A Privacy-Preserving Method with Flexible Charging Schedules for Electric Vehicles in the Smart Grid

Sabrina Afrin
sa3213@rit.edu

Follow this and additional works at: http://scholarworks.rit.edu/theses

Recommended Citation
A PRIVACY-PRESERVING METHOD WITH FLEXIBLE CHARGING SCHEDULES FOR ELECTRIC VEHICLES IN THE SMART GRID

BY

SABRINA AFRIN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN COMPUTER ENGINEERING

DEPARTMENT OF COMPUTER ENGINEERING
KATE GLEASON COLLEGE OF ENGINEERING
ROCHESTER INSTITUTE OF TECHNOLOGY
ROCHESTER, NEW YORK
JULY 2017
A Privacy-Preserving Method with Flexible Charging Schedules for Electric Vehicles in the Smart Grid

by

Sabrina Afrin

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Engineering

Supervised by

Dr. Andres Kwasinski
Department of Computer Engineering
Kate Gleason College of Engineering
Rochester Institute of Technology
Rochester, New York
July 2017

Approved by:

Dr. Andres Kwasinski
Thesis Advisor, Department of Computer Engineering

Dr. Amlan Ganguly
Committee Member, Department of Computer Engineering

Dr. Stanisław Radziszowski
Committee Member, Department of Computer Science
Dedication

To my family
Acknowledgments

I am indebted to many individuals for their guidance, support, and encouragement, in completion of this thesis. I would like to take this opportunity to thank all the people who supported me, directly and indirectly, throughout my journey of reaching this milestone.

First and foremost, my sincere gratitude and thanks to my thesis advisor, Dr. Andres Kwasinski. I am very fortunate to have Dr. Kwasinski as my thesis supervisor, whose support, feedback and guidance have been the principal influence behind the content of this thesis. I would like to express my heartfelt appreciation to Dr. Amlan Ganguly and Dr. Stanisław Radziszowski, for agreeing to be on my thesis defense committee, for their valuable time and useful feedback. My graduate experience benefited greatly from the courses I attended at RIT, and I want to thank all the faculty members of RIT with whom I have taken courses. Furthermore, I would like to acknowledge the support to my graduate studies by the Department of Computer Engineering and the GCCIS, RIT.

My deepest gratitude to Shuvo bhaia, Susmita apu, and Dhrubo, for their support when I decided to pursue an MS. I also want to acknowledge the
supports from Shahriar’s family, and the help from Mitul bhai and Meraj during my coursework. A very special thanks goes to both Naseef bhai and Zaima, for being there when my family was away (next time they need to whine and complain, they should know who to reach and who owes them one!). Thanks to Naseef bhai for always helping me out (sometimes, without being asked), also, for his treats to the numerous cups of coffee. That reminds me, I am deeply grateful to the Java coffee shop at RIT for their splendid coffee!

Oftentimes, we don’t acknowledge and thank something that is always there, like, our family. Fortunately, I have a large one. I want to express my gratitude and thanks to Amma, Abba, Anny apu, Ashik bhaia, Cynthia, and Shahriar, for their unconditional love, for allowing me to be my weird self without any complaints, for always being by my side (even when I am being my utmost annoying self), and for every other countless things. They are the reasons for who I am today, and also for the fact that I am irrevocably spoiled!

Almighty Allah has always been boundlessly kind and gracious to me, despite all my shortcomings. I can never express enough gratitude towards him, and will forever be in his debt.
Abstract

A Privacy-Preserving Method with Flexible Charging Schedules for Electric Vehicles in the Smart Grid

Sabrina Afrin

The Smart Grid (SG) is an emerging modernized electrical power system with advanced monitoring and control mechanism, and improved fault-tolerance. The SG converges traditional power grid with a bidirectional communication and information system into the same infrastructure. Electric Vehicles (EVs), with their energy storage capacity and bidirectional communication capability, are envisioned to be an essential component of the SG. EVs can play the role of distributed energy resources by storing energy in off-peak hours and providing energy to the grid during peak hours or system contingencies. The energy stored by an EV is equivalent to the average energy drawn by multiple residential houses. As a result, simultaneous charging by a large number of EVs can create sudden energy imbalance in the grid. The mismatch between the energy generation and demand can create cascading faults resulting in load shedding. To prevent such situation, EVs are required to pre-schedule charging events at a Charging Station (CS). To efficiently manage a scheduled event, an EV is required to transmit information such as a valid ID, state-of-charge, distance from a CS, location, speed, etc. However, the data transmitted by an EV can be used to reveal information such as the movement of the vehicle, visits to a hospital, time to arrive at office, etc. The transmitted information can be used to create profiles of the owners of the EVs, breaching their location privacy.

In the existing literature, it is recommended to use pseudonyms for different transactions by an EV to achieve location privacy. The majority of the works in the literature are based on anonymous authentication mechanism, where missing a charging event by an EV is considered as malicious and the corresponding EV is penalized (e.g., blacklisted). However, missing a charging event may happen due to many valid reasons and flexibility
of scheduling can encourage consumer participation. On the other hand, missing charging events results in monetary loss to the CSs. In this thesis, an authentication method is developed to provide anonymity to EVs. The proposed method also addresses the cost-effectiveness of flexibility in charging events for the EVs and the CSs. A network setup that sub-divides a regional area into smaller zones to achieve better privacy, is proposed. A MATLAB simulation is designed to demonstrate the Degree of Anonymity (DoA) achieved in different stages of the proposed method and the optimal number of missed charging events. Additionally, a method to determine sub-division of zones from the simulation results, is studied.
# Contents

Dedication .................................................. ii

Acknowledgments .......................................... iii

Abstract ....................................................... v

1 Introduction ................................................ 1
   1.1 Smart Grid ........................................... 1
   1.2 Electric Vehicles (EVs) in the SG .................... 4
       1.2.1 Vehicle-to-Grid (V2G) Communications ........ 5
       1.2.2 Charging and Discharging Events of EVs ........ 8
       1.2.3 Privacy of EVs .................................. 11
   1.3 Thesis Objectives .................................... 14
   1.4 Organization of the Thesis .......................... 15

2 Related Work .............................................. 16
   2.1 Privacy-Preserving Methods for EVs ................. 16
   2.2 Network Setups and Adversarial Models Considered in the Literature ........................................... 19

3 Background ................................................ 22
   3.1 Blind Digital Signature .............................. 22
   3.2 Partially Blind Signature ............................ 23
   3.3 Degree of Anonymity .................................. 24
# System Model

4.1 Network Setup and Adversarial Model .......................... 27  
4.2 Assumptions .................................................. 29

# Methodology ...................................................... 32

# Results and Analysis ............................................ 38

6.1 Variation of DoA in the Proposed Method ..................... 38  
6.2 Number of Missed CSs w.r.t. Electricity Price ............... 39  
6.3 Sub-division of a Regional Area .............................. 40

# Future Works ..................................................... 44

# Conclusion .......................................................... 45

Bibliography .......................................................... 46
List of Tables

1.1 Transmitted data associated with V2G networks and their privacy impacts [1] .......................... 12
List of Figures

1.1 Elements of a traditional power grid [2] ........................................ 2
1.2 The seven-domain conceptual model of the smart grid [2] ........ 3
1.3 An abstract view of the vehicular communication [3] .......... 6
1.4 Charging points for EVs in the SG [4] ................................. 8

4.1 An example of the proposed network setup .................... 28

5.1 Steps taken by an EV and the associated service providers
in different phases of the proposed method .......................... 33
5.2 Steps followed by an EV in the registration and token col-
lection phase .......................................................... 34
5.3 Steps in the selection of CSs phase ................................. 35
5.4 Steps in the scheduling of charging events phase ........... 36

6.1 Variation of DoA in pre-arrival, timing window and post-
arrival time slots ......................................................... 39
6.2 Number of missed CSs vs. scheduled and real time electric-
ity price ................................................................. 40
6.3 Determining the number of EVs in a sub-divided zone .... 41
6.4 Determining the number of EVs in a sub-divided zone .... 42
6.5 Steps of the method to sub-divide a regional area .......... 43
Chapter 1

Introduction

1.1 Smart Grid

The Smart Grid (SG), also known as the “intelligent grid” [2] or the “Internet of energy” [5], is a modernized version of the electric power grid. The traditional power grid was designed in the 20th century, based on a hierarchical and centralized SCADA (Supervisory Control And Data Acquisition) control system architecture, where electricity flows from central generators to the customer domain [1]. In this radial power system, after being generated, electricity flows through the transmission lines and reaches the end users via the distribution system (e.g., transformer), as shown in Fig. 1.1

The occurrence of large-scale power outages (e.g., the 2003 Northeast blackout, the California energy crisis, etc.) during the last few decades has necessitated the convergence towards an efficient, fault-tolerant and intelligent power system. One of the main reasons of power outage is the mismatch between electricity generation and demand. The diminishing carbon-based energy resources (e.g., coal, gas, etc.) are not sufficient to meet the electricity demand of today’s large population [1]. Moreover, the traditional energy sources have a negative impact on the environment by emitting green-house gas. As a result, the integration of renewable energy sources (e.g., solar, wind, hydro, etc.) into the grid has become necessary. However, the power generated from different energy sources have different frequencies and qualities. A distributed control system is required to coordinate the heterogeneous grid components to meet the nominal grid conditions. On the other hand, the hierarchical topology of existing power system causes
a domino-effect failures of faults in the distribution system [6]. A bidirectional communication infrastructure can make the grid situation-aware by collecting real-time information from the entities connected to it. In this way, an abnormal condition or a fault can be isolated before it cascades through the interconnected system. By converging the traditional power system with a communication and information system, the SG emerges as a distributed power system with pervasive monitoring and control mechanism [6].

