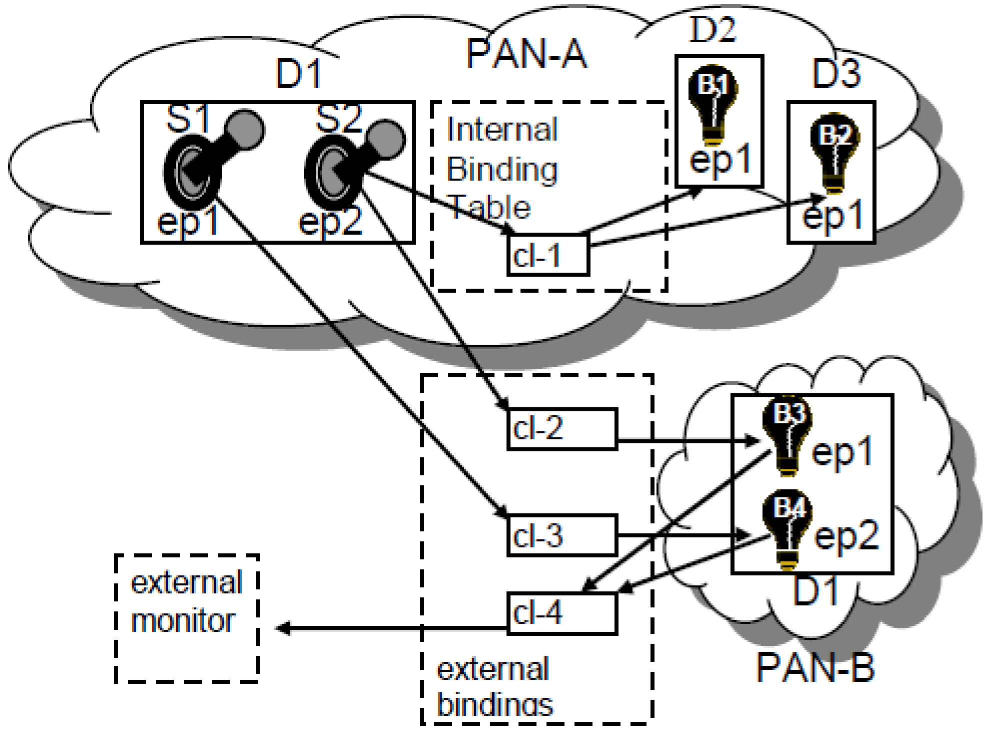

Figure 23: Distributed Zigbee Application [42].

The output clusters cl-2 and cl-3 are implemented at switch S2 and switch S1 respectively. These switches send ON or OFF messages to the cl-2 and cl-3, which are the input clusters at bulbs B3 and B4. As the switches S1 and S2 are in PAN-A while PAN-B has the bulbs B3, B4. In order to control or access these bulbs, external bindings have to be established. The proposition of this architecture is to establish these external bindings by means of SIP. The external monitor shown in the figure receives the status messages of the bulbs. For example, if there is a change in the status of the bulb B4, the external monitor receives the message from the output cluster cl-4.

In table 1, we can observe the configuration of the application whose profile ID is referred to as ApA.

Table 1: Description of the Application [42].

Function	Device	PAN	App Profile ID	End Point	Cluster ID
switch S2	D1	PAN-A	ApA	ep2	Output cl-3
switch S2	D1	PAN-A	ApA	ep2	Output cl-2
switch S1	D1	PAN-A	ApA	ep1	Output cl-1
bulb B1	D2	PAN-A	ApA	ep1	Input cl-1
bulb B2	D3	PAN-A	ApA	ep1	Input cl-1
bulb B3	D1	PAN-B	ApA	ep1	Input cl-2
bulb B4	D1	PAN-B	ApA	ep2	Input cl-3
bulb B3	D1	PAN-B	ApA	ep1	Output cl-4
bulb B4	D1	PAN-B	ApA	ep2	Output cl-4
monitor	D1		ApA		Input cl-4

The client software at the user side can implement corresponding input/output clusters for a particular Zigbee application and also send or receive messages which are embedded in the SIP messages [41]. Figure 24 depicts the SIP-Zigbee interworking architecture along with the elements of the SIP presence framework.

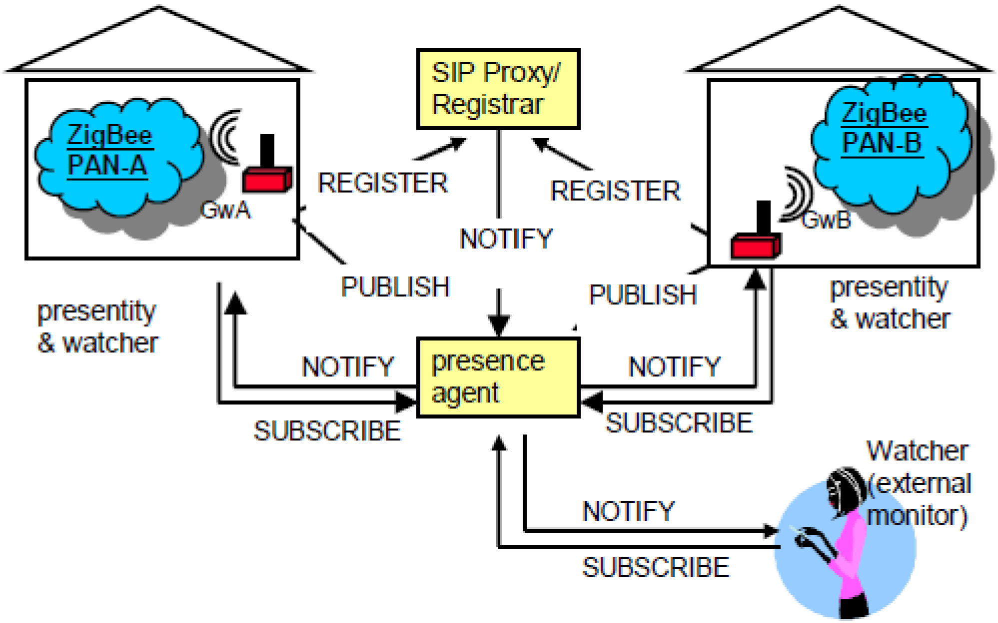

Figure 24: SIP-Zigbee Interconnecting Architecture [42].

