Novel Distributed Load Management Algorithm (NDLMA) for Local Level Management in Smart Grid

Author,
Usman Ali
MS Computer Software Engineering
00000205297

Supervised By
Dr. Usman Qamar

DEPARTMENT OF COMPUTER & SOFTWARE ENGINEERING
COLLEGE OF ELECTRICAL & MECHANICAL ENGINEERING
NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY
ISLAMABAD

Nov 2020

Novel Distributed Load Management Algorithm (NDLMA) for Local Level Management in Smart Grid

Author,

Usman Ali

Fall 2017 MS-17 (CSE) 00000205297

A thesis submitted in partial fulfillment of the requirements for the degree of

MS Computer Software Engineering

Thesis Supervisor:

Dr. Usman Qamar

Thesis Supervisor's Signature:-____________________________________

DEPARTMENT OF COMPUTER & SOFTWARE ENGINEERING

COLLEGE OF ELECTRICAL & MECHANICAL ENGINEERING

NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY, ISLAMABAD

Nov 2020

DECLARATION

I declare that this research work titled *"Novel Distributed Load Management Algorithm (NDLMA) for Local Level Management in Smart Grid"* is my own work under the direction of Dr. Usman Qamar. The work has not been presented somewhere else for assessment. The material that has been used from other sources it has been appropriately acknowledged.

____

Student Signature

Usman Ali

Fall 2017-MS-17 (CSE) 00000205297

LANGUAGE CORRECTNESS CERTIFICATE

Any type of spelling, typing, grammatical and semantic mistakes are not present in this research work. The thesis is formatted in accordance with the template provided for MS thesis work.

____

Signature of Student

Usman Ali

Fall 2017-MS-17 (CSE) 00000205297

____

Signature of Supervisor

Dr. Usman Qamar

COPYRIGHT STATEMENT

ACKNOWLEDGEMENTS

With the blessings of **Almighty Allah (SWT)**, I was able to do this work. Indeed none be worthy of praise but the Almighty Allah. In addition, my admirations be upon **Holy Prophet Hazrat Muhammad (PBUH)** and his Holy Household.

I would like to express my special thanks to my supervisor **Dr. Usman Qamar** for his generous help throughout my thesis, and for being available even for the pettiest of issues.

I am thankful to **Dr. Wasi Haider** and **Dr. Urooj Fatima** for an excellent guidance throughout this journey and for being part of my evaluation committee.

Lastly, I would like to thank the individuals who helped me in this period.

“*I dedicate this to my phenomenal parents and siblings.*”

ABSTRACT

The world is adopting renewable energy sources to produce clean energy and save the environment. The conventional grid systems are facing a lot of problems due to this new adaption, for example, effective control of consumers, the recompense of supply instability, and fluctuation in power generation due to change in weather. The conventional electric grids have to ensure operability by adapting to energy demand. The smart grid can conquer these shortcomings. However, it requires data as precise as possible so that it can manage the demand of the grid and obtain good results. As a bigger quantity and accurate data reduce the privacy of consumers. Thus, it raises the conflict among privacy and Quality of Information (QoI). In this study, we are considering a model of a smart grid that has three levels: transmission, micro-grid, and local level. We propose a distributed algorithm for energy management at the local level which ensures the privacy of the user. For user data, it uses smart encryption. This algorithm categorizes smart home appliances into three categories: baseload, adaptable load, and shift-able load. Privacy is attained by taking different measures for privacy. However, privacy costs data volume overheads. This algorithm can normalize the peak demand and control the preference of home appliances, through distributing energy among appliances depending on their consumption and priority, without exceeding the predefined total energy consumption threshold.

Keywords—Smart grid, Smart home, Distributed Algorithm, Optimization and Demand Side Management.

Table of Contents

Table of Figures

Table of Tables

Chapter 1

INTRODUCTION

Chapter 1: Introduction

This chapter contains a brief introduction of the research performed. Section 1.1 explains the background study. Section 1.2 elaborates the problem statement. The proposed methodology explained in Section 1.3. In Section 1.4 we explained our research contribution and Section 1.5 states the organization of thesis.

This chapter gives a detailed intro of our research work. The main purpose is to present an outline of the work done in this thesis, the goals of the work and approach used for performing this research work. This chapter also includes motivation for the research work, objective of the research work, scope, assumptions and exclusions.

1.1. Background:

Electricity plays an important role in the development of a nation. With the increasing population, increasing urbanization and change in energy usage patterns, electricity demand is also increasing continuously. Pakistan's energy infrastructure is based on traditional system hence it is under developed and poorly managed. Pakistan is facing severe energy crisis from the past few years but the government is making no serious efforts to increase generation capacity. Demand is rising continuously resulting in load-shedding which has become a routine for households of Pakistan.

Pakistan is facing woes related to energy. Electricity demand is increasing and so are the energy costs which makes it difficult to supply continuous electricity at affordable rates. Electricity deficit in the country is increasing day by day. The residential consumers are depending on alternative energy supplies to fulfil their primary needs. Non-renewable resources used to generate electricity are depleting causing a rise in energy costs. Integrating renewable energy sources into the grid can cause imbalances in the grid due to their random and intermitting nature.

Keeping in view the current situation in Pakistan, there is a dire need to better manage the electricity demand and supply and use alternative methods to generate electricity. If Pakistan is successful in adding renewable sources to generate electricity, smart grids will be needed to manage problems caused by intermittency and distributed power. Power theft is quite common in Pakistan. In last five years our country has lost 90 billion rupees in line losses and electricity theft. (ICCI Lauds PM's Move against Power Theft. 2013, July 17. The

Nation, Karachi, Pakistan). The 44 percent of electricity losses due to transmission line and theft need to be stopped. The existing grid system needs to be modernized to be able to accommodate traditional energy sources and renewable ones such as solar and wind.

Installation of smart grids will enable two-way communication with WAPDA allowing for more efficient operation and more detailed usage information to customers. The smart meters will help cut down power theft as well. This will help to make Pakistan's energy system more efficient, reliable and secure.

The frequent power outages have led to residential property dwellers looking for backup power systems. Most popular of these are fuel powered solar panels, generators and UPS inverter. The fuel powered solar panels and generators are more sporadic where UPS inverters are quite common and have become an essential household appliance. UPS inverters are more common than generators and solar panels because their initial cost is lower than the other two options. The generators and solar panels are not grid tied to serve as energy backups. Whereas, UPS inverters charge the batteries using electricity from the grid. It charges batteries when the electricity is coming from the grid and then supply the stored energy to essential loads connected via UPS during load shedding hours. This results in two stage inefficiency where energy is lost in charging batteries and then in providing power to loads during power outage. UPS inverters have led to an addition to the household appliances hence adding to the grid supply-demand shortfall.

1.1.1. The Demand of Energy & Supply Gap

Energy sector is the primary driver of a country's economy. It is a major fuel for various industries like power sector, steel, chemical, textile, fertilizers, paper, cement, transport, etc.

The growth in energy demand that the countries are facing is mainly because of growing population, increased agricultural and industrial production, technological advancement, and improvement in quality of life.

With the growth in Pakistan's economy in the last few years, demand for energy has also increased. Pakistan's energy sector needs to fill the demand supply gap by integrating renewable sources into the system and by improving transmission and distribution network. The total installed power generation capacity of Pakistan is 34,282 MW. (Ministry of Finance, 2019, Pakistan Economic Survey 2018-19)

In 1947, the country's total electricity generation installed capacity was 60 MW for a population of 31.5 million, yielding 4.5 units per capita consumption, but by 2019, the total electricity generation installed capacity from all sources has reached 34,282 MW (Ullah, K. 2013, Electricity Infrastructure in Pakistan: an Overview. International Journal of Energy, Information and Communications). Despite installed capacity exceeds demand, but due to lack of information about demand usage pattern, installed capacity is not being used optimally. The bureaucratic processes to use energy efficiently are also not effective for installed capacity to be used optimally. In spite of these additions, there is shortfall of electricity and even the major cities do not get round the clock power supply. This fact sums up the power demand supply gap scenario of the country. The demand supply gap, the country is facing a number of hours of load-shedding daily.

According to the analysts, Pakistan receives abundant solar energy in most of its regions throughout the year and can easily generate more than 100 kW of electricity.

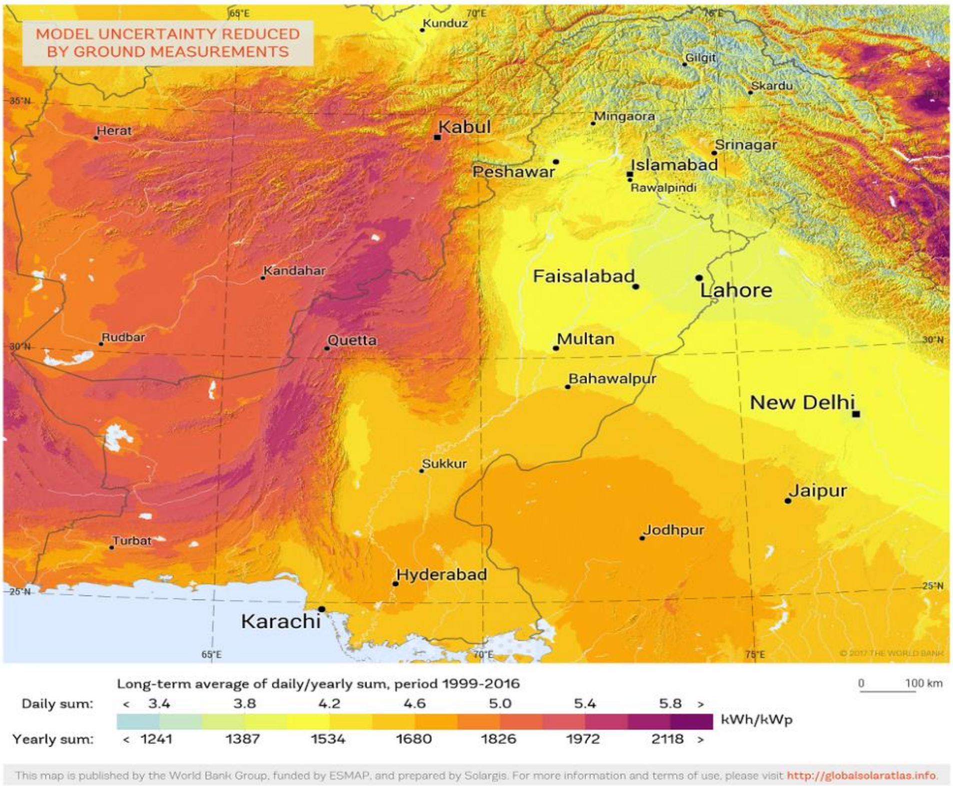

Figure 1 Map shows Solar Radiation in Pakistan

As shown in the figure above, most regions of Pakistan receive high solar radiation. Baluchistan, Southern Punjab and Northern Sindh receive very high solar radiations in the range of 5 to 7 KWh per m2 per day while the rest of Pakistan receive around 4.5 to 5 KWh per m2 per day. The projects for developing solar energy plants are currently in progress in

Kashmir, Punjab, Sindh and Baluchistan. The retail and awareness of solar panels are increasing in Pakistan.

The increasing awareness of solar panels and other domestic solutions show that households are using alternative energy sources but it is not planned and not according to demand. The electricity storage mediums are expensive, have high replacement cost, short life span and cannot be deployed at a large scale (e.g. batteries). Currently, the alternatives for electricity are not environment friendly and economically efficient. Making cities smarter and adopting smart grid technologies could not only hold the answer to energy shortfall but also help produce and consume electricity optimally.

1.1.2. Pakistan's Power Crisis

Since 2007, energy crisis has been a major issue in Pakistan. Demand of energy has increased greatly in the last decade because of population growth, changes in lifestyle and industrial development. Whereas, generation of electricity does not meet the increased demand resulting in power crisis. The government has not made sufficient effort to increase the generation capacity. Consequently, load-shedding has become a routine for households. Power breakdowns are severe in the rural areas and can also not be controlled in urban areas.

Energy crisis can be curtailed by improving power transmission system to decrease line losses, developing new energy resources and most importantly utilizing alternative energy sources. To solve the issue of severe power crisis in Pakistan, our policy should focus on demand based energy conservation and changes in demand patterns, and an effective implementation plan. The current distribution systems are based on outdated demand patterns. Only increasing generation capacity is not the answer to energy crisis.

1.1.3. Smart Grid

The conventional electrical grid is a system of different things. It consist of power plant, transmission lines, sub stations and customer. It has no system of communication from power plant to customer and vice versa. Whereas, the SG is an intelligent grid system which helps to improve a number of things i.e. production, transmission, distribution, fault recovery and the consumption of electric energy [1]. By introducing the information and communication technology (ICT) to existing conventional electrical grid system, we shall be able to balance the demand and distribution of grid. It has proper communication system between power generators and customers. So, it is a combination of conventional electric grid system and the ICT [2].

There are several definitions of the SG concept, but in short it is the future of power grid. It is the merger of electric energy system and ICT at all levels of the conventional power grid. It requires a continuous flow of information among all the contributors connected to SG.

In contrary to the conventional power grid, which has a vertically integrated architecture and power flow is one way, the SG is bi-directional, supports a greater penetration of Distributed Energy Generation feeding to the grid. Some researchers refer this structure as the "Energy Cloud", with reference to the internet architecture with multiple sources feeding into one common platform.

In particular, SG technology collects and integrates data from manufacturers, consumers or from the distribution of electricity. Further, Smart Grid insightfully processes the data. This knowledge is dispersed across the various levels of the network i.e. output, control and consumption.

In addition to the goals of a smart network, we mentioned:

1. Improved integration and regulation, under profitable conditions, of energy from distributed sources.
2. An enhancement in the efficiency and control of electricity.
3. An rise in consumer engagement (i.e. active customers and optimization of consumption).
4. Enhanced energy efficiency (fewer losses).
5. Better coordination between the transport network and the delivery of the network.

The SG is a complicated framework that can be split into several layers, and optimizing it is a difficult task that requires complex methodologies. SG aims at balancing demand and supply, at reducing total consumption, at regularizing the consumption curve and at incorporating emerging technologies into the traditional system[3]. Some of the SG's constraints are the sending of energy requirements, the improvement of energy flow, power, preventive maintenance, and the reduction of cost variations of electricity in order to increase investments and to make do with the generation and storage of renewable energy. The below given picture explains differences between convention and smart grid.

