The Count of EV Charging: Attacking, Mitigating and Reenvisioning the Infrastructure

Hossam ElHussini

A Thesis

in

The Department

of

Electrical and Computer Engineering

Presented in Partial Fulfillment of the Requirements

for the Degree of

Master of Applied Science (Electrical and Computer Engineering) at

Concordia University

Montréal, Québec, Canada

May 2020

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: **Hossam ElHussini**

Entitled: **The Count of EV Charging:**

Attacking, Mitigating and Reenvisioning the Infrastructure

and submitted in partial fulfillment of the requirements for the degree of

Master of Applied Science (Electrical and Computer Engineering)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the Final Examining Committee:

_____ Chair
Dr. Donyiu Qiu

_____ External Examiner
Dr. Amr Yousef

_____ Examiner
Dr. Donyiu Qiu

_____ Supervisor
Dr. Chadi Assi

_____ Co-supervisor
Dr. Ali Ghrayeb

Approved by _____
Yousef R. Shayan, Chair
Department of Electrical and Computer Engineering

_____ 2020

_____
Amir Asif, Dean
Faculty of Engineering and Computer Science

Abstract

The Count of EV Charging:
Attacking, Mitigating and Reenvisioning the Infrastructure

Hossam ElHussini

For a genuinely connected smart world, the overlapping of the Internet of Things (IoT) services from different sectors becomes inevitable. One of the rather interesting collaborations is that between Intelligent Transportation Systems (ITS) and Smart Grids. Particularly, a perfect manifestation of such integration of services is the rise of Electric Vehicles (EVs) and their charging infrastructure. Although the full integration of ITS and smart grid services would alleviate the development of self-driving intelligent vehicles, there are major challenges that are yet to be resolved, one of crucial importance is their security. To contextualize such security issues, it is essential to have a clear understanding of the status-quo of EVs and charging ecosystem. In that regard, we survey the entities, protocols, deployment types and major manufacturers of Electric Vehicles Charging Stations (EVCS) and identify the key weaknesses causing security issues. Moreover, we propose a novel attack that exploit the vulnerabilities in the EVCS to create a botnet of them, tamper their schedules and cause frequency disturbances to the power grid. In order to mitigate such an attack, we explore the role of Artificial Intelligence (AI) and Blockchain individually and collaborate in both securing the EV charging ecosystem and efficiently manage the energy trading among EVs, EVCS and power grid. Consequently, we expand on the collaboration of AI and Blockchain and propose an anomaly detection engine to detect the proposed attack demonstrating is effectiveness in flagging anomalous charging behavior. Finally, we re-envision the EV charging ecosystem by integrating both AI and Blockchain to secure both public and private EVCS from the proposed attack.

Acknowledgments

This thesis has been a unique journey, full of handwork, sleepless nights but most importantly unforgettable sense of achievement. However, as a wise man once said: All Good Things Must Come To An End. So, Thanks to everyone who has contributed in a way or another, directly or indirectly to this journey.

My deepest gratitude and appreciation goes to my supervisors: Dr. Chadi Assi and Dr. Ali Ghrayeb whom without their help, I could have never started this journey, let alone completing it.

To my friends, thank you for your support and lifting my spirits when I needed it. I would like to give special thanks to my friend: Nouha Kherraf for helping, supporting and guiding me throughout this journey, and Bassam Moussa for his support and honesty. I also give my sincere thanks to Yacine Kadri for his outstanding help and generosity.

Last but not least, I would love to thank my parents: Yasser ElHussini and Basma AlGohray for all their prayers.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Internet of Things: The Arrival

In 1906, Lewis Baumer, a cartoonist at the British humor and satire magazine; the Punch [2], drew what could only be described as a letter-perfect depiction of our lives today shown in Figure 1.1. Two people, thou "not communicating with one another", are building a relationship through "receiving an amatory message, and ... some racing results".

Figure 1.1: Lewis Baumer Illustration in the Punch in 1906

Whether this was a mere coincidence or an exquisite prophecy, the illustration portrayed two main themes that would be the most predominant in our modern lives; remote communication and human-machine interfacing. Fast forward to almost eighty years later, the Internet was born [3], marking the beginning of a new era. The promise of the Internet was to enable seamless communication through providing a decentralized, border-less and transparent medium. Steadily, the thought of communicating with another person anywhere in the globe was no longer part of science fiction but a tangible reality that shaped the last century. From the World Wide Web to Mosaic and Netscape all the way to its commercialization, the Internet was slowly but surely becoming an intrusive part of every household [4]. This revolution enabled the envisioning of novel services and technologies and paved the road for another revolution known as the Internet of Things (IoT).

The term IoT was first coined by Kevin Ashton in 1999 in an attempt to sell the RFID technology to senior management at Procter&Gamble. The gist of his presentation was that information on the Internet was human-dependent and with the inadequacies of the human nature, we will fail to coup up with collecting the tremendous amount of data being generated. With that, he proposed a turn of tables in which humans rely on computers to collect, process and share information between each other to make our lives easier [5]. What Kevin suggested at that time was a conceptual realization of the IoT paradigm that was only popularized 10 years later on 2009. In essence, the IoT paradigm encompasses the technology of embedding sensors and actuators into everyday objects, transforming them into smart objects capable of data collection, analysis, and sharing between different entities. With that abstraction in mind, these IoT devices would enable a whole new set of applications and services from intelligent transportation systems and smart cities to smart grids and Industry 4.0. However, in order to realize such services, IoT devices, both generic and application-specific, are needed in the market. Accordingly, there has been an exponential growth in the number of IoT devices since its inception in 2009. To put it in perspective, major companies such as Ericson predicted that the number of IoT devices would reach $30Bn$ devices by 2020 and would continue to grow to $50Bn$ by 2030 [6]. Nowadays, the IoT paradigm has become so intrusive that almost all households have at least one kind of smart device [7]. For instance, it is not abnormal to see a household with a smart lighting system, a voice-enabled temperature control system and a remote-controlled home surveillance system.

1.2 Electric Vehicles: The Marriage Feast

The rapid increase in the number of IoT devices coupled with advancements in communication technologies will enable more applications and services become readily available for the end user. Two examples of such services are:

1.2.1 Intelligent Transportation Systems

Intelligent Transportation Systems (ITS) are one of the interesting services that are enabled by the IoT paradigm. Typically, ITS consist of four main subsystems; vehicular, stationary, monitoring and security, each with its own functionalities and devices. For instance, the vehicular subsystem consists of IoT devices such as Global Positioning System and On Board Unit (OBU) and its main functionality is to communicate vehicle information with the other subsystems. In addition, the security subsystem is responsible for detecting malicious behavior, authenticating the different entities, etc. All these subsystems interact together with the main goal of efficiently monitoring and managing the transportation network [8].

1.2.2 Smart Grids

Another interesting service enabled by IoT is smart grids. While ITS focus on the transportation network, smart grids leverage IoT devices to better manage the energy consumption, generation and transmission. Through the use of different IoT devices (such as sensors, smart meters, smart actuators), power suppliers, building managers, etc. can dynamically manage their energy production/consumption based on the data obtained from these devices. Further, the data obtained from such IoT devices can be monitored and analyzed to provide better services to the energy consumers, avoid potential failures and detect anomalous behaviors [9].

While these two services deal with two completely different networks; transportation and energy, a new service has emerged which in its core is a perfect combination of both ITS and smart grid. This service is the Electric Vehicle (EV) and its charging infrastructure. In essence, EVs are part of the vehicular subsystem in the ITS service and their charging infrastructure are part of the

smart grids. To put it in perspective, an EV with low battery level would connect to the nearest EV charging station whether at home or at public. Through the use of smart meters and controllers within the charging stations, data about EV charging could be sent to the power utility to better manage its energy production to accommodate for EV charging during the different times of the year. Further, full integration of these two services within the context of EVs would mean that self-driving EVs could automatically drive to the nearest charging stations to recharge their batteries. Although the road for full integration is yet to be fully developed, the EV industry have witnessed exponential growth over the past few years. Nowadays, almost all car manufacturers are producing at least one type of EV. Coupled with government incentives and subsidies, the number of EV on the road is expected to reach $30M$ by 2030.

1.3 EV Charging: The Story

Despite the growth of the EV industry, one would expect that the EV adoption among consumers is skyrocketing. Unfortunately, this is not the case due to some obstacles. One of the major obstacles facing EV adoption is the lack of an adequate charging infrastructure. According to CleanTechnica, almost 50% of EV drivers believe that charging stations are neither located conveniently nor adequate for long distance trips. As a result of such barriers, there have been major investments in the field of EV charging. Similar to the EV industry, major companies including Siemens, Schneider Electric, etc. are now manufacturers of EV charging stations (EVCS). Further, lots of car companies including Porsche and Tesla are providing EVCS specific to their EV. Moreover, new companies have emerged and started to lead the field of EVCS manufacturing such as ChargePoint and EvBox. Beside procuring EVCS in the market, the EVCS themselves have transitioned into being part of the IoT paradigm. In particular, EVCS are now internet-connected transmitting data between them and the EVs, as well as communicating with a management server to monitor and control the charging process. This transition to the IoT paradigm has opened the door for new challenges, one of critical importance is the security.

Security has always been a critical aspect of the IoT devices. Given their limited computing capacities and storage, IoT devices are not fitted for heavy security protocols, leaving them with very

weak authentication mechanisms for example. In addition, their availability in the markets, homes, buildings, etc. make them a more lucrative victim for cyber-attacks. For instance, the Mirai botnet infected more than half a Million IoT device in a matter of days exploiting their default credentials. Circling back to the EVCS, it becomes clear that they are no exception either. Particularly, they are becoming more readily-available to the consumers with low prices due to government incentives. Further, their developed security protocols are not matured yet, require limited to no security measures and riddled with vulnerabilities [10]. What make the EVCS a much more crucial entity than the other IoT devices are that they are the linking point to a more critical infrastructure and their unique characteristics. Specifically, EVCS have higher power ratings that almost all consumer IoT devices (more than Electric water heaters and Air conditioners). Further, current protocols of EVCS allow for bidirectional power flow, meaning that the EVs can also discharge their batteries to the power grid. Thus, if an EVCS is compromised, the communication link between the EVCS and the EV can also be compromised. The implications of this is that the EV driver data could be stolen and tampered with. To exacerbate the situation, false commands can be injected into the EV causing damage to the batteries and more hazardous impacts. On the other side, a compromised EVCS can cause some disturbances on the power grid.

1.4 Contributions

In this thesis, we study, in great detail, the security of the EV Charging infrastructure as part of the IoT paradigm. In particular, we survey the current infrastructure in terms of the protocols, communication links, participating entities and major players. Further, we propose a novel attack targeted towards the EVCS that can cause major disturbances to the power grid. Given the severity of such an attack and other proposed attacks in the literature, we explore the different mechanisms leveraging Artificial Intelligence (AI) and Blockchain that could be leveraged to secure such a critical infrastructure. From there, we further expand on one of the proposed mechanisms, namely anomaly detection, to propose a detection mechanism for the proposed attack and a reenvisioning of the charging infrastructure. Our contributions can be summarized as follows:

1.4.1 A Tale of Two Entities: Contextualizing Electric Vehicle Charging Stations Cyber-Fingerprint on the Power Grid

With the growing market of V, the procurement of their charging infrastructure plays a crucial role in their adoption. Within the revolution of IoT, the EV charging infrastructure is getting on board with the introduction of smart EVCS, a myriad set of communication protocols and different entities. With such, we provide in this chapter an overview of this infrastructure detailing the participating entities and the communication protocols. Further, we contextualize the current deployment of EVCSs through the use of available public data. In the light of such survey, we identify two key concerns; the lack of standardization and multiple points of failures, which renders the current deployment of EV charging infrastructure vulnerable to an array of different attack s. Moreover, we propose a novel attack scenario that exploits the unique characteristics of the EVCSs and their protocol (such as high power wattage and support for reverse power flow) to cause disturbances to the power grid. We investigate three different attack variations; sudden surge in power demand, sudden surge in power supply and a switching attack. To support our claims, we showcase using real-world example how an adversary can compromise an EVCS and create a traffic bottleneck by tampering the charging schedules of EVs. Further, we perform a simulation-based study of the impact of our proposed attack variations on the WSCC 9 bus system. Our simulations show that an adversary can cause devastating effects on the power grid which might result in blackout and cascading failure by comprising a small number of EVCSs.