The SG is an information-centric, bidirectional, and heterogeneous electrical power infrastructure. The SG incorporates entities from different sources which can play multiple roles in the grid mechanism. For example, the energy consumers in the SG can generate (e.g., with solar panels) and store energy, and later, sell it back to the grid. Therefore, they can simultaneously play the role of electricity consumer and supplier. Fig. 1.2 shows the conceptual model of the SG proposed by the National Institute of Standards and Technology (NIST) [7]. The dotted orange and the solid blue lines represent the electricity flow and the information flow, respectively. The two-way flow of electricity and information in the SG is envisioned to support advanced metering infrastructure, real-time monitoring and smart management system. The smart energy management system in the SG will enable the consumer domain and the grid to interact with each other and
Figure 1.2: The seven-domain conceptual model of the smart grid [2]

exchange electricity, price and demand information [8].

The SG offers different distinguishing features such as dynamic pricing, demand response, peak-shaving, etc. Dynamic pricing provides variable electricity prices based on the current load-demand condition in the grid, i.e., high price when demand is high and low price during off-peak hours. In the traditional grid, 20% of its generation capacity is reserved to meet peak time demand [6]. During emergency, reserved generators are used in a minute-by-minute basis to balance load-demand, which is very costly. In the SG, this situation can be improved by demand response and peak-shaving, in which consumers change their energy usage pattern to balance the grid. As the SG offers dynamic pricing of energy, customers can subscribe to the demand response feature. During the peak-hour (e.g., at noon or evening), the subscribers refrain from performing the tasks requiring high energy and schedule them to the off-peak hours (e.g., at night). If a large number of consumers participate, the total demand will be reduced in the peak time. As a result, the grid will not be required to use back-up generators. On the other hand, if there is not enough number of consumers changing the energy usage pattern, the price is increased, which in turn discourages the consumers from continuing the usage. Consequently, the peak-demand is reduced. Another method of load-demand management in the SG is the remote appliance control. In this method, during emergency or when demand
is high, appliances or devices are remotely turned off by the grid operators. By collecting real-time information from the smart appliances, the SG offers ubiquitous system monitoring and control mechanism, and facilitates the transformation towards a self-healing and reliable power grid.

1.2 Electric Vehicles (EVs) in the SG

Plug-in Hybrid Electric Vehicles (PHEVs) and Plug-in Electric Vehicles (PEVs) are becoming popular due to their low pollution (green-house gas) emissions, reduced dependency on petroleum or fossil fuel, potential utility applications, and economy [9], [10], [11]. Both types of Electric Vehicles (EVs) are capable of storing energy in on-board storage devices (i.e., battery) by plugging into the grid. PEVs are entirely powered by on-board batteries, and PHEVs have an additional combustion engine along with the battery [12], [13]. In addition to the energy storage capacity, EVs are equipped with power interface and computing platform with communication interfaces (e.g., Ethernet, USB, Bluetooth, and IEEE 802.11, etc.) [14]. As a result, EVs can work as mobile energy storage devices [15] in the bidirectional SG. As EVs are parked 95% of the time [16], they can charge their batteries at night when the price is low and provide the energy back to the grid during peak time or system contingency. This feature benefits both the utilities and the consumers by reducing the cost of reserved generators and utilizing dynamic pricing, respectively.

In the traditional electrical power system in the U.S., the cost associated with power outages is approximately 100 billion dollars per year [17], due to the shortage of available energy. Renewable energy sources are a potential substitute of the traditional fossil fuels. However, the cost and difficulties associated with building power plants based on a renewable source, specially, in large metropolitan areas, have not produced the anticipated effects for renewable energy sources [1]. The introduction of large number of EVs would be an accelerator of the energy crisis, however, the unique characteristics of the EVs make them a potential solution too. The batteries in the EVs can be powered by small renewable energy sources such as
solar panels installed at home. The mobility and the bidirectional communication mechanism enable the EVs to sell the excessive electricity back to the grid at various places and times. Moreover, as the market share of EVs increases, the demand of petroleum by traditional vehicles will be reduced, making the automobile industry more environment-friendly. Due to their fast charging/discharging capability, the EVs are considered as a potential solution for spinning reserves and frequency regulation in the grid [9]. These services are lucrative to the consumers, as the vehicles are paid for their availability even if charging/discharging operation is not required at a moment. As EVs are active 4% of the time in a day, the cumulative payment for the other 96% results in a considerable benefit for the owner [9]. As a result, EVs are considered as an integral part of the Distributed Energy Resources (DER) in the SG.

1.2.1 Vehicle-to-Grid (V2G) Communications

Vehicle-to-Grid (V2G) communications enable the grid and the EVs to interact and share information, and support the grid operators in monitoring available capacity in real-time. V2G communications also help to coordinate the charging/discharging events of EVs to maintain grid stability. For example, an EV can store more than 10 kWh energy, which is equivalent to the average energy demand per hour of 10 residential houses in the U.S. If a large number of EVs start drawing energy simultaneously, the sudden electricity demand can create a mismatch between the generation and load, thus, causing a deviation from the nominal grid operating frequency. With the support of the V2G communications, EVs can schedule charging events depending on the availability in the grid. It is envisioned that Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications will enable future EVs to be context-aware and avoid road accidents [14], and participate in the road traffic management.

The security and privacy of Vehicular Communication (VC) systems are imperative for the safety and reliability of the infrastructure and the customers. For instance, roaming vehicles can frequently transmit data about road constructions or obstructions, congestions, road accidents or hazards,
etc. The data transmitted by the vehicles helps the road safety management system to be more reliable and rapid [3]. Similar ideas have already been implemented in mobile applications (e.g., Waze) to determine road conditions. However, the advantages of the VC systems open doors for exploitation by malicious entities. Malicious attackers can intercept messages transmitted by vehicles to track their movement or transactions, breaching their privacy. A compromised vehicle can transmit forged messages containing false information and mislead other vehicles to leave or follow a particular road, causing traffic congestion. Fig. 1.3 shows an abstract view of the future VC system considered in [3]. According to this concept, Road-Side Units (RSU) act as the gateway of the vehicular network with the help of other infrastructures (e.g., cellular network). Certification Authorities (CAs) are in charge of managing the identities, credentials of the nodes (EV and RSU) in a region (national territory, district, county, etc.). The secure V2V and V2I communications comprise of VC-specific TCP/IP protocol stacks. The presence of a CA is considered in the majority of the works addressing security and privacy of the EVs, in the literature. The functionality of the CA enables a protocol to achieve basic security requirements such as confidentiality, authentication, non-repudiation, etc. The confidentiality means the content of a message is accessible only to the intended recipients [18]. Authentication refers to the mechanism of confirming if a message or entity is valid/authorized [18]. A CA in a network manages public keys of the users and certifies them. A message encrypted with a certified public key
of the receiver provides confidentiality. On the other hand, if a sender signs a message with its own private key and the signature is verified as true, it can prove the authenticity of the sender. The non-repudiation on the other hand, prevents a sender from denying that s/he did not transmit the message [18]. A message digitally signed by a sender provides non-repudiation to the message if the public key of the sender is certified by a trusted CA.

The emerging smart grid communication infrastructure is envisioned to accommodate the coordination of intelligent charging of EVs [19]. Based on the seven domain model of the SG, authors in [4] have proposed a model of EV charging infrastructure, as shown in Fig.1.4. According to this model, an EV can charge its battery and participate in the V2G communication, by being part of different networks. For instance, when it connects to the home plug inside the residence of the owner, it acts as a part of the Home Area Network (HAN). If it charges inside the building complex of the owner, or a visiting home, it acts as a part of the Building Area Network (BAN) or the host home network. An EV can also charge inside a commercial (industrial) building, as a part of the Industry Area Network (IAN), or in a public infrastructure, or third party power station. The electrical sensors and smart meters at the charging stations are capable of collecting/exchanging high-frequency data from/to the charging/discharging events and monitor in real-time through two-way communication in the premise [10]. The authors in [20] compared three wireless technologies based on their applicability in the SG. The chosen technologies are HomePlug, ZigBee and cellular network, and the comparison metrics are interference, power consumption, and security. HomePlug devices do not require additional battery and are not subject to other wireless traffic as they are powered through the wall outlet. HomePlug is able to achieve high-speed broadband communications over low-voltage power lines and faster than ZigBee or a cellular network. As a result, it is suitable for a HAN. Zigbee devices have low power consumption, and have a low device and installation cost, which make them suitable for commercial deployment at large-scale charging facilities. An application layer standard for ZigBee has already been developed, based on energy profiles to support different devices, e.g., load control devices, EVs, etc. [5]. Cellular network, on the other hand, provides long-range wireless data
network, which makes it suitable for roaming EVs [5], [20].