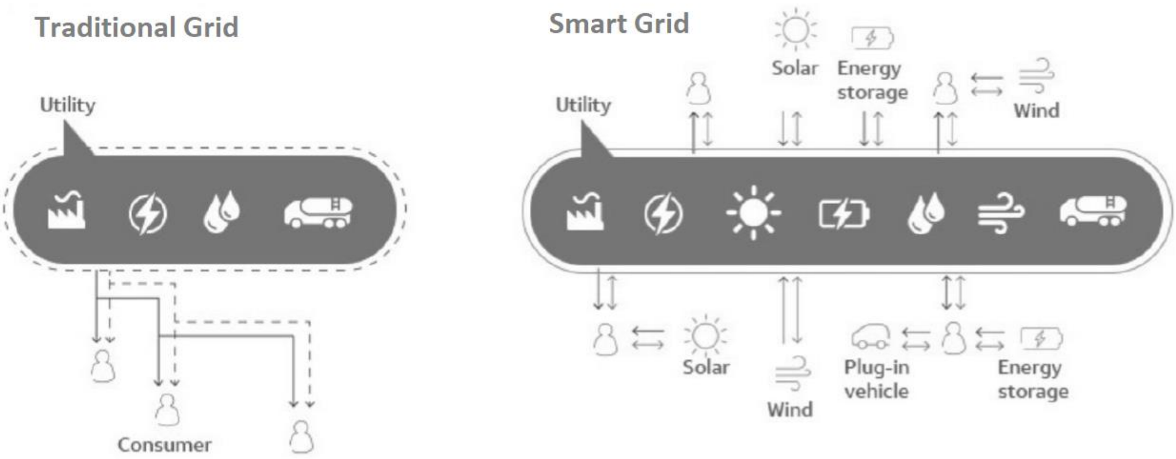

Figure 2 Conventional Grid vs. Smart Grid

1.1.4. Demand Side Management

Demand side management (DSM) encourages the consumers of energy to change their energy usage patterns. This is done by different methods including behavioral changes and fiscal incentives. As a result, the consumer uses less electricity during peak hours or shift their usage to off-peak hours i.e. night time or weekends. This helps to achieve the goal of DMS by consumer using the energy more efficiently. (Energy demand management. 2019, February 15)

DSM objective of allowing the consumers to control their energy consumption by adjusting their usage pattern will help households to save money and will help utilities to operate more efficiently.

1.2. Problem Statement

Load-shedding is one of the major problems faced by households of Pakistan. A DSM is crucial for Pakistan community as it helps to avoid the load peaks. The available Home Energy Management Systems (HEMS) are centralized and control the smart household appliances. A centralized infrastructure leads to several downsides when it comes to sharing information among systems via a network. Even if the data structure and semantics could be agreed upon in order to overcome the described interoperability issues, further challenges arise in terms of security, data ownership, data consistency, and data privacy.

Moreover, these centralized control systems have direct access to household appliances. Which put the user privacy at risk. Securing data for a centralized infrastructure is a challenging task as it becomes susceptible to eavesdropping and remote attacks. This implies that an extensive effort needs to be done in order to assure that patient information are secured in terms of privacy, assuring that only authorized parties are able to access the data [5].

The focus in this thesis will be on development of distributed energy management system which can help to ensure better energy management, user data security and privacy.

Given the fact that the SG technology is a rather new concept in Pakistan, A very little research has been conducted. This highlights why scientific research is needed to conclude sufficiently on the realistic potential of the SG technology with better energy management, security and privacy challenges to which this master thesis shall contribute.

1.3. Research Objectives

The top most objective of this research is to provide a secure solution to satisfy increasing energy requirement by supplying electricity to homes round the clock using smart grid. This objective is further divided into following specific objectives, achieving the following objective will result in achieving the main objective: What are the major problems in power management system that compromise the user data?

- Study the current power management system of Pakistan at local level.
- Analyzing the problems in the current management system, security related issues and their impact on demand supply gap.
- Resolve energy shortfall problem by proposing a solution to balance energy usage by reducing electricity demand and increasing efficiency of the system.

1.4. Research Questions

Based on the research objective, following are the research questions:

- What are the major problems in energy management systems that compromise the user data?
- How to control and monitor electricity usage pattern of household loads to manage the peaks?
- How demand side management and smart grid can help fill demand supply gap and decrease load on the grid while preserving the user privacy?

1.5. Research Contribution

The main focus of research is on the security of user data and decentralize energy management system. In this we document proposed a solution to improve the energy management system for optimal power usage and it is privacy friendly. Also, this research will be of great value because it will give an overview of the current scenario of power system in Pakistan focusing on electricity demand, supply and its usage.

This thesis proposed a distributed energy management algorithm for SG which is not only autonomous but also a privacy-friendly. With the proposed methodology is in impossible for the consumers and third parties to gain any information of any other consumer. In this proposed algorithm the server acts as beginning and ending point. As hybrid encryption is used to encrypt the data before transmission. Also, we combined it with another algorithm called, the bucket principle, which strengthen the privacy as the bucket principle have a separate encrypted space for every member. This helps in attaining a higher level of privacy. Nevertheless, as attaining security has its own cost, these privacy measures have data overhead which increase the data size.

The current energy crises in Pakistan calls for immediate measures so that energy needs could be met. Government has declared power sector to be its top priority in investment. Elimination of load shedding is top priority of present government. In 2019-20 budget, power sector is the priority with a total investment plan of PKR 74,236.350 million. (Source: http://www.finance.gov.pk/budget/Budget_in_Brief_2019_20.pdf) (14/Feb/2020).

1.6. Rationale

The residential electricity demand is growing continuously. The network needs to be improved to cope with the increasing demand. To increase the user acceptance the HEMS has to secure and privacy friendly. The current electricity grid system needs to be equipped with smart grids to accommodate the developments.

1.7. Research Limitation

Research limitations are the conditions or influences that cannot be controlled by the researcher and they might impact the conclusions and findings of the research, like the weather conditions, user comfort and real-time pricing of the electricity. The limitations faced in this research were access and sample size so the research design was chosen accordingly.

1.8. Target Audience

This thesis is targeted towards policy makers in order to ground lay work for adopting technologies like smart grid. It is a proposal to the government of Pakistan for providing continuous electricity to households of Pakistan. So the target audience is the government, investors, power distribution companies and the general public of Pakistan.

1.9. Research methodology

The methodologies and procedures used to accomplish research objectives include:

- Studying theoretical background and literature review on power system in Pakistan, smart grid, demand side management, alternative energy sources and renewable energy sources.
- Data collection from different sources.
- Implementing the proposed methodology in Python 3 and peer to peer architecture.
- Results compilation.

1.10. Thesis Outline

The chapters of this thesis, in chronological order, are:

Chapter 1: Introduction - Information about the research background, problem definition, research objectives and research question, intended outcomes of this study, societal and scientific contribution of research and organization of thesis.

Chapter 2: Theoretical Background - An introduction to the theory that the thesis is based on.

Chapter 3: Review of the Literature - based on the read papers, the main problems of the currently used databases and healthcare systems are described, and confronted with the valences of the SG technology. After that, some problems and challenges of this technology in are expressed, and also, some implementations and solutions, already developed by other researchers.

Chapter 4: Proposed Algorithm - Highlights the proposed methodology and a presentation of the methods used to design and implement the proposed methodology.

Chapter 5: Results and Discussion - Discussion about the research outcome, evaluation of the developed system and further improvements on the system.

Chapter 6: Conclusion - A conclusion derived from the obtained results.

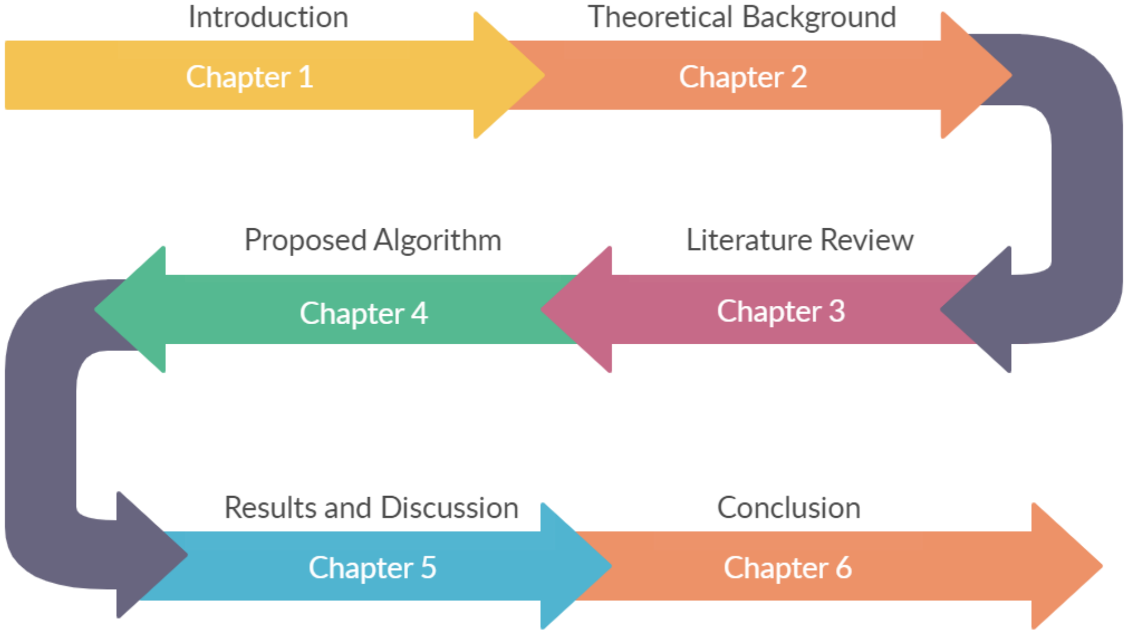

Figure 3 Thesis outline

Chapter 2

THEORETICAL BACKGROUND

Chapter 2: Theoretical Background

As explained in the introduction, extensive research was required to answer the initially posed research question in a scientifically sound manner. This chapter will cover the literature review performed for our research named "*Novel Distributed Load Management Algorithm (NDLMA) for Local Level Management in Smart Grid*".

Life cannot be imagined without energy. We are dependent on energy for living a quality life. Hence, demand of electricity is also increasing with time and we need to produce electricity from renewable energy sources on large scale to meet the increasing demand. If energy demand keep on increasing, it is expected to be at least twice as today by the year 2050. (Home energy research, European commission). If no serious effort is made to increase the generation capacity, the increasing demand will increase the dependency on imported energy resulting in unreliable energy supply and higher energy rates.

Energy supply should be made reliable, diverse, efficient and sustainable to meet the future energy demand.

2.1. Electricity Usage in Pakistan

Household electricity consumption makes up about a half of total electricity consumption. The rest half is consumed by industrial, agricultural and commercial consumers. Hence, the major usage of electricity is by residential consumers.

In Pakistan, most electricity, more than 55% is used by households. The demand for electricity in Pakistan has raised considerably in the last few years. It has been estimated that it has increased by about 80 percent in the last 15 years. It is expected that the demand will increase to 40,000 MW by the year 2025.

To meet the growing electricity demand and minimize wastage, the power distribution and management systems are in a dire need of improvement. Keeping in view the issues faced by energy sector, these issues can be overcome through transitioning a smart grid. Pakistan is highly dependent on fossil fuels like oil, natural gas and furnace oil for electricity generation.

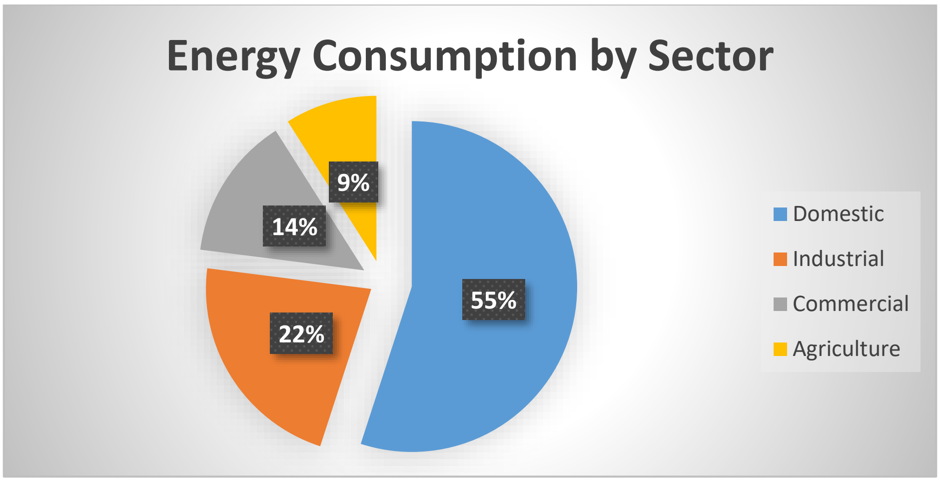

Figure 4 Energy Consumption by sectors

2.2. Architecture of Smart Grid

The smart grid combines ICT with the traditional grid in order to effectively generate, transport, distribute and consume electricity. SG has all the criteria of a complicated framework [9, 10]. We must know its characters, objectives, structure and its dynamics in order to model it later. There are three systemic layers of an electric grid: the producer mesh network, the middle linear network, and the consumer. A network of underground and overhead power lines that is comparable to the road network is used as soon as electricity is generated. Electricity transits across the network, which relies on the following: total generation, full consumption and network architecture.

Some of the main smart grid priorities are as follows:

- Self-diagnosis and failure-self-healing.
- Robustness versus any attachment.
- Customers' constructive involvement.
- Ensure the efficiency of energy as consumers need it.
- Balance the output according to demand.
- To satisfy the demand of consumers, avoid congestion using successful transmission and distribution strategies.
- Normalize consumption locally and internationally.
- T&D supplies the electricity to the poles of customer utilities. It is primarily related to the issue of optimum flow or routing.

The different smart grid levels are reflected in Figure 9. The second ring (in dark blue) represents the intermediate SG level, known as the micro-grid, which connects the production of energy and the consumption of energy. It is a tree structure that reflects a sub-station area and it is a broader view of resident clients.