1.4.2 Blockchain, AI and Smart Grids: The Three Musketeers to a Decentralized EV Charging Infrastructure

The EV charging industry have been a lucrative opportunity for investors and research community. Accordingly, many efforts have been made towards providing the end-user with an extraordinary Quality of Service (QoS). However, given the current protocols and deployment of the Electric Vehicle (EV) charging infrastructure, some key challenges still need to be addressed. Particularly, we identify, in this chapter, two main EV challenges (1) vulnerable charging stations and EVs, and (2) non-optimal charging schedules. With these issues in mind, we evaluate the integration of

Blockchain and AI with the EV charging infrastructure. Specifically, we discuss the current AI and Blockchain charging solutions available in the market. In addition, we propose a couple of use cases where both technologies complement each other for a secure, efficient and decentralized charging ecosystem. This letter serves as starting point for stakeholders and policymakers to help identify potential directions and implementations of better charging systems for EVs.

1.4.3 An Anomaly Detection Engine for Securing the EV Charging Ecosystem with Blockchain and AI

Motivated by the attack in the first contribution, we focus, in this chapter, on early detection and build an anomaly detection engine. Particularly, we leverage AI to be the backbone of the detection engine that analyzes the EV schedules and raise alerts of anomalous ones. First, we detail a generic detection engine and test it using the Irish public EVCS and power grid data. Under extensive simulation and testing different learning algorithms (statistical, auto-encoders and distance-based), we evaluate the performance of the proposed engine. Our results show the effectiveness of the proposed engine in the early-detection of the described attack, while providing enough flexibility to tweak its performance for more complex attack variations. Further, to provide a more comprehensive solution, we discuss a Blockchain network integration with the proposed engine to secure the private EVCS from such an attack.

1.5 Thesis Organization

The rest of the thesis is organized as follows: Chapters 2, 3, 4 detail the first, second and third contributions respectively. We then conclude and discuss future work in chapter 5.

Chapter 2

A Tale of Two Entities: Contextualizing Electric Vehicle Charging Stations Cyber-Fingerprint on the Power Grid

2.1 Introduction

In the current era of IoT, everyday items or "Things" are enhanced with embedded sensors, actuators and Internet connection, giving them the capability to collect, analyze data and perform actions accordingly, turning them into smart things [11]. With such enhancements, the IoT will bring a wide range of invasive technologies in various sectors (i.e. health care, industry, transportation, etc.). Two of the promising use cases of IoT are ITS and Smart Grids. In an ITS environment, people, roads and smart vehicles are connected together providing smart traffic management [7]. In a truly connected environment, different smart sectors would collaborate together giving rise to new business and technological opportunities. One of the rather interesting opportunities is the emergence of EV and their infrastructure.

The EV industry has witnessed a tremendous growth over the past few decades with forecasts of reaching 30 Million EVs by 2030 [12]. EVs are considered a stepping stone towards a genuinely connected smart environment by linking two major sectors; Transportation systems and electric

grids [10]. With such a promising future, the adaptability of EVs has been increasing at a steady rate of almost 42% since 2013 [13]. However, for the EV industry to reach its potential as an alternative for fuel-powered vehicles, different components have to be made available to the end users. The first component is the EVs themselves which was procured by many of the car companies including Toyota, Tesla, Hyundai, etc. The other major component is the availability of the EV charging platform. These two components constitute the infrastructure of the EV industry.

EVCS are considered the backbone of the EV industry. Their availability is crucial to the continuation of EVs and to providing the end user with a seamless driving experience. Consequently, there has been many efforts, both in the academic and industry sectors, that focused on the procurement of EVCS. For instance, researchers focused on optimizing the scheduling, charging and placement of EVCS [14, 15, 16]. On the industry side, many companies (e.g. Schneider Electric, ChargePoint, Shell, etc.) have ventured towards manufacturing EVCS and successfully providing the end users with a variety of options. In addition, many companies have embraced the IoT paradigm and provided smart charging stations, allowing customers to schedule, manage, and pay for their EV charging with little to no effort. Although the rise of smart EVCS has brought many benefits to the end users, it added some challenges; one that is particularly interesting is their security.

With every new addition to the IoT paradigm, a novel threat landscape is introduced upon the cyber security field. Within the context of EV charging, different entities and communication protocols coexist to realize such an infrastructure. These entities range from the EV driver, to the charging station all the way to the power utility. Inspite of contributing to the EV charging realm, each entity brings about its intrinsic vulnerabilities and thus, it represents an entry point to the system from the adversary perspective. Therefore, the adversary's reward could be as simple as physically damaging the charging station to a more devastating impact as remotely controlling the charging station and redeeming it unavailable. In light of this discussion, we explore one particular threat that can render major leverage to an adversary. Specifically, we demonstrate how an attacker can exploit EVCS to derange the more critical entities, Power Grid.

Although the security of EVCS has not been discussed thoroughly in the literature due to its novelty, some contributions have been made. For instance, the authors in [10] discussed the security of EVCS on the protocol level. In addition, the authors in both [17] & [18] discussed the security

of EVCS from the infrastructure level. However, given the growth of the EV charging industry and wide deployment of EVCS, there is a need to survey and analyze the security of existing EVCS solutions. Moreover, some work has been done in targeting the power grid through the EV charging stations. For instance, the work in [19] and [20] analyzed how an adversary can utilize public charging stations to cause frequency instability to the power grid. Although both works built up on the same foundation, that is EVCS can cause major disturbances to the power grid, the authors explored one dimension of such disturbance; a sudden increase on the load. Unlike the work in the literature, we provide a more comprehensive view of the EVCS security and explore novel measures an adversary can take to cause more disturbances to the grid.

To this end, we provide a wide view of the different EVCS solutions currently deployed, and an overview of the distribution of the EVCS in terms of locations, levels and types. Further, we survey the different protocols used within the infrastructure of the EVCS and analyze their security. In addition, we demonstrate how the growth of the EVCS and EVs could represent a new attack surface on the grid. Particularly, we propose an innovative coordinated multi-stage attack that allow an adversary to disturb the power grid. We first demonstrate how an adversary can remotely access and control EVCS by exploiting common IoT vulnerabilities and public data available from Internet wide scans. Further, we exploit the intrinsic properties of EVCS that allow for bidirectional power flow, high wattage consumption and coexistence of a variety of protocols. From there, we perform a simulation-based study on how an adversary can cause frequency instability and cascading failures to the grid by performing three different kind of attack variations; sudden load increase, sudden surge in energy supply and switching attack.

The remainder of this paper is organized as follows. We discuss the EVCS protocols, infrastructure and the state-of-the-art deployments in Section 2.2. The security of EVCS is analyzed in Section 2.3 in terms of the protocols used. We then demonstrate real-world test cases and evaluate the different attack vectors in Section 2.4. Section 2.5 covers the literature review. We propose a set of countermeasures in section 2.6 and we finally conclude in Section 2.7.

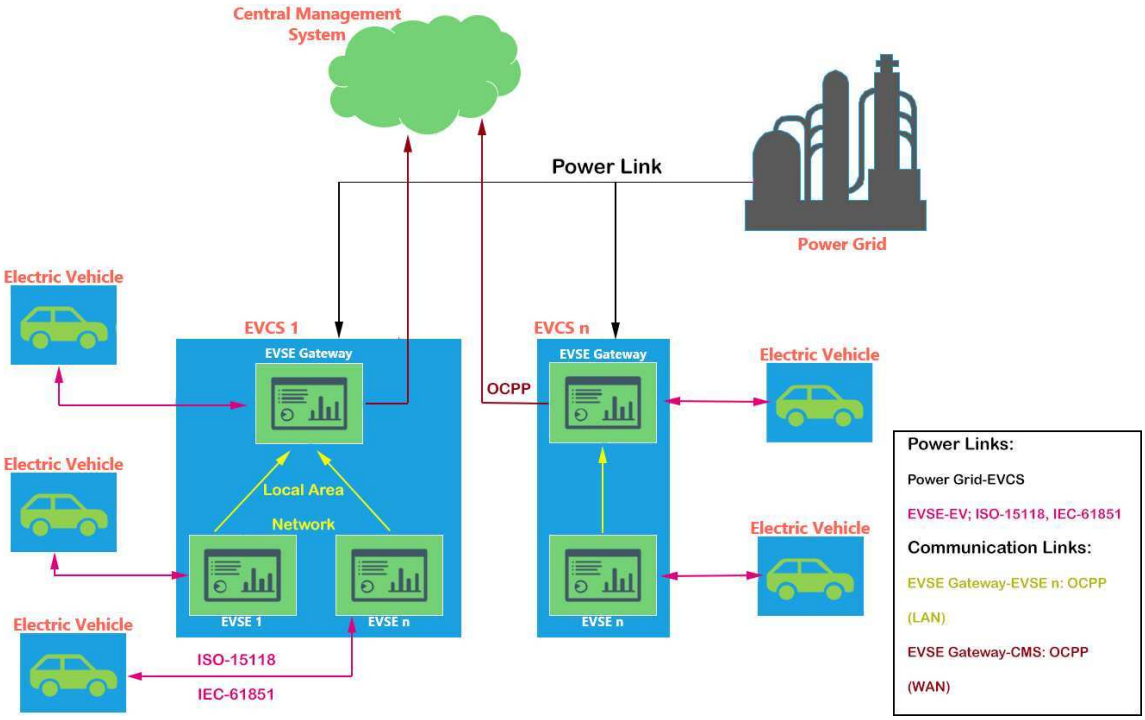


Figure 2.1: Electric Vehicle Infrastructure and Protocols

2.2 Electric Vehicles Charging Stations: Protocol, Infrastructure & Deployment State of the Art

EVCS is composed of different entities communicating and interacting together. Figure (2.1) gives an overview of the main entities composing the infrastructure of the EVCS along with the different protocols used for communications. In what follow, we provide an overview of the different entities and the protocols specifications.

2.2.1 Infrastructure

The EVCS infrastructure consists of four main entities:

EV

EV are the raison d'etre of the EVCSs; their growth over the past few decades stimulated the need to procure their charging. According to the International Energy Agency (IEA), the number of Electric Vehicles in 2018 was 5.1M across the globe which was double the number of EV from the

previous year. Further, the IEA is estimating an exponential increase of EVs reaching up to 250M by 2030 [21]. Generally, EVs can be categorized into three main types [22]:

- **Hybrid Electric Vehicles (HEV):** Those are Electric Vehicles powered with both a fuel engine and a battery engine. The battery engine operates at lower speeds and when idle, while the fuel engine operates at high speeds. The charging of HEVs is accomplished through regenerative breaking and the fuel engine. Hence, they can not be plugged in to a charging station.

- **Plug-In Hybrid Electric Vehicles (PHEV):** The PHEVs follow a similar concept of HEV. However, they can be plugged-in to a charging station. Further, PHEVs are equipped with more batteries and more powerful traction motors, allowing them to travel for longer distances [22].

- **Battery Electric Vehicles (BEV):** BEVs are powered entirely by an electrical engine, hence they rely fully on charging stations to power their engines. One major advantage of BEV is that they produce zero emissions resulting from internal combustion engines. [23]

In this work, we only consider about PHEVs and BEVs since they utilize the charging stations.

Power Grid

The power grid is the main source of power that feeds EVs through the charging stations. Electric Supply and Demand along with the speed of the generators are used as an essential indicator for grid stability and reliability. Particularly, the speed of the generators directly translates to the frequency of the system. Further, when the electrical demand increases, the grid responds to this increase by reducing the speed of the generators, releasing its kinetic energy into the system and vice versa. To ensure the stability of the grid, it has to operate within a certain frequency range; any deviation from that range would result in instability or degradation in the system performance. Table (2.1) shows the different operating zones of frequencies in North America [24]. As can be seen, when the frequency of the system drops below $59.5Hz$ or raises above $61.5Hz$ due to significant imbalance between supply and demand, the system is operating in a critical region and any

further variations would cause shutting down the protection relays and the equipment. Hence, extreme measures should be taken to bring the system frequency to its nominal range by controlling the mechanical input of the primary and secondary controllers. [25]

Supply-Demand	**Frequency Range**	**Operation Zone**
supply >>Demand	f >61.5	Critical
Supply >Demand	59.95 <f <60.05	Stable
Supply = Demand		
Supply <Demand		
Supply <<Demand	f <59.5	Critical

Table 2.1: North America Frequency Ranges

Central Management System (CMS)

The CMS is simply a cloud server responsible for monitoring and managing the different charging stations. Its functionality includes scheduling and monitoring the charging, keeping the logs, managing authorized and unauthorized transactions as well as performing remote diagnostics and adjustments.

EVCS

The EVCS is the backbone that connects the different entities together. Topologically, an EVCS is composed of one or more Electric Vehicle Supply Equipment (EVSE) responsible for delivering power to EVs. Further, each EVSE can have one or more terminals allowing for multiple EVs to be charged at once. In addition, an EVSE can be configured as a gateway or non-gateway. For the gateway configuration, the EVSE acts as a relay of information between the central management and the rest of the non gateway EVSEs within the EVCS.