In this proposed architecture, an entity named SIP/Zigbee gateway is used to interconnect the PAN-A and PAN-B networks. The SIP and Zigbee stack is implemented in the SIP/Zigbee gateway which also acts as both Zigbee PAN coordinator, SIP UA and SIP Presence UA. This gateway is denoted by GwA in PAN-A and as GwB in PAN-B. The clusters and the application objects are implemented at PAN-A and PAN-B and makes use of the PUBLISH and SUBSCRIBE service based on the SIP presence framework [39]. Active end-points, applications and clusters are discovered by the GwA and GwB which act as the Zigbee coordinators while the UAs register with the registrar and link the GwA/GwB with PAN-A/PAN-B [40]. Now the PUAs at both the gateways PUBLISH the URI of the active applications and also the requested binding of the input/output clusters. The NOTIFICATION message establishes relation for both the gateways GwA and GwB by describing their watcher/presentitiy role. For example, a cl-3 message to shut off the bulb B4 is first translated at the GwA into a SIP message and the message is again retranslated into a Zigebee message at the GwB and is then forwarded to the bulb B4. So, now an SIP stack enabled user device with a monitor like a PDA phone etc, can be used to not only REGISTER and SUBSCRIBE for data but also get NOTIFICATIONS and status messages from PAN-A or PAN-B over GwA or GwB respectively [42].

The goal of this proposed architecture is to provide SIP users with a ubiquitous access over the Zigbee networks and to transport Zigbee control and data messages among remote PANs.

3.3. PEV

There are many challenging areas based on scenarios for the successful deployment of PEVs. The support of SIP for ‘mobile metering’ helps in addressing one of them.

Support for mobility in SIP:

A user can be found independent of the location and the network device he is using like PC, wireless IP phone with the help of SIP which is designed to support personal mobility. This is made possible because of the SIP registration and location services of SIP [15]. The redirection of the ‘call establishment’ is implemented in SIP, which makes it mobile. The current location of the ‘called party’ is discovered with the help of location register. SIP supports the mobility of a device from place to place while it is active in a session. SIP redirect server maintains the information on current location of the mobile device and redirects the INVITE sent by the other device [30]. In figure 25, we observe how a remote (mobile) SIP device remains active in a session with the help of global location database.

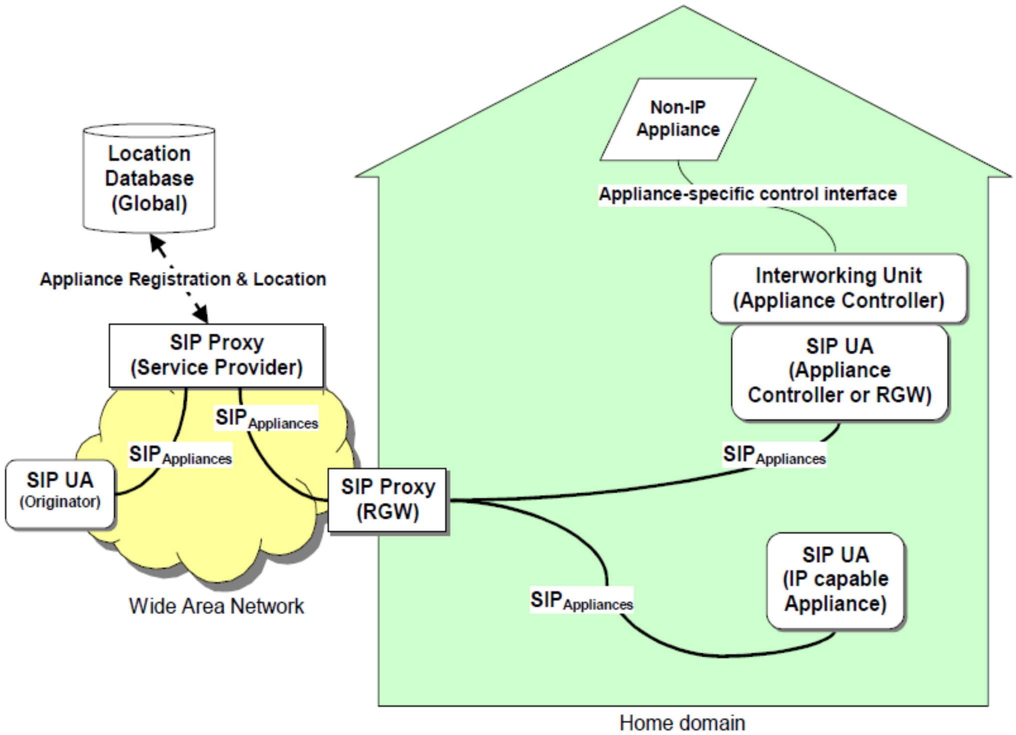

Figure 25: Support for Mobility and Remote communication with HAN appliances [36].

Charging of batteries is very important for PEVs as they also contribute to the grid during peak usage times. Sophisticated and advanced metering is required to support the debiting and crediting of energy accounts linked with the using and supplying to the grid [15]. Support for mobile metering is required for PEVs. Take the example of an owner who wants to charge his PEV at a friend's place. There should be a proper mechanism, which should ensure that the bill should be charged to the account of vehicle's owner and not the owner of the house he is plugging in. The native support for the PEV is provided by SIP for device and user mobility as this functionality is critical to support mobile metering [30].

3.4. Demand Response

SIP is widely popular for its involvement as the 'session-establishment' protocol in the VOIP telephony and this reason often over shadows the potential benefits it offers in other areas which are not related to voice transmission. The IETF SIMPLE describes the event service model and instant messaging service offered by SIP. These mechanisms are already deployed in many organizations and wireless carriers that offer IP telephony. An open Automated Demand Response (ADR) system can be modeled and realized based on this event service model offered by the SIP [34].

This chapter analyzes the architecture and advantages of using SIP as a candidate protocol for realizing an open ADR. Some of the advantages, which can benefit the execution and the management of a Demand Response (DR) program are as follows [34]:

a) Push Architecture: The event service model of SIP enables the participants to subscribe to any state of the event as well as each other's state [39]. An entity at the utility such as the DRAS can be the publisher of a DR event as well as be a subscriber for a particular event change of another participant in order to get feedback. This publisher/subscribe mechanism is based on the very powerful 'Push architecture' [34]. This architecture is considered to be superior to 'Pull architecture'. Most of the traditional web services are based on the pull strategy where the client initiates a request for data to the server. In pull architecture, the request for a transaction is initiated at the 'Publisher' or the server side. The publisher pushes the information or data of a particular event to the participants or clients who subscribed for it [48]. The push model has far more data accuracy and performs efficiently than a pull model.

b) Firewall/Network Address Traversal (NAT): For an application protocol such as SIP, it is usually conceived that a problem exists with the firewall/NAT traversal. The general problem occurs when an entity outside the secured firewall is trying to communicate with someone inside it. To avoid these types of firewall issues, there are several ways around these. For example, SIP can make use of protocols like Session Traversal Utilities for NAT (STUN) etc. for the automatic firewall traversal. As SIP has been a de-facto standard for VOIP telephony in the enterprises, the infrastructure for SIP has already been established and the demand response architecture can make use of this.

c) Scalability: The scalability feature of SIP is a proven factor. It is being widely deployed in many enterprises and till date the demand for SIP still exists which describes the capability of SIP to handle growing demands.