1.2.2 Charging and Discharging Events of EVs

The number of cars in the U.S. is approximately 250 million, and it is predicted that by the year 2020, with a 10% penetration of EVs into the industry will amount to an energy storage capacity of 500 GWh [10]. However, the large capacity and the large load can present EV as a “two-edged sword” [3] to the utility. Works have shown that it will be difficult to control customer behavior (i.e., driving and charging habits) completely, which in turn may have adverse effects on the distribution system thermal loading, voltage regulation, transformer balance, harmonic distortion levels, etc. [9], [13]. Due to the large interconnection of the power grid, system failures can affect a large geographical area if an abnormal condition is not resolved quickly. As a result, EVs as energy consumers and suppliers are required to respond quickly to power commands.

The charging management of EVs can be categorized into two types, 1) centralized and 2) decentralized approach [13]. In the centralized approach, a central entity (i.e., aggregator) uses direct control signals or indirect incentives. As the control signals, electricity price (day-ahead or threshold price) is used to shift charging requests of EVs from peak-hours to off-peak hours. This type of utility coordinated charging of EVs through the V2G communications, known as “smart charging”, is designed to facilitate load-demand
management in the SG [9]. Considering real-world constraints (e.g., communication and infrastructure variations among individual vehicles), a centralized aggregator can regulate multiple battery loads from a cluster of EVs, and maximize customer satisfaction and minimize grid disturbances [10], simultaneously. In comparison to the amount of energy required for a power grid regulation, the energy stored by an individual EV is small. A small energy storage needs frequent charging/discharging operations to offer an ancillary service. Therefore, a large energy storage is more suitable for grid regulations [21]. The control operator can set a minimum ‘bid size’ as the required energy for regulation which in turn meets the time of availability. As a result, if a utility works as a ‘middleman’ between the EVs and the grid, it needs to aggregate multiple EVs to offer ancillary services (e.g., voltage control, frequency regulation, regulation reserve, spinning reserve, and non-spinning reserve) [10]. Similarly, in a decentralized approach, EVs optimize their charging schedules based on the broadcasted price signal. This approach requires V2V communication to maintain aggregated charging behavior within the distribution grid constraints [13].

In both of the approaches, the grid operator requires the knowledge of current demand to determine the grid constraints. Moreover, the stability of power grid is maintained by performing hourly power regulation to prevent generation capacity from ramping up or down from the nominal level. As a result, the EVs are required to frequently transmit certain information to the grid. Some of the motivations behind the collection of real-time data from the EVs, found in the existing literature, are summarized below.

- The current electric power distribution grid cannot support the predicted increase in load-demand introduced by the EVs [12]. Optimization methods for the distribution grid constraints require the collection of high-frequency data from the EVs [13].

- The grid monitoring and quick response to emergencies require utility companies to collect information from the connected entities [13].

- The V2G communication facilitates the integration and energy management of renewable energy sources. The projected peak power load
of the EVs is at solar noon and the peak grid load is at mid-to-late afternoon [10]. The V2G communication can facilitate shifting of charging/discharging of EVs to coincide with periods of strong wind or sun, before they can be used as energy backup [22].

- The work in [23] shows that the addition of EVs and V2G communications into the power system reduces carbon dioxide (CO₂) emissions.

- The remotely controlled smart charging of EVs is performed based on grid conditions and user preferences. Information transmitted by the EVs, such as time-of-use and real-time price, minimizes the billing cost for charging [23].

- By collecting information about energy demand and time to charge, the grid operators can shift charging schedules from peak-hour to maintain the grid stability.

- EVs work as the DER in the SG by working as reserved energy sources during system contingencies, peak-hour or during islanding. Islanding in a power grid happens, when a small geographical area gets disconnected from the main grid. If EVs work as the DER, the cost associated with the reserved generators in the traditional grid is avoided [24]. The V2G communication enables the coordination of DERs in a microgrid.

- The ancillary services provided by the EVs require the exchange of large volume of information between the vehicle, the charging station, and the utility for efficient power transaction between the EV and the grid.

- Uncoordinated and random charging of EVs can make the demand side management challenging by causing power loss, overloads, voltage fluctuations, degraded system efficiency and sub-optimal generation dispatch. The development of V2G infrastructure will provide a high-speed bidirectional communication network for effective coordination of transmission, distribution, and end-user assets [19].
1.2.3 Privacy of EVs

The operational decisions of the SG depend on the information transmitted by the entities connected to it. For instance, the variable price offered by the dynamic pricing feature depends on the current load-demand condition of the grid. Whereas, the load-demand condition is determined from the information collected from the customer and generation domains. The pervasive monitoring and control mechanism of the SG utilize information collected from the devices such as transformers, feeders, etc. and provide early detection and isolation of faults in the transmission and distribution domains. Automated control is a distinctive feature of the SG, where devices are controlled remotely in case of an abnormal condition. The anomaly is detected from the transmitted information of the devices, by finding the deviation of behavior from the nominal condition. The promising features of the information-centric SG have accelerated the transformation from the traditional power system. However, the information transmitted by the consumers poses threat to privacy of the end-users and has stirred protests against the roll-out of the SG [1]. The NIST has identified privacy as one of the seven major challenges to be addressed before the full deployment of the SG [25].

In a V2G communication, the grid operator frequently transmits information such as power commands, dynamic price, charging rate and time, charging/discharging location, etc., to the EVs. Depending on the information, EVs schedule a charging/discharging event with a charging station, at a specified time. The scheduling requires the EVs to transmit information such as State-of-Charge (SoC), current location, speed, a valid identity, expected time of arrival, etc. However, the information transmitted by the EVs can pose threats to the privacy of the owner of the vehicle. It is possible by the electricity provider, data aggregator or a network of charging stations to extract personal information of the owner of the vehicle, such as the place of residence, travel patterns, time to leave for office, visit to a hospital, and create customer profiles [14]. Authors in [1] discusses the typical data transmitted in a V2G network and the type of data considered as privacy-sensitive, as shown in Table 1.1. The data associated with the
Table 1.1: Transmitted data associated with V2G networks and their privacy impacts [1]

<table>
<thead>
<tr>
<th>Data</th>
<th>Billing relation</th>
<th>Reliability relation</th>
<th>Security relation</th>
<th>Privacy relation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer ID</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>Customer name, vehicle ID</td>
</tr>
<tr>
<td>Location data</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>Charging location and schedule</td>
</tr>
<tr>
<td>Meter data</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>Electricity consumed or supplied over a time period</td>
</tr>
<tr>
<td>Configuration data</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>System operational settings, thresholds for alarms, task schedules, policies, etc.</td>
</tr>
<tr>
<td>Control commands</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>Inquiries, alarms, events, and notifications</td>
</tr>
<tr>
<td>Access control policies</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>Permitted communication partners, their credentials and roles.</td>
</tr>
<tr>
<td>Time, clock setting</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>Used in records and sent to other entities.</td>
</tr>
<tr>
<td>Payment and tariff data</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>Informing consumers of new or temporary tariffs as a basis for purchase decisions.</td>
</tr>
<tr>
<td>Firmware, software, and drivers</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>Software components installed and may be updated remotely.</td>
</tr>
</tbody>
</table>

billing services, security or control commands are required for the functionality of both the EV and the grid, and is not considered as sensitive customer information. On the other hand, ID, location, access control policy, and payment and tariff data are the four types of data considered as privacy-sensitive in this paper. In the load-demand optimization method proposed in [13], Charging Service Providers (CSPs) collect and store historical trip data, customer information and billing information of the EVs. The historical trip data includes time-of-departure for a trip, time-of-arrival from a trip, state-of-energy at time-of-departure, state-of-energy at time-of-arrival, location at time-of-arrival, location at the end of the trip, etc. Based on these
data, a CSP is able to predict near-future trips of the customer EVs.

The information transmitted by an EV, during the charging/discharging session, can be used by an adversary to pinpoint the position of a customer [19]. The utilities in the SG provide data management services such as data collection, aggregation, storage, and publication. The high-frequency data collection for grid monitoring yields a large amount of data, which may contain user information, charging strategies, locations, and billing information. The storage cost associated with the large amount of data is high. Utility companies and appliance manufacturers can sell these information to third parties for benefit, which can be considered as sensitive to the customers [1]. The peer competition may motivate a utility company to create customer profiles by analyzing these data, for advertising purposes [1]. Moreover, individual employees can spy on the data of some customers. Additionally, the risk of data leakage by malicious hackers is always there.

In the SG, EVs work as both customer and service provider by charging and discharging, respectively. As a customer, the personal information of an EV needs to be hidden from the utility and as a service provider, its customers should not know who provides the service [1]. Nevertheless, the information required for grid functionality needs to be provided to the utility companies, whereas, customers’ right to keep their data private should also be preserved.