EVSE can be further broken down into three main tiers based on their power output:

- **Level 1:** Level 1 EVSEs are the most basic charging stations. They draw power from the standard outlet; grounded 120V/15A single phase outlet for North America. This corresponds to a power output of $1.5-2$kW, and accordingly, it is considered to be the most time consuming; 12-24 hours to fully charge an EV[26].

- **Level 2:** Level 2 EVSEs are the most common chargers for EVs. They typically utilize a 240V connection, allowing peak powers of up to $19kW$. Typically, level 2 EVSEs outputs on average 7.2kW of power allowing drivers to fully charge their EVs in a couple of hours [27].

- **Level 3:** Level 3 EVSEs are the most powerful with peak power of up to $240kW$ utilizing a $480V$ outlet. Typically, Level 3 EVSEs utlizies $44 - 120kW$. They are usually referred to as DC fast Charging, and are capable of charging an EV in a matter of minutes[28].

Aside from the power variations of the EVSEs, EVSEs could be categorized as public or private. Public EVSEs are usually found in public places such as parks, roadsides, public parking lots etc. On the other hand, private EVSEs are found in homes, companies, etc., and their owner could make them available for public use as well. In addition, EVSEs can support unidirectional or bi-directional power flow allowing EVs to charge and discharge from and to the grid. As for the actual charging process, EVs batteries require a DC power voltage while the power from the grid is AC. Thus, the EVs chargers are equipped with an AC/DC rectifier or converter that rectifies the AC power to the required DC power of the EVs. In case of DC chargers, the charger uses additional DC/DC converter to stabilize the power and improve power conversion [29]. Moreover, the connection between the EV and the EVSE happens through a connector. Each connector follows specific standards that define the connection, safety and charging requirements. Such standards will be discussed in details in Section 2.2.2.

2.2.2 Protocols and Standards

To complete the infrastructure of the EV charging, a set of communication protocols exists to enable the exchange of data between the different entities. These communication protocols can be categorized according to the participating entities. Particularly, we have:

EV - EVCS

The communication between the EV and EVCS is considered as a link between the EV and the grid. It depends on the region where the EVSE is deployed, and is mainly provisioned through the following standards:

- **Society of Automotive Engineers (SAE)** The SAE issued multiple standards that all together would regulate the charging process of EVs in terms of communication, safety and security. For instance, the SAE J-2293 describes the communication requirements and network architecture for an energy transfer system for an EV [30]. Further, SAE J-1772 standard describes the requirements for the charging connector which is used in most Level 2 chargers across North America [29]. Contributing to a smart connected world, SAE defines the SAE J-2847 and J-2836 which detail the communication between the utility, EV and EVSE. One interesting aspect of the latter standards is that they describe, in details, the requirements for reverse power flow in which EVs can discharge their batteries back to the grid [30] [31].

- **International Electromechanical Commission (IEC)** The IEC is another organization that has put many efforts in standardizing the communication, energy transfer and safety of EV charging. Their efforts are mainly concentrated in the European Union. Similar to SAE, IEC defines multiple standards that address different aspects of the EV charging. For instance, the IEC 62196 specifies the socket/connector types that connects from the EVSE to the EV. Further, the energy transfer and the communication messages are managed through the IEC 61851. Unlike the SAE, IEC has specified no standards nor requirements for reverse power flow of EVs. [30]

- **International Standardization Organization (ISO)** Similar to SAE and IEC, ISO defined some standards with regard to vehicle to grid communication. Particularly, the ISO-15118 details the communication infrastructure within the charging environment. The ISO-15118 defines the roles of the different entities in the EV charging infrastructure including the EVs, EVSEs, utility and charging stations operators. Further, the ISO-15118 relies on the IEC-61851 plug detection in and out of the EV. Moreover, ISO-15118 supports reverse power flow from EVs [32] [33].

- **ChAdeMO** The chAdeMO standard was originally released as a national standard in Japan in 2012. It typically deals with the DC fast charging (i.e Level 3 charging stations). The chAdeMO standard was then added to IEC-61851 and IEC-62196 [29] [34].

EVCS - CMS

The communication between EVCS and CMS is of critical importance as it would manage the schedule of charging EVs, safe-keep all the logs of EV users and their charging, and maintain the status of the EVCS itself. Hence, a protocol is much needed to supervise such crucial communication. As mentioned earlier, the CMS is essentially a central cloud and the EVCS could be considered as an IoT device, thus, the communication between these two entities could be handled in multiple ways; peer-to-peer communication, WiFi, 4G, etc. Due to the variety of EVCS operators and the critical-nature of such communication, different operators devise their own protocol. However, by surveying the vast majority of the operators, it was evident that although the exchanged messages and interfaces differ, most of them follow simple HTTP/HTTPS communication between the EVCS and the CMS. In effort towards a standardized communication protocol between the EVCS and CMS, the Open Charge Point Protocol (OCPP) [35] was established by the Open Charge Alliance. Over the past few years, OCPP has undergone huge improvements since its introduction in June 2012. Initially, OCPP 1.5 supported only SOAP protocols and 24 unique messages. With security in mind, OCPP 1.6 offered support for both SOAP and JSON as well as new functionalities including smart charging. Lastly, OCPP 2.0 was published in early 2018 with support for only JSON and up to 65 unique message types. Although OCPP 2.0 added a wide array of new features, there were three main improvements that are worth noting:

- **Support for EV-grid standards:** One of the rather interesting improvement of OCPP 2.0 is supporting ISO-15118 standard. According to [36], the charging process supervised by the ISO-15118 standard can now be remotely started/stopped from the CMS. Further, EVs can now authenticate to the EVCS using the certificates already installed on them. Moreover, the ISO-15118 control pilot signal; a signal sent from the charging station to the EV to notify the EV of the maximum current limit, can now be changed by the CMS. This coordination between both protocols/standards would allow seamless experience for the user and better management of the charging station.

- **Support for remote control:** Another interesting feature of OCPP 2.0 is full remote control of the charging station. This allows operators to monitor and modify the status of the charging

station in real time, change its configuration and start/stop charging and transaction. Further, the remote control functionality allows remote unlocking of the connector.

- **Support for smart charging:** OCPP 2.0 supports different smart charging scenarios:

  1. *Internal load balancing* where the CMS sets known power limits to the charging stations according to the grid requirements. In that case, the CMS sets the power limits, based on physical grid connection limits, for each charging station, thus, no EVCS could exceed these limits.
  2. *Central Smart Charging* where the CMS directly sets the power limits to the charging stations. The CMS receives the power limits from a grid connection or capacity forecast from a grid operator.
  3. *Local Smart Charging* In that case, the CMS does not set the power limits. On the contrary, a local controller - usually installed by the grid operator - sets the power limits to the charging stations.
  4. *External Smart Charging* this scenario is similar to the Local Smart Charging. However, along with the local controller, an External Management System (EMS) collaborate together to determine the limits and priority of utilizing the power for EV charging.

  To fully enable smart charging, charging profiles are added along with the smart charging scenarios. Charging profiles describe the behavior, in terms of schedule, power, duration, etc., of EV charging. A sample of OCPP 2.0 charging profile is shown in Figure 2.2. The charging profile in Figure 2.2 sets the power limit to $6kW$ from 8:00 AM to 8:00 PM and $11kW$ for the rest of the day. Thus, the CMS sends charging profiles to the charging stations to notify the EVCS of the power limits and its durations during the day.

Besides OCPP, the Open Charge Point Interface (OCPI) [37] is another protocol to manage the data sharing between the different EVCS operators and e-mobility service providers.

ChargingProfile			
chargingProfileId	**100**		
stackLevel	**0**		
chargingProfilePurpose	**TxDefaultProfile**		
chargingProfileKind	**Recurring**		
recurrencyKind	**Daily**		
chargingSchedule	*(List of 1 ChargingSchedule elements)*		
	ChargingSchedule		
	duration	**86400 (= 24 hours)**	
	startSchedule	**2013-01-01T00:00Z**	
	chargingRateUnit	**W**	
	chargingSchedulePeriod	*(List of 3 ChargingSchedulePeriod elements)*	
		ChargingSchedulePeriod	
		startPeriod	**0 (=00:00)**
		limit	**11000**
		numberPhases	3
		startPeriod	**28800 (=08:00)**
		limit	**6000**
		numberPhases	3
		startPeriod	**72000 (=20:00)**
		limit	**11000**

Figure 2.2: OCPP 2.0 sample charging profile*

* Adopted from [36]

2.2.3 Deployment

The rise of EVs over the past few decades led to a surge in the number of deployed charging stations all over the world. Most charging stations operators offer map functionalities for EV drivers to locate their charging stations. For instance, ChargePoint, the largest EVCS manufacturers in North America, offers a map interface for EV drivers to locate, not only ChargePoint charging stations, but also EVCS from different manufacturers such as Flo, EVLink, etc. Beside the manufacturers' map interfaces, third party websites; PlugShare, ChargeMap, are contributing to offer EV drivers seamless charging experience. One of the rich data resources could be found on OpenChargeMap [38]. It not only provides open source data on EVCS from different manufactures but it also acquires its data from multiple resources (users of EVs, local energy and mobility providers). Thus, in order to contextualize the current deployment of EVCS and their types, we relied on OpenChargeMap data to construct a wide view on current deployment of EVCS.

To date, the number of EVCS deployed worldwide is 153771 across 75355 locations. Figure 2.3 shows the distribution of deployed EVCS around the globe. The USA takes the lead in terms of the number of EVCS with an outstanding 25000+ EVCS. Germany follows the US with almost 20000

EVCS. Netherlands and the UK have a similar number of EVCS making them along with Germany the top three countries in the EVCS market in Europe.

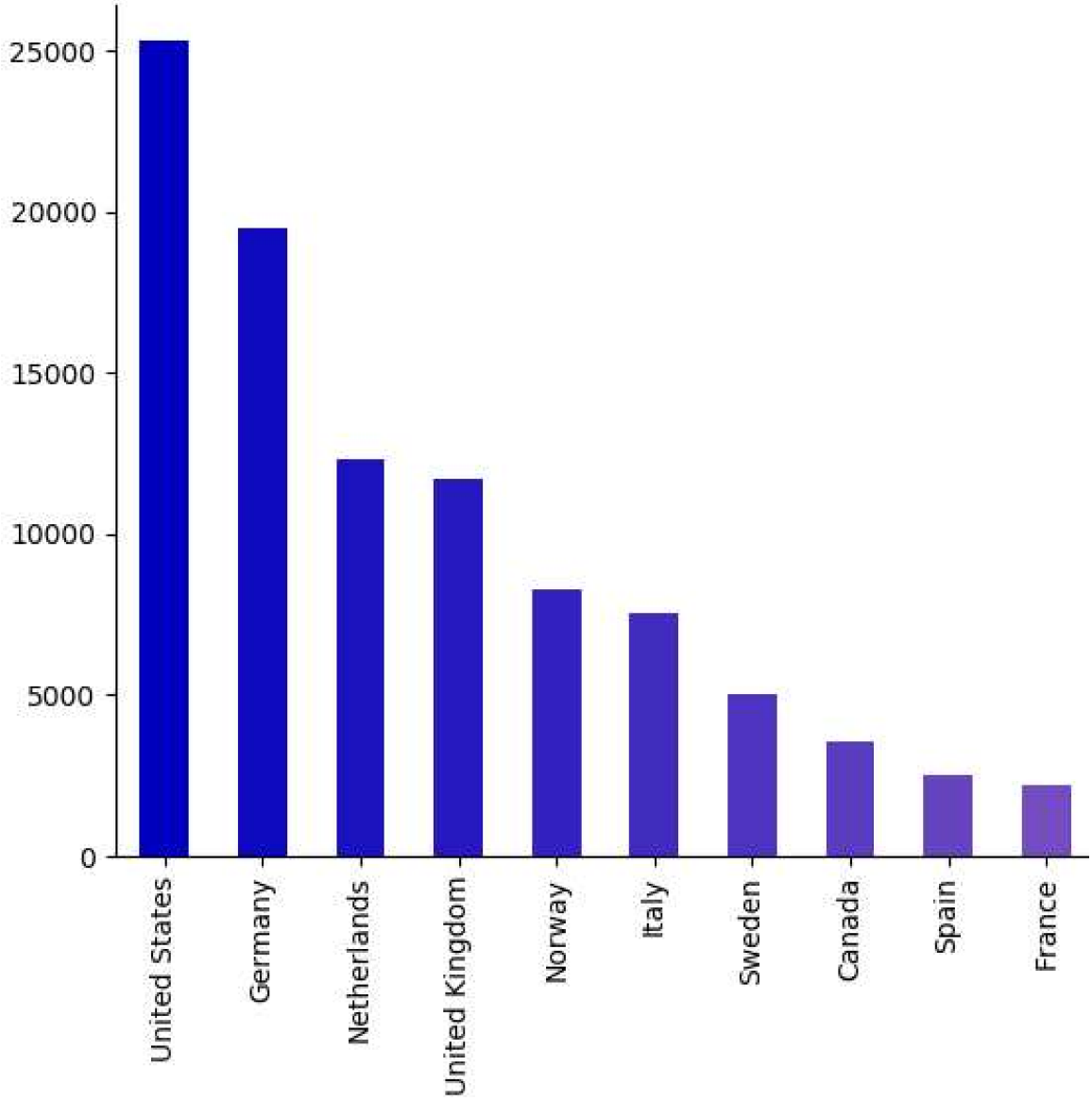


Figure 2.3: Electric Vehicle Charging Stations Country Distribution

In addition, by looking at the distribution of EVCS operators as shown in Figure 2.4, one can note that Tesla and ChargePoint contribute to almost 15% of all deployed EVCS. Due to privacy concerns, a large number of EVCS was not associated with any network operators. Further, due to the large number of operators, Figure 2.4 shows only the top 10 operators in terms of the number

of EVCS. Although many tech giants and EV manufacturers are entering the EV race and procuring their charging infrastructure (e.g. Schneider Electric, Siemens, Huyndai, etc.), the only EV manufacture that is in the top 10 operators is Tesla. More interestingly, ChargePoint is the leading operator in North America. This infers that the EV charging infrastructure opens new business opportunities with an easy-to-access market.