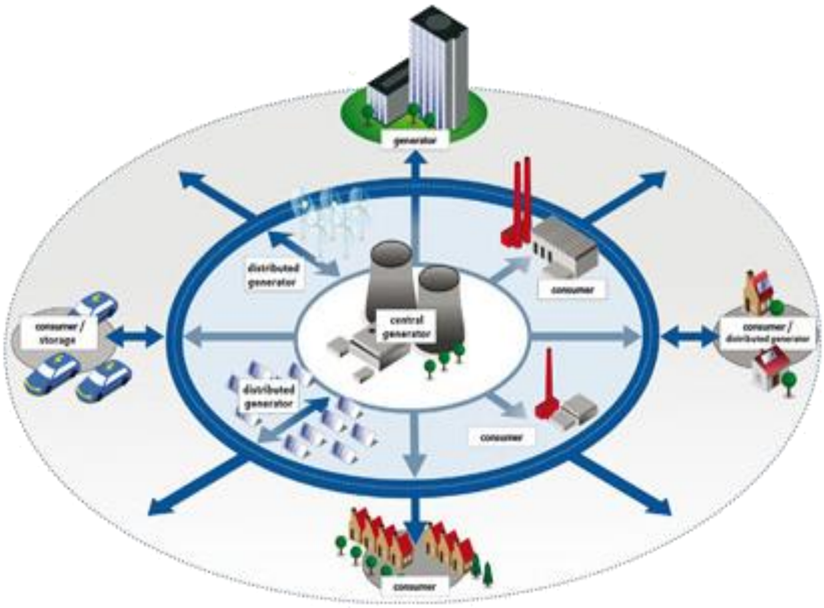

Figure 5 Subcomponents of Smart Grid

It regulates the delivery of energy and orders a definite amount of electricity for local customers in T&D. Similarly, representing the local bodies, the outer ring represents the third floor. These are the customers connected via the transmission and distribution network to a sub-station. The isolated buildings are local communities connected to one community, i.e. homes and factories that help the use of energy. In other words, the grid's local level is determined by the area managed by a smart meter or some form of Home Energy Management System (HEMS).

We are more involved in local level science, as well. We will therefore, address it in-depth.

2.3. Local Level Management

At this stage, management includes the automation of a house containing various types of equipment, such as lighting, air conditioning, water heater, washing machine, dishwasher, etc. [11]. There is a variable for each unit in home automation to represent its significance for immediate consumption [12]. As an example, air conditioning is more important during a heatwave, while heating has no significance. Therefore to control usage, a variable is applied to the priority of each system at the local level. Thus if the battery is full, an electric vehicle will be charged at night, the start of a washing machine will be delayed in the event of over consumption, a laptop will temporarily disable consumption. For a limited period, a range of devices can be stopped or their start-up can be halted. In housing areas, without affecting the user's comfort, about half of the consumption can be managed. Any of the equipment that should essentially work are lights, desktop computers and refrigerators. Such appliances therefore have a default priority value of 0, which guarantees the supply of electricity. Other appliances have values according to use and user activity statistics.

The operational priority for appliances is handled by the home automation controller. Smart meters, for example, can keep track of the electricity generated, control power flow, and even provide the consumer with an understanding of their usage patterns.

Every appliance is associated with a priority value. For SG's best operations, the regulation of priority variation is important. For this, there are many management techniques:

- Based on electricity consumption trends, many statistics and analysis of potential repetitions can be made in the medium and long term projections, based on feedback, as it constantly needs data.
- Alternative functionality, rather than simulating the world. In order to evade the similar patterns, stochastic patterns then simulate certain functions. It is internal management where all equipment can run independently.

2.4. Demand Side Management

The transition of electric grid will provide a sustainable energy supply. The new power system with smart grids will require more efficient operation of the grid system. DSM is a vital aspect of SG development.

DSM consists of programs that aim to change the electricity consumption pattern with the objective of reducing the electricity demand. DSM enables the customers to control their consumption of electricity. In DSM technique, we reduce the peak demand of the current system. This helps to prevent the new investments to increase the generation, transmission and distribution of electricity. The DSM technique can be deployed directly or indirectly. In direct one, customers' loads are controlled by the utility. There is a priority list set for different loads. The utility shuts down the loads when needed. The loads are connected via smart switches. The indirect method aims to change the consumer's electricity consumption pattern. The consumer reduces their energy costs by using more electricity at times of low rates and shift their time of use to off-peak hours. DSM technique if well applied contributes to energy efficient residential areas.

DSM addresses the key issue of peak demand. Peak demand causes the problem of power breakdowns. Instead of investing money to increase the generation capacity to meet peak demand, it is less expensive to address the issue of peak demand through modification of energy usage which will help save energy and increase the quality of service.

The six load management strategies used to remodel the load curve are shown in figure and explained below.

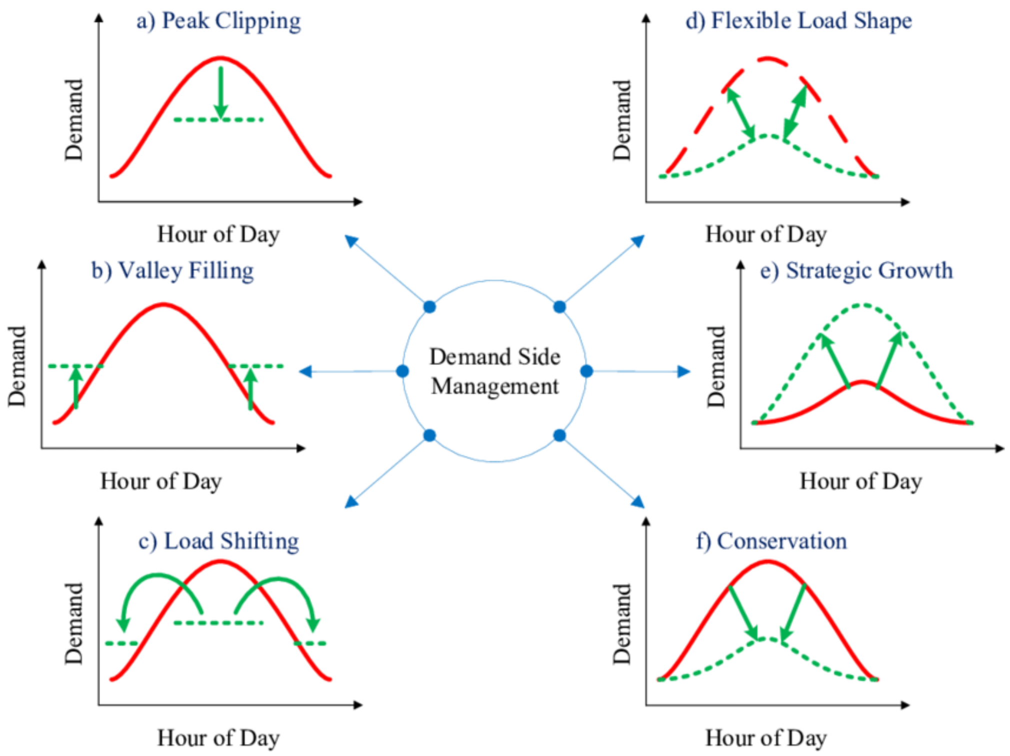

Figure 6 DSM Strategies

a) Peak Clipping: decrease in load in peak hours. It controls the load directly using direct load control. It is mostly suitable for industrial setups.

b) Valley Filling: in this we use heavy loads, i.e. heater, in off peak hours rather than during the peak hours. This improves the load factor.

c) Load Shifting: this focuses on shifting load to off peak hours from peak hours. This increases the peak to average ratio during off peak hours.

d) Strategic Growth: in this we add load to fill the valleys. As a result the overall load is also increased.

e) Flexible Load Shape: in this we give consumers some incentives to meet the reliability constraints.

f) Conversion: it is not even DSM method. It uses the smart energy efficient appliances. Like, photo sensitive control to turn off street lights. Therefore, this results in reduction of overall load.

DSM can help utility in maintaining the desired shape of load curve with minimum PAR and benefits users by supplying electricity at minimum cost. Deployment of DSM technique will promote sustainable development. The available generating capacity will be used more efficiently resulting in higher utilization in power grids rather than wasting resources to increase capacity of power system.

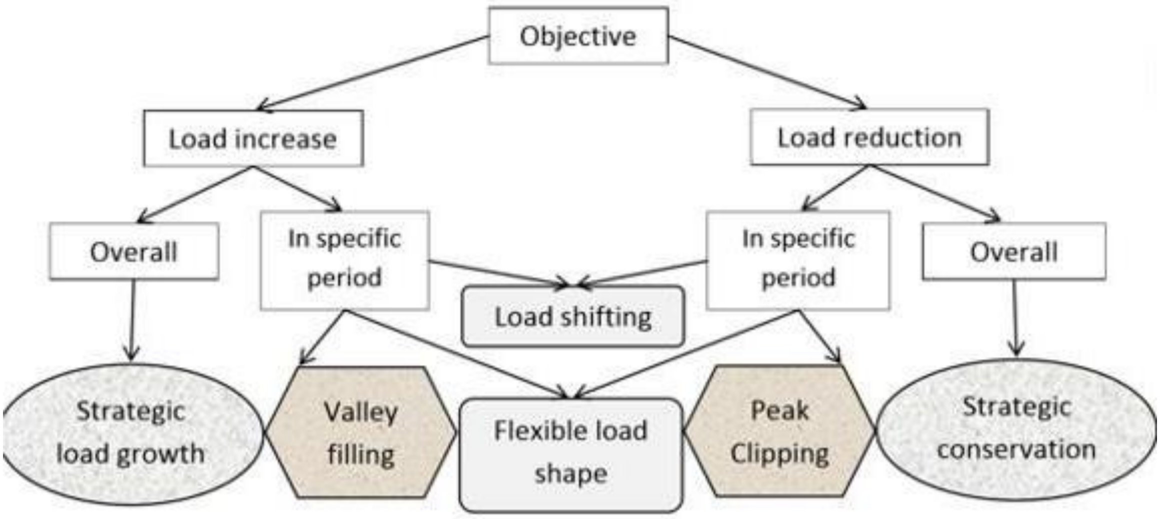

Figure 7 DSM Objectives

The use of DSM technique to reduce residential sector's electricity demand will prove to be successful. The biggest consumer of energy is the residential sector. DSM will help reduce household's electricity consumption. The consumers of electricity can decrease the energy cost by shifting loads to off peak hours.

2.5. Smart Home

Smart home is a building that consists of a system for managing and controlling renewable energy sources, house appliances and energy consumption using most often a wireless communication technology. ICT enables smart buildings to communicate both with its inside devices and appliances, which they can also control, and with its surroundings. Furthermore, they can adapt to grid's conditions and communicate with other buildings, hence creating active micro grid or virtual power plants.

As shown in figure below, in general the smart house consists of renewable energy source e.g. solar panels, energy storage, sensors, controllers, actuators, central unit, user interface, communication network and smart meter. These components automate the building and make a small renewable energy source.

The smart home comprises of two types of loads:

- Base loads: this kind of loads are mandatory to run regardless of time. These can't be shifted to later times of the day. These are usually comprise of fans and lights.
- Shiftable loads: They are defined as loads which are not time dependent. These can be shifted to different times of the day. Washing machine, water-tank motor and dishwasher are examples of non-essential loads.
- Adaptable loads: these loads can increase or decrease their energy usage. Such loads have to states i.e. these can be fixed or controllable. Which usually this depends on the time of the day.

Figure 8 Smart Home

2.6. HEMS (Home Energy Management Systems)

Also known as Home Energy Monitoring system. This usually consist of two main parts, hardware and software. This provides energy consumption monitoring, also rule and network based control of household appliances. For example an application can turn on or off at certain time based on rules added.

Hardware: it can be wired or wireless to monitor the energy consumption depending on the house.

Software: it collects the data and responsible for the communication through some user interface. Also, it allows user to control appliances using remote control or through rule based control which is based on scheduling and optimization.

2.6.1. Types of HEMS

The following are the different types of HEMS discussed in literature:

a) User Interface Products: it is user intensive as it requires a lot of user involvement.

b) Smart Hardware: it requires appliances which can receive, interpret and respond to signals received from controller. Example of few such appliances are smart appliances, smart thermostat, smart lighting, smart plugs and smart bulbs.

c) Software Platform: the software of the HEMS have to be really good. Because it decides how good a HEMS is. As people by smart appliances for different manufacturers so the communication with all software and hardware of the household appliances is a troublesome task.

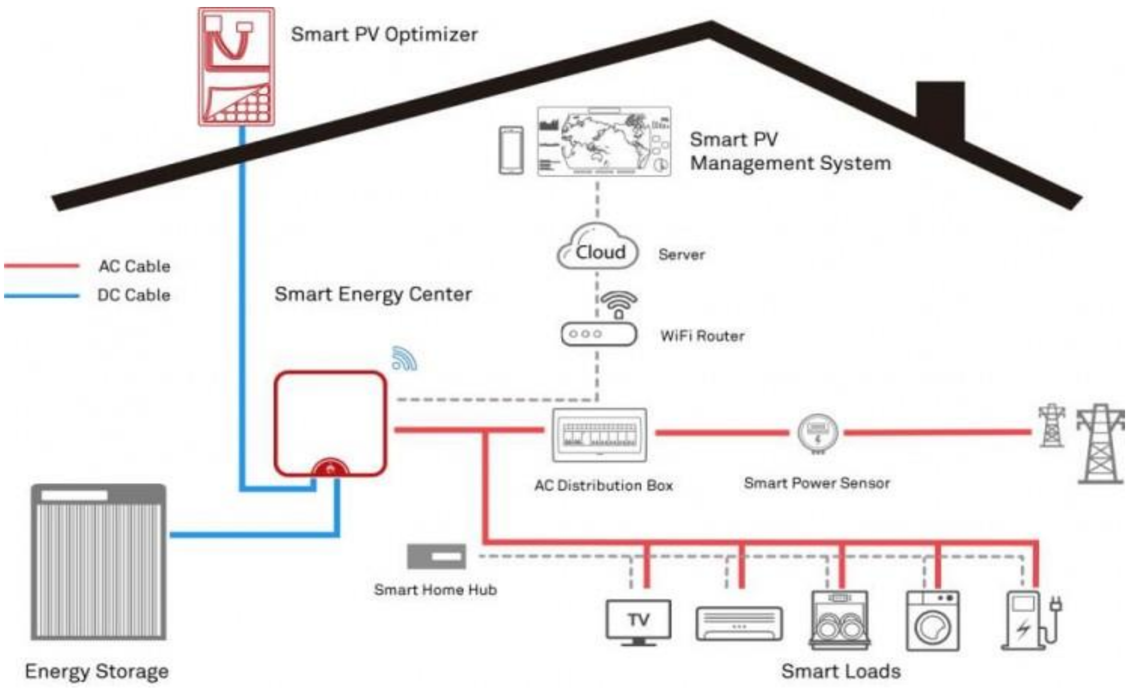

Figure 9 Home Energy Monitoring and Control System (Huawei)

2.6.2. Disadvantages of HEMS

The few disadvantages to of HEMS are given below:

i. These are expensive. As users have to install all the smart appliances.

ii. Most users don't use these to their full potential. As most users don't know full the potential and functionality of HEMS.

iii. Security is an issue. As the HEMS usually connects via some cloud and the internet.

iv. As HEMS are complicated and requires regular interaction from user. So, most users find it difficult to use and some even put the system away after using it few days and forget about the system.