d) Customization of DR event package: With the help of SIP based event architecture, the utilities can create a DR package that can serve the specific needs of the DR management.

e) Capability: The participants can receive a part or a complete set of the DR attributes depending on their capability and functionality. For example, the attributes required for a residential home will be a subset of that of a commercial building. Through this architecture, it is possible to send only the required set of attributes to the respective participants.

f) Multiple Events: A single participant can subscribe to more than a single event at the same.

g) Network Optimization: The support for event aggregators and customizable participant s by SIP helps in reducing the network load during high global demand for the events.

h) Partial Notification: Significant bandwidth can be reduced when only the modified (partial) attributes are sent instead of all the attributes for a particular change in a descriptive DR event.

i) Opt in, Opt out: The opt-out feature enables the users are not compelled to participate in the DR program, they can opt out of it where as the opt-in mode enables the participants to subscribe for an event.

j) Package Discovery: This feature supports a discovery mechanism, which enables the participants to query and get notified when a new DR event package is applicable.

k) Multimodal Communication: SIP supports many modes of communication like the event based, transaction based and session based using a single common participant identity.

l) Third party payload friendly: The ability of SIP to carry multiple payload formats as part of its messages like XML, MIME, binary, etc. makes it a third party payload friendly protocol.

Generic Demand Response Architecture:

In the demand response architecture, the Demand Response Automated System (DRAS) is a critical infrastructure component. The DRAS is responsible for facilitating communication between the utilities, ISOs that generate and distribute electricity and the other entities such as the aggregators etc, which are involved in managing the consumption of the electricity [33]. The information associated with the communication is regarding the demand pricing, ADR programs and the updates, reliability messages etc. The main functionality of the DRAS is to automate these various communication channels for the efficient execution and management of the DR programs.

The generic architecture is shown in figure 26 as follows:

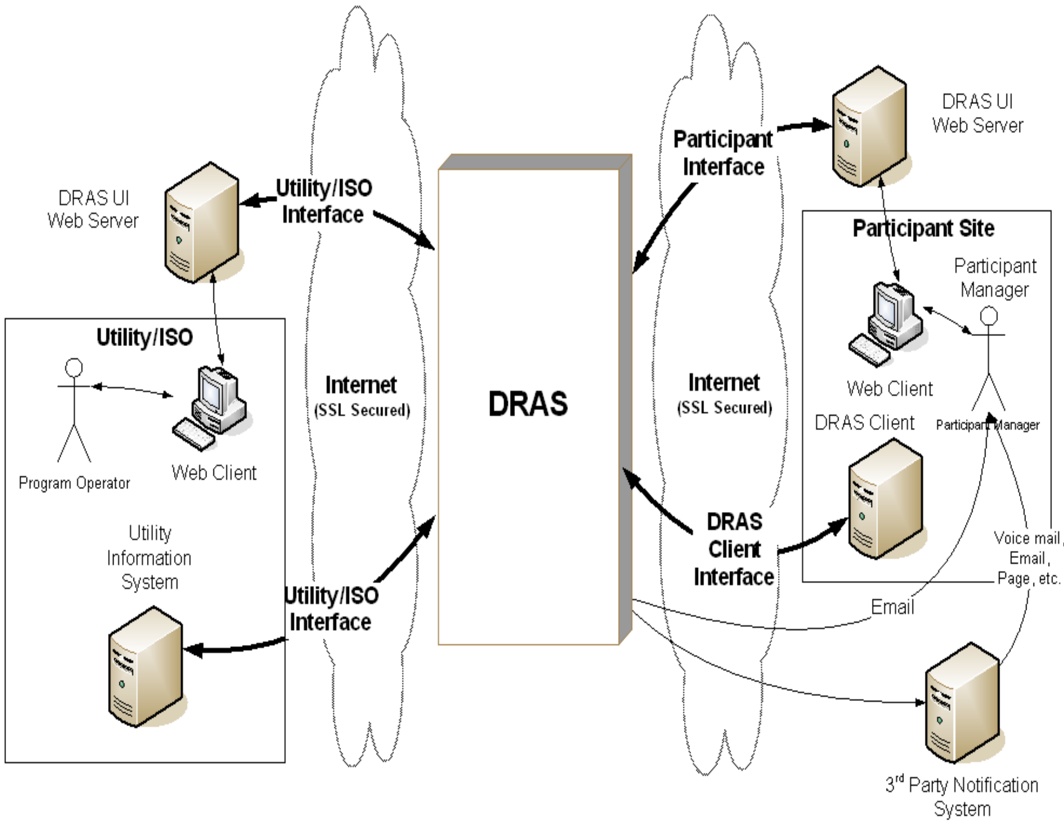

Figure 26: Generic DRAS Architecture [33].

As shown in figure 24, depending on the type of entity that DRAS interfaces, the three distinct types of interface groups are as follows [33]:

a) Utility and ISO Operator Interfaces: This interface enables the utilities and ISO to set up, monitor and manage the new and existing DR programs.

b) Participant Operator Interfaces: This interface enables the DR program participants to convey their demand request for electricity to the DRAS.

c) DRAS Client Interface: This interface helps the DRAS to send new event updates to the automation sub systems of the clients and to receive notifications about the feedback regarding the state of the event.

SIP based proposal for DRAS architecture:

Figure 27 describes the demand response architecture based on SIP, which is in compliance with Open ADR. Few of the high levels components seen in the figure are as follows [34]:

- Utilities/ISO: These entities are responsible for creating and monitoring DR events.
- DRAS: This entity is responsible for the automation and management of the demand response events between the participants and the DR system.
- Participants: They can be either industrial like hospitals, enterprise etc. or residential participants such as the home owners. We can observe in the figure that the residential network is further decomposed to show the two cases of interfacing where one case shows how the DR system interfaces with the EMS and how EMS interacts with individual devices for the power management. The second case shows the interfacing with the constrained devices (CoGii) in the residential network.