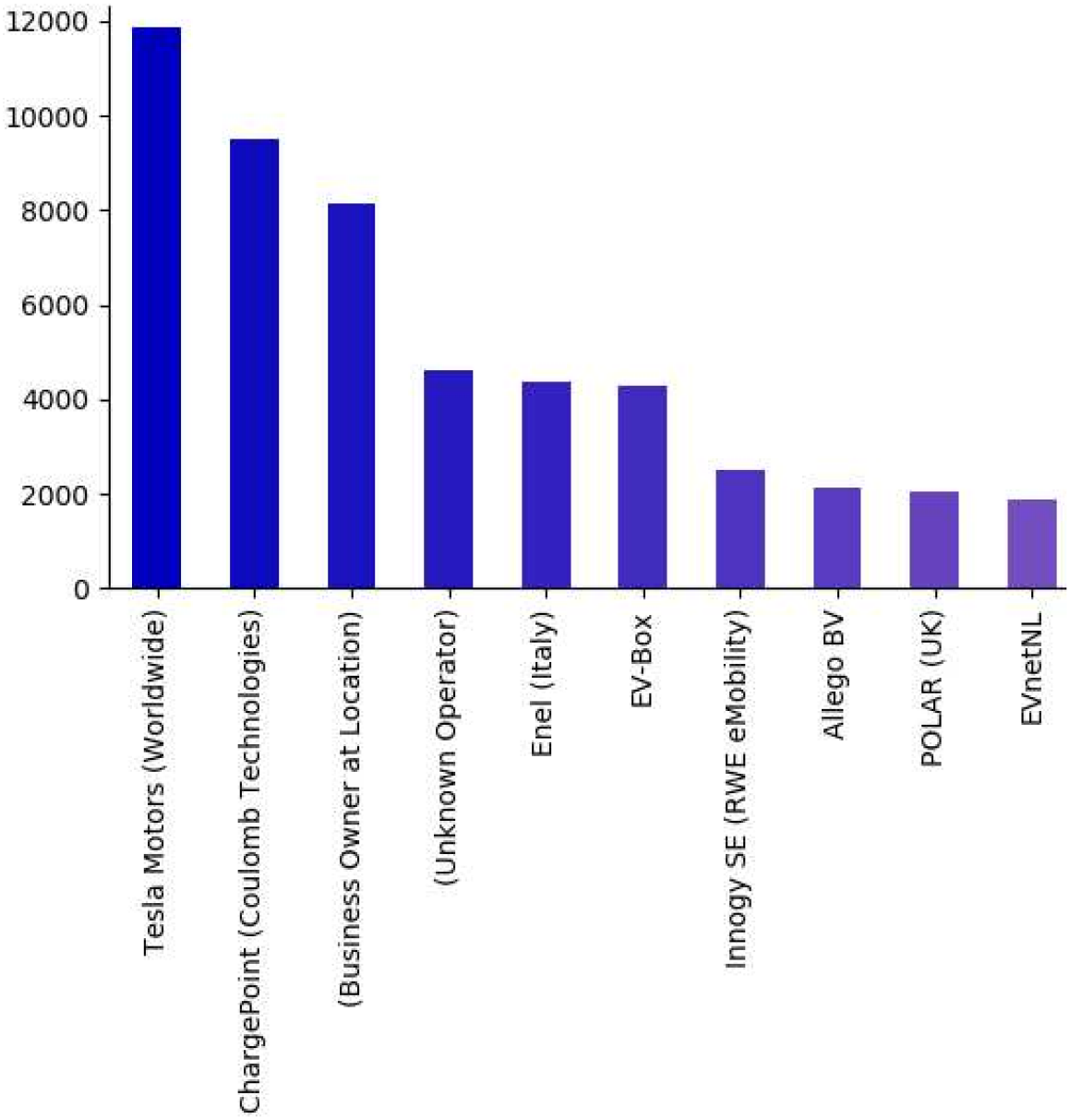


Figure 2.4: Electric Vehicle Charging Stations Operators

Another essential classification of EVCS is their access types as shown in Figure 2.5. According

to the current deployment of EVCS, almost 75% of deployed EVCS are public, that is, they are publicly accessible by the EV drivers in return for charging fees. Moreover, public EVCS could be sub classified into further categories. On the other hand, private EVCS represent as little as 20% among all deployed EVCS. In addition, Figure 2.5 shows the gap between the availability of data between public and private EVCS.

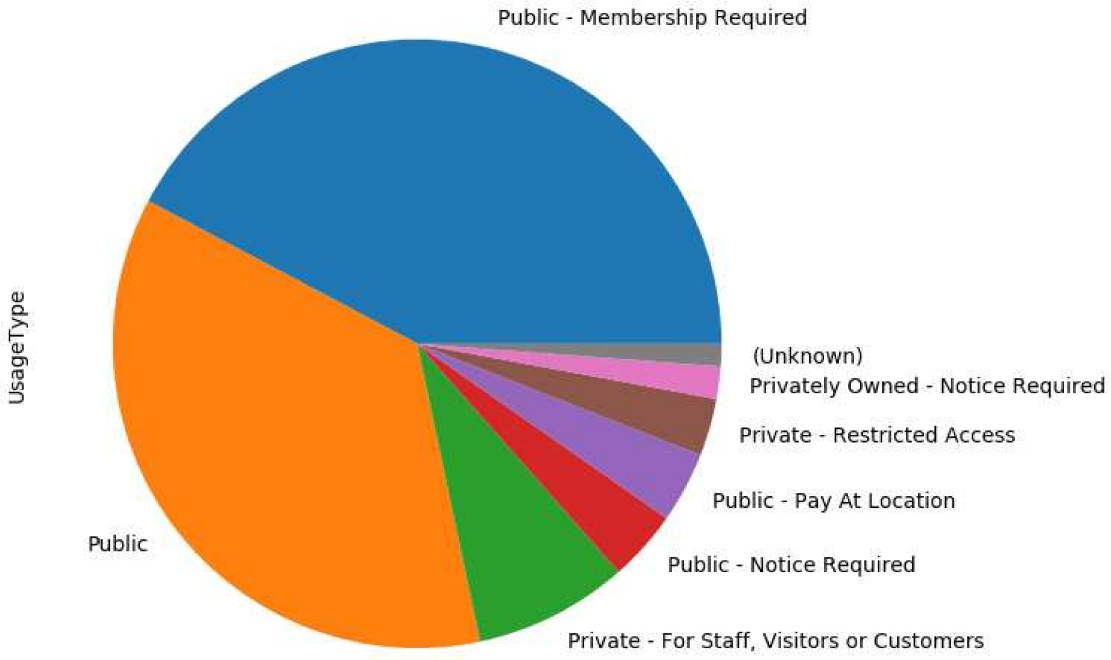


Figure 2.5: Electric Vehicle Charging Stations Types of Usage

Another critical classification is the level rating of the EVCS as shown in Figure 2.6. It is obvious that level 2 chargers are dominating the deployed EVCS by contributing to almost 75% of all EVCS. More interestingly, level 3 chargers contribute to more than 15% of EVCS albeit their dramatically high prices. The distribution of the power levels of EVCSs shows that, with the current deployment, the power utility needs to accommodate for these high wattage devices as most level 2 chargers utilize $7.2kW$. Further, future deployment would witness a surge in the number of level 3 chargers thanks to their fast charging capabilities. However, this surge would represent a major concern for the utility as the power ratings of level 3 chargers are usually over $40kW$ and up to $120kW$.

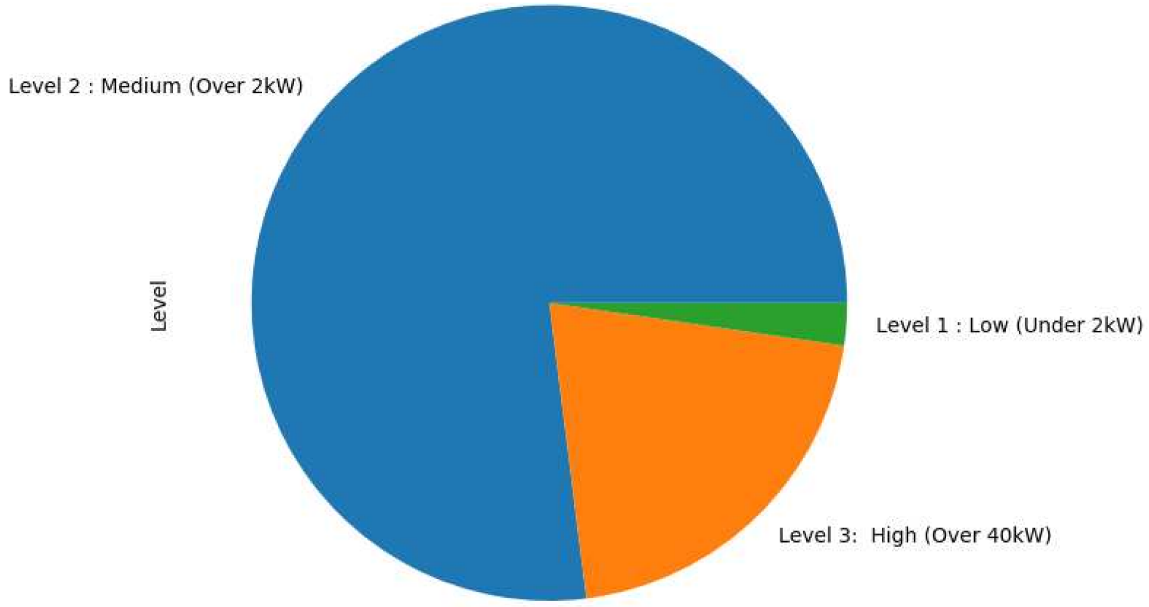


Figure 2.6: Electric Vehicle Charging Stations Level Distribution

The current deployment of EVCS discussed above hints to some crucial issues. One rather important is that the power utility would need to devise different mechanisms to better manage the EVCS load. This becomes more of a crucial concern when the market share of level 3 chargers increase in the future. Further, private EVCS in residential areas needs to be surveyed to determine their true impact on the grid.

2.3 Electric Vehicles Charging Stations: Security Analysis

With the expansion of the charging infrastructure, the increase in EV utilization, diversity of involved actors and the variety of charging technologies and protocols, security across the EVCS system becomes a critical and essential aspect. Although the security of the different protocols and entities were studied in the literature, we demonstrate a new attack surface that results from having myriad variety of protocols and multiple entities within the EV charging infrastructure.

2.3.1 Threat Landscape

The aforementioned architecture of EV charging represents an attack surface for adversaries and malicious entities mainly due to two reasons:

Multiple points of failures

The EV charging infrastructure relies on the coexistence of four main entities communicating and interacting together. These entities utilize a set of protocols to transfer data and energy. Such composition and variety result in a vulnerable system by nature as each protocol brings its unique set of vulnerabilities. For instance, most of deployed EVCS lack the physical security with little to no supervision [39]. Hence, an adversary could easily damage the EVCS, or even install malware through USB ports available in the EVSE. Such malware can then be used to steal energy and users data or cause Denial of Service (DoS) on EV charging [40]. Another concern of having multiple entry points is that an adversary can abuse the weak links in the system to gain more leverage on the more critical points. For instance, if an attacker gained access to vulnerable charging stations within an area, he/she could abuse the EV charging by disabling all chargers. To exacerbate the situation, access to vulnerable EVCS can cause disturbances on the grid [19]. This kind of coordinated multi-stage attack would be explained in further details in the following sections.