Chapter 3

LITERATURE REVIEW

Chapter 3: Literature Review

This chapter presents research work conducted in the area of Energy Management System for Smart Grid. After a brief literature review of work conducted in this area we enlightened the research gaps that we found in previous works. The first sections of this chapter are based on revision articles about energy management techniques. In the last section some implementations of techniques is discussed.

3.1. Threat Model

A distributed algorithm is proposed in upcoming section 4.1 which helps in achieving a primary level of privacy. In proposed algorithm each participant calculates its own calculation for DSM. Thus, users do not have to share the load profiles means they have to exchange lesser information with the server. Nevertheless, there are always a few threats to the privacy. Some of the threats are discussed in the following section.

3.1.1. The Overview of Data

A brief overview of data to be transmitted, will helps us to understand the privacy threads. The data required by the proposed algorithm has three core parts. The table 1 shows the data in detail. The data is shared inform of a token. Firstly, the token has list of members which are taking part in algorithm. This list has the addresses of the participants in chronological order in which they were connected. The participants which receive the token, remove the first entry from the list which is the address of their successor to send the token. In this way, the data size in reduced at every step. The size of second part of token be determined by the number of rounds.

In the first round of the algorithm, all the participants are ask to compute their future energy consumption. In this, this participants produce their load profiles after performing the load shifting. This forecast has a certain time interval like one day profile in form of minute interval. Additionally, for the load adaption our algorithm needs overall consumption at present time. In the consumption list the first entry is the overall energy consumption at present time. The load shifting is required only one round and done in the first round. After this, the potential share of energy and deficit is required. This information is needed for the load adaption. The potential share and deficit can be negative or positive, so it needs single number. When it is negative, it means too much energy feeding from the grid. Similarly, when it is positive it mean too much energy consumption by the participant.

The third and last part of the token data is a list of members which are still adaptable. It is empty at the beginning of the first round and if a participant is still adaptable for the upcoming round then it puts its address in it.

Table 1 Token Data Overview

No. of Round(s)	Name	Details
all	Adaptable participants	List of participants which are still adaptable.
1	Future Energy Consumption	The future load profile of the participant.
2+	Potential Share	The share required by all the participants of the round.
2+	Potential Deficit	The deficit which needs to be handled.
all	Participants	List of participants.

3.1.2. Eavesdropping Attack

The first attack to discuss is the eavesdropping. It is shown in figure 9. This attack can be carried out in two different ways and both have different level of threat.

The first way is, the sniffing message of a participant. In this, the attacker can sniff the messages of particular participant travelling through the network. The attacker can exploit different private data. Firstly, the attacker can make a list of participants by recording the addresses of the all the participants in the network. Secondly, by comparing the inbound and outbound consumption lists, an attacker can get the load profiles of the participants. Similarly, the load profile of the predecessor can be made. For this, the attacker has to simply compare the previous and current states to get the load profile of the predecessor. This enable the attacker to know that when a certain device is activated by the load curve. Thirdly, with the list of adaptable participants, it can be easily be determined if a participant has any adaptable appliance or not. All the successors knows if their predecessor is adaptable or not. With little bit more information any radical attack is possible. If somehow the attacker knows that some participant has only one adaptable appliance for example Electric Vehicle (EV). The presence of EV can be decided by the adaptable state of the participant. This can leads to some dangerous circumstances e.g. a break-in. Moreover, the attacker can access the current share and remaining deficit.

The second way of this attack is, sniffing the messages of the whole network. In this, the attacker can sniff all the messages of all the participants in the network. This makes the stated attacks significantly easier. Firstly, the list of participants is known only after first round as the path of token can be traced by the attacker. Secondly, the list of shiftable loads is available to attacker at any time as future consumption states are accessible. Also, all the previously stated attacks are possible.

3.1.3. Threat Actor

Another attack can be a malicious threat actor. In this, the hacker is an authorized registered participant. The hacker acts as a secret agent with an intension to spy on the participants. This hacker has all the threats of attacker who can sniff the inbound and outbound messages of a specific user in a network. It means hacker has the access to load profile of the participant e.g. adaptable and shiftable loads.

This attack is also known as spoofing attack, in which a hacker imposes as a legal participant. Moreover, a threat actor not only can sniff the information in network but also can alter the information. Nevertheless, it’s not the motivation of this thesis.

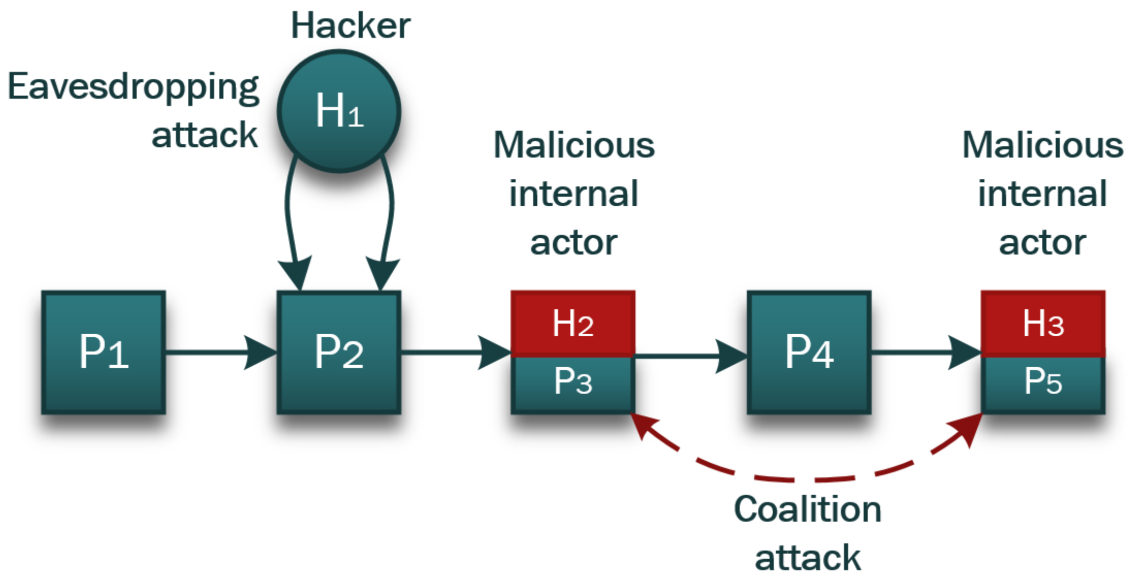

Figure 10 Privacy Attacks

3.1.4. Coalition Attack

The hackers can make a coalition in order to reduce the complexity of the attack. With this coalition the hackers can get the load profiles more easily. A hacker can be a threat actor or can be a spoofing attacker who sniff the data. If predecessor and successor of any participant are two hackers then they can get the load profiles very easily by comparing the states of the load profiles. Likewise, a bigger coalitions can be done.

3.2. Literature Review

In smart grid, Demand Side Management (DSM) plays an important role in energy management. It supports SG functionalities in many areas such as electricity market, distributed energy sources, utility grid stability and management of whole infrastructure.

The privacy is one of the essential point of energy management in SG. The information of the behaviors of participants both producers and customers is required for the efficient DSM. The more information mean the more improved results of energy management. On the other hand, this causes the clash with privacy. If we want to use more data then we have to take some countermeasures to ensure the privacy of the participants. Some latest studies show that a central nonintrusive system can be used to monitor operating schedules.

The multimedia content like TV can be monitored if the data measurement interval is in seconds. This can be a privacy concern and a barrier in acceptance of SG by users. A decentralized/distributed system can results in some privacy problems. As, not only the data is in a decartelized place but also the participants have access to it. Thus, the privacy of the participants has to be taken care of if we want to use the distributed algorithm.

There are solutions available manage homes individually. Some of the existing techniques are described in detail.

A knapsack based algorithm has to parts for the management of household appliances. First part is priority management algorithm. It manages the household appliances on the basis of priority. The second part is an optimization algorithm named branch and bound. It promise to find the best possible solution set from a solution set.

Distributed Algorithm based on Game Theory [1]. This algorithm uses peak to average ratio (PAR) which minimize the peak and consumer energy demand. It has two main parts. First is players which are consumers and other is strategies which are different daily load schedules. This algorithm achieve the Nash Equilibrium, a solution for non-cooperative games.

Vickrey Clarke Groves (VCG) [2]. It is based on sealed bid auction of multiple items. In this participants are unaware of the other participant's strategies. Total energy cost imposed on utility company from the aggregate consumer utility function. This algorithm maximize the social welfare by a utility function VCG.

Real time energy consumption, it is based on a renowned scheduling algorithm [3]. It takes account 'load uncertainties' and minimize the consumption payments. It uses the dynamic programming approach to reduce the complexity of the problem. Unlike, other DSM techniques which require a proper load profile, it can do the same with some estimates of future demand.

This algorithm based on Real Time Pricing (RTP). It reduces Peak to Average Ratio (PAR). This shift the household appliances from peak hours to off peak hours. The global optimization is divided into 2 processes:

a) Demand side: customers try to maximize the payoff according to prices. This process is achieved either by closed form or by an algorithm.

b) Supply side: the utility company does the real time pricing using consumers' behavior to forecast the future loads. Also, this uses the simulated annealing based price control (SAPC) algorithm.

Another algorithm based on Game Theory [4]. It uses the 2 game theory techniques, a) Non cooperative game between different participating consumers and b) Stackelberg game between different utility companies. It uses a convex log function to sell energy back to grid. Consumers have direct access to energy storage devices.

This algorithm is also based on Game theory [5]. In this, researcher mapped consumption problem to Mixed Integer Programming (MIP) and optimized consumer objective function. Also, they have integrated RES to lower the energy demand.

Home Energy Management System (HEMS) [6]. Aka Home Energy Monitoring System. It has 2 main parts a) hardware and b) software. It manages the home appliances. It can turn on or off appliances according to consumer given schedule or on the basis of load peaks. Its disadvantages are: it is very expensive, very complicated to use and requires periodic interaction of user, most users don't use it to its full potential and security is also an issue as it is connected to cloud.

This author implemented scheduling algorithm using Approximate Dynamic Programming. Along with managing the energy from different Renewable Energy Resources (RES), this algorithm allows you to utilizing and sell back electric energy from your RES to smart grid.

In author proposed a scheduling algorithm with integration of renewable energy resources. This algorithm predicts the consumer's consumption one day ahead, in order to reduce the peak demand to smart grid. This algorithm tries to maximize the utility of all renewable energy resources in the house. Also, this optimize the demand and storage utilization alongside of Real Time Pricing (RTP).

In this the research suggest real time pricing. While other available RTP algorithms ignore the uncertainties of electric grid. This algorithm accounts the uncertainties of the grid. Also, it calculates the real time prices for the consumers of the smart grid. This helps the grid to reduce the peak hour load by increasing the prices.

In author proposed an energy management method and tried to mitigate the voltage floatation problem which is a huge problem in increase of the loads. Also, this incorporated the Photo Voltaic (PV) system in the overall system.

In the researchers proposed a methodology based on the Demand Response Exchange (DRX). In this they used a bidding system to done the trade between the participants of the system.

There are many researches available on this topic and list goes on. Lastly, I want to mention is the []. In this researcher proposed a cloud based two-tier architecture for the demand side management. In this they consider that a micro grid has multiple regions. A separate edge system for each region which calculate the optimal usage timings (schedules) for all the household appliances of that region. Like all other mentioned techniques in the above, this also requires a direct access to the household appliances to control them.

3.3. Research Gap

Already carried out researches have done the demand side management using different techniques based on different parameters. But, all of these total ignored the privacy of system consumers. Also, these systems require a direct access to household appliances. To work properly an energy management system need the accurate and real time data of consumers load profile. Thus, the consumers have to share way more information with the systems.

The above mentioned research papers have one thing in common. Either these have completely ignored the privacy of users or only focus on communication security of the SG. In this thesis, we have proposed an algorithm which is distributed and privacy friendly for the energy management in SG. It does the load adaption and load shifting. The communication security is consist of availability, confidentiality and integrity. This thesis emphases on privacy of user data while proposing an energy management algorithm.

As, these already carried out researches have done the demand side management using different techniques but the totally ignored the privacy of the consumers. As these techniques requires direct access to the home appliance. Also, consumers share more information to these algorithms than our algorithm requires. Consumers share way more information than they should which results in security and privacy issues. Even the distributed algorithms are not robust to link failures.

There are methods already available for energy management but they completely ignore the consumer privacy and requires a direct access to the household appliances. We want to ensure the privacy of the consumers and avoid the direct access or control of the household appliances. Rather than managing a single home we are trying to manage a small street with few houses.

Chapter 4

PROPOSED ALGORITHM

Chapter 4: Proposed Algorithm

This chapter contains details of the proposed algorithm. Section 4.1 discusses the proposed algorithm, Section 4.2 talks over the proposed algorithm and Section 4.3 provides detailed proposed solution.

4.1. Proposed Algorithm

In this section, we have proposed a distributed algorithm for energy management in SG. This proposed algorithm tries to lessen the variations in the energy demand of the SG with the help of DSM. The participant of the algorithm must be a smart home having smart appliances. The participant must also has to approve the server to control its appliances at street level. A distributed environment is show in figure 11. The server is at the level of local power transformer and different homes connected to the transformer are shown in the figure.

There are two types of homes in our scenario i.e. conventional home and smart home. The conventional home is home with no smart appliances or does not want to be a part of the energy management. While the smart home is home having the smart appliances and wants to be a part of the energy management in smart grid. The conventional home cannot communicate with our server and it is only consider to get the load profile. While, the smart homes can communicate with the server. For the communication, every smart home and server have an interface which mean no direct access of the smart appliances from the server.