In the existing literature, it is recommended to employ different pseudonyms for different transactions by an EV to provide anonymity to its owner [14]. The use of pseudonyms for data transmission prevents correlation of sensitive information to the original identity of the customer even if the data is compromised. However, an authentication mechanism is required to ensure that only valid EVs participate in the charging events. Otherwise, malicious entities can schedule charging/discharging events randomly without participating in the event. The authentication mechanism requires that no entity have enough information to correlate different transactions to an EV. Therefore, the majority of the privacy-preserving protocols for EVs in the literature are based on anonymous authentication mechanism [16], [26], [27], [28], [29], [30].
1.3 Thesis Objectives

In this thesis, a privacy-preserving method is developed to achieve location privacy of EVs and to enable a Charging Station (CS) to check the authenticity of an anonymous pseudonym used in a transaction. The anonymity of the proposed work is achieved partly by the use of Blind Digital Signature (BDS) method and Partially Blind Signature (PBS) method. Additionally, the proposed method addresses flexible charging schedules for the EVs. Missing a pre-scheduled charging event by an EV causes monetary loss to the CSs or electricity provider. As a result, in the existing literature, an EV not arriving in a scheduled event is considered as malicious and the corresponding EV is penalized (e.g., blacklisted, or refused further services) [27]. However, missing a scheduled event can happen due to different valid reasons such as road obstruction, road accident, GPS taking a different route, etc. Additionally, a vehicle is usually owned by a customer for long period of time and being refused from further services for missing a charging event will prevent benefits to both the customer and the grid. Flexibility in scheduling can encourage more consumer participation in the demand management of the grid. On the other hand, the CSs should also get compensation for the missed charging/discharging events. A mechanism is required which balances flexible charging events for the EVs and monetary loss to the CSs. In the proposed method, EVs can schedule charging events for a timing window. The EVs arriving at the pre-scheduled window, can normally perform charging operation. On the other hand, the EVs which arrive earlier or later than the pre-scheduled window, can still authenticate and participate in the charging event, but, with a penalty cost paid to the CS. Additionally, a network setup that sub-divides a regional area into smaller zones is proposed to prevent service providers in the SG from having enough information to breach privacy of EVs.

The experimental results presented in this work are based on a MATLAB simulation. The arrivals of the EVs are assumed to follow a Poisson distribution and the achieved anonymity is represented by a metric named Degree of Anonymity (DoA) proposed in [31]. The simulation results are used to study the following aspects of the proposed work,
1. The variation of achieved anonymity in different stages (i.e., pre-arrival, timing window, and post-arrival) of the proposed method with respect to (w.r.t.) the arrival rates.

2. The cost-effective number of missed CSs allowable for an EV w.r.t. real-time and dynamic electricity pricing. The cost-effective number of CSs means the maximum number of CSs an EV can miss on its route and provide penalty cost to them while balancing the energy cost.

3. A method of sub-dividing a regional area into groups of EVs based on the arrival rates of EVs in the area. The goal of the sub-division is to achieve a preferred threshold DoA defined by the achieved DoA in an ideal scenario.

To the best of our knowledge, this is the first work on privacy of EVs addressing flexible scheduling of charging events and presenting a formal analysis of DoA to address the aspects stated above.

1.4 Organization of the Thesis

The rest of the thesis is organized as follows. Chapter 2 discusses related works in the literature. The discussed related works include different proposed privacy-preserving methods and network setups. Chapter 3 describes the methods from the existing literature which are used in this work, such as the BDS method, PBS method and DoA. Chapter 4 discusses the system model considered in this work, such as network setup, adversarial model and the assumptions. Chapter 5 describes the steps of the proposed privacy-preserving method. The simulation results are presented in chapter 6, followed by future works in chapter 7. Chapter 8 consists of the conclusion.
Chapter 2

Related Work

2.1 Privacy-Preserving Methods for EVs

The privacy preserving protocols for EVs found in the literature are based on anonymous authentication methods. To achieve location privacy, it is recommended in [14] that EVs use different authenticated pseudonyms for different transactions, and the pseudonyms should not be associated with the original identity of its owner, except by a regional or national authority [14]. However, different methods focus on different aspects such as revocable anonymity for malicious EVs, batch authentication to reduce delay, authentication based on battery status, context-awareness, etc.

The authors in [26] have identified the privacy issues associated with the V2G interactions and proposed a reward-based incentive mechanism for EVs working as service provider. In this method, the EVs use permits generated with an ID-based partially blind digital signature method [28]. The permit is used for anonymous transactions with a local aggregator. It is suggested that the EVs receive the payments in E-cash which should be used in exchange of maintenance services of the vehicle. This method aims to achieve privacy of an EV as service provider when it provides ancillary services to the grid. However, this method does not address privacy of an EV as a consumer against the energy utility.

In [32], the authors propose an anonymous protocol for roaming EVs. This method addresses charging by multiple users of the same vehicle and fair billing to different hosts of electricity. The EVs receive signed pseudonyms from the electricity supplier, utilizes the pseudonyms to authenticate to a CS and generates anonymous billing statements. Thus, the identity of the owner
is hidden from the CS. However, in this method, the electricity supplier of an EV can correlate its pseudonyms, charging sessions and original identity.

In [27], an anonymous authentication method is proposed in which the anonymity of malicious EVs can be revoked. In the network setup considered in this paper, the EVs register with a Certificate Authority (CA), and a Department of Motor Vehicles (DMV). The encrypted ID of the EV is shared with these two entities with a threshold secret sharing scheme such that two out of three shares can be used to recover the ID. The EV receives a certificate from the CA, which is used to collect tokens and pseudonyms from a CS. The pseudonyms are used to schedule and participate in a charging event, thus, the identity of the EV is hidden from the CS. If the EV does not arrive at a pre-scheduled time, it is considered as malicious. The CA and the DMV recover the identity of this “now labeled” malicious EV and the EV is blacklisted. The proposed method assumes that the DMV and the CA are always online and the CA needs to participate in the protocol every time an EV charges. The revocation mechanism assumes that not arriving at the scheduled time always means that the vehicle is malicious.

A privacy-preserving authentication protocol named Portunes+ for dynamic contactless EV charging is proposed in [33]. Dynamic contactless charging enables moving EVs to charge while driving with contiguous charging pads installed in a roadbed. The system considered in this paper consists of Charging Service Providers (CSP), charging Pad Owners (PO) and Electric Vehicles (EVs). This paper addresses fast authentication mechanism between an EV and a charging section, and considers the CSP and the PO as trusted entities. The EVs use pseudonyms in the transactions to achieve privacy against external attackers. However, this method does not address privacy against internal entities.

Authors in [16] propose a batch authentication protocol to meet the stringent timing requirement in a V2G communication. In this paper, control centers perform real-time monitoring of the grid and an aggregator collects data and manages charging/discharging events of EVs. The EVs are considered as both consumer and supplier of energy. The proposed method allows the aggregator to check the authenticity of a batch of EVs before they participate in an event. However, this method does not address privacy of EVs
against the aggregator.

In [29], an authentication method based on different battery statuses (i.e., charging, discharging, or fully charged) is proposed. The EVs can play the role as energy provider or consumer, and their power transmission and communication to the grid are established via an aggregator. The roles of an EV depends on battery status, e.g., energy provider when fully charged, and consumer when charging. Depending on the role, the EVs transmit and receive different types of information to/from the aggregator. Considering these factors, this paper proposes three interlinked authentication protocols to achieve privacy of the EV. This method assumes the presence of a trusted Central Authority (CA) which participates in all the communications and performs billing services.

In [30], an anonymous authentication protocol is proposed to achieve privacy of EVs and generate anonymous receipts for energy transactions. An EV collects blind signature on tokens from the electric utility and generates pseudonyms for each token. To establish keys for the pseudonyms, this method requires the EVs to use high latency anonymizer such as MIX or TOR. Additionally, to generate anonymous receipts, the EVs are required to use group signatures or anonymous network (e.g., TOR). However, this requirement demands significant change in the communication infrastructure, or computationally intensive or time consuming operations by the EVs.

The work in [19] proposes a Real-Time Smart Load Management (RT-SLM) algorithm for coordinating charging activities of groups of EVs. The RT-SLM algorithm focuses on reducing system stress impacting grid reliability, security and performance while enabling EVs to perform fast charging. This algorithm addresses cost minimization and voltage profile improvement and does not address privacy of the EVs.

Authors in [11] propose a decentralized authentication mechanism for Plug-in Electric Vehicle (PEV) to address the issues associated with centralized authentication systems. However, the adversarial model considered in this paper includes external attackers. The proposed method does not address privacy against internal entities or service providers.

An authentication method based on partially blind digital signature and certificateless public key cryptography is proposed in [34]. In this method,
EVs use pseudonyms to communicate with local aggregator before accessing V2G network to achieve privacy. However, this approach does not consider roaming mode of EVs.

The authentication protocol proposed in [35] considers EVs in home mode and visiting mode, which is similar to the method proposed in this work. However, this method requires the presence of a virtual battery vehicle for the privacy preservation. Moreover, this work does not consider the flexibility of charging schedules for roaming EVs and differs in the authentication mechanism.

2.2 Network Setups and Adversarial Models Considered in the Literature

The NIST introduced an abstract model for smart grid infrastructure in [7]. The works in the literature considers different network models based on the goal and adversarial model of the proposed methods. The mechanism of an anonymous authentication method depends on the adversarial model. Depending on the adversarial model, entities in a network setup are considered as trusted or adversary. Some methods in the literature considers entities in the network setup as trusted and not deviating from the protocol (e.g., [33]). In some methods, entities are considered as semi-trusted or untrustworthy, which do not have enough information to breach privacy (e.g., [27]).

The V2G communication system considered in [36] is comprised by three entities: users, network nodes, and authorities. Authorities are trusted entities which issue and manage the identities and credentials for other entities in the network. Users are the owner or individuals operating the EVs. Network nodes are the processes that run on the computing devices (e.g., Road-Side Units (RSUs), EVs, etc.) with wireless communication capability.