Lack of Standardization

With the aforementioned discussion on the different protocols used within the EV charging infrastructure, there is an evident lack of standardization among these protocols. To put this in perspective, OCPP is used to communicate between an EVCS and a CMS, while a different set of protocols (SAE, ISO, etc.), exist to communicate between the EV and the EVCS/Grid. Although some of these protocols are uniquely used in their corresponding region (North America, Europe, etc.), some others are used internationally (ISO for instance). To exacerbate the situation, some of the EVCS operators use their own set of protocols. From an adversary point of view, each protocol comes with its unique set of vulnerabilities whether its design or implementation flaws as was discussed in [10], [32]. When combined together in one system, these vulnerabilities renders the whole system vulnerable to different attack scenarios.

In the light of these reasons, multiple attack scenarios on the EV charging infrastructure is possible. To formalize the analysis of the attack vector, the National Institute of Standards and Technology (NIST) identifies four different areas where an adversary could attack the system [41].

- **Remote** This threat vector is when an attacker exploits the system over the network, i.e. remotely. Given that the EVCS communicates with the CMS through the Internet , the EVCS can be compromised remotely.

- **Limited Remote** This attack vector relates to when an adversary carries out an attack remotely but within certain constraints due to range limitations. For instance, an attacker tries to sniff messages exchanged between the EVCS and CMS sent through WiFi. In order to achieve this, the adversary needs to be in a close proximity to the router in order to be able to capture the packets.

- **Local** This area defines an attack vector where the malicious party has logical local access to the device; through SSH for instance. Although this attack area would require a more skilled attacker, the security team in Kaspersky lab [42] were able to reverse engineer the firmware of ChargePoint home charger and obtain root access. Further, based on our investigation, the firmware updates for Schneider Electric is available online and can be downloaded by anyone [1]. This opens the door for an adversary to discover vulnerabilities and obtain root access to the EVSE as illustrated in [43].

- **Physical** This last area requires the attacker to have physical access to the EVCS. As mentioned earlier, the EVCS are usually deployed in public places under no supervision. Hence, an adversary could inject malicious code into the USB port of the EVSE or cause physical damage to the device.

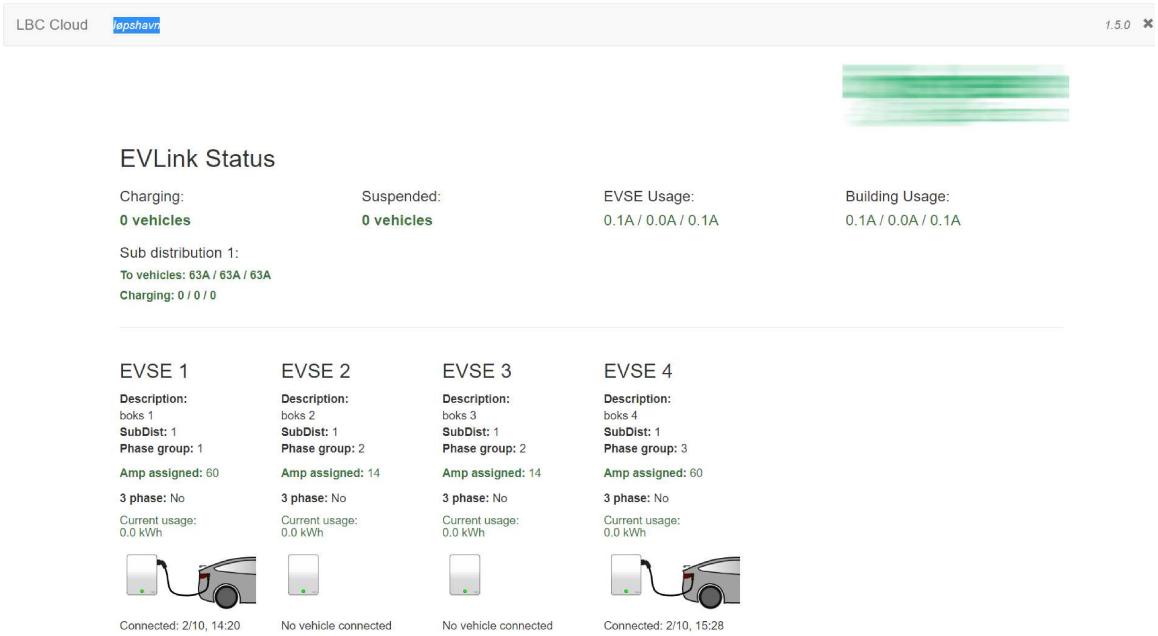
To support this discussion, we demonstrate a multi-stage attack scenario where an adversary exploits the weak links in the EV charging infrastructure to cause grid disturbances.

2.3.2 Attack Scenario

Based on the aforementioned analysis, we substantiate it by proposing a new multi-stage attack where an adversary exploits the weak links in the EV charging infrastructure to cause large scale aftermath. Particularly, we demonstrate how an attacker could exploit the vulnerabilities in the EVCS to cause power grid disturbances. The attack scenario is broken down into the following stages:

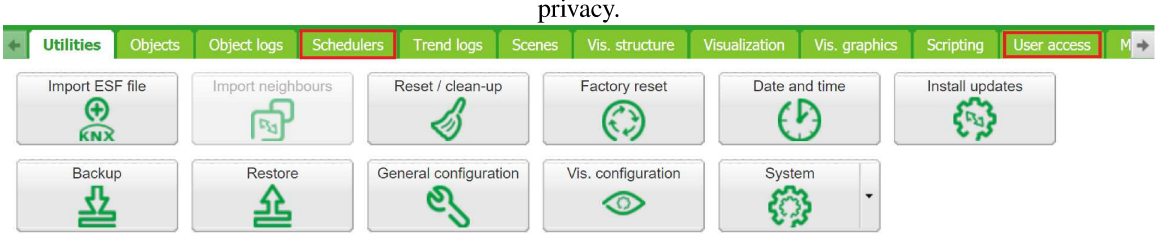
[1] https://www.schneider-electric.com/en/download/document/QGH7213000/

(a) Locating EVCS

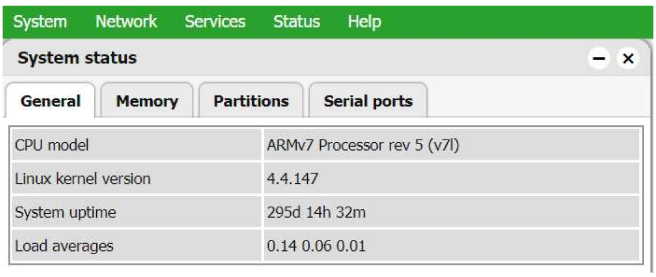


(b) Take control of EVCS (*)

* Highlighted text indicates the password used to get admin access. The manufacturer name is blurred for privacy.



(c) Take control of EVCS



(d) View system level details and status

Figure 2.7: An example of successful operation of stage 1 of the attack

Take control over EVSE

The first stage of the attack is to exploit the vulnerabilities in the EVCS itself and take control over the supply equipment. This is a two-step stage where an adversary would first locate EVCS and then take control over them:

- **Locate EVCS** The first step of this stage is to locate EVCS. As mentioned earlier, location and properties of deployed EVCS could be found online from maps offered by third parties and EVCS operators. However, the data they offer is usually limited and will not help the adversary to remotely access them. Further, an adversary could physically access the devices by installing malicious code into their USB ports. However, given the large scale of this attack, this will not be feasible. Thus, we leverage tools like Shodan and Censys that perform port scans of all IPV4 addresses, to obtain the IP:port of EVSEs. To automate the process, we wrote a python script that do simple banner analysis to filter out EVSEs. We run this script on a weekly basis from a period of five months. The banner analysis was a keyword-based search which looks for devices with 'OCPP', 'Charging Station', 'EVCS', 'EVSE' in their banner. We were able to obtain a dataset of 360 EVCS. Moreover, we looked up for model numbers and types of EVSEs from the top 10 manufactures as shown in Figure 2.4. In addition, we looked for OCPP related ports, however, most deployment run on a generic $HTTP$ port set of $80, 81, 8080, 8081$ and thus no further results were obtained. Although this is a small dataset, the current forecasts of smart EVCSs deployment and EV market growth would definitely contribute to obtaining much larger dataset.

- **Take control** The second step of this stage is to take control over the discovered EVCSs. Since the promise of IoT is to enable invasive applications with a seamless experiences, most of the IoT devices and protocols are designed to be lightweight with most of the processing happening on the Cloud or at the Edge. Unfortunately, this comes at the expense of creating millions of vulnerable devices [44]. For instance, the Mirai Botnet, largest reported attack on IoT, has affected millions of IoT devices. It was reported that in September 2016, Krebs was receiving 600 Gbps of data from the botnet. Further, many major websites such as Amazon, Netflix, Dyn, Reddit, Spotify were taken down by such an attack [44, 45]. While the aftermath was devastating, the root cause of such attacks was that attackers exploited the default user-name and password for most IoT connected

devices to take control of them. The EVCS is no exception either; through our investigation of the discovered EVCS on Shodan and Censys, we found out that most of the EVCS management lacks proper security measures and that remote access to those EVCS, (30% of the discovered EVCS), is available through default usernames and passwords from the manufacturers manuals. Exacerbating the situation, one major manufacturer even displayed the password, status of the EVSEs within the EVCS and the EVs connected and their power consumption on the web interface of the device.

Figure 2.7 demonstrates stage 1 of the attack applied to a vulnerable EVCS. As shown in Figure 2.7, once we had access to the device through the default username and password, we were able to view system-level details (OS, partitions, connected EVSEs, etc.), reset the device, restrict access to specific users, download system images, download the logs and most importantly, tamper the charging schedules.

Create traffic bottleneck

After locating and taking control of the EVCS, an attacker can simply render it unavailable for an extended period of time causing a DoS attack. Further, an attacker can steal user data by downloading the device logs and thus compromise end user privacy. Although these attacks are valid, the adversary can exploit these vulnerabilities to cause a large scale attack on the power grid. To do so, the attacker would need - after locating and taking control of EVCSs - to orchestrate the schedules of the EVCSs to redirect the EV traffic to cause unexpected surge in load. As shown in Figure 2.7, it is feasible for an adversary to tamper the schedules of the drivers planned to charge their EVs at specific times. Further, given the current and forecatsed penetration of EVs and their charging infrastructure, millions of geographically distributed EVCSs would be available for an adversary. Hence, the adversary can render some of them unavailable and force drivers to charge their EVs at EVCSs in the targeted locations. With that, an adversary can target peak times - which can easily be obtained from public power grid data - and either residential or suburban locations - where the grid is not as powerful as a downtown area - to create the bottleneck. Hence, the adversary can tamper both locations and times of charging.

Disturb the power grid

Once stage 2 is complete and the adversary was able to reschedule the EV drivers to charge their vehicles at the targeted times and locations, the more critical and final stage starts. In stage 3, the adversary's ultimate goal is to disturb the grid. To achieve this goal, the attacker creates an EV charging bottleneck to initiate disturbances at the grid level. Accordingly we propose three different attack variations:

- **Sudden surge in demand** We first study the simplest attack variation which is caused by causing a surge in power demand. In this scenario, the adversary orchestrates the compromised EVCS to start the charging of EVs at the same time instant through a manipulation of charging schedules at the compromised EVCS. This variation is similar to the work studied in [46] and [19] and can cause frequency instability and cascading failures. The attacker can cause more impact by targeting peak times to overwhelm the power grid. For instance, an adversary could target a holiday season during Winter or Summer where the families are usually at their homes and another set of high wattage devices - besides EVCS - are turned on (air conditioners or heaters). By synchronously turning on large-scale EV charging in the presence of high system load, the adversary can initiate a sudden load increase to cause imbalance between the demand and supply of electricity, and thus frequency instability at the grid level.

- **Sudden surge in supply** In this variation, we exploit the unique characteristics of EVCS and their protocols. Particularly, the adversary exploits the EV-Grid protocols to perform reverse power flow and discharge the EVs to the grid. This attack is possible because OCPP 2.0 allows the integration of ISO 15118 which is responsible for charging and discharging the EV. Since OCPP is the most used communication protocol between the EVCS and the CMS, controlling the EVCS or the CMS would allow the adversary to tamper with the power flow through the web interface of the EVCS. Specifically, the power flow is determined through the charging profile set by either the CMS or a local controller and sent to the EVCS as per OCPP 2.0 specifications. Thus, an adversary - having control over the EVCS, CMS or even the local controller set by the power utility - can tamper with the charging profile to cause a reverse power flow from the EV to the grid. Hence, in this variation, the adversary synchronizes all compromised EVCS to start the discharging of EVs

at the same time instance, causing a sudden surge in power supply. This sudden surge in supply violates the required balance between power demand and supply to keep the grid stable.