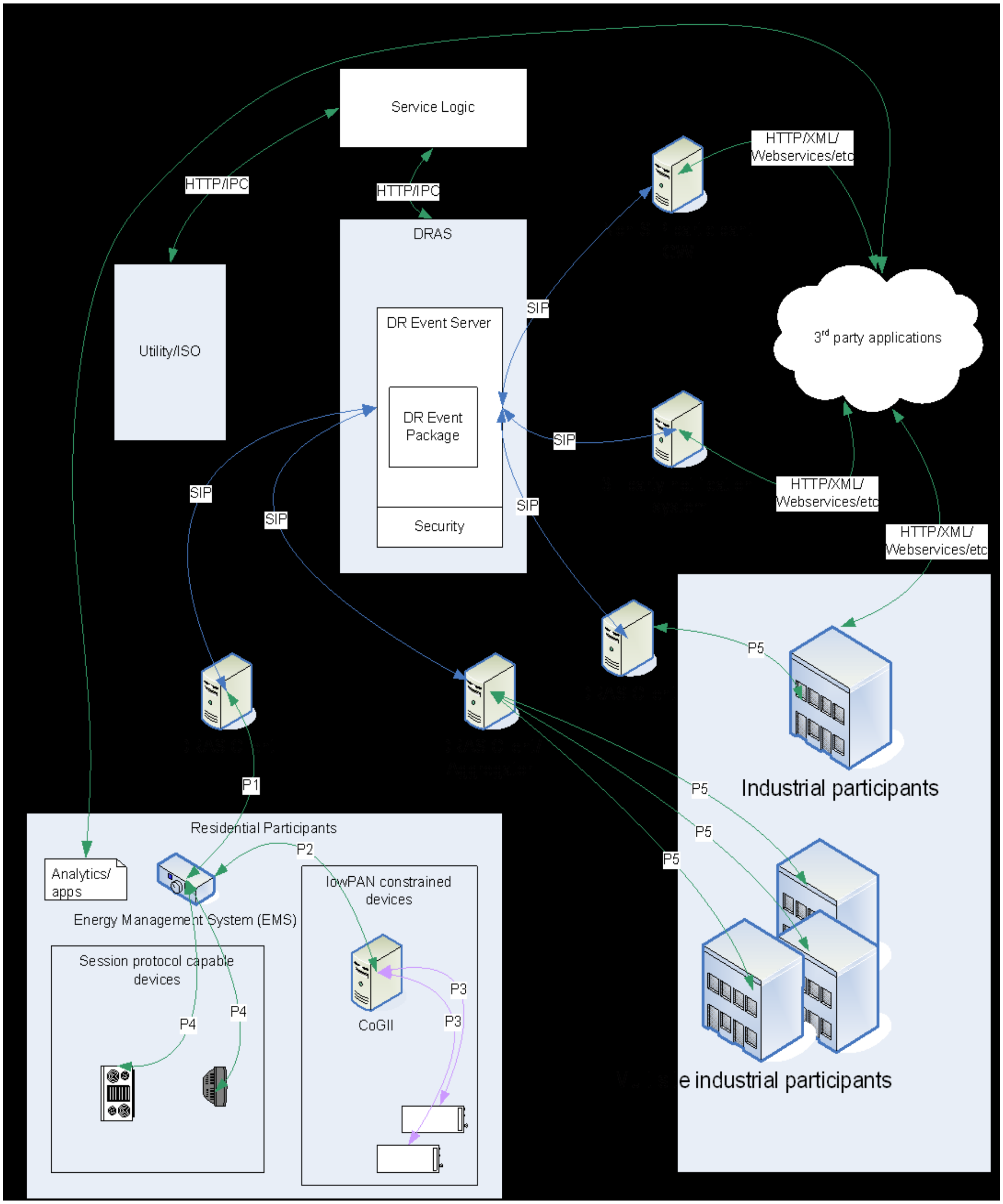

Figure 27: Architecture Based on SIP [34].

In this architecture, the proposed DRAS can serve as an Event Notifier, Real Time Pricing Notifier, Program Notifier and as a Bidding Proxy. It consists of the following components:

a) DRAS Event Server:

   This event server has many roles and one of them is to receive updates from the Utilities through the SIP PUBLISH message for DR pricing schemes and it also receives SUBSCRIBE requests from entities to participate in a DR program. It also issues NOTIFY commands to particular entities to indicate a change of state for the DR event. A package manager forms an integral part of this event server. This package manager consists of XML representation of all the state and attribute information required by the participants.

b) DRAS Business Logic: This can be said as a layer, which works intelligently in concurrence with the event server module and the service logic to create unique DR programs.

c) Service Logic:

   This can be said as an entity which is independent logically and schedules the DR events intelligently which also allows complex distribution and routing of DR participants depending on different factors like time of the day, current location of participants etc.

d) Event Aggregator:

   If there are many objects in a system, then subscribing to an event becomes complex as the client has to search for the object and then register individually. If there are multiple events for a single object, then a subscription is required for each event. An event aggregator can be said as an answer to this which can be defined as a single source of events for many objects. It registers for all the events of all the objects by just registering as the aggregator. On behalf of many participants, the aggregator can subscribe to the event package and this will result in reducing the network load. The event aggregator acts as a kind of 'trusted proxy' for all the participants.

e) Third party Notification System:

This acts as an opening for developing new applications based on allowable security parameters in order to subscribe a DR event selectively.

f) Non-SIP Gateway:

This gateway makes sure that all the participants including the ones which are not compliant with SIP are also able to participate in the DR program.

g) DRAS Client:

The main role of a DRAS client is to integrate the EMS (Energy Management System) to the DRAS. It is a logical entity, that interfaces with the EMS.

With the help of use case diagrams, we can observe the role of SIP in Generic Event Based Process (GEP) and Generic Bidding Program in figures 28 and 29.