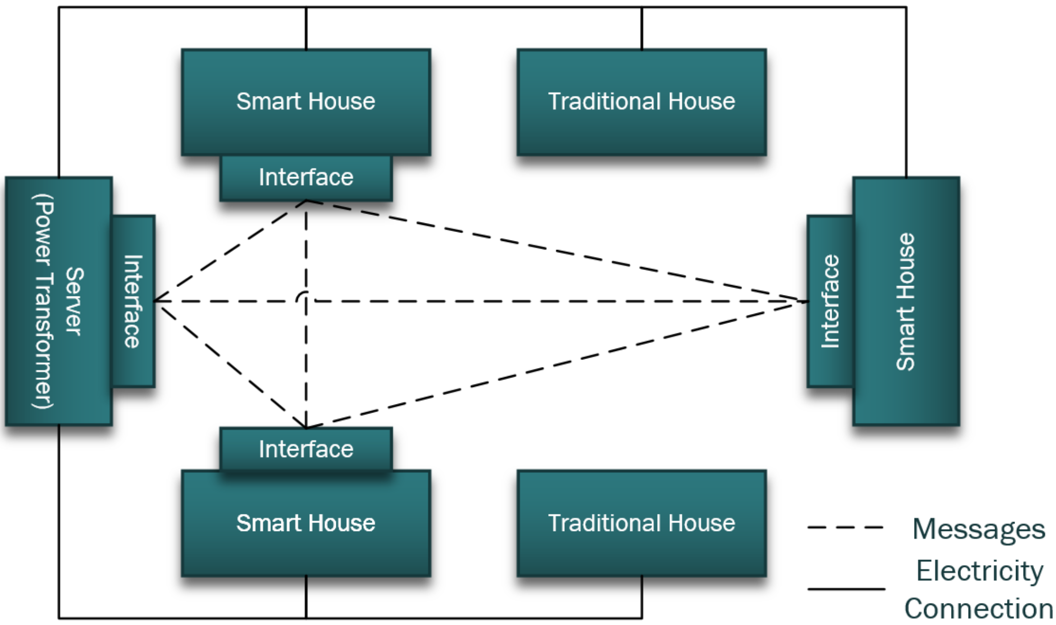

Figure 11 Distributed architecture proposed algorithm

4.2. Management of Energy

There are different types of loads in the SG. We have identified three types of different loads. The first type is base loads. When they are activated they have to be served without any condition such load are television, lights etc. The second type loads are time shiftable loads. Such load can be run in the later times. When such loads are activated and a point in time is defined before which these have to run and complete the task. The third type of loads are adaptable loads. Such loads can adapt their energy demand while running up to some amount.

The structural design of energy manager of our algorithm is shown in figure 12. It shows that the different types of distributed scheduling algorithms are used for different types of the energy loads. Here the load of the conventional houses and base loads of the smart homes is total base load. Also, we need the expected future energy consumption to shift the shiftable load to later periods of time. This can be predicted using load profiles and weather data.

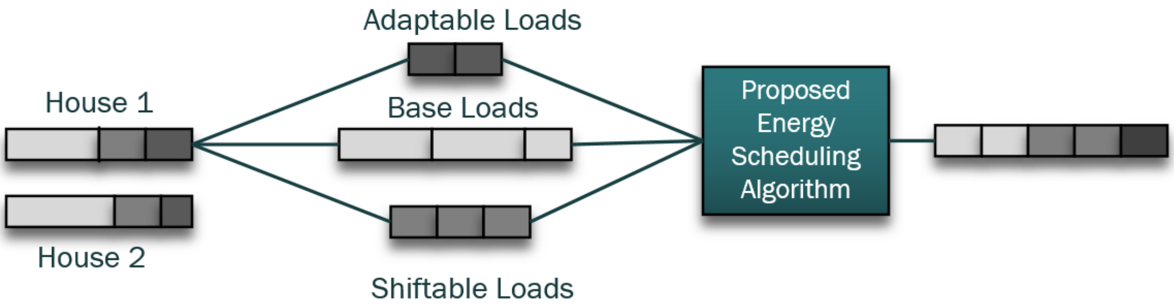

Figure 12 Architecture of Energy Scheduler

4.2.1. Load Shifting Algorithm

This algorithm handles the shiftable loads like tumbler dried, dishwasher or washing machine. To understand this algorithm, let us consider a scenario in which a washing machine is filled with the cloths and activated at 9:00 a.m. We need to define a finish point in time like 6:00 p.m. when we need cloths and before which the washing machine has to complete its job. The scheduling algorithm computes the optimal operating time for the washing machine based on their deadlines. With this shifting of activation of the shiftable loads the algorithm tries to avoid the load peaks and to smooth whole energy consumption.

When many shiftable appliances needs handled at particular time the algorithm uses the FIFO (First In First Out) scheduling principle to calculate the activation times of the shiftable appliances. To sanction easy adaptation and to find the optimal activation time we introduced a cost function. The following equation 1 shows the *cost*(*t*). A load barrier *b* is defined. The total consumption of should not be exceed the load barrier at any given time. The algorithm observes the load barrier as closely as possible. The expected future energy consumption *e(t)* and load of an appliance *l(t)* is added together the by the cost function. If it exceeds the load barrier then surplus value is penalized by *f* factor. For every potential activation time, the algorithm computes the cost function. Then it select the activation time which has the least cost value. In the end, to make the appliance to be measured in the future energy consumption, the load profile of the appliance is added to future load profile.

Calculating the optimal activation times for d appliances and potential s minutes becomes an exponential problem i.e. (s^d). Which is not practical as the appliances increases. So, we used the FIFO, which reduce the computation dramatically to just $(s * d)$.

$$c_t = e(t) + l(t) \qquad (1)$$

$$c_t = \begin{cases} b + (c_t - b) * f, & c_t > b \\ c_t, & c_t \leq b \end{cases} \qquad (2)$$

$$n = s^d \qquad (3)$$

$$\frac{s^d}{v} = t \Rightarrow d = \log_s(t * v) \qquad (4)$$

4.2.2. Load Adaption Algorithm

This algorithm manages the adaptable loads of the smart homes in smart grid during the computation. This algorithm has the goal to reduce the peak load deficit which occurs due to operation of multiple appliances at the same time. For example an EV is being charged, it can stop or reduce the charging so that the total energy consumption can be reduced and the consumption can adhere to the load barrier. It aids power grid to attain steadiness. Moreover, just like the positive load barrier, a negative load barrier adhere to the system. To understand the negative deficit, we consider a photovoltaic (PV) system which is integrated with the smart grid. On a sunny day, the PV system produces too much energy and it results in negative load deficit. To handle this negative load deficit we can activate multiple appliances at the same time to utilize the maximum energy.

The algorithm uses a principle known as max min fairness. This distribute the adaptable share fairly between the adaptable appliance thus decrease the overfeeding or overconsumption of energy. In the beginning, the algorithm handles the uncontrollable base loads. Using load curves or by some other method we need to consider the load of unconnected conventional houses. As their load is also considered as base load. It helps us to compute the remaining energy capacity.

The algorithm fairly distributes the remaining energy between all adaptable appliances. Thereby, we used max min fairness principle. It ensures the fairness in the adaptable share of the appliances. It divides the residual energy such that every participants be given the energy share at most. For example, the algorithm has *n* adaptable loads and they need energy resources as following r_1, r_2, r_3 ... r_n. The total remaining available energy capacity is *C*. This algorithm is based on cycles. In initial round, the *n* appliances gets a cut of *C/n* each. Then, if the cut is bigger than the remaining capacity of the first appliance, it gets the remaining cut of $C / n – r_1$, with this first appliance is completely served. Similarly, in next round, the cut will be $C / n + (C / n - r_1) / (n - 1)$ and each appliance gets the mentioned cut. The algorithm carry on till every appliance is completely served or till there is no remaining energy deficit to be handled.

4.3. Client Server Methodology

The figure shows a client server methodology in which all participants have smart meters. In this approach, the participants have to notify the server each and every time if any shiftable load is activated. The load profile of shiftable appliance and the deadline have to be sent to server by the participant. Then the server carryout the load shifting and finds the ideal activation time. After this, the server sends back the activation time of shiftable appliance to the participants.

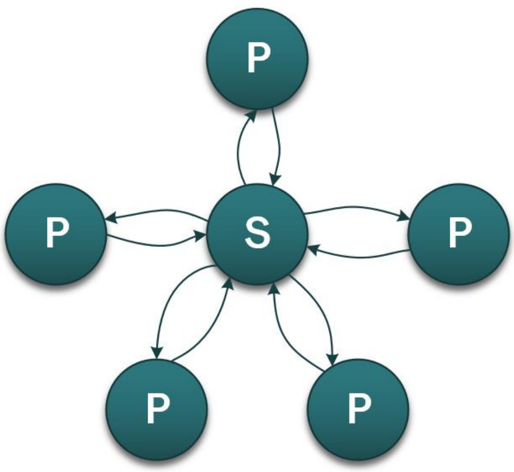

Figure 13 Client Server Architecture

The adaption of load is done in intervals. Firstly, the participants have to send their adaption potential and their load curve to the server. The server then computes the best possible cuts of remaining energy for each participant and send it back to participants.

In client server methodology, all the calculations are done the sever side thus all the data which is required by server to done the calculations need to be send by the participants. This certainly affects its user acceptance. For that reason we proposed a distributed approach in the subsequent section. Although, we can enhance the client server architecture. Such as the load profiles of the appliances can be generalized and used so that there is no need to be communicated. But, it has adverse impact on the DSM and also negative impact on the user privacy. This is not part of the thesis and is not discussed.

4.5. Distributed Methodology

The main reason to use the distributed methodology is to ensure the privacy of participants. As, all the necessary calculations are conducted on the participant side. Therefore, no need to share the load profiles of the server. The proposed algorithm uses a token which is used for the communication in the network. It associates the both load adaption and load shifting. The server generates the token and it has the list of participants. It makes a virtual ring using the provided information. The figure 14 shows the virtual ring.

The first round starts when the server sends the token to the first participant in the list. This round generates, an empty list of adaptable appliances and estimated future consumptions. The participants do their own calculations. For example, with the help of load shifting participants calculates the best activation time shiftable appliances and add the load profiles of appliances to future consumption.

Additionally, each participant in the list adds the required share and also it tells if it is still adaptable or not. If yes, then it needs to specify either positively or negatively adaptable. With every step passing, every participant which receives the token, removes itself from the list of participants. When the first round is completed, the last participant calculates the energy deficit based on loads required by the participants and if needed a new round can be started. In the upcoming rounds, the adaptable loads need to be handled. Thus, we can skip the participants which are no longer adaptable. The last participant completes the process by sending back the token to the server. In some cases, there are some participants left which are still adaptable. They are informed that the algorithm is finished. The server sent an alert message to all these participant in parallel which helps to avoid the additional rounds.

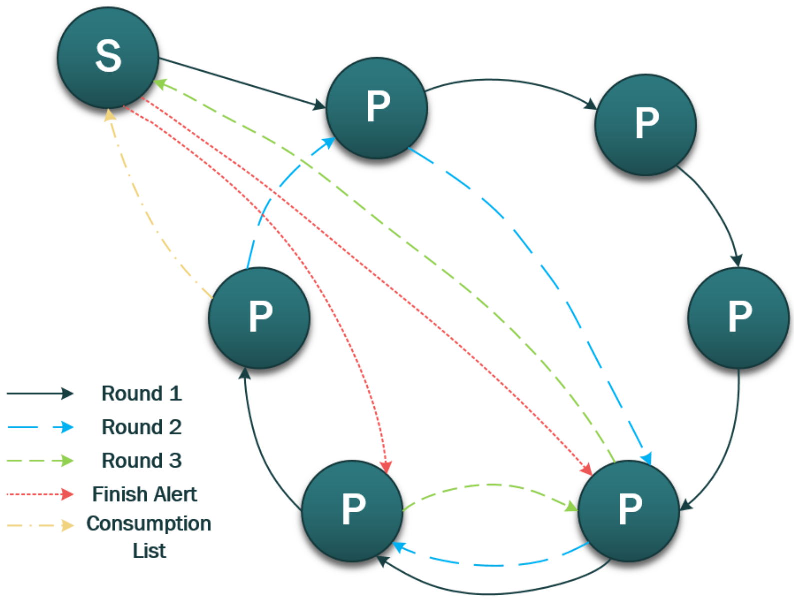

Figure 14 Distributed architecture and virtual rings

4.6. Encrypted Distributed Methodology

In this section, we explain how the privacy and secure communication are critical for the distributed algorithm. In this algorithm we use a number of methods to further ensure the privacy of the user. With data overhead, we need to secure and reduce the size of data so it cannot be accessed by the other participants. Moreover, different privacy measures to algorithm are also incorporated.

4.6.1. Hardware Model

The proposed energy management algorithm will be a black box. The black box has the sealed hardware with very few communication links to outside. With this the hardware is not accessible. We call this the energy manager. This energy manager require two types of communication links. First is in-house communication, which enables the energy manager to control the smart appliances or controllable appliances of the smart home. Similarly, the energy manager requires the communication linkage with server and other participants. As the smart meter has a communication linkage thus the energy manager can be integrated with it.

4.6.2. Cryptographic model

For encryption of the data, we used a PKI (Public Key Infrastructure). In this system, every participant has its own digital key. With the help of encryption system, the network communication of the whole network is encrypted and digitally signed by each participant.

Nevertheless, lot of computational power is required for such asymmetric encryption so it is not suitable to use for some real time scenarios i.e. SG. Thereby, we used a hybrid methodology of both types symmetric and asymmetric. In which, the keys are exchanged with the asymmetric encryption and data is encrypted with the symmetric encryption. Nevertheless, the $n(n-1)/2$ keys need to be exchanged by the n participants. So that, every participant can store the corresponding keys.

This exchange of keys should be done in earlier phase of the algorithm so that is does not affect the algorithm at all. With is data encryption, the data is secured and only be accessible by the intended recipient and sender itself. However, the malicious internal actor attack is still possible as it only make the data inaccessible to third parties. A malicious internal actor still can have access to the data.

4.6.3. Structure of Token

In this section, we explain the structure of the extended token. This token is based on the bucket principle. In which there is a dedicated space for each participant. Only the intended participant has access of the space i.e. a key is required to decrypt the data. To communicate with the server the participants have to use the dedicated space. The figure 15 depicts the described bucket principle.

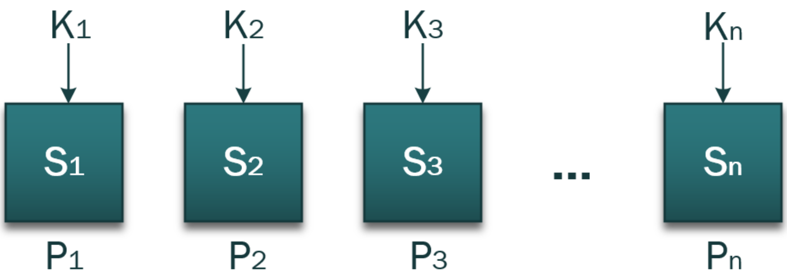

Figure 15 Bucket Principle

Let's assume we have a function for the encryption $E_{(k,m)} = C$. Here C is cipher text which is computed by encryption function. The function uses the key k to encrypt the plain text m. Every participant i exchange the k_i key with the server. As the keys need to be exchanged with each participant and server. The keys are exchanged using Diffie Hellman key exchange in beginning of the algorithm. The server uses these keys to store the address of the successor s_i in the intended space in the bucket of the participant i. This address is encrypted before adding it to bucket using some renowned encryption techniques like OFB mode or AES with CTR. Moreover, in every round the server randomly permute the list of the participants. The earlier list including the server and the participants $\{S, P_0, P_1 \ldots P_n,\}$

has become $\{E_{(k0, s0)}, E_{(k1, s1)} \dots E_{(kn, sn)}\}$. When the participant i receives the token, it decrypt its data from the bucket using key k_i and gets the address of its successor without knowing the further list of participants.