- **A coordinated switching attack** A more interesting variation that we also consider is the possibility of a coordinated switching attack. A switching attack is when an adversary takes control over a set of breakers and alternate their signal between on and off. This cause frequency disturbances as well as cascading failures as shown in [47] and [48]. Within the context of EV charging, an attacker will use the EVCS as an attack surface and exploit the grid's vulnerability to the switching attack. The attacker will coordinate a significant variation in charging and discharging activities within short time intervals to induce variations to the grid stability margins.

To demonstrate the impact of these attacks on the grid, we perform - in the following section - a simulation based analysis of the different attacks an adversary can perform against the power grid. Due to the lack of grid data, we base our simulation on a sample grid model; the WSCC 9 bus system, as it is widely used in the literature [46].

2.4 Experimental Evaluation

We detail in this section the simulation setup and the different attacks that can be performed by the adversary to disturb the grid.

2.4.1 Simulation Setup

As mentioned earlier, our power grid model constitutes of the WSCC 9 bus system as presented in Figure 2.8. We simulate this system in the PowerWorld simulator [49] and perform transient stability analysis for different scenarios.

The WSCC 9 bus system consists of 9 buses and 9 lines; Bus 1 is configured as a slack bus while buses 2 and 3 are configured as generators with a specific inertia. The loads in the system are in buses 5, 6 and 8. All generators are modeled according to the IEEE-G2 model. The total demand of the system is $315MW$. We consider three different scenarios: $1)$ all Level 2, $2)$ all Level 3 and $3)$ both Level 2 and Level 3 EVCSs are uniformly distributed across Buses 5,6 and 8. We assume

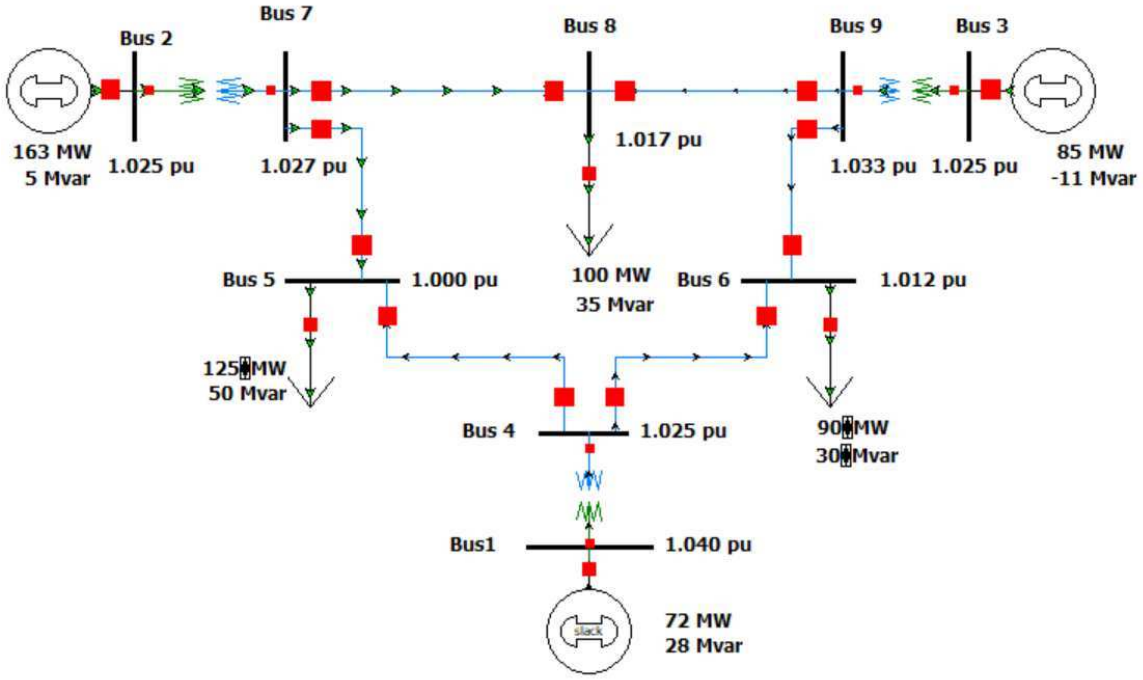


Figure 2.8: WSCC 9 bus system

that the attacker controls some of these EVCS and is creating a bottleneck by either redirecting the traffic to bus 5 or simply starting the charging process at the compromised EVCSs at the same time with no redirection of traffic.

2.4.2 Attack evaluation

We will perform three different types of attacks which are both based on frequency instability.

Frequency instability by increasing demand

In this attack, the adversary tries to cause a system overload by controlling a large number of EVCS and forcing EV drivers to start charging during peak times at the same time instance. Figure 2.9 demonstrate the effect of increasing the load on bus 5 by $25.2MW$ at $t = 10s$.

As can be seen from Figure 2.9, the system was operating at its nominal frequency ($60Hz$). However, at $t = 10s$, the synchronous charging of the EVs started causing a sudden surge in the demand and hence an imbalance between the system's demand and supply. This caused the system's frequency to drop below the critical operating region ($< 59.5Hz$). The minimum increase

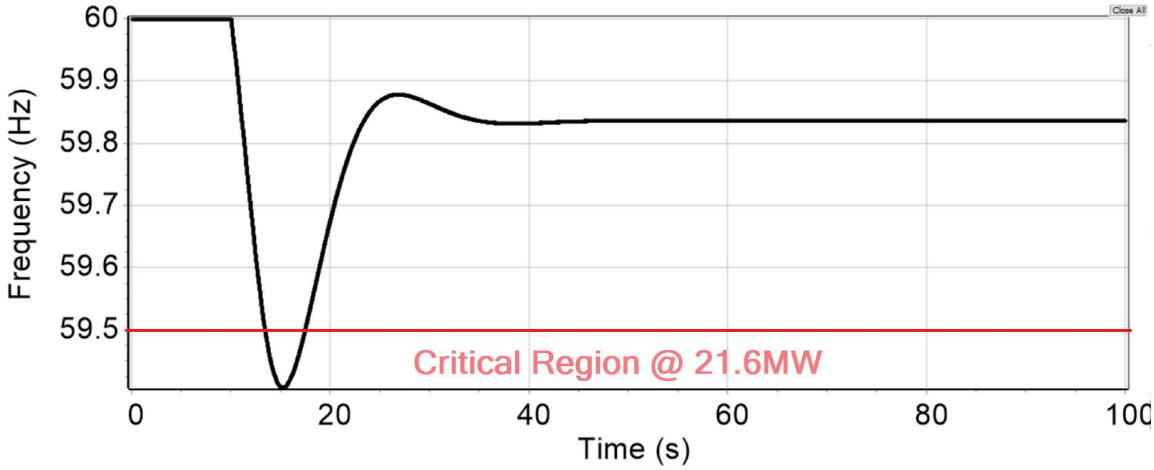


Figure 2.9: Transient Stability Analysis - Demand Surge

in the demand/load on one of the load buses that would cause the system to go into critical region (below $59.5Hz$) is $21.6MW$. Thus, assuming an average of $7.2kW$ power consumption for Level 2 chargers and $104kW$ for Level 3 chargers, this increase in the load corresponds to almost 3000 EVs charging using Level 2 chargers or 210 EVs charging using level 3 chargers. In case of the third scenario where both Level 2 and Level 3 EVSEs are present in the system, this instability corresponds to 1500 level 2 chargers and 105 Level 3 chargers. Further, the same impact on the system happens when the loads on buses 5,6 and 8 increase by an equal amount of $8.4MW$.

The adversary can initiate this impact by simply tampering the schedules so that all EVs start their charging activity at the same time instance without the need of redirecting any traffic. This is due to the fact that causing a surge in the load across all load buses have a similar impact to increasing the load on one specific load bus.

Frequency instability by increasing supply

In order to simulate such an effect, we modify the WSCC 9 bus system to encompass the reverse power flow of the EVs. Therefore, we modify bus 5 to no longer be a load on the system but a generator to simulate the effect of the EV discharging. Further, we assume an average EV; Chevy Volt with the same charging and discharging limit of $3.3kW$ [50]. The discharging effect is shown in Figure 2.10.

From Figure 2.10, a frequency instability of more than $1.8Hz$ was caused due to discharging

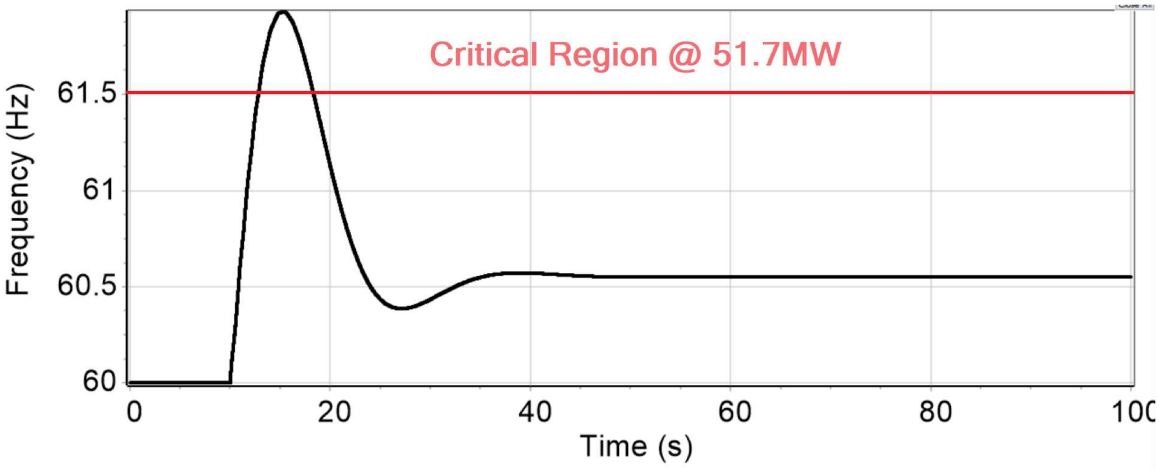


Figure 2.10: Transient Stability Analysis - Supply Surge

20000 EVs at the same time instant ($t = 10s$). This instability is caused due to a sudden injection of power to the grid at a specific time instance. Further, the minimum power supply to cause the system to go into its critical operating region is $51.7MW$ which corresponds to almost 15000 EVs. It is evident that this number of EVs is much larger than the previous attack. This - in return - increases the complexity of such an attack. However, the aftermath caused by this attack is more devastating as the power utility operator may not be prepared for such sudden increase in supply which might cause equipment damage, increase in operation costs and eventually a blackout.

Coordinated Switching Attack

In this variation, the adversary forces the compromised the EVCSs to alternate between charging and discharging the vehicle. In order to simulate such attack variation, we had the same setup as the previous attack variation. However and for sake of simplicity, we assume that the adversary carries out the charging on compromised EVCS located at Bus 6, while the discharging takes place at EVCS at Bus 5. Further, as can be observed from Figures 2.9 and 2.10, the system takes approximately 10 seconds after reaching to its peak to return to its nominal frequency range. Thus, in our coordinated switched attack, we assume the adversary would first start the charging at $t = 10s$ causing a load surge of $25.2MW$. Once the system falls back into its nominal frequency range, we supply the system with $66MW$ corresponding to discharging EVs at $t = 20s$. We then repeat the cycle at $t = 30$ by initializing the charging process, then discharging again at $t = 40$ and finally charging at

$t = 50s$. The impact of this attack is shown in Figure 2.11.