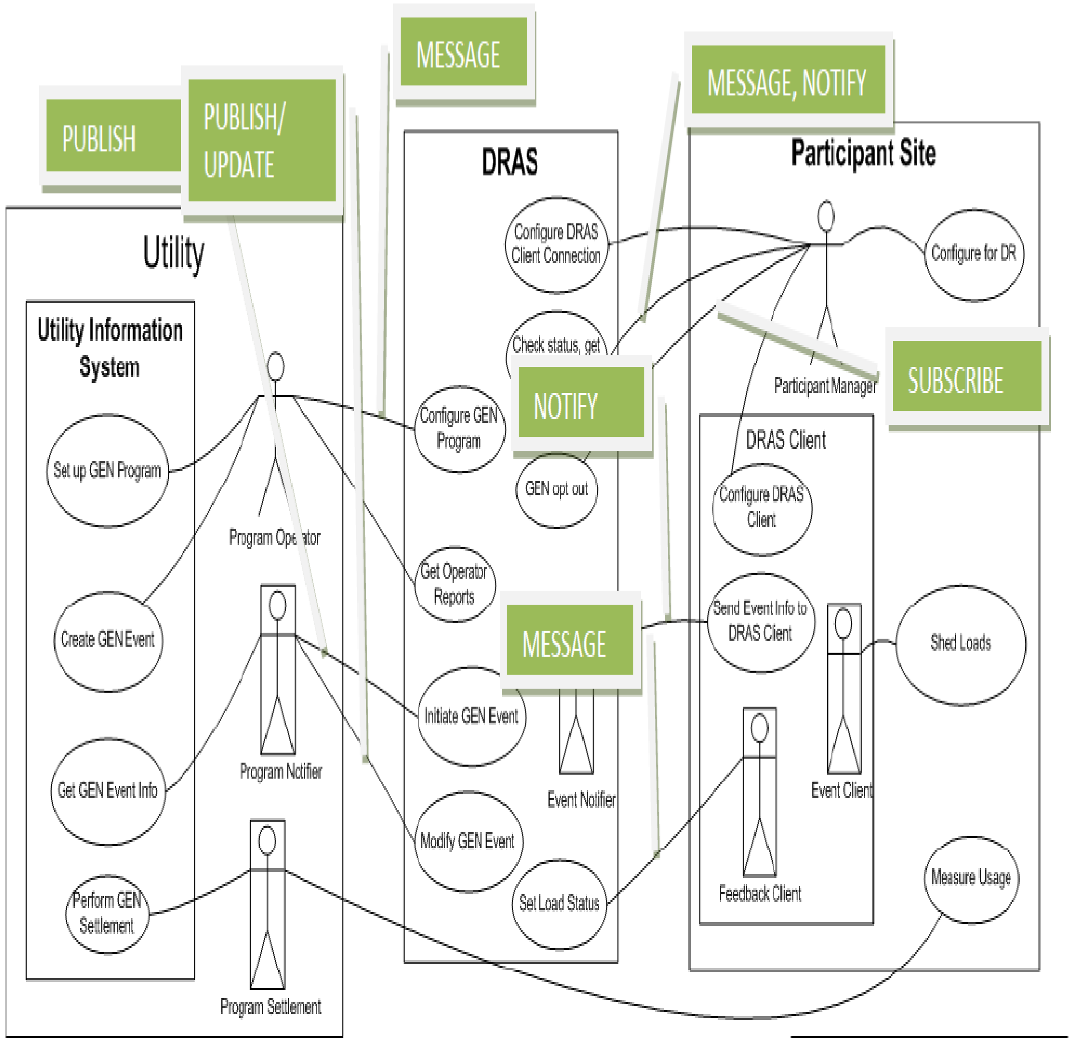

Figure 28: Generic Event Based Process [33].

In figure 28, the PUBLISH/SUBSCRIBE/NOTIFY methods of SIP are used for the realization of a generic event based program, which comprises of the setting up of a GEP program during the configuration phase, the creation and execution of a GEP event during the execution phase and the opt-out, communication, etc. of the GEP program during the maintenance phase.

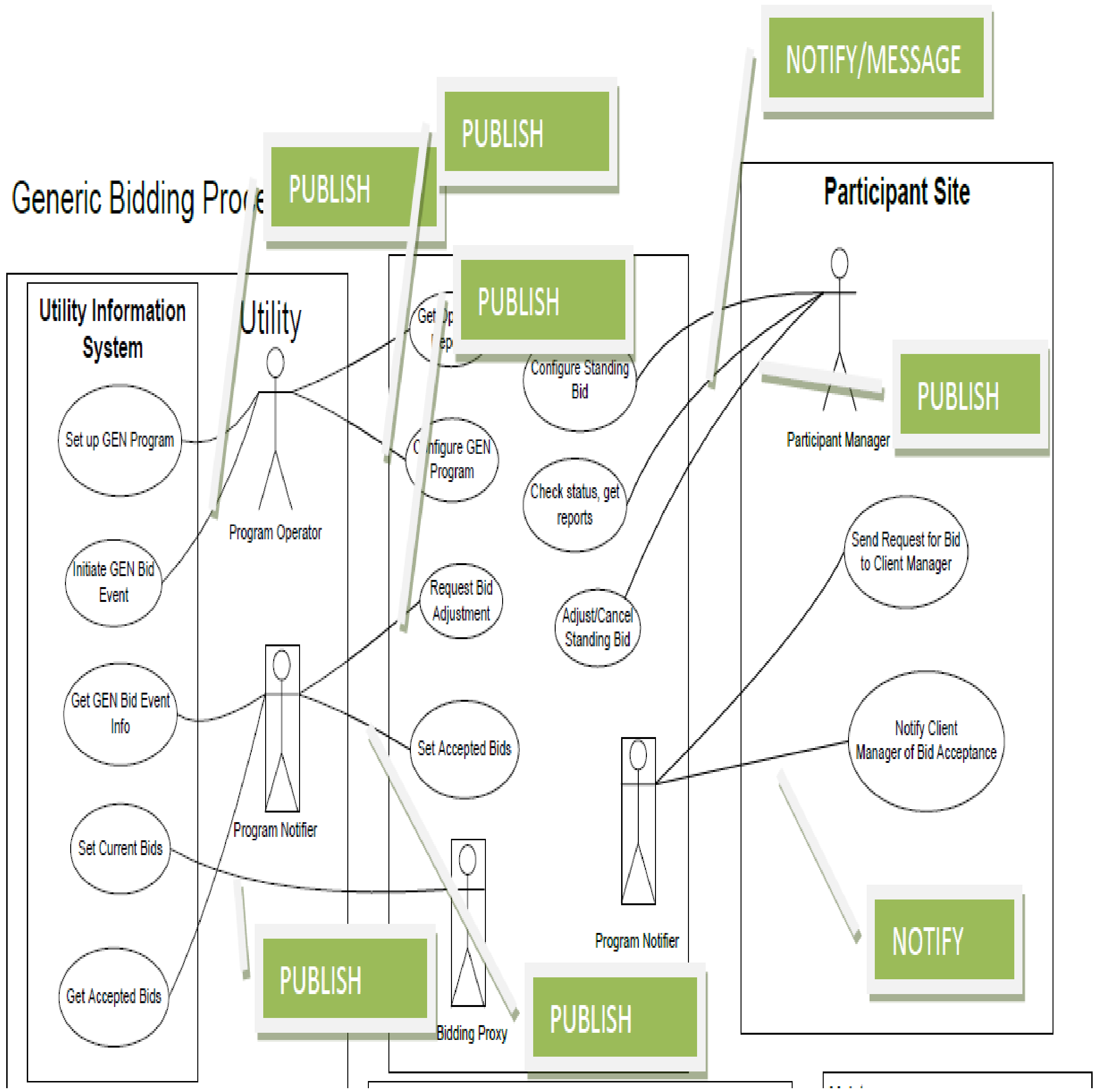

Figure 29: Generic Bidding Process [33].

In figure 29, the mapping of SIP methods like PUBLISH/NOTIFY takes place in order to realize a generic bidding process program for the demand response management. As seen in figure, we can observe the configuration, program bidding execution phase and the maintenance phase of the generic bidding process program.

Chapter 4

SECURITY CONSIDERATIONS

4.1. Security Threats

The security aspects should always be given high priority when designing a system specially when there is critical information exchange among different entities like utilities, consumers etc. The scenario becomes more sensitive when it involves use of private information for the remote monitoring and controlling of home appliances [36]. Privacy will be a major concern for the users as the entire information about the existence and use of appliances within their house will be contained in the messages. The scope for misuse of this data is very high. Therefore, there is need for private encrypted methods to be implemented in this regard. Any fabrications or modifications done in the messages can also lead to improper billing. Some of the commonly faced security threats and their impacts are listed in table 2 as follows:

Table 2: Attacks and their Impact [49].