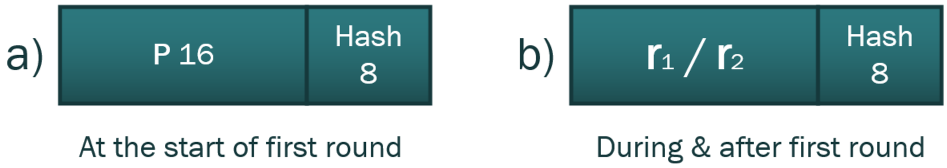

Figure 16 Bucket Content before and after first round

The participants use the bucket principle for both to store and receive data. Each participant add values to its own counter for adaption C_{up} and C_{down} depending on its potential of adaption p_i. A random value r_{0i}, generated by the participant, is added to adaption potential value to make it untraceable. The value is as following $C_{\text{up}} = r_{10} + p_0 + r_{11} + p_1 \dots r_{1n} + p_n$. As, the server requires the exact number of the adaptable participants to carry out the energy management. Thus, a random value r_{1i}, which is added to adaption potential of participant i, is stored in the allocated bucket space. To get the number of adaptable participants the server needs to decrypt and deduct the random values stored in the bucket spaces. From the second round and on, we can use this mechanism to securely store the deficit value. The value of deficit is substituted by the share S and the counter C_A. The adaption value a_i of an adaptable participant with the second random r_{2i} value is added to counter such that $C_A = r_{20} + a_0 + r_{21} + a_1 \dots r_{2n} + a_n$. The algorithm store this random value r_{2i} in the intended space of the bucket with the previous random value r_{1i} such that $(b_i = \{r_{2i}, r_{1i}\})$. From second round, this helps us to attain a high level of the privacy. Because of this the algorithm needs to exchange a lot of messages. The algorithm cannot get the list of adaptable participants if all participants add random values in the deficit counter.

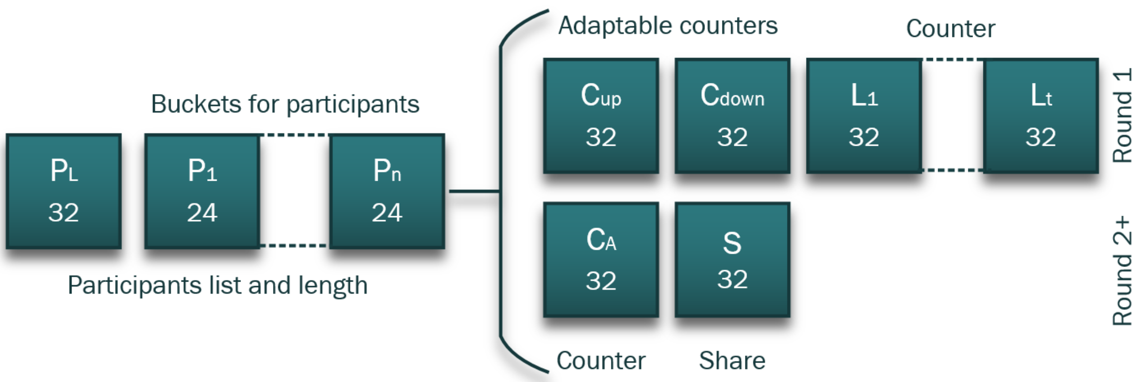

Figure 17 Encrypted data packet

All the privacy measures which are introduced for the better privacy is syndicated by this extended token. As required by the algorithm every participants has a unique identifier. The list having the address of the participants is circulated in the beginning. The data packet contains buckets, size of the participants list and a list of participants. In the first round, token has a list having the future loads and pointers for participants which are adaptable for upcoming round. On or after the second round, we need to keep track of the required current share and load adaption.

Chapter 5

RESULTS & DISCUSSION

Chapter 5: Results and Discussion

For our algorithm we simulated a town environment that has one street with 4 houses having 25 to 30 households. The base load of the houses (e.g. stove, lighting, entertainment devices, etc.) that is not controllable by the algorithm has been simulated beforehand and is available in form of base load curves, as defined in [12]. The figure 5 shows an average base load curve of all appliances in a house. All devices that are handled by the algorithm are not included, thus reducing the overall consumption. These devices are shown in Table 1. Shiftable devices (washing machine, tumble drier, dishwasher) are simulated by probability curves [12] which depict activation probabilities during the day whereas photovoltaic devices are defined by a generation curve. For electric vehicles different scenarios can be considered. In the main scenario, the EV is not at home in office time and it will be charge during the night.

5.1. Simulation Results

A period of 40 hours is simulated starting from 12 a.m. to 4 p.m. the next day. Results are shown from 8 a.m. to 8 a.m. next day. Figure 18 shows the average consumption of the 100 households compared by different optimization levels. Without any optimization, which represents conventional homes, the consumption follows the base load curve during the day. The overall consumption is slightly reduced during this time because the photovoltaic systems feed into the grid and balance a part of the loads. In the evening and night the consumption is clearly increased which is caused by the electric vehicles. Starting at 5 p.m. vehicles arrive at home after work and get charged during the night. If we consider a smart home optimization where every smart home optimizes its own consumption locally and intends to reduce its individual costs the problem of simultaneity is clearly visible (blue line): All shiftable loads are shifted into the night time because of lower energy prices. This produces the load peak between 4 a.m. and 5 a.m. where all washing machines, etc. are running.

The smart grid optimization shows the effects of the distributed algorithm. An average load limit of 600 watts per participant is defined and not violated at any time. This is accomplished by load shifting and adaption as shown in Figure 18. The shiftable loads are mostly moved into the night. Some of the shiftable loads have deadlines during the day so that they usually run in the afternoon. The consumption of adaptable loads is reduced during the evening resulting in electric vehicles reducing their charging rate and extending their charging procedure thus operating within limits. Through this load shifting and adaption the consumption is distributed over the whole day including night times. This clearly results in a more balanced overall consumption while avoiding load peaks.

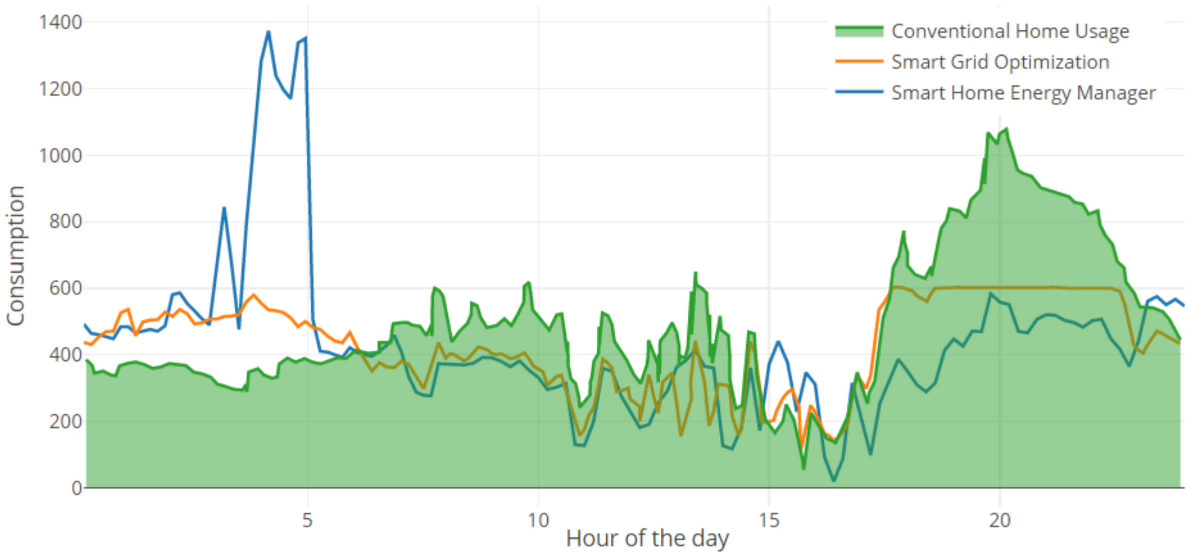

Figure 18 Simulation results of distributed energy management

5.2. Run time

The run time of the algorithm simultaneity is mainly affected by the round based token principle, as shown in Figure 4. In the best case the algorithm only requires one round where no error occurs that needs to be corrected in following rounds. After the first round the server is contacted and it alerts all still adaptable participants in parallel which counts for two additional messages. This results in a best case of $p + 1$ messages with p participants. In the worst case, shown in formula 9, a capacity limit has been violated, thus some extra rounds are required to reduce error in which respectively only one participant is not adaptable any more. This means that p extra rounds are needed to complete the algorithm.

Since the simulation is based on a minute clock, a computation window of 30 seconds is defined for the algorithm. In addition a transmission time of 100 milliseconds is supposed for a message which results in a maximum of 300 messages that can be sent in the computation window. This implies that 23 participants can be handled by the algorithm according to the theoretical worst case. The simulation results in Figure 19 show that the worst case scenario (quadratic dependence) is not reached because more adaptable devices offer a more flexible optimization and adaption to a specified load limit. Figure 20 depicts that the number of rounds does not exceed three even for 500 participants.

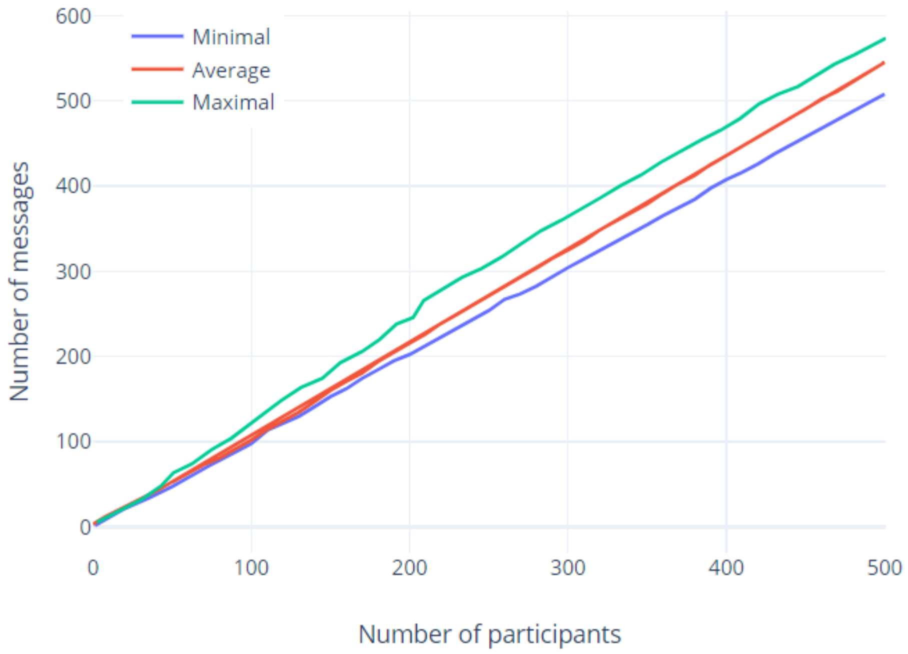

Figure 19 Number of messages

This also results in a linear increasing amount of messages as shown in Figure 19 so that 246 participants can be handled in a 30 second time frame. With this amount of participants the goal is met to perform an energy management on a street level.

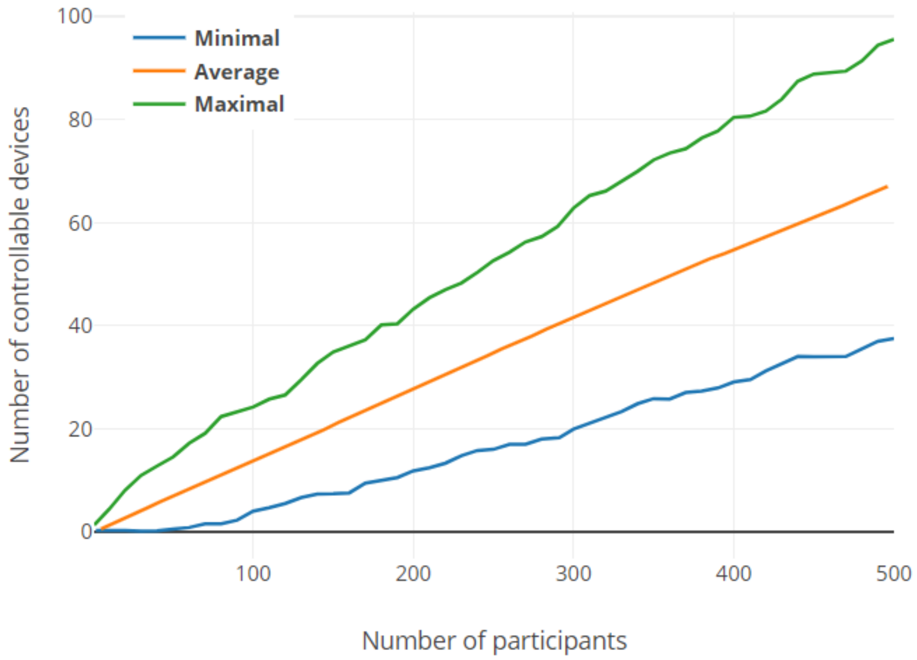

Figure 20 Number of devices

5.3. Simultaneity

One goal of the algorithm is to eliminate the negative effects that are produced by multiple smart homes which solely optimize their own consumption and thus take the same decision based on e.g. a price signal. Figure 21 shows the impact with 40 self-optimizing smart homes in a street of 100 households which produce negative peaks during the day (photovoltaic feed-in) and positive peaks during night (charging of electric vehicles, etc.). If half of the smart homes are controlled by the distributed algorithm the overall load can be smoothened and distributed over the day resulting in a more balanced load curve without any peaks.

However it should be noted that the 20 smart homes that are controlled by the algorithm have to counteract all other smart homes which means that they may have to e.g. reduce their consumption drastically. Thus an incentive model has to be used so that the participants do not have any disadvantages.