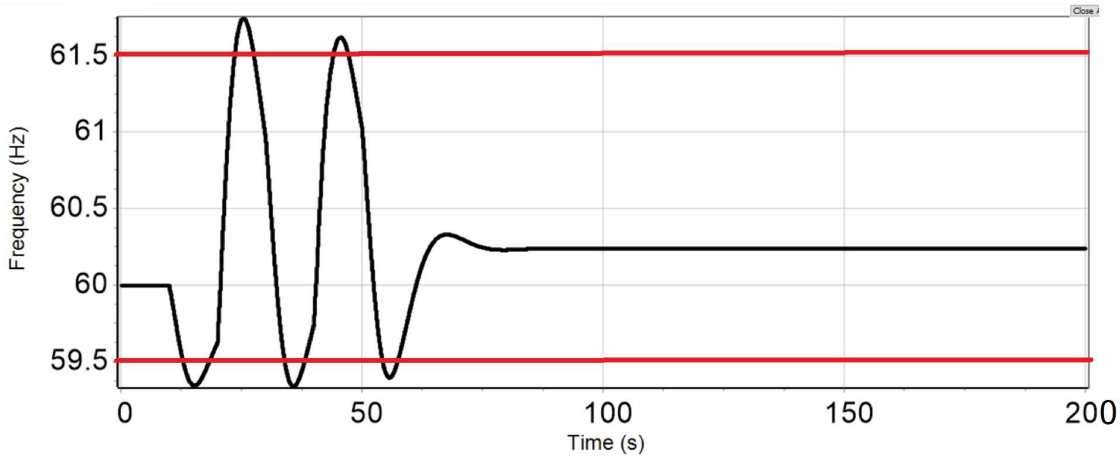


Figure 2.11: Transient Stability Analysis - Switching Attack

As depicted in Figure 2.11, a similar impact is shown as in Figure 2.9 due to the sudden surge in power load causing the system to fall into the critical frequency region (below $59.5Hz$) at $t = 15s$. At that point, different protection mechanisms start to take place and the system corrects itself. Meanwhile, the adversary changes the system status by starting the discharging process at $t = 20s$. Consequently, the system goes into the critical region at $t = 25s$ due to the sudden increase in supply. The attacker then repeats the charging process again at $t = 30s$. However, in order to cause the system to fall into the critical region again, the adversary needs to compensate for the high frequency caused by the supply increase. Thus, the adversary increases the load to $35MW$ instead of $25.2MW$. As a result, the system falls back into the critical region at $t = 35s$. As illustrated in Figure 2.11, the adversary can repeat the cycle by switching between charging and discharging EVs and compensating for the difference between both load values.

2.5 Literature Review

Over the past few years, there has been much work in the literature that focused on the different aspects related to EV charging; from optimizing the energy usage to optimal scheduling and charging placement. Further, given the unique protocols and characteristics of EVCS, some work has addressed the effect of EVCS on the grid [51, 52]. As for EVCS security , the work in the literature

falls in two categories:

Infrastructure Security Analysis This includes approaches discussing the security of different entities of the EVCS infrastructure. For instance, the authors in [18] discussed the security of EVs, EVCSs, building automation and energy management systems, and electric power grids. The authors identified different threats and devised a set of security principles that would prevent and detect cyber-attacks against the EVCS infrastructure as a whole. In addition, the work of [53] analyzed the security of the EV charging infrastructure according to a set of security goals. Particularly, the authors defined the different threats and how they would violate the security triad; confidentiality, integrity and availability. The authors, then, gave different measures to prevent these attacks from the software, hardware and design perspective. In addition, the authors in [54] surveyed the different attacks on the EV infrastructure. However, the authors focused on the security of the communication links between the different entities; vehicles, sensors, grid, road and network.

Protocol Security Analysis While the infrastructure security analysis provides a broad view of the different threats and how to mitigate them, the protocol analysis provides a deeper understanding of the attack surface that would uniquely target the EVCS. Consequently, most of the literature focused on the security of the protocols. For instance, the work in [10] addressed the security of the Open Charge Point Protocol (OCPP) (to be discussed in Section 2.2.2) and its vulnerability to a wide array of Man-In-The-Middle (MITM) attacks. The authors then provided different mitigation strategies for these attacks in [55]. Moreover, the authors in [32] analyzed the security of the ISO 5118 charging protocol by considering different scenarios that would compromise the availability, confidentiality, authenticity and integrity of the charging process. More recently, the authors in [56] focused on the physical layer security of the EVCS and demonstrated how an adversary can eavesdrop on the wireless EVCS traffic, decrypt it and obtain sensitive data such as users' credentials.

On the other hand, the authors in [46] introduced a novel attack that exploits vulnerabilities in high wattage IoT devices to cause disturbances to the grid. Starting from such an attack surface, the authors in [19] extended the victims of such an attack to include the EVCS. They further included public grid data to estimate the grid topology and hence perform a more accurate attack. The authors

however did not exploit the unique characteristics of the EVCS such as bidirectional power flow. Moreover, in both aforementioned works, the authors assumed an adversary has a botnet of high wattage device without demonstrating how feasible this is.

Unlike the work in the literature, our work is the first to address real-world exploitation of EVCS and contextualizing their deployments. We provide a wide-eye view of the EV charging infrastructure by surveying the participating entities and their communication protocols. In addition, we leverage public data on EVCSs to provide statistics on their deployment in terms of their location, operators, etc. Based on such survey, we evaluate the current threat landscape and identify some of the root vulnerabilities in the system. We then propose a novel attack vector that stems from such vulnerabilities and evaluate its effectiveness on disturbing the power grid through a real-world test case and a simulation-based study. Our proposed attack consists of multiple stages:

- **Take Control of EVCS** Given that the EVCS are part of the IoT paradigm, they are connected to the Internet. In this stage, we leverage Internet wide scanning tools such as Shodan, Censys, Zmap to locate EVCS by their IP:port. After locating the EVCS on the Internet, an adversary attempts to remotely access and take control over them. Given that EVCS protocols usually run on top of web servers, we leverage publicly available data to gain full admin access to the EVCS.

- **Create traffic bottleneck** After taking control of a set of EVCS, we investigate the feasibility of creating a traffic bottleneck by tampering the charging schedules of EVs.

- **Disturb the power grid** The last yet most devastating step of the attack is to cause disturbances to the power grid. For that, we exploit one unique property of the EVCS which is bi-directional power flow that allow EVs to discharge their batteries back to the grid. Thus, we investigate three different variations and study their impact on the power grid. The first variation is similar to the ones studied in [46] and [19] which is frequency instability by causing a *sudden surge in the load of high wattage devices*. However, in the second variation, we investigate a novel attack variation caused by a *sudden increase in power supply due to synchronously discharging EVs*. More interestingly, we study another novel variation which is caused by *synchronously charging and discharging EVs in a switching attack*. Although switching attacks on power grids have been discussed in the literature through controlling a set of breakers [47], [48], our work is the first to evaluate this

attack scenario within the context of EV charging.

2.6 Countermeasures

According to the evaluation of our proposed attacks, the aftermath could have devastating impact on the power grid and thus, we propose a set of countermeasures. As illustrated previously, for the proposed attack to be successful, different stages have to be performed successfully, the first one being locating EVCSs remotely. Thus, the first countermeasure is that EVCS operators and owners should better configure their EVCS so that they are not accessible from the outside world. Assuming this step failed and EVCSs were located, it should be impossible for an adversary to gain remote access. Thus, the second proposed mitigation is utilizing strong credentials and/or authentication methods (such as Two Factor Authentication) to prevent an adversary from gaining remote access. In addition, it was noted earlier that there is a lack of standardization within the current charging infrastructure which cause miscommunication between the different entities in the system. Thus, efforts should be made to standardize the protocol with the infrastructure. A promising technology that could aid in such standardization is Blockchain where the different entities can communicate together in a trustless, decentralized and districted environment.

2.7 Conclusion

In this paper, we provided a wide overview of the EV charging infrastructure in terms of its entities and communication protocols. Further, we provided a security analysis of the different protocols and analyzed the possibility of various attacks on the different entities. In addition, based on our survey, we exploited the inherited vulnerability of the charging infrastructure and proposed a novel attack vector in which an adversary can cause large scale disturbances to the power grid. We demonstrated the feasibility of such an attack through real-world experimentation and simulation. We concluded that the current deployment of the EVCSs would allow adversaries to have full access to critical information which threatens user privacy as well as energy theft. Further, with the lack of standardization of the communication protocols, their integration together increases the adversaries chances in compromising the more critical entities in the infrastructure. As a future work, we plan to

study the mitigation of such a coordinated attack by proposing a decentralized system of all entities with the EV charging system. Moreover, we are planning to investigate how an attacker can estimate the power grid to locate its weak links and thus create a more devastating bottleneck.

Chapter 3

Blockchain, AI and Smart Grids: The Three Musketeers to a Decentralized EV Charging Infrastructure

3.1 Introduction

When the movie "Back To The Future" was released in 1985, it boggled the viewers' minds with futuristic technologies which at that time people could hardly believe they would exist. From 3D movies, tablets, and Augmented Reality to flying cars and biometric scanners, these technologies were thought of as science fiction 34 years ago. However, at a glance, it becomes evident that almost all of these technologies are realized as an intrinsic part of our daily lives. Thanks to a paradigm called IoT, sensors, actuators and Internet connectivity could be embedded within everyday "things" transforming them into smart ones [7]. This gives rise to a set of novel use cases including smart transportation, smart cities, smart health-care, etc. Considering its prominent influence, the IoT market is expected to contribute up to 6.2 Trillion in annual income by 2025 [8]. One of the rather interesting services within IoT are ITS and Smart Grids [8].

ITS encompasses a wide range of different services including self-driving cars, street surveillance and traffic monitoring. When put together, such services would form an intelligent network of

cars, Road-Side Units, traffic lights, etc. to offer the users with seamless driving experience [57]. In addition, in a smart grid environment, energy usage is monitored and managed through smart meters and controllers [58]. While each sector provides its unique services, new opportunities arise from their overlapping, one of which are EVs and their charging infrastructure. Although flying cars are yet to exist, there have been major advancements in vehicular technologies that rendered EVs as a lucrative opportunity for both industry and academic sectors. To put it in perspective, according to the International Energy Agency (IEA), EVs have exceeded 5.1 Million globally in 2018. Further, by 2030, it is projected that the EV stock would reach up to 250 Million cutting the demand for oil products by almost 130 tonnes [59]. In addition, Norway projects that by 2025 all new car sales would come from EVs. Other countries like the United Kingdom and France are proclaiming the same projections by 2040 [60]. With such a vision, a set of challenges needs to be addressed for a more robust EV ecosystem.

The high stakes set by policymakers and the high penetration rate of EVs create an urgent need for procuring a charging infrastructure to match the EV drivers' demands. As a result, many companies (such as Siemens, Shell, etc.) ventured towards manufacturing EVCS. Further, new companies including ChargePoint and Enel, are leading the EVCS market. From custom payments to membership cards, all the way to EVCS localization, what all these companies have in common is providing the EV drivers with beyond-satisfactory driving experience. Nevertheless, the current charging solutions lack some of the most essential properties. The two most prominent challenges facing the EV charging infrastructure is the scheduling of EV charging along with privacy and security.

The scheduling of EVs represents a dilemma as of to whether satisfy the EV driver by providing fast and reliable chargers at every possible location or minimize the number of chargers to avoid disturbances on the power grid. With that in mind, many research efforts have focused on leveraging different technologies and techniques such as AI, and Optimization, etc. to provide improved charging schemes while satisfying both the power grid and EV drivers. On the other side of the spectrum, security and privacy are the long-lasting enemy of the IoT paradigm. Being part of the IoT environment, it has been shown in different research contributions that EVCSs are vulnerable

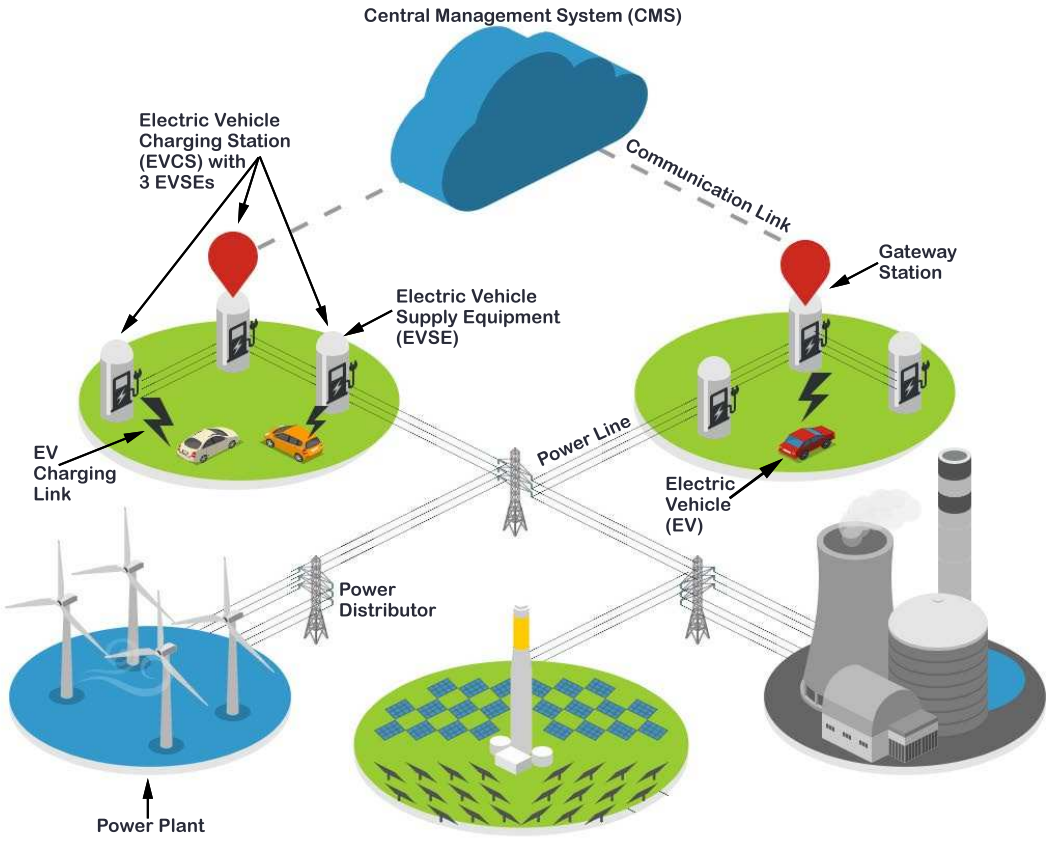


Figure 3.1: Electric Vehicle Infrastructure and Protocols

to an array of cyber-threats including DoS and RCE. Such vulnerabilities may not only lead to energy and users' private data theft, but also to threatening the charging infrastructure as a whole, all of which would impact the adoption of EVs [18]. Accordingly, there has been major research efforts to mitigate such vulnerabilities by proposing lightweight security protocols and leveraging technologies such as Blockchain and AI.