THREATS	**IMPACT**
Eavesdropping: Unauthorized interception decoding of signaling messages	Loss of privacy and confidentiality
Viruses and Software bugs	DoS / Unauthorized access
Replay: Retransmission of genuine messages for reprocessing.	DoS, Incorrect Billing

THREATS	**IMPACT**
Spoofing: Impersonation of a legitimate user	Unauthorized Access, Improper Billing
Message tampering or Integrity: The message received is different from the message that was send (Fabrication)	Loss of integrity, DoS, Improper Billing
Prevention of access to network services e.g. by flooding SIP proxy servers / registrars /.	DoS, Improper Billing

4.2 Countermeasures

SIP security mechanisms:

SIP does not include any particular security mechanism in its specification. It takes help from other well established internet security protocols like Hypertext Transfer Protocol digest, Transport Layer Security (TLS), SIP Secure (SIPS), IP security (IPsec) and Secure MIME (S/MIME). The security for SIP can be deployed in an end to end or a hop to hop fashion as seen in figure 30.

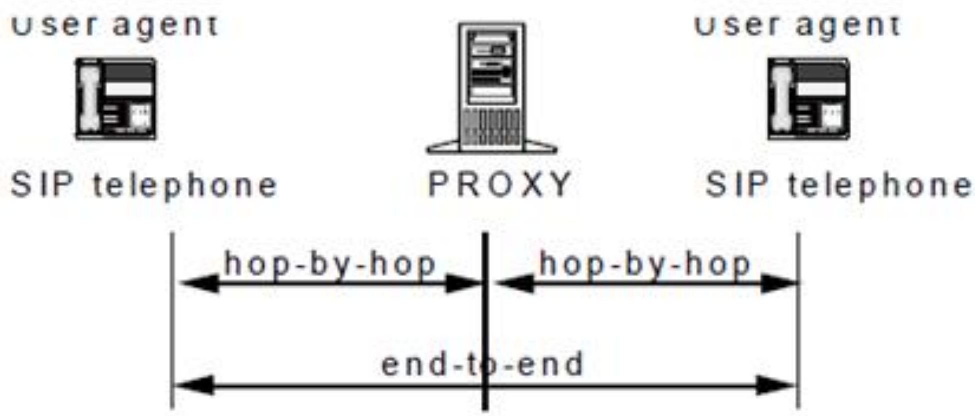

Figure 30: SIP Security Mechanism [36].

- HTTP Digest Authentication:

HTTP digest authentication is a challenge-response based authentication protocol. The authentication of SIP is based on this protocol. This mechanism is used by an SIP server like a registrar, proxy or a redirect server for authenticating messages exchanged with a user or another server [52]. Due to the absence of any encryption technique, it has no way to ensure confidentiality and integrity, which is a disadvantage.

- IP security:

IP is used to transport SIP messages and is vulnerable to attacks like session hijacking, sniffing etc. IPsec is a general purpose mechanism which protects SIP messages at the network level itself [51]. The IP packets are protected from such attacks by a set of services provided by the IPsec suite. Confidentiality, integrity, data origin authentication services as well as traffic analysis protection are provided in IPsec.

- Transport Layer Security (TLS):

SSL/TLS can be used to protect SIP messages. SSL/TLS has many of the advantages offered by IPsec and it runs above TCP/IP and below higher-level protocols such as HTTP or FTP and consequently the TCP header is not encrypted [50]. TLS provides end to end security mechanism and it requires the use of TCP as a transport protocol (tcp/sip) and requires a public key infrastructure. Though TLS does not support UDP as the transport protocol, this problem has been resolved with DTLS (TLS over UDP). SIP secure (SIPS) requires TLS on the whole path to the destination [50].

- Secure/Multipurpose Internet Mail Extension (S/MIME):

Secure MIME is a security mechanism, which protects the MIME contents carried by the SIP messages in order to ensure both confidentiality and integrity by means of the multipart/signed and application/pkcs7-mime [54]. MIME types. Digital certificates are used to identify the users. The implementation of a global S/MIME Public Key Infrastructure (PKI) is required for the success of S/MIME.

The following table lists out the countermeasures corresponding to their threats:

Table 3: Threats, impact and their countermeasures [49].

THREATS	IMPACT	COUNTERMEASURES
Eavesdropping: Unauthorized interception decoding of signaling messages	Loss of privacy and confidentiality	Use IPsec, TLS to encrypt the transmitted data.
Viruses and Software bugs	DoS / Unauthorized access	Install antivirus applications or apply software patches.
Replay: Retransmission of genuine messages for reprocessing	DoS, Improper Billing	Use S/MIME to encrypt and sequence messages (Cseq and Call-ID headers).
Spoofing: Impersonation of a legitimate user	Unauthorized Access, Improper Billing	HTTP digest can be used for address authentication between call participants.
Message tampering or Integrity: The message received is different from the message that was send (Fabrication)	Loss of integrity, DoS, Improper Billing	Use IPsec, TLS to encrypt the transmitted data.
Prevention of access to network services. Example: By flooding SIP servers.	DoS, Improper Billing	Configure devices to prevent such attacks.

Chapter 5

CONCLUSION

5.1. Summary

This report mainly focussed on analyzing the role of SIP in the Smart Grid environment. This report has provided a basic understanding on the concepts of Smart Grid, SIP and a review of concepts such as the HAN, Zigbee, PEVs, Demand Response. It gave an overview of the present scenario for HAN in the Smart Grid and the improvements that can be brought in with the deployment of SIP through the concepts like Forking, Grouping, Addressing, Discovery etc. It talked about the Offer-Answer model based on RFC3264, the Event Service model based on RFC3265 and the SIP presence framework based on RFC3856. Then the proposition of a SIP-Zigbee interworking Architecture model was explained. This model was based on the mapping between the binding mechanisms of the Zigbee and the PUBLISH/SUBSCRIBE mechanisms of the SIP presence framework. This proposed model has brought in a possibility to remotely monitor and control the Zigbee HAN devices from an SIP enabled user device. It described the Plug in Electric Vehicles (PEVs) and how SIP's support for mobile metering benefited the PEVs. Then the architecture of an automated demand response system based on the SIP's Event Service model was analyzed. The benefits included the introduction of a powerful push architecture in the Open ADR based on the PUBLISH/SUBSCRIBE model. Then the report discussed about the threats faced by SIP like Message Hijacking, Replay, Message fabrication etc. and their impacts such as Denial of Service (DoS), incorrect billing etc. Some of the countermeasures considered SIP in the report are TLS, IPsec, Secure MIME, HTTP Message Digest Authentication, SIPS.