Authors in [11] proposed a peer-to-peer cross-certification method for communication between power systems across international borders to enable each authority to achieve maximum control over its own territory. The
multi-domain network architecture in this paper considers the presence of an aggregator which works as the liaison between EVs and energy suppliers. It is assumed that the CSs are involved in constant communication with the aggregator. The network setup also considers the presence of an Independent System Operator (ISO) or a Regional Transmission Organization (RTO), and Energy Service Providers (ESPs). The ISO/RTO operates and controls the bulk power system, and the ESPs supply electricity to the consumer domain. The aggregator assembles groups of EVs and coordinates with other entities, to provide DER services. To enable the ISO/RTO to validate the transactions of the EVs, the aggregator is assumed to be able to identify locations of the EVs.

The method in [5] considers a V2G network consisting of Battery Vehicles (BVs), Local Aggregators (LAGs), and a Central Authority (CA). A LAG communicates with the power distribution network and works as the service access point for the BVs. A LAG collects information from the BVs and manages the charging/discharging events, monitors power status, and schedules the load.

The work in [13] proposes a centralized approach for charging of EVs. The entities considered in this approach are a Charging Service Provider (CSP) or EV aggregator, a Distributed System Operator (DSO) and an Electricity Retailer (RET). The DSO is in charge of managing the distribution grid to avoid overloading. Also, depending on the power usage propositions of the RET and the information of grid congestion transmitted by the DSO, the CSP schedules individual charging events for the EVs. Depending on the information transmitted by the customer vehicles, the CSP determines a preferred aggregated load curve. The preferred aggregated load curve is then used to minimize energy cost, as well as, to avoid grid congestion. This work proposes that the CSP can work as a RET if it does not have sufficient number of EVs to bid for ancillary services.

In [37], the entities considered in the V2G interaction are the grid operators, the energy providers, the aggregators and the EVs. The aggregators are considered as the adversary and this method considers collusion among multiple aggregators to find the identity of the owner of an EV. The adversarial model considered in [32] consists of the CSs. An Electricity Supplier
(ES) is considered as a trusted entity, which is aware of a charging session of an EV and provides signed pseudonyms to the EVs for anonymous transactions with the CSs. In [27], the entities considered in the framework are a Certificate Authority (CA), a Department of Motor Vehicles (DMV), the EVs and the CSs. Both the CA and the DMV participate in the vehicle registration, pseudonym collection and signing. The DMV and the CA are semi-trusted, that is, both of them need to cooperate to recover the identity of the owner of an EV. The identity of the EV is hidden from the CS and can be revoked by the DMV and the CA, in case of malicious behavior. The network model in [26] considers a Central Aggregator (CAG), Local Aggregators (LAGs), individual Battery Vehicles (BVs), and a Trusted Authority (TA). The LAGs monitor groups of BVs and the CA participates in the load-demand management of the grid. The TA is trusted by all the other parties. There is no direct trust relationship between individual BVs and the CAG or the LAGs, as they belong to different organizations. On the other hand, the method proposed in [33] considers Charging Service Providers (CSP), charging Pad Owners (PO) and EVs in the network setup, where CSP and PO are trusted entities.
Chapter 3

Background

3.1 Blind Digital Signature

The Blind Digital Signature (BDS) method [38] enables a user to get signature on a message without revealing the content of the message to the signer. In a fully blind signature method, a signer knows nothing about the message [1]. In this subsection, a BDS method based on the RSA encryption scheme is described.

Suppose, the signer has a (public, private) key pair \((pk, sk)\) for signing purposes only, where \(pk\) is publicly known, and \(sk\) is known only to the signer. According to the RSA algorithm, a signature on a message \(m\) is \(\sigma(m) = m^{sk} \mod N\), where \(N\) is publicly known. If a verifier needs to check the signature, \(\sigma(m)\) is raised to the signer’s public key \(pk\). Due to the relation between a public-private key pair generated by RSA algorithm, a valid signature follows, \((\sigma(m))^{pk} \mod N = (m^{sk})^{pk} \mod N = m \mod N\).

In the BDS method, the user generates a random value \(r\) such that \(gcd(r, N) = 1\). Here, \(r\) works as a blinding factor to mask the original message, i.e., \(masked(m) = m \times r^{pk} \mod N\). The signer signs the masked message instead of the original message. As a result, the content of the message is hidden from the signer.

\[
\sigma(masked(m)) = (masked(m))^{sk} \mod N
\]
The user unblinds the signed masked message and extracts the signed original message as follows.

\[ \sigma(m) = \sigma(\text{masked}(m)) \times r^{-1} \mod N \]
\[ = (m \times r^{pk})^{sk} \times r^{-1} \mod N \]
\[ = m^{sk} \times r \times r^{-1} \mod N \]
\[ = m^{sk} \mod N \]

Blind signatures can be classified into two categories, 1) Certificate (CA)-based: a CA generates key pairs for the entities in the network, and 2) ID-based: the ID of an entity is used as the public key. The implementation of BDS methods in V2G networks is simple, and the communication overload depends on the complexity of the authentication process [1]. In this work, the theory of a BDS method is used in the pseudonym and token generation process, to achieve anonymity. However, the simulation results do not include the implementation of BDS method and its impact on the computation and communication process.

3.2 Partially Blind Signature

The Partially Blind Signature (PBS) method [39] is a variant of the BDS method. This method differs from BDS such that the signer and the user can agree on a common message [1]. The signature is done on the common message and the blinded message. Suppose, \( info \) is the agreed common information. A public hash function is used to transform \( info \) into a random public key, i.e., \( pk' = hash(info) \), whose private key is not known publicly. The signer signs the blinded message and \( hash(info) \) with its private key, \( sk \). The signatures are bound to the public key \( pk \). As a result, \( hash(info) \) is also bound to the signature but remains unblind [39]. In restrictive partially blind signature methods, the message needs to follow rules agreed by the signer and the user.
3.3 Degree of Anonymity

The definition of privacy adopted by the NIST is “The right to be left alone” [25]. However, a metric is required to quantify the privacy (or, anonymity) achieved in different scenarios or methods. According to the definition of Pfitzmann and Köhntopp, anonymity is to be unidentifiable within an anonymity set [40]. Anonymity set is the set of users with a possibility of performing an action in a system, i.e., senders, receivers, or, in this case, charging/discharging EVs. A user’s probability of being in the anonymity set is assigned by an adversary. This is because, based on the behavior of the users in a system, every user has a probability of doing an action, perceived by the adversary.

Degree of Anonymity (DoA) is a metric representing the level of anonymity achieved by the users of an anonymous system. The authors in [41] have defined the DoA as $1 - p$, where $p$ is the probability assigned by the adversary to a user. In other terms, if a user has the probability $p$ (perceived by the adversary) of doing an action, then s/he has $1 - p$ probability of not doing it. Hence, the user gets a DoA of $1 - p$ against the adversary. If $p = 1$, for doing an action by a user, then s/he has a DoA $= 0$ and no privacy in the system. However, this metric represents the anonymity achieved by an individual user in the system. Therefore, it is not useful to represent the comparative anonymity achieved by the entities in the anonymity set [42]. For example, according to this metric, if user $i$ has $p_i < 0.5$, s/he supposedly has a good anonymity. However, if all the other users have probability $p < p_i$, user $i$ is the most probable of doing an action, thus, achieves the worst anonymity in the system.

Authors in [43] have defined the DoA as $\log_2(N)$, where $N$ is the total number of users in the system. According to this metric, all the users in a system achieve the same anonymity. This metric assumes that the adversary only has the knowledge of the value of $N$ and the probabilities associated with the users is considered as $\frac{1}{N}$. This metric does not consider the impact of probabilistic information obtained by an adversary in different types of attacks [42], which can impact the DoA achieved by individual users.
Authors in [42] and [31] proposed DoA metrics based on Shannon’s definition of entropy [44]. In general, entropy refers to the uncertainty within a system or event. According to Shannon, entropy is the maximum limit on the average length of a lossless compression of an information source [44]. In other words, the Shannon entropy indicates the maximum number of bits required to represent a message without loss. The entropy of a discrete random variable $X$ with probability mass function $p_i = Pr(X = i)$ can be represented as,

$$H(X) = - \sum_{i=1}^{N} p_i \log_2(p_i) \tag{3.1}$$

where $i$ represents every possible value taken by $X$ and $N$ is the total number of values taken by $X$.

In the metrics proposed in [42] and [31], the entropy $H(X)$ is used to represent the information contained by a system after an attack has taken place. In these metrics, $p_i$ is the probability of user $i$ being in the anonymity set (perceived by the adversary), where, $\sum_{i=1}^{N} p_i = 1$ (as the summation of probabilities of performing an action by the users in a system is 1). A system achieves maximum anonymity when all the entities in the system have equal probability of performing an action. So, the maximum entropy a system can achieve is,

$$H_{\text{max}}(X) = \log_2(N) \text{[when } p_i = p_j \ldots = p_N \text{]} \tag{3.2}$$

(3.2) is also the metric for DoA considered in [43]. The information learned by the adversary after an attack (or, observation) is $H_{\text{max}}(X) - H(X)$. In [31], the DoA is defined as,

$$\text{DoA} = H(X) = - \sum_{i=1}^{N} p_i \log_2(p_i) \tag{3.3}$$

On the other hand, in [42], the DoA is represented after normalizing by the
maximum entropy, as shown below.

$$\text{DoA} = 1 - \frac{H_{\text{max}}(X) - H(X)}{H_{\text{max}}(X)} = \frac{H(X)}{H_{\text{max}}(X)} = -\frac{\sum_{i=1}^{N} p_i \log_2(p_i)}{\log_2(N)}$$  \quad (3.4)

The metrics in (3.3) and (3.4) are applicable for cases when the entities in the anonymity set have different probabilities.