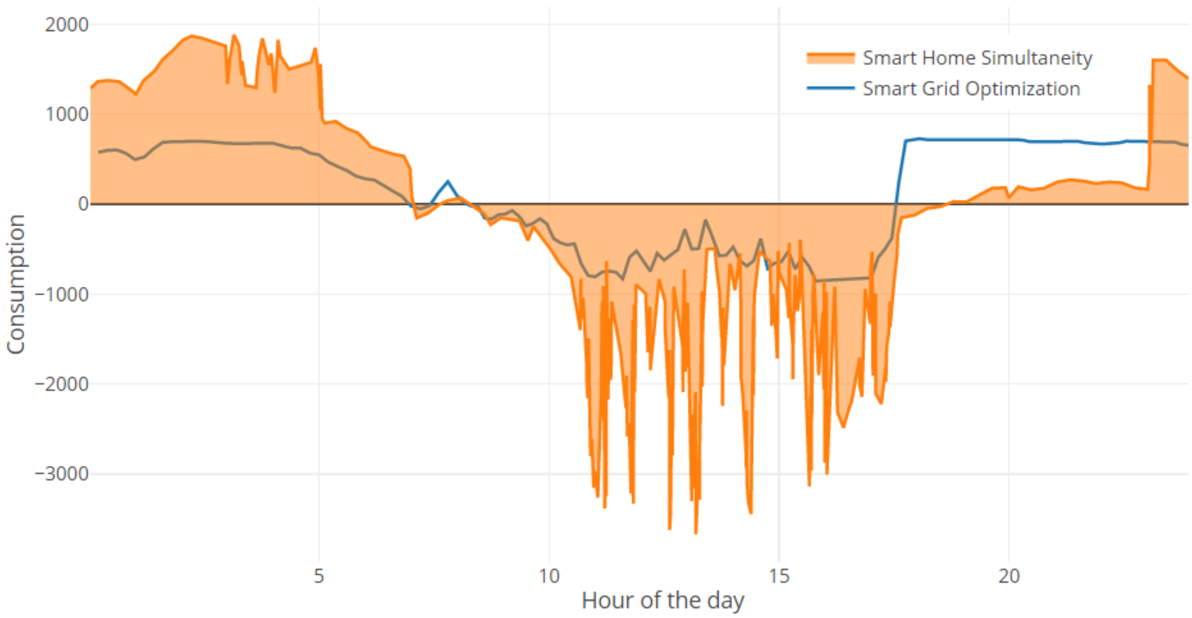

Figure 21 Impact of share of smart homes controlled by the distributed algorithm

5.4. Energy Management Interval

As stated before the simulation is based on a minute interval which means that the algorithm distributes capacities for the next minute. Figure 23 shows the consumption between 7 p.m. and 10 p.m. with a load limit of 500 W. With the one minute interval an average deviation of 0.36% with a maximum of 1.17% (505.85 W) can be reached whereas a 15 minute interval has an average deviation of 5.97% with a maximum of 32.80% (664 W).

The deviation is due to the fact that a smart home may not be able to react to a newly activated device because of a lack of adaptable devices during the interval. Furthermore devices are only adaptable in certain levels which causes the minor deviation in the one minute interval.

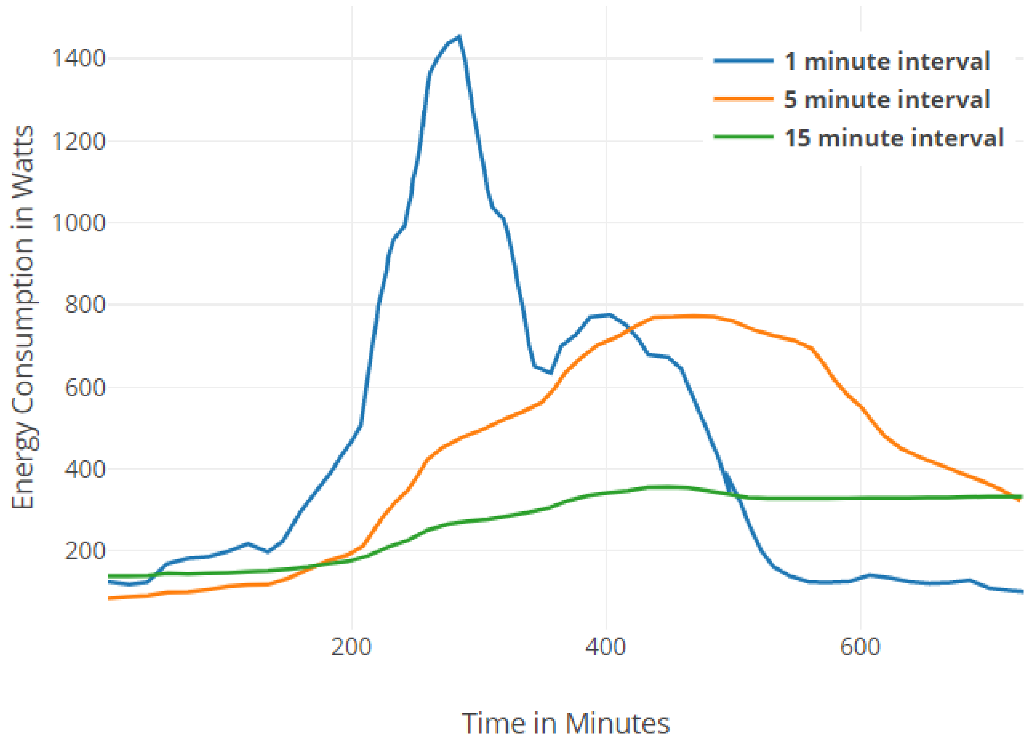

Figure 22 Impact of energy management interval

Accordingly the simulation results show that energy management interval should not go above the five minutes to guarantee an average deviation of 3.4%.

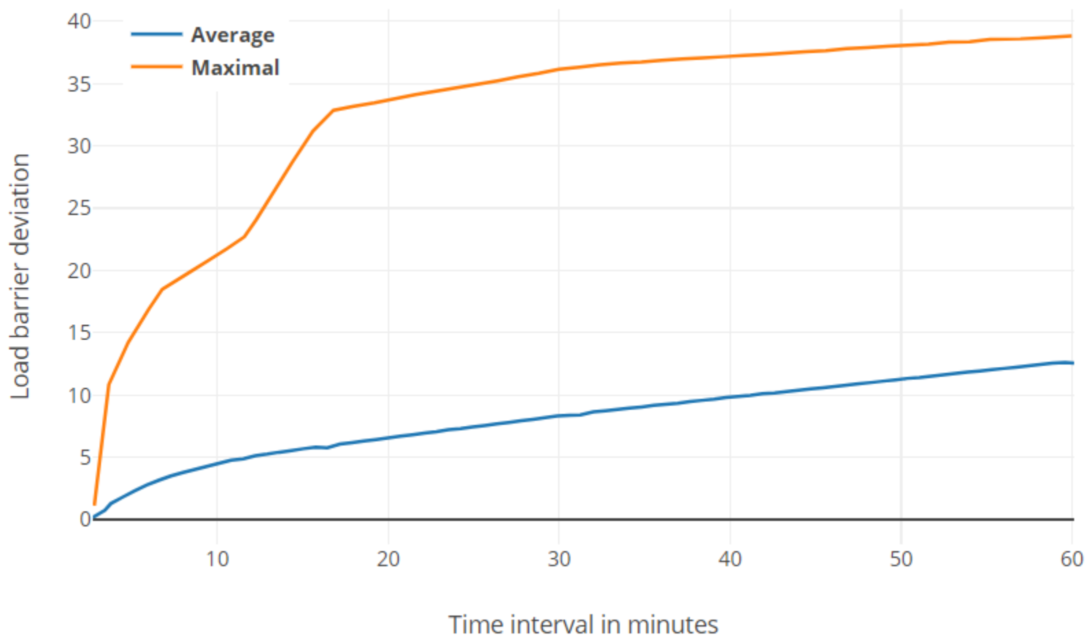

Figure 23 Deviation from load limit for different energy management.

5.5. Security Analysis

We have considered the six key measures brought together to guarantee the privacy of participants. Measures are shown in figure 24. To prevent external access on basic level to our system, we suggest to in cooperate the hardware with smart meter or we can use a black box means sealed hardware. As we have suggested an algorithm based on distributed design principle, we are doing most of the calculations on the participants' side. It means the participants only have to share the control messages with other participants in the network. With the help of pseudonymization, the addresses of the households for the communication can be anonymized. It means with a specific appliance does not has a specific address. The third party access can be prevent by encrypting the all communication data. The data which is shared can be anonymized with aggregation. The shared data refers to the aggregated future consumption of all the participants. Moreover, to protect from inside attacks we used the bucket principle. The token using to send data between participants and the server is also encrypted which makes the coalitions very complicated.

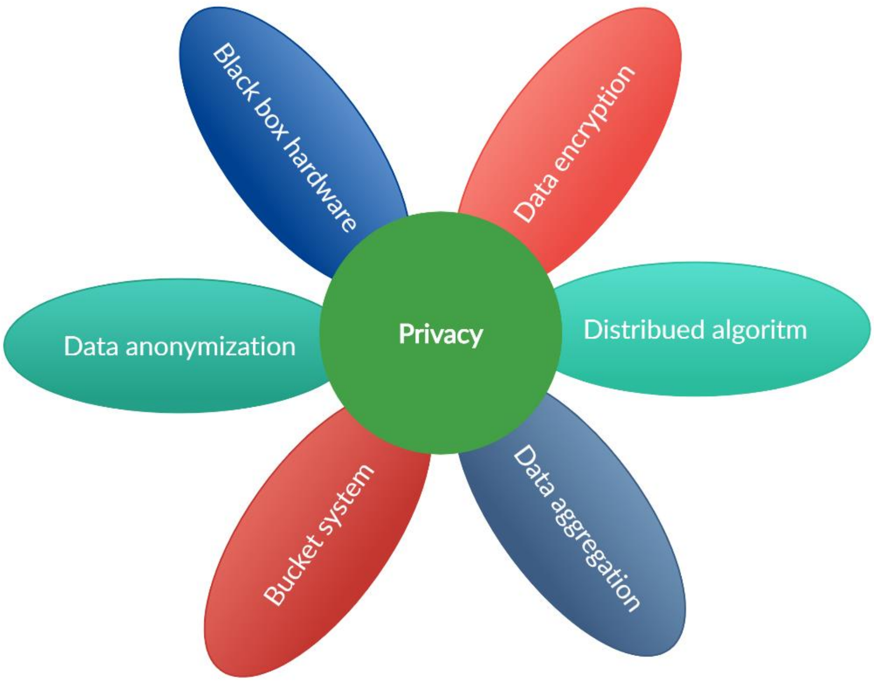

Figure 24 Privacy measures

With the help of Public Key Infrastructure (PKI) encryption, we tried to mitigate the risk of an outside access using eavesdropping attack. In case of an attack, a private key of participants would be required to access the encrypted information. With the limited computing resources, it is impossible to decrypt the PKI encrypted data without the private key.

The scenario in which there is an internal participant act as a legal participant and spies on other participants. Every participant in the network has its own encrypted space in the bucket to store and get the data from the token. The server does not know about the spaces of the participants. If the virtual ring is by some means is accessible to any malicious actor, he will has access to only three parts of data. First of all, to the list of the participants available in the token. The list has the address of the predecessors and successors in random order. As, all the data in the bucket is PKI encrypted so he can only decrypt his own information. Secondly, the counters using to hold the share and load adaption value. Even these values have been protected using randomization. Every participant has to add the value to his own bucket and only server can deduce these values. Lastly, the value which is accessible is the future consumption of the participants. This information is used for the load shifting. Single malicious actor cannot access this information. To access this, a coalition is required.

As we have hidden the address of the successor in form encrypted data into the bucket which makes a coalition attack difficult. But coalition attack still can be carried out. Let assume two participants are forming coalition attack to know whether a participant has any shiftable load or not. Also, to get the current load of the participant. For this, attackers have to be immediate predecessor and successor of the victim participant to carry out the coalition. It has very low probability. If we have 100 participants than the probability of two users to be a predecessor and successor of any user is 0.02%. On the other hand, the attackers only access to the address of the participant but without additional information they cannot assign it to specific appliance of the participant.

$$P = \frac{2n-4}{n(n-1)} \cdot \frac{1}{n-2} = \frac{2}{n(n-1)} \qquad (3)$$

In other words, any participant has very little information accessible like share of load adaption, future consumption and the addresses of its predecessor and successor. The algorithm starts at the server. The server is a trusted party in our algorithm so it has registry of all the participants. Other than this, the accessible data is in aggregated form e.g. the no. of adaptable participants and their share. But this data does not refer to any specific appliances. Now the only data on risk is information of shiftable loads and this can be get by a coalition attack.

In the first round, with the help of these measures we are able to achieve a good privacy. But from the second round, complete privacy achieved. While client-server architecture cannot offer such privacy of the participants. In this approach, the server required the whole data in order to carry out the DSM. It means we have to transmit the participants' data to server which put the data at risk. If some unauthorized party gets the data, it can use the information to make load profiles and future expected consumption of the participants.

Nevertheless, both approaches are different from each other. In client server methodology all of the calculations are done on the server side for which server needs essential data of all the participants. In this approach participants do not have any communication with one another. The server must be trusted party as it has access to a lot of private information of the participants. A hacker can has access to all the private information of the participants by just attacking the server. On the other hand, the distributed methodology enable each participant to carryout necessary calculation own its own and just pass the control messages through the network for which a token is used. Even the server cannot access the private data of the participants. These control messages are exchanged in aggregated form so these do not represent a specific participant. This small comparison of these two different methodologies shows that distributed methodology has better privacy.

5.6. Analysis of Communication

The above mentioned measures help us to achieve better privacy of the participants. The privacy measures mean data overheads which affects the communication of the participants in the network. In the following section we have presented a comparison of the data overheads of client server, simple distributed and encrypted distributed methodologies.

5.6.1. Client Server Data Packet

In this, we are analyzing the data packet in the client server methodology. As mentioned in the earlier section the data of participants need to be transmit at specific rate or interval. The data includes the load profiles of participants, potential adaptable loads and shiftable loads. The figure 25 represents the data packet.

The variables $V^{cs}{}_{Ppart}$ and $V^{cs}{}_{Pserver}$ represents the data packets of the participant and the server in chronological order. The algorithm needs to run completely if we want to observe the best and the worst cases. For example, in the worst case, each participant has the maximum possible no. of the shiftable loads. The participants have to pass the information of the load profiles of these appliances and their deadlines. Then, the server transmit the activation times of these appliances to every participant. While in the best case, the participants have no shiftable load at all. Thus, the potential of the adaptable load needs to be share with the server. The server only transmit their share of the adaption. This has to be transmitted with everyone in the network.