5.2. Future Work

This report has given a generalized and broader perspective of SIP's role in Smart Grid. Apart from the Smart Grid infrastructure discussed in the report, there are various areas (Power generation and transmission involving SCADA etc) within the Smart Grid Ecosystem that SIP as a protocol may be applicable for. So, the future work can comprise of conducting research and detailed study on the mechanics of how SIP can map, its advantages and/or challenges. The result may be an increasing applicability of SIP in the Smart Grid environment. The scope for the possibility of future work is vast. The fact that SIP, is being considered as a candidate protocol for future generation networks to promote ubiquitous connectivity has motivated many enterprises like Avaya, Cisco and many independent groups to fund the research in this perspective [50]. Most of the aspects explained in this report are still at a proposal stage and have not been in implementation. There is still a lot of research to be done before SIP is widely implemented in the Smart grid infrastructure. Few of the independent special interest groups like "Smart Grid SIG" are trying to evaluate applicability of SIP in the priority list identified by the Federal Energy Regulatory Commission (FERC) identified in the document "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)", dated September 2009 [53].

GLOSSARY

ADR	Automated Demand Response
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
ATM	Asynchronous Transfer Mode
CoGii	Constrained-to-General-Internet Intermediaries
Cseq	Command Sequence
DDP	Device Description Protocol
DLC	Direct Load Control
DMP	Device Messaging Protocol
DoS	Denial of Service
DR	Demand Response
DRAS	Demand Response Automation Server
EMS	Energy Management System
FERC	Federal Energy Regulatory Commission
FFD	Full Functional Device
GE	General Electric

GEP	Generic Event Based Program
GTM	Green Tech Media Company
GwA/B	Gateway A/B
HAN	Home Area Network
HTTP	Hyper Text Transfer Protocol
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security
ISO	Independent System Operator
MAC	Media Access Control
MIME	Multipurpose Internet Mail Extensions
NAN	Neighborhood Area Network
NAT	Network Area Traversal
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology

OCMS	Oracle Communication and Mobility Server
OSI	Open System Interconnection
PA	Presence Agent
PAN	Presence Area Network
PDA	Personal Digital Assistant
PEV	Plug in Electric Vehicle
PHY	Physical Layer
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
PUA	Presence User Agent
RFC	Request for Comments
RFD	Reduced Functional Device
RTCP	Real Time Transport Control Protocol
RTP	Real Time Transport Protocol
S/MIME	Secure Multipurpose Internet Mail Extensions
SDP	Session Description Protocol
SIG	Special Interest Group

SIMPLE	SIP for Instant Messaging and Leveraging Extensions
SIP	Session Initiation Protocol
SIPS	SIP Secure
SLP	Service Location Protocol
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
STUN	Session Traversal Utilities for NAT
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
US DOE	U.S. Department Of Energy
V2G	Vehicle to Grid

VCR	Video Cassette Recorder
VOIP	Voice over Internet Protocol
WPAN	Wireless Personal Area Network
XML	extensible Markup Language
ZC	Zigbee Coordinator
ZDO	Zigbee Device Object
ZED	Zigbee End Device

REFERENCES

[1] US Department of Energy, "The Smart Grid: An Introduction", [Online].

Available: http://www.oe.energy.gov/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf

[2] NIST, "Smart Grid: FAQs", [Online].

Available: http://www.nist.gov/smartgrid/faq.cfm

[3] US Department of Energy, "Understanding the Benefits of the Smart Grid", [Online].

Available: http://www.smartgrid.gov/sites/default/files/pdfs/understanding_benefits.pdf

[4] US Department of Energy, "What is the Smart Grid", [Online].

Available: http://www.smartgrid.gov/sites/default/files/pdfs/what_is_smart_grid_03-2009.pdf

[5] NIST, "The Smart Grid and Consumer Electronics", [Online].

Available: http://www.nist.gov/smartgrid/upload/ArnoldWEF01102011-2.pdf

[6] The Smart Grid Frontier: Wide Open; David Heyerman; May 3, 2009, [Online].

Available: http://tinycomb.com/2009/05/03/what-is-the-smart-grid/

[7] NIST, "Framework and Roadmap for Smart Grid Interoperability Standards", Release 1.0 Draft, [Online].
Available: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf

[8] James Wright, "SIP: An Introduction", [Online].
Available: http://www.konnetic.com/Documents/KonneticSIPIntroduction.pdf

[9] IETF, RFC3261, "SIP: Session Initiation Protocol", [Online]
Available: http://www.ietf.org/rfc/rfc3261.txt

[10] Bradley Mitchell, "SIP-Session Initiation Protocol", [Online].
Available: http://compnetworking.about.com/od/voipvoiceoverip/g/bldef_sip.htm

[11] Agilent Technologies:Thomas Doumas, "Next Generation Telephony", [Online].
Available: http://literature.agilent.com/litweb/pdf/5968-6297E.pdf

[12] Radvision, "SIP: Protocol Overview", [Online].
Available: http://www.radvision.com/NR/rdonlyres/51855E82-BD7C-4D9D-AA8A-E822E3F4A81F/0/RADVISIONSIPProtocolOverview.pdf

[13] Nortell, "SIP and the new network communications model", [Online].
Available: http://www.nortel.com/products/01/succession/es/succession_csemx/doclib/nn106700-060204.pdf

[14] IETF(2010), "Multiparty Multimedia Session Control (mmusic)", [Online].
Available: http://datatracker.ietf.org/wg/mmusic

[15] Joe DiAdimo, "SIP:The Clear Choice for Smart Grid Communications", [Online].

Available:http://www.smartgridnews.com/artman/publish/commentary/SIP_

The_Clear_Choice_for_ Smart_Grid_Communications-604.html

[16] Bill Leslie, "The Role of SIP in Smart Grid Networks", [Online].

Available:http://www.sipforum.org/component/option,com_docman/task,cat_

view/gid,93/Itemid,261/

[17] IETF, "Motivation for SIP as an application protocol for 6lowpan devices draft-

roychowdhury- 6lowappsip", [Online].

Available: http://tools.ietf.org/html/draft-roychowdhury-6lowappsip-00

[18] Burns&McDonnel, "Home Area Networks", [Online].

Available: http://www.burnsmcd.com/portal/page/portal/Internet/Service/Electrical_

Transmission and Distribution1/SmartGrid/Home%20Area%20Network

[19] Greentech Grid (Article), [Online].

Available: http://www.greentechmedia.com/articles/read/smart-grids-han-market-to-

hit-750-million-by-2015/

[20] K. Stouffer, J. Falco, K. Scarfone, Guide to Industrial Control Systems (ICS) Security,

National Institute of Standards and Technology (NIST), Sept 2008 [online].

Available: http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

[21] Nathan Ota, "The Home Area Network: Architectural Considerations for Rapid Innovation", [Online].