In a system of $N$ users, if an adversary isolates $S$ number of entities as possible members of the anonymity set, then, the other $N - S$ entities have zero probability of performing an action. If each of the $S$ entities has equal probability, the DoA of the system will be $\log_2(S)$ (according to [31]) or $\frac{\log_2(S)}{\log_2(N)}$ (according to [42]). The normalized DoA metric is useful for comparing a system with an ideal anonymous system [42]. An anonymous system is considered as ideal when the only information known to an adversary is the number of users in the system. The normalized DoA metric represents how much information is leaked in different attacks compared to the ideal situation. However, in this work, the metric proposed in [31] is used, i.e.,

$$\text{DoA} = \log_2(S)[p_i = p_j = ... = p_S]$$  \quad (3.5)

This is because, as EVs are roaming entities, the maximum number of entities in a particular region is random (i.e., $N$ is variable). Moreover, the probabilities of different entities depend on the type of attack [42] and the method proposed in this thesis does not focus on the impact of different attacks on the anonymity. As a result, it is assumed that all the entities in the anonymity set have equal probability. This metric depends on the size of the anonymity set, i.e., the larger the anonymity set the higher the DoA. Ideally, in a V2G communication using pseudonyms, it should be impossible for any observer to distinguish between the EVs in a charging/discharging event as pseudonyms are used for short-term and are changed periodically [3].
Chapter 4

System Model

4.1 Network Setup and Adversarial Model

In the electrical power grid, usually a single Electric Utility (EU) provides services to groups of consumers in a regional area [26]. For example, according to the Department of Public Service in New York state, in the city of Syracuse, Pennsylvania, and Rochester, electricity is supplied by the National Grid, the Pennsylvania Electric Company, and the Rochester Gas & Electric Corp., respectively. The EU in a region perform the billing, energy supply, maintenance services for its customers. In this paper, it is assumed that every EV is subscribed to an EU which is referred to as the primary EU ($EU_{pr}$) for its subscribers. An $EU_{pr}$ is interested in providing services to its own customers, hence, it manages the charging events of its subscriber EVs by communicating with different CSs. The charging events are performed at different geographically dispersed CSs which receive the energy from the EU in its region. For a roaming EV, when it moves to an area which is supervised by another EU other than its $EU_{pr}$, this EU is referred to as the visited EU ($EU_v$) for this EV.

In the proposed method, an EV schedules a charging event via an EU. However, the aim is to prevent any service provider (i.e., an EU, or a CS) from correlating the charging events of an EV to its owner’s identity. In the proposed method, every regional area under the supervision of an $EU_{pr}$ is further divided into zones of smaller areas. Each zone is supervised by a subsidiary entity ($EU_{sub}$). All the $EU_{sub}$s in a region are maintained by the $EU_{pr}$ of that region. However, the division of a large area into smaller zones denotes the division of information system (e.g., database, servers,
Figure 4.1: An example of the proposed network setup

etc.) rather than the electricity service. The motivations behind the subdivision are, 1) micro-management of smaller zones for efficient operation, 2) better scalability, 3) limited access to information of EVs, thus, better privacy and anonymity, etc. In the heterogeneous power system, sometimes, companies are integrated vertically and become part of a single entity [13] as it reduces communication overload. In this case, the different companies provide different services to the customers. However, entity owning the companies can possibly possess the information owned by the individual companies.

According to the proposed network setup, every regional $EU_{pr}$ has sub-utilities in charge of the information management of the EVs in small zones, i.e., $EU_{sub}^1$, $EU_{sub}^2$, and $EU_{sub}^3$ supervise zone 1, zone 2 and zone 3, respectively. The scheduling of charging events in each zone is managed by its supervising $EU_{sub}$. In other words, when an EV moves from one zone to another zone to participate in charging events, the management of the event is ‘handed over’ to a new $EU_{sub}$. On the other hand, the CSs in a different regional area receive energy services from the supervising EU in that area. Hence, when a roaming EV moves from one regional area to another, the scheduling of events is handed over to the visited EU ($EU_v$). In the proposed
method, an $EU_{pr}$ provides the authentication credentials to its valid customers to communicate with an $EU_{sub}$ or an $EU_v$, and the $EU_v$ provides the required credentials to the valid roaming EVs to schedule charging events with the CSs under its supervision. In this hierarchical approach, each entity (an $EU_v$, an $EU_{sub}$, or a CS) is capable of checking the authenticity of an EV participating in a charging event without knowing the original identity of its owner.

Fig. 4.1 shows an example of the proposed network setup in this work. An EV participates in charging events at different CSs on its route. In this figure, the CSs are situated in different zones (i.e., zone $i$, zone $j$, zone $k$, and zone $l$) and the zones are supervised by different $EU_{sub}$s (i.e., $EU_{sub}^i$, $EU_{sub}^j$, $EU_{sub}^k$, and $EU_{sub}^l$). Different zones are part of a larger regional area and the $EU_{sub}$s in different zones are supervised by the $EU_{pr}$ in the regional area (i.e., $EU_{pr}$ and $EU_v$).

The majority of the work in the literature considers the presence of a data aggregator which collects information from the entities in the grid and provides the data to the utilities such as EU, grid operator, etc. However, the scheduling of charging events in the proposed method does not include interaction between an EV and the aggregator. Hence, an aggregator is not included in the network setup considered in this work.

The adversarial model considers the EU and the CS as internal and honest-but-curious adversaries [36]. Internal adversaries are equipped with certain credentials and they participate in the execution of protocols [36]. The honest-but-curious model assumes that these entities do not deviate from the specified protocol but are interested in finding information about the owner of an EV. The EU, and the CS are part of the same or different organizations.

### 4.2 Assumptions

1. The entities in the network setup are equipped with trusted components, i.e., built-in hardware and firmware capable of performing cryptographic operations [36].

2. Standard security protocols are followed in the communication among
the entities. For example, transmitted messages are encrypted with a reliable encryption scheme (e.g., AES), mutual keys are set up with a secure key setup protocol (e.g., Implicitly Authenticated DHKE protocol), etc. The security standards also depend on the underlying protocol. For instance, Zigbee Smart Energy specification recommends employing Elliptical Curve Cryptography (ECC) in cryptographic authentication and key generation for secure, efficient, and low-bandwidth networking.

3. The simulation considers the arrival of EVs as a random Poisson distribution. The charging events follow a standard M/M/1 queue system. The impact of factors such as electricity price, time of the day (i.e., peak/off-peak hour), load-demand condition, etc., on the arrival rate is not considered in the experiment.

4. An EV and its owner are considered as the same entity, and these two terms are used interchangeably.

5. There are more than one EV requesting the scheduling of charging events to an EU, (i.e., $EU_{pr}$, $EU_{sub}$, or $EU_v$). This assumption is practical, as the Electric Power Research Institute (EPRI) projects that by the year of 2050, 62% of the vehicles in the U.S. will consist of PHEVs/PEVs [9]. In many countries, the transformation towards EVs is emphasized. For example, in the U.K., it is announced that new gas or disel fueled vehicles will not be allowed after year 2040. The total EV penetration is predicted to be small, however, the possibility of localized concentrations is high. The study in [45] concludes that EV loads are likely to be clustered in certain areas.

6. The individual EVs own multiple tokens or pseudonyms to achieve anonymity. Each of the tokens or the pseudonyms should have separate certified public keys so that no transaction can be linked to the original identity of the owner. Different credentials are used for different transactions. These are standard assumptions in the literature [3], [27].
7. Tasks such as certification, authenticating public keys, etc. require the presence of a Certification Authority (CA) which is recognized and trusted by the entities in the network. In this work, the presence of the CA is implicit and assumed to follow procedures as specified by the underlying communication standards [14].
Chapter 5

Methodology

In this chapter, the different phases in the proposed method of scheduling flexible charging events are described. The method aims to enable the EVs to anonymously communicate with different entities other than its $EU_{pr}$ (i.e., an $EU_{sub}$, an $EU_{v}$ or a CS), and simultaneously enable the entities to check its authenticity. An $EU_{pr}$ provides the authentication credentials to its subscribed EVs for this purpose. An EV is considered as valid if it is registered with an electric utility. As a result, the signature of an $EU_{pr}$ on an EV’s credentials is verified by a network entity to check the authenticity of an anonymous vehicle. An $EU_{pr}$ participates in the signing process of anonymous tokens for its registered EVs or a valid roaming EV, to enable it to communicate with an $EU_{sub}$ under its supervision. On the other hand, $EU_{sub}$s participate in the signing of pseudonyms of an authentic EV to enable it to communicate with the CSs under its supervision. The flexible charging method enables the EVs to participate in charging events with CSs within a scheduled timing window as well as before and after the scheduled timing window. Fig. 5.1 shows the sequence of events participated by an EV and the corresponding network entities, in the proposed method.

**Registration and Token Collection:** We assume that after a customer purchases an EV, the vehicle is registered with an EU as a valid energy subscriber with its original information such as the owner’s name, address, Vehicle Identification Number (VIN), etc. After the registration, an EV and its $EU_{pr}$ agree on the authentication credentials (i.e., ID and password for online account, mutual keys, etc.) for future communication. The scheduling of charging events is done via different $EU_{sub}$s and an EV uses an authenticated token to anonymously communicate with an $EU_{sub}$. The EV receives
the list of supervising $EU_{sub}$ of different zones from the $EU_{pr}$. Furthermore, it is assumed that the owner of an EV knows about its approximate movement in the upcoming days. This means the owner is aware of the battery status, the need for charging and the tentative route along which s/he prefers to charge the vehicle.