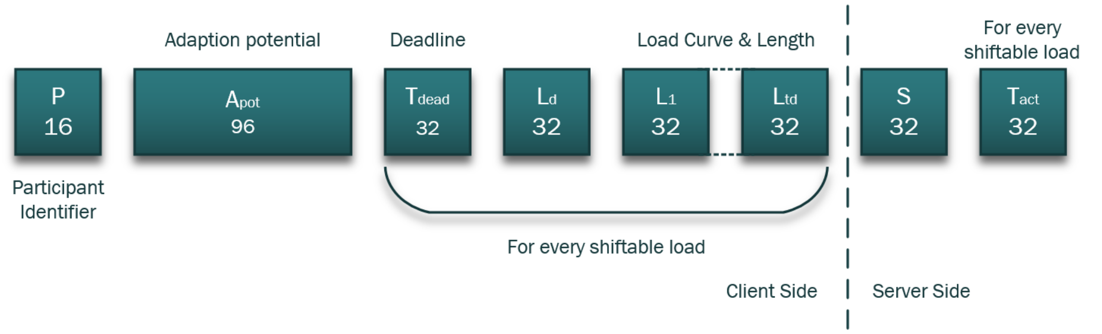

Figure 25 Client-Server packets

5.6.2. Unencrypted Distributed Data Packet

The figure 26 shows the unencrypted distributed data packet. The figure shows that the unencrypted packet has 2 things i.e. list of the addresses of participants and dimensions of the list. The proposed algorithm can handle up to 250 participants if we run it for thirty seconds. Therefore, we set a 16-bit size for the address of participant which makes it to handle the future expansions. The load profile, min and max capacity, size of list and expected future consumption of the participants are required in the first round of the algorithm. With this the shiftable loads have been handled and only the deficit is required from second round and on. Additionally, the packet also contains a list of the participants which are still adaptable. The entry for adaption potential has only 4 values i.e. up, down, none or both.

The variable V_d represent the whole size of packet. The packet has lowest data when there are no adaptable load available and the algorithm requires only one round to complete. With every round passing the list of the participants is reducing by one as before forwarding the token to next participant, the participants get rid of its successor's address from the list.

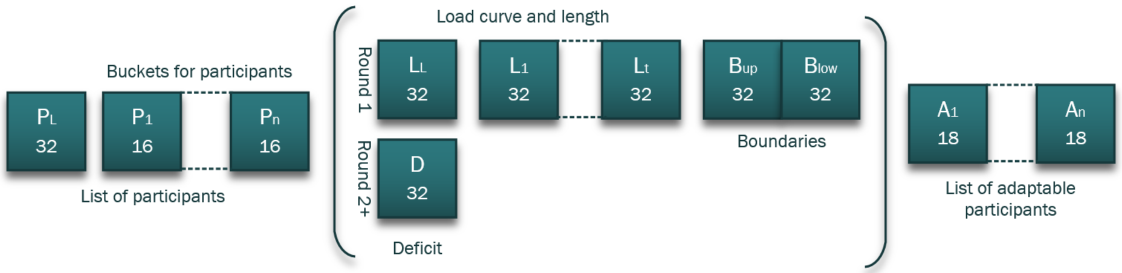

Figure 26 Unencrypted version of distributed packet

In case of the worst case the data packet has the maximum volume. It is happen, when in some round every participant is adaptable except the last participant which means the algorithm requires another round. For that reason, if we have *n* total participants then *n* rounds can be possible, where *n-r* adaptable participants in r^{th} round.

5.6.3. Encrypted Distributed Data Packet

As described earlier list of participant remains same in the first round of algorithm. From the second round and on it is reduce by one in each round which depends on the potential adaptable participants. This affect the best and the worst case of the algorithm. In the worst case there is some deficit which needs to be handled but in each round last participant is not adaptable or deficit is too much for the last participant so another round is required. This does not affect the token size. With the little modification in the algorithm, for *n* participants, a token needs to be send to *n (n + 1)* times. On the other hand, only one round is required for the best case scenario. It means token is sent to all the *n* participants and back to the server *(n + 1).* There are no adaptable loads in this case so, the token size remains the same.

5.6.4. Data Overhead

The figure 27 shows the average volume of the data when the algorithm run completely and successfully. In distributed methodology, we need significantly more data than the client server methodology. As in client server methodology, participants do not communicate with each other and it requires only one round as the multiple rounds are handle by the server internally. Thus the data volume is smaller. Yet, distributed methodology offers a high level of privacy which client server methodology does not.

The data overhead has a small impact as compared to the privacy offers by the distributed methodology. For this purpose, we consider a scenario, a street which has around 100 appliances. The data overhead is very small in the best case scenario i.e. (611.2 KB/591.9 KB) which is almost 3.5%. This overhead of data is because the list of the participants is encrypted and it remains same throughout the algorithm as the algorithm does not remove any participant from the list. In the worst case data, the data overhead has greater effect. In encrypted version, the algorithm does not reduce the size of the list while in unencrypted version the list of the participant is reduced with each round. For 100 participants this causes data overhead of almost 178% (3744.1 KB/1342.6 KB). It is still practical to implement the algorithm with the privacy measures with this overhead of the data and without decreasing the participants. The time interval for the energy management to achieve the best results should be one minute. The bandwidth required for the running the proposed algorithm for 30 seconds in shown in figure 28. The 30 seconds are sufficient to carry out the supplementary calculations. Only 124.8 KB/s is required for 100 participants which means it is a practical solution.

Figure 27 Average volume of data required by algorithm

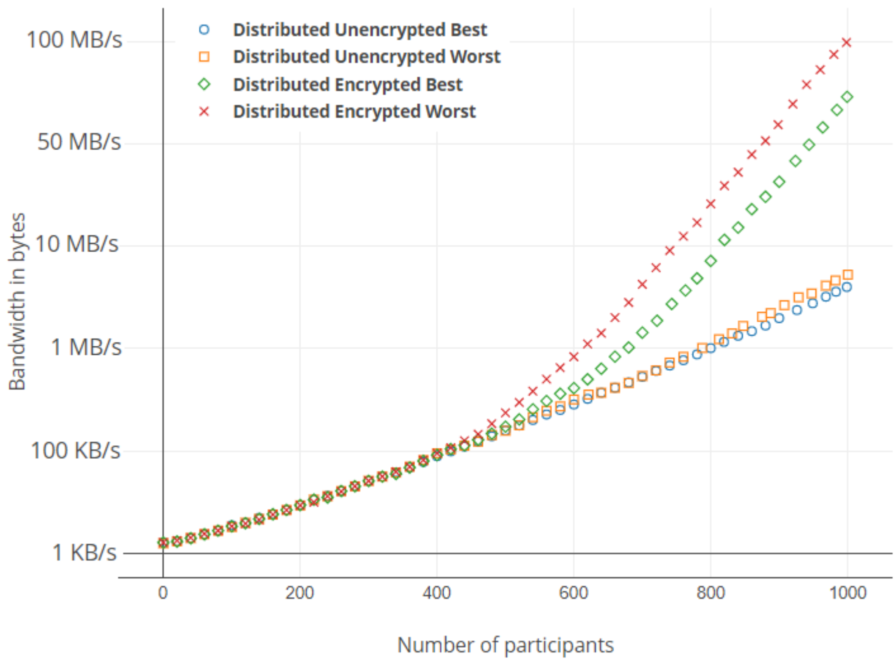

Figure 28 Bandwidth required by algorithm to run for 30 seconds

Chapter 6

CONCLUSION

Chapter 6: Conclusion

6.1. Conclusion

In this thesis, we introduced a distributed algorithm for the energy management in smart grid. Three distinctive smart grid levels exist: T&D, micro-grid and local level. As it is a complex system and a daunting task is its optimization. We proposed an algorithm for the autonomous control of home appliances in this study based on their priorities. We have categorized household in to three distinct categories like adaptable load, base load and shiftable load. Base load have to run immediately as they turned on. The shiftable loads can be shifted to later times of the day to avoid the peak the demand. Similarly, the adaptable loads can increase or decrease their power consumption based on deficit of energy. The proposed algorithm seeks an optimal set of solutions that aim to conform as closely as possible to the predefined maximum permitted energy consumption. This optimization helps escape the peak load and smooths the overall curve of consumption.

This thesis proposed a distributed energy management algorithm for SG which is not only autonomous but also a privacy-friendly. With the proposed methodology is in impossible for the consumers and third parties to gain any information of any other consumer. In this proposed algorithm the server acts as beginning and ending point. As hybrid encryption is used to encrypt the data before transmission. Also, we combined it with another algorithm called, the bucket principle, which strengthen the privacy as the bucket principle have a separate encrypted space for every member. This helps in attaining a higher level of privacy. Nevertheless, as attaining security has its own cost, these privacy measures have data overhead which increase the data size.

6.2. Future Work

The future work of this study can be algorithm for management at the micro-grid level of smart grid. In future, we can further work on the left over part of security of communication for example availability, integrity, and etc. With these measures for privacy, we can achieve security at all levels of distributed algorithm.

References

[1] CDU, CSU, and SPD, “Deutschlands Zukunft Gestalten - Koalitionsver- trag zwischen CDU, CSU und SPD,” 2013.

[2] C. Laughman, K. Lee, R. Cox, S. Shaw, S. Leeb, L. Norford, and P. Armstrong, “Power signature analysis,” *Power and Energy Magazine, IEEE,* vol. 1, no. 2, pp. 56–63, 2003.

[3] U. Greveler, B. Justus, and D. Loehr, “Multimedia content identification through smart meter power usage profiles,” *Computers, Privacy and Data Protection*, 2012.

[4] H. Morais, P. Kdr, P. Faria, Z. A. Vale, and H. M. Khodr, “Optimal scheduling of a renewable micro-grid in an isolated load area using mixed-integer linear programming,” *Renewable Energy,* vol. 35, no. 1, pp. 151–156, Jan. 2010.

[5] S. Bu, F. R. Yu, and P. X. Liu, “Stochastic unit commitment in smart grid communications,” in *IEEE Conference on Computer Communi- cations Workshops (INFOCOM WKSHPS), 2011*. IEEE, 2011, pp. 307–312.

[6] A.-H. Mohsenian-Rad, V. Wong, J. Jatskevich, R. Schober, and Leon-Garcia, “Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid,” *IEEE Transactions on Smart Grid,* vol. 1, no. 3, pp. 320–331, 2010.

[7] D. Behrens and C. Gerwig, “Selbstregulierende verbraucher im smart grid: Design einer infrastruktur mit hilfe eines multi-agenten-systems,” *Multikonferenz Wirtschaftsinformatik*, 2014.

[8] S. Lehnhoff, *Dezentrales Vernetztes Energiemanagement: Ein Ansatz Auf Basis Eines Verteilten Adaptiven Realzeit-Multiagentensystems*. Springer DE, Mar. 2010.

[9] K. Mets, M. Strobbe, T. Verschueren, T. Roelens, F. De Turck, and C. Develder, “Distributed multi-agent algorithm for residential energy management in smart grids,” in *2012 IEEE Network Operations and Management Symposium (NOMS)*, 2012, pp. 435–443.

[10] Bundesamt für Sicherheit in der Informationstechnik (BSI), “BSI TR- 03109,” 2013.

[11] C. Efthymiou and G. Kalogridis, “Smart grid privacy via anonymization of smart metering data,” in *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm),* Oct. 2010, pp. 238– 243.

[12] K. Kursawe, G. Danezis, and M. Kohlweiss, “Privacy-friendly aggrega- tion for the smart-grid,” in *Privacy Enhancing Technologies*, ser. Lecture Notes in Computer

Science, S. Fischer-Hbner and N. Hopper, Eds. Springer Berlin Heidelberg, Jan. 2011, no. 6794, pp. 175–191.

[13] P. McDaniel and S. McLaughlin, “Security and privacy challenges in the smart grid,” *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May 2009.

[14] A. Barenghi and G. Pelosi, “Security and privacy in smart grid in- frastructures,” in *2011 22nd International Workshop on Database and Expert Systems Applications (DEXA)*, Aug. 2011, pp. 102–108.

[15] C. Rottondi and G. Verticale, “Privacy-friendly appliance load schedul- ing in smart grids,” in *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2013, pp. 420–425.

[16] D. Brettschneider, R. Tönjes, P. Roer, and D. Hölker, “Distributed algorithm for energy management in smart grids,” in *2014 World Telecommunications Congress (WTC 2014)*, Berlin, Germany, Jun. 2014.

[17] CDU, CSU, SPD: Deutschlands Zukunft gestalten, Coalition Agreement, 2013

[18] AGEE Stat: Erneuerbare Energien 2012, Technical Report, 2013

[19] A. Parisio and L. Glielmo: A mixed integer linear formulation for microgrid economic scheduling,

[20] IEEE International Conference on Smart Grid Communications (SmartGridComm), 505–510, 2011

[21] K. Clement-Nyns, E. Haesen and J. Driesen: Analysis Of The Impact Of Plug- Hybrid Electric Vehicles On The Residential Distribution Grids By Using Quadratic And Dynamic Programming, In World Electric Vehicle Journal, 2009

[22] A.-H. Mohsenian-Rad, V. W. S. Wong, J. Jatskevich, R. Schober and A. Leon-Garcia: Autonomous Demand-Side Management Based on Game- Theoretic Energy Consumption Scheduling for the Future Smart Grid, IEEE Transactions on Smart Grid, 320–331, 2010

[23] S. Lehnhoff: Dezentrales Vernetztes Energiemanagement: Ein Ansatz Auf Basis Eines Verteilten Adaptiven Realzeit-Multiagentensystems, Springer DE, 2010

[24] B. Ramachandran, S. K. Srivastava, D. A. Cartes and C. S. Edrington: Distributed energy resource management in a smart grid by risk based auction strategy for profit maximization, IEEE Power and Energy Society General Meeting, 2010

[25] K. Mets., M. Strobbe, T. Verschueren, T. Roelens, F. De Turck and C. Develder: Distributed Multiagent Algorithm for Residential Energy Management in Smart Grids, IEEE Network Operations and Management Symposium (NOMS), 435–443, 2012

[26] M. Steinheimer, U. Trick and P. Ruhrig: Energy Communities in Smart Markets for Optimisation of Peer-to-peer Interconnected Smart Homes, International Symposium on Communication Systems, Networks and Digital Signal Processing, 2012

[27] D. Nestle: Energiemanagement in der Niederspannungsversorgung mittels dezentraler Entscheidung, kassel university press, 2008

[28] Y. Zhang, N. Gatsis, and G. B. Giannakis: Robust Distributed Energy Management for Microgrids with Renewables, IEEE Third International Conference on Smart Grid Communications, 510–515, 2012

[29] D. Hölker, M. Fischer and R. Tönjes: Abschätzung der notwendigen Speicherkapazitäten bei volatile Energieerzeugung unter Berücksichtigung der haushaltsspezifischen Lastverschiebepotentiale, 3. Energie & Technik Smart Home & Metering Summit, 2013.