Available: http://www.pennenergy.com/index/power/smart-grid/display/3151828412/articles/pennenergy/ugc/smart-grid/the-home-area-network-architectural- considerations-for-rapid-innovation.html

[22] Wikipedia, "Zigbee", [Online].

Available:http://en.wikipedia.org/wiki/Zigbee

[23] Meshnetics, "Zigbee FAQ", [Online].

Available:http://www.meshnetics.com/zigbee-faq/

[24] Mikhail Galeev, "Home networking with Zigbee", [Online].

Available:

http://www.media.mit.edu/resenv/classes/MAS961/readings/embeddedmag/zigbee.html

[25] OECD (2009, Dec). “Smart Sensor Networks: Technologies and Applications for Green Growth,” [Online].

Available: http://www.oecd.org/dataoecd/39/62/44379113.pdf

[26] Zigbee Alliance, "Zigbee Specification", [Online].

Available: http://webstaff.itn.liu.se/~jinzh/thesis/STD%20Document/ZigBee%20feature%20 speciication/1_053474r17ZB_TSC-ZigBee-Specification.pdf

[27] Bob Gohn, "Zigbee-based demand-response systems reduce home energy usage", [Online].

Available: http://www.insurancetech.com/articles/212200388

[28] Paar, Christof, Andy Rupp, Kai Schramm, Andre Weimerskirch, Wayne Burleson. "Securing Green Cars: IT Security in Next-Generation Electric Vehicle Systems".

[29] Wikipedia, "Vehicle to Grid", [Online].
Available: http://en.wikipedia.org/wiki/Vehicle-to-grid

[30] Siemens, "Open Communications for Smart Grid Devices", [Online].
Available: http://www.smartgridnews.com/artman/uploads/1/SIP_-_Open_Communications_for_SmartGrid_Devices.pdf

[31] U.S. Federal Energy Regulatory Commission (FERC), 2007 "Assessment of Demand Response and Advanced Metering", [Online].
Available: http://www.ferc.gov/legal/staff-reports/09-07-demand-response.pdf

[32] Kevin Lauckner; HoneyWell, (2009, Jul), “Honeywell Smart Grid Perspective,” [Online].
Available:
http://www.demandresponsetownmeeting.com/presentations/ppt/2009/Kevin%20Laucker,%20Honeywell_SESSION%20D,%207.14.09.ppt

[33] M.A. Piette, G. Ghatikar, S. Kiliccote, E. Koch, D. Hennage, P. Palensky, and C. McParland (2009, April), “Open Automated Demand Response Communications Specification (Version 1.0),” [Online].
Available: http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf

[34] Arjun Roychowdhury, "Realizing the Open ADR Demand and Response Specification using SIP", [Online].
Available:
http://www.sipforum.org/component/option,com_docman/task,doc_view/gid,375/Itemid,261/

[35] Patrice Kadionik, Charles Consel, "HomeSIP: Building a smart Space with SIP Protocol", [Online].

Available: http://www.enseirb-matmeca.fr/cosynux/HomeSIP/

[36] IETF, "Framework Draft for Networked Appliances using the Session Initiation Protocol", [Online].

Available: http://tools.ietf.org/html/draft-moyer-sip-appliances-framework-01

[37] IETF, "A Presence Event Package for the Session Initiation Protocol", [Online].

Available: http://tools.ietf.org/html/rfc3856

[38] IETF, "An Offer/Answer Model with the Session Description Protocol", [Online].

Available: http://www.ietf.org/rfc/rfc3264.txt

[39] IETF, "Session Initiation Protocol (SIP)-Specific Event Notification", [Online].

Available: http://www.ietf.org/rfc/rfc3265.txt

[40] IETF, "SIP Extensions for Communicating with Networked Appliances", [Online].

Available: https://www3.tools.ietf.org/tools/rfcmarkup/rfcmarkup.cgi?draft=draft-tsang-sip-appliances-do-00.txt

[41] IETF, "SDP: Session Description Protocol", [Online].

Available: http://www.ietf.org/rfc/rfc2327.txt

[42] Slobodanka Tomic, Petia Todorova, "SIP meets Zigbee", [Online].

Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4299120

[43] IETF, "Device Message Protocol (DMP): An XML based format for Wide Area Communication with Networked Appliances", [Online].
Available: http://www.research.telcordia.com/iapp/draft-khurana-dmp-appliances-00.txt

[44] Voxeo, "Speaking of Standards", [Online].
Available: http://blogs.voxeo.com/speakingofstandards/category/simple/

[45] Oracle, "Communication and Mobility Server Administrator Guide", [Online].
Available: http://download.oracle.com/docs/cd/B32110_01/ocms.1013/b31497/about_sdp.htm

[46] California Energy Commission's Public Interest Energy Research Program, PIER Buildings Program (2008, Dec 03), "Automated Demand Response Cuts Commercial Building Energy Use and Peak Demand, Technical Brief," [Online].
Available: http://www.esource.com/esource/getpub/public/pdf/cec/CEC-TB-31_AutoDR.pdf

[47] S. Kiliccote, M. A. Piette, J. H. Dudley; Lawrence Berkeley National Laboratory (LBNL), E. Koch and D. Hennage; Akuacom (2009, July), "Open Automated Demand Response for Small Commercial Buildings," [Online].
Available: http://drrc.lbl.gov/pubs/lbnl-2195e.pdf

[48] Wikipedia, "Push Technology", [Online].
Available: http://en.wikipedia.org/wiki/Push_technology

[49] Dimitris Geneiatakis, Georgios Kambourakis, Tasos Dagiuklas, Costas Lambrinoudakis and Stefanos Gritzalis, "SIP Security Mechanisms: A state-of-the-art review", [Online].
Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1684926

[50] Andreas Steffen, Daniel Kaufmann, Andreas Stricker, "SIP Security", [Online].

Available: http://security.hsr.ch/docs/DFN_SIP.pdf

[51] Cisco Systems, "Security in SIP-Based Networks", [Online].

Available: http://www.cisco.com/warp/public/cc/techno/tyvdve/sip/prodlit/sipsc_wp.pdf

[52] IETF, "HTTP Authentication: Basic and Digest Access Authentication", [Online].

Available: http://www.ietf.org/rfc/rfc2617.txt

[53]SIP Forum, "SIG", [Online].

Available: http://www.sipforum.org/content/view/351/266/

[54] IETF, "Security Multiparts for MIME: Multipart/Signed and Multipart/ Encrypted", [Online].

Available: http://tools.ietf.org/html/rfc1847

[55] Tutorials.org, “Networking”, [Online].

Available:

http://etutorials.org/Networking/network+management/Part+II+Implementations+on+the+Cisco+Devices/Chapter+4.+SNMP+and+MIBs/Technology-Specific+MIBs+for+Accounting+and+Performance/

[56] SIP Methods, “Basic Call Example”, [Online].

Available: http://facers.blog.ithome.com.tw/post/70/797