After selecting a route, depending on the price information received from the grid and the SoC, the owner of the EV decides on the timing window and the preferred zone for charging. The preferred zone for charging is not necessarily the first zone in the route selected by a customer. The selection of preferred zone depends on the battery status of the EV and price of electricity at time of arrival at a CS. If a route selected by an EV goes through $x$ number of zones, it requires maximum $x$ number of random tokens ($\Phi_{sub}$) for the $EU_{sub}$s in these zones. Two cases of token collection for a route are considered: 1) the first preferred zone is under the supervision of the $EU_{pr}$, or 2) the first preferred zone is under the supervision of an EU in a different region. In both cases, the EV generates a random token and blinds it with a random value. The EV and the $EU_{pr}$ mutually agree on a common $Info$, which includes the time frame for which the token is valid. The validity time frame of the token is different from the timing window (TW) for charging and should be long enough to allow an EV to schedule charging events within its planned trip. Next, the $EU_{pr}$ signs the masked token and the common $Info$ with a PBS method. In the first case, the signed token is used to communicate with the $EU_{sub}$ in the first preferred zone. In the second case, the signed token is used to communicate with the visiting EU
Selection of CSs: If the preferred CS is situated in a zone under the supervision of the $EU_{pr}$ of the EV, it sends an authentication request to the $EU_{sub}$ for scheduling a charging event.

$$EV \rightarrow EU_{sub} : Req(sch)|\Phi_{sub}|T_{val}|\sigma_{EU_{pr}}(\Phi_{sub}|T_{val})$$

where, $Req(sch)$ contains the information required for scheduling (e.g., required energy, $\varepsilon$, timing window, TW for charging, route information, etc.), $\Phi_{sub}$ is the token for the $EU_{sub}$, $T_{val}$ is the time frame during which the token is valid, and $\sigma_{EU_{pr}}$ indicates that the contents are signed by the $EU_{pr}$ supervising this area.

The $EU_{sub}$ checks the signature of its supervising $EU_{pr}$ and the validity of the token. Next, the $EU_{sub}$ checks the availability of energy within the TW at the CSs in its zone. Depending on the availability, congestion of charging events, or predicted load-demand conditions, the $EU_{sub}$ selects a set of available CSs. Suppose, the CSs are recognized by different identifiers ($ID_{CS}$), which are unique in an area. The $E_{sub}$ creates a message ($M_{cs}$) consisting of $\varepsilon$, TW, and $ID_{CS}$ for each of the available CSs, and sends the messages to the $EU_{pr}$. The $EU_{pr}$ signs the messages using its private key and sends them back to the $EU_{sub}$.

$$\sigma_{EU_{pr}}(M_{cs}) = \sigma_{EU_{pr}}(\varepsilon||TW||ID_{CS})$$

Next, the $EU_{sub}$ sends the $M_{cs}$ and the signed $M_{cs}$ to the EV.

If the first zone is under the supervision of a different supervising EU ($EU_{v}$), the EV authenticates itself to the $EU_{v}$ using the token signed from its $EU_{pr}$. The $EU_{v}$ provides the required credentials to communicate with
the \textit{EU}_{\text{sub}s} under its supervision. The communication with the \textit{EU}_{\text{sub}s} in the visited zone follows the same procedure as described before. Fig. 5.3 shows the steps followed in the selection of CSs phase, where, the events are executed according to the order of the numbers on the arrows following them. The tasks in the square boxes are performed by the corresponding entity.

**Scheduling of Charging Events:** In this phase, the EV generates a set of pseudonyms for each of the selected CSs and the \textit{EU}_{\text{pr}} (or, the \textit{EU}_{\text{v}}) blindly signs the pseudonyms. Next, the EV forwards the list of pseudonyms associated with each CS to the \textit{EU}_{\text{sub}}.

From the scheduling requests of the EVs in an area (assumption 5), the \textit{EU}_{\text{sub}} makes lists of CSs and the corresponding requesting pseudonyms with their \textit{TW}. For example,

\[
ID_{CS1} : \Phi_1(TW_1), \Phi_2(TW_2), \Phi_3(TW_3) \\
ID_{CS2} : \Phi_2(TW_2), \Phi_3(TW_3) \\
ID_{CS3} : \Phi_1(TW_1), \Phi_3(TW_3)
\]

where, \(ID_{CS1}, ID_{CS2}, ID_{CS3}\) are the IDs of different CSs and \(\Phi_1, \Phi_2, \Phi_3\) are the pseudonyms belonging to the same or different EVs, and the \(TW_1, TW_2, TW_3\) are the corresponding charging time window of the requested charging events. Next, the \textit{EU}_{\text{sub}} forwards the set of pseudonyms and \(TW\)
After the communication with an $EU_{sub}$, the EV generates, blinds and sends a random token to the current $EU_{sub}$. The $EU_{sub}$ forwards the blind token to its supervising $EU_{pr}$ and receives the required credentials (e.g., signed token, validity time frame). Next, the credentials are forwarded to the EV which uses them for scheduling the next charging event via next $EU_{sub}$.

**Participation in Charging Events:** For a moving EV, there can be multiple routes to a destination. After an EV schedules for charging event, the available CSs distributed along its potential routes have the set of valid pseudonyms. The maximum distance ($d_{max}$) a moving EV can travel can be determined based on the current State-of-Charge (SoC), as $d_{max} \propto$ SoC. Depending on the value of $d_{max}$, the EV selects a CS and calculates the expected arrival time, $t_{exp} = \frac{d}{v}$, where, $v$ is the speed of the EV and $d \leq d_{max}$ is the distance from the CS. In current technology, smartphone navigation applications are fairly accurate in predicting the time of arrivals considering factors such as traffic conditions. The EV sends a request for participation in a charging event. The request consists of a signed pseudonym, $t_{exp}$ and the required energy ($\varepsilon$).

$$EV \rightarrow CS : \Phi_i || \sigma_{EU_{pr}}(\Phi_i) || t_{exp} || \varepsilon$$

The CS checks the signature of $EU_{pr}$ on the pseudonym. The CS also has
the TW associated with this pseudonym (received from the $EU_{sub}$). If this signature is valid and if $t_{exp}$ is within the TW, this request is considered as valid. After the EV arrives at the CS, it participates in the charging event.

**Flexible Charging Operation:** If an EV does not arrive at a pre-scheduled event, it causes the CS some monetary loss because of the reserved time and energy. In this paper, we assume that in case of failing to meet a schedule, a penalty cost ($C_P$) is paid to the CS. The $C_P$ can be a fixed percentage of the electricity price (real-time or scheduled). Suppose, an EV reserved a charging event for $U$ units of energy. The scheduled price ($P_{Sch}$) is referred to as the price of electricity determined when the charging event was scheduled and real-time price ($P_{RT}$) is the electricity price when bought without scheduling. If the EV pays a flat penalty cost for each of the missed CSs, total penalty cost for missing $m$ number of CSs is $m \times C_P$. The EV can afford to miss a scheduled charging event if the summation of total scheduled energy cost and the total penalty cost is less than the total real-time energy cost,

$$U \times P_{Sch} + \sum_{i=1}^{m} C_P(i) \leq U \times P_{RT} \quad (5.1)$$

where, $C_P(i)$ is the penalty cost for CS$i$. The maximum number of missed CSs that can be afforded by the EV is the value of $m$ for which the left side of the equation is equal to the right side.

In this work, three stages for the arrival of an EV are considered, 1) Timing Window (TW): the EV arrives at a CS within the designated TW, 2) Pre-Arrival (PrA): the EV arrives at a CS before its TW, and 3) Post-Arrival (PoA): The EV arrives at a CS after its TW is passed. There are two cases of missing a scheduled charging event, 1) the EV misses the charging event after communicating with the CS, and there are other CSs situated on the routes which have its valid pseudonyms, 2) the EV has missed all the CSs in the pre-planned route. In the former case, the EV reschedules for charging event with another CS. In the latter case, the CSs in its actual route do not have its pseudonyms and the EV schedules a charging event with its token for the $EU_{sub}$, signed by the $EU_{pr}$ and pays real-time price for the energy.
Chapter 6

Results and Analysis

In this section, an analysis of the DoA achieved by the proposed method, cost-efficient number of missed CSs and the regional sub-division, based on MATLAB simulation, is presented. The arrival of EVs are independent and identically distributed (i.i.d.) Poisson process, and the arrival rate (\( \lambda \)) is varied from 0.1 to 0.9 at an interval of 0.2. In the plots against time slots, the X-axis shows the cumulative time slots (not the local clock time, e.g., 12AM). The DoA achieved by the system is determined by (3.5), and the cumulative number of arrivals is considered as the anonymity set in each time slot.

6.1 Variation of DoA in the Proposed Method

Fig. 6.1 demonstrates the variation of DoA with varying \( \lambda \), in the Pre-Arrival (PrA), Timing Window (TW) and Post-Arrival (PoA) stages of the proposed method, from the perspective of a roaming EV. In other words, this plot demonstrates the DoA achieved by an EV when it arrives at a CS in the PrA, TW or PoA. Each curve in the figure corresponds to the DoA achieved for a different \( \lambda \). The value of \( \lambda \) corresponds to the number of arrivals, which in turn determines the size of the anonymity set (i.e., DoA). It can be assumed that the EVs are interested in participating in a charging event within its TW to avoid the penalty cost. Moreover, each EV generates a single token to communicate with an \( EU_{sub} \) or an \( EU_{pr} \), and multiple pseudonyms for a CS. As a result, the number of participations using pseudonyms is larger than the number of participations using tokens. Therefore, in Fig. 6.1, the \( \lambda \) shown in the legends are the arrival rates in the TW,
and the arrival rates in the other two stages vary at a lower rate. It should be noted that these different values of $\lambda$s do not indicate that the arrival rate in an area varies, rather, the number of transactions using token (in PrA and PoA) or pseudonyms (in TW). The legends in the figure show the total number of EVs that arrived in the three stages. The number of entities in an anonymity set is represented by the number of possible customers participating in the transactions in a stage. Therefore, in Fig. 6.1, as more EVs arrive in the cumulative time slots in each stage, the size of the anonymity set increases, hence, the DoA increases. Similarly, a higher $\lambda$ yields a higher number of arrivals, thus, higher DoA. An EV achieves higher DoA if it arrives within its own TW, and lower DoA if arrives earlier or later than the TW.

6.2 Number of Missed CSs w.r.t. Electricity Price

Fig. 6.2 shows the variation of number of missed CSs allowed by the proposed method w.r.t. the electricity price (real time and scheduled), and the penalty cost. The allowed number of missed CSs means the maximum
number of CSs an EV can miss when the price is cost-effective, i.e., \((\text{total } P_{Sch} + \text{total } C_P) \leq \text{total } P_{RT}\), which is derived from (5.1). The X-axis shows the percentage of the \(P_{RT}\) that equals the \(P_{Sch}\), where price is the total price and not the per unit price. In existing literature, it is assumed that the information of \(P_{RT}\) is frequently broadcast to an EV. Depending on this price, an EV can decide on the number of CSs it can miss without spending more than the electricity price.

### 6.3 Sub-division of a Regional Area

In this work, a network setup that sub-divides a region into smaller zones (under the supervision of different \(EU_{subs}\)), is proposed. One of the motivations behind this network setup is to prevent a single entity (e.g., \(EU_{pr}\)) from having enough information to correlate multiple transactions by an EV (using tokens or pseudonyms) to its owner’s original identity. Suppose, there is no sub-division in an area. An EV collects blind tokens and schedules a charging event via the \(EU_{pr}\). If the time interval between the collection of token and scheduling is short, there might be cases when no other EV has scheduled an appointment. As a result, it would be possible for the
Figure 6.3: Determining the number of EVs in a sub-divided zone

EU_{pr} to correlate this charging event with the identity of the owner of the EV, although, s/he used a blind token. On the other hand, in the proposed network setup, an EV collects a token from the EU_{pr} for the first EU_{sub} on its route. Later, it collects tokens from one EU_{sub} to communicate with the next EU_{sub}. As a result, if an EU_{pr} needs to correlate all the charging events of this EV, it needs to prevent all the EVs under the supervision of these EU_{subs} from scheduling.

In this subsection, the proposed method to determine the size of the sub-divided areas w.r.t. λ and DoA is studied based on the simulation results shown in Fig. 6.3 and 6.4. The arrival of EVs in Fig. 6.3 is shown for one of the three stages (e.g., PrA, TW or PoA).

Fig. 6.3a shows the probability density function (pdf) of the arrival of EVs for varying λ, represented as normal distribution. Each of the curves corresponds to an arrival rate and extends from its mean to (3× standard deviation) on each side. Fig. 6.3b depicts the cumulative distribution function (cdf) of the same arrivals w.r.t. different λ. The cdf represents the probability that the mean number of arrivals (S_{mean}) in a time slot is less than a certain value. For example, for an arrival rate of 0.1, the probability that S_{mean} is less than 10 is 1, i.e., \( \text{Prob}(S_{\text{mean}} < 10) = 1 \). On the other hand, for an arrival rate of 0.9, \( \text{Prob}(S_{\text{mean}} < 40) = 1 \), \( \text{Prob}(S_{\text{mean}} < 15) = 0.05 \), \( \text{Prob}(S_{\text{mean}} < 10) = 0 \), and so on. Similarly, for an arrival rate
Fig. 6.4: Determining the number of EVs in a subdivided zone of \( \lambda = 0.7 \), \( \text{Prob}(S_{\text{mean}} < 15) = 0.1 \) and \( \text{Prob}(S_{\text{mean}} < 10) = 0 \).

The values from Fig. 6.3b are used to show the variation of probabilities of different \( S_{\text{mean}} \) w.r.t. \( \lambda \) in Fig. 6.4a. Fig. 6.4b, on the other hand, shows the DoA achieved for different \( \lambda \) and the DoA achieved in an ideal scenario is assumed as ideal when the total number of arrivals in cumulative time slots is equal to the maximum number of EVs (\( \lambda \)) scheduling charging events at the CSs in a region.

From Fig. 6.4a, it can be seen that a \( \lambda \) of 0.7 has a higher probability of achieving the threshold \( S_{\text{mean}} \). Therefore, the desired \( S_{\text{mean}} \) (i.e., DoA) is not achieved. In Fig. 6.4b, the total number of arrived EVs for \( \lambda = 0.7 \) and \( \lambda = 0.9 \) are 198 and 212, respectively.

Without loss of generality, suppose based on statistical data, the maximum number of arrivals in each time slot is 330. For an ideal scenario, the number of arrivals of EVs in each time slot equals to \( S_{\text{mean}} \). If the DoA achieved in the first time slot in the ideal case, and the minimum desirable DoA in the system is 0.8 of \( d_{\text{ideal}} \) or 80% of \( d_{\text{ideal}} \), then, desired \( S_{\text{mean}} \) is \( \approx 15 \).

From Fig. 6.4a, it can be seen that a \( \lambda \) of 0.3 never achieves a mean arrival of 15. On the other hand, a \( \lambda \) of 0.7 has a higher probability of achieving the threshold \( S_{\text{mean}} \). Therefore, the desired \( S_{\text{mean}} \) (i.e., DoA) is not achieved. In Fig. 6.4b, the total number of arrived EVs for \( \lambda = 0.7 \) and \( \lambda = 0.9 \) are 198 and 212, respectively.
As a result, the sub-division of a region into smaller zones should be such that the number of EVs in a zone is on average $200 \sim 300$, to achieve the desired DoA.

Another method of determining the number of EVs in a zone is to compare the DoA in different cases. In Fig. 6.4b, the curves associated with $\lambda = 0.1$ and $\lambda = 0.3$ achieves lower DoA than the desired $80\%$ DoA, i.e., the cyan (curve with triangle marker) and orange curves (curve with rectangle marker) are lower than the red curve (curve with asterisk marker). The DoA achieved by $\lambda = 0.5$ is less than the desired DoA in $40\%$ (approx.) of the time. On the other hand, the DoA achieved by $\lambda = 0.7$ and $\lambda = 0.9$ are more than the minimum desired DoA in approximately $88\%$ and $90\%$ of the time. Hence, the desired arrival rate is $0.7$ or $0.9$. Consequently, we get the same conclusion.

Fig. 6.5 summarizes the steps of the proposed method of sub-dividing a regional area into smaller zones to achieve a desired level of DoA. In this figure, the ascending numbers indicate the consecutive steps of the proposed method.
Chapter 7

Future Works

In this work, a privacy-preserving method to authenticate anonymous EVs in the SG is proposed. The proposed method also provides flexibility in charging schedules to provide flexibility in charging by the EVs and compensate monetary loss to the CSs for missed charging events by EVs. However, in the MATLAB simulation in this work, the impact of factors such as dynamic pricing, load-demand, etc. has not been considered. These factors are likely to have an impact on the arrivals of EVs in charging events, thus, in DoA. An investigation of the variation of anonymity w.r.t. grid conditions is part of the future work.

In the proposed network setup in this work, a method to sub-divide large regional area into smaller zones is proposed to achieve improved privacy. In future work, a comparative analysis (theoretical, mathematical or experimental) of the anonymity achieved in the sub-divided network setup and a network setup without sub-division will be conducted. Additionally, an analysis of the impact of dynamic pricing and load-demand on the cost-effective number of missed CSs is also part of the future work.
Chapter 8

Conclusion

The efficiency of the operations in the smart grid depends on the ancillary services and information provided by the heterogeneous entities connected to it. The threat to consumer privacy in the SG is likely to discourage consumer participation in the grid operation. To maximize the facilities offered by different SG features, privacy-preserving methods should be embedded in the communication and information system in the grid. In this work, a method is proposed to achieve privacy of the EVs participating in charging events. Additionally, the method addresses flexible charging schedules for EVs. Simulation results are presented to show the variation of Degree of Anonymity (DoA) at different stages of the proposed method, and cost-effective number of missed CSs. Moreover, a network setup is proposed to achieve better privacy by sub-dividing a regional area into smaller zones. A method is demonstrated to determine the size of a sub-divided zone from the simulation results depending on the desired DoA. Future works will focus on analyzing the impact of factors such as electricity price, demand, etc., and the sub-division of an area on the achieved DoA.
Bibliography