While different technologies could be leveraged to mitigate the aforementioned challenges, we focus in this paper on Blockchain and AI. Blockchain is a secure distributed and decentralized ledger of transactions, allowing different entities to perform transactions between different entities in a trust-less, decentralized and secure environment through the use of Hashing, Consensus mechanisms and Smart Contracts. On the other hand, AI has excelled in determining unrecognized patterns and making decisions accordingly. With the aforementioned discussion, our main contributions are:

- Providing a wide-eye view of the current deployment and protocols of EV charging and identifying the key challenges being faced with the EV infrastructure, specifically regarding scheduling and security.

- Evaluating the role of AI and Blockchain in solving such challenges. Specifically, we survey the different solutions from both the industry and academic sectors that leverage these two technologies separately opening the door to further identifying gaps and unsolved issues.

- Evaluating how the two technologies could be exploited in a complementary fashion to provide a more robust charging ecosystem.

The remainder of the paper is organized as follow: we discuss, in Section 3.2, the current deployment and protocols of the EV charging infrastructure, as well as the challenges being faced. We then discuss how AI and Blockchain could be used to solve these challenges in Section 3.3 and 3.4. Further, we evaluate in Section 3.5 how both technologies can be used jointly to deliver the best charging service to the end-user. We finally discuss possible research directions in Section 3.6 and conclude in Section 3.7.

3.2 EV Charging: Deployments, Protocols and Challenges

The EV charging infrastructure is composed of multiple entities communicating via a set of different protocols. Figure 3.1 shows an abstraction of the current deployment of the EV charging infrastructure and its constituents are:

- **Energy Supplier:** The Energy Supplier could be any entity that is able to supply sufficient energy to operate the charging stations.

- **Electric Vehicle Charging Station:** With the energy supplied from the power grid, the EVCS is the medium at which EVs drivers can charge their vehicles. The EVCS itself is compromised of the EVSE which are the actual physical devices that EVs connect to via connectors/plugs. Typically, EVSEs come in three different types depending on their power rating; Level 1, 2 & 3, with Level 3 being the most powerful [19]. In addition, EVSEs could be

public or private depending on their access methods. Further, depending on the deployment, a set of EVSEs are usually connected to the gateway station via Local Area Network (LAN). The gateway station then connects the CMS via Wide Area Network (WAN).

- **Central Management System:** The CMS is a software responsible for managing the charging stations in terms of scheduling EVs, logging transactions, creating a database of authorized users, etc.

- **Electric Vehicles:** EVs are the end users that receive the power through their physical connection to the EVSE.

In terms of communication protocols, there is a myriad set of protocols being used within the EV charging ecosystem. For instance, OCPP is an open source communication protocol between the EVCS and the CMS. It manages the registration of EVCS as well as remotely controlling their operations. Moreover, different companies such as Schneider Electric, Siemens, etc. utilize their own proprietary communication protocols between the EVCS and the CMS. Also, the power flow from the EVSEs to the EVs is managed by a set of communication protocols. The most prominent ones are: ISO-15118, IEC61851, SAE-J2293 and chAdeMO [18].

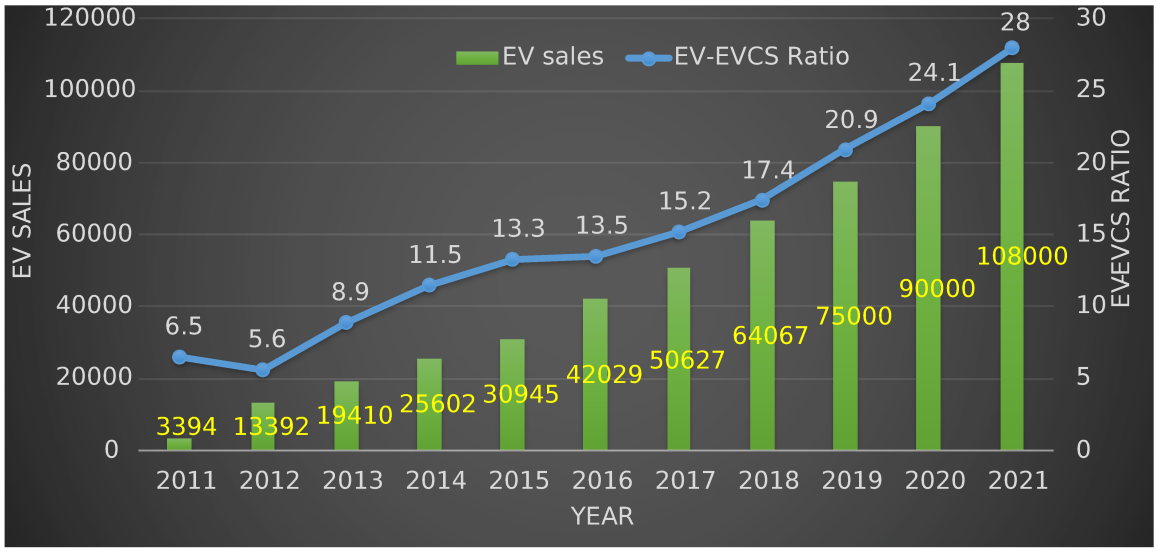


Figure 3.2: US EVs to EVCS ratio*

*Data Source: https://afdc.energy.gov/

Besides the infrastructure and protocols, the EV market has been evolving over the past decade

and accordingly the business of its charging ecosystem is booming. Figure 3.2 contextualizes the sales of EVs and their ratio to EVCSs over the past 10 years in the US. As can be seen from Figure 3.2, the number of EVs has been increasing in almost a linear rate every year. However, the number of deployed EVCS is not increasing at the same rate causing an increasing gap between EVs to EVCSs.

With the aforementioned discussion on EV charging deployments and protocols, we identify two main challenges facing the charging ecosystem:

3.2.1 Security and Privacy

Security and privacy are always a major concern when a new service comes into existence. The EV charging infrastructure is no exception. By observing closely the current charging infrastructure, two major concerns become evident. The first concern is having multiple protocols. This variety imposes vulnerabilities to the system as each one of these protocols brings about its own unique set of vulnerabilities. For instance, OCPP was found vulnerable to Man-In-The-Middle Attacks (MITM) [10]. Thus, having a set of protocols used with the current charging ecosystem renders the overall system insecure. This, in return, leads to the second challenge which is having multiple entry points to the system. Each of the entities and protocols within the charging infrastructure could be exploited and compromised. For instance, many EVCSs by major operators were found to be vulnerable to RCE, and Buffer Overflow attacks [18]. Thus, an adversary could exploit the most vulnerable entities to compromise the more critical ones (Power Grid). These scenarios can render huge leverage to an adversary giving him/her the capability of stealing users' critical data, energy theft, and causing a DoS attack. To exacerbate the situation, given that these EVCSs have high power ratings, compromising them and synchronously tampering the schedules can cause disturbances to the grid due to a sudden increase in load [19].

3.2.2 Optimal Charging Schedules

The second most critical challenge facing the EV charging ecosystem is the lack of optimal scheduling schemes. According to CleanTechnica, 40% of 3000 EV drivers believe that EVCSs are somewhat conveniently located for their needs. Further, almost half of these drivers found that the

current infrastructure is somewhat adequate for long-distance trips. By correlating these statistics with Figure 3.2, this trend of mediocre satisfaction is likely to remain as the gap between the EV and EVCSs is increasing over time. Although there have been major research efforts targeting the problem of EVCS placement and EV charging, as well as developments in batteries technologies allowing EVs to travel longer distances per charge, the major challenge resides in trading-off customer satisfaction in terms of waiting time and reliability, and minimizing load fluctuation on the power grid.

There have been major research efforts that tackle the aforementioned problems by introducing lightweight secure charging protocols, proposing improvements on existing protocols or restructuring the infrastructure for secure charging ecosystem. On the other hand, different optimization techniques and game theoretic approaches were proposed to solve the scheduling and placement problem. In what follows we evaluate the use of AI and Blockchain technologies to tackle such challenges.

3.3 AI: Towards Intelligent EV Charging

Artificial Intelligence has been around for a couple of years and it has proven its applicability and efficiency in solving complex problems in different fields. The edge of AI is its capability to detect complex patterns and provide forecasts accordingly. Within the context of EV charging, AI could be the solution towards devising optimal charging schemes. As a result, many research contributions from patents, publications, books, etc. have explored the role of AI in the EV charging ecosystem. We scrapped Google Scholar to collect data on publications and patents on the use of AI within the EV charging environment and demonstrated the results in Figure 3.3.

As demonstrated in Figure 3.3, over the past decade, there has been an increase of almost 500 publications per year. More interestingly, the number of patents has also been increasing over the past decades. By closely observing the publications, the role of AI in the EV charging ecosystem becomes more evident. To contextualize this role, consider a scenario where a large number of EV drivers need to charge their vehicles during peak times. If the charging of those EVs starts at the same time during peak hours, there would be a surge in load on the power grid. Thus, a

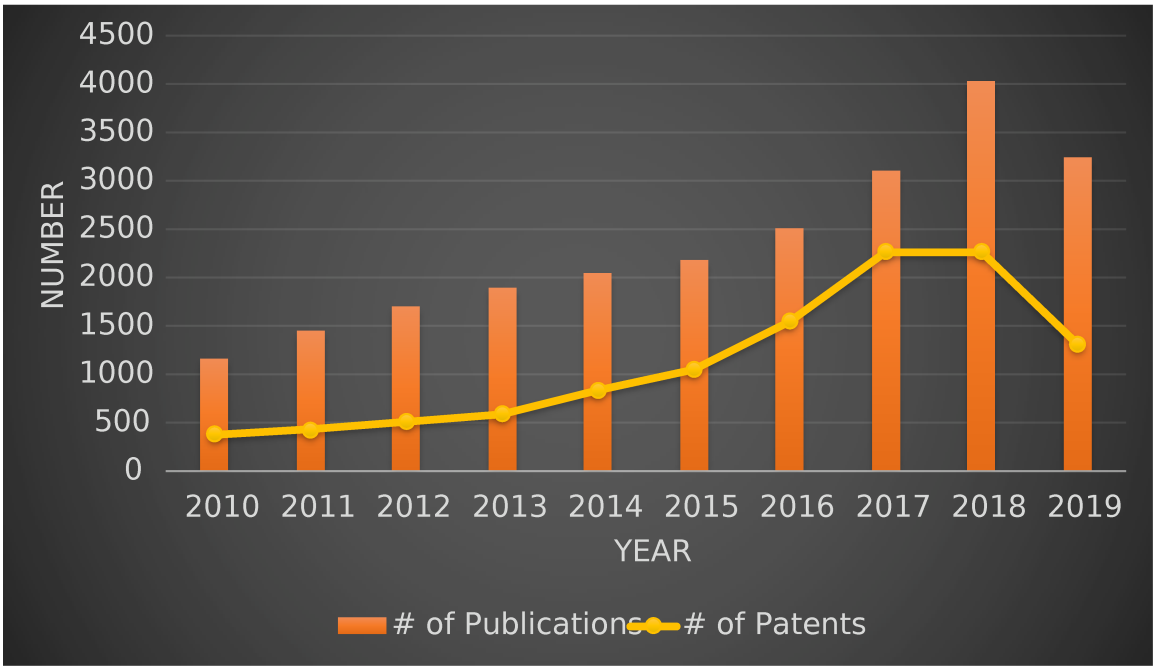


Figure 3.3: The Use of AI within the EV charging environment in terms of publications and patents over the past decade

dilemma exists as to how to satisfy these EV drivers without causing a huge load increase on the grid. This could be solved using optimization or game theory. However, in order to solve this scheduling problem, the EV drivers' charging behavior should be considered. This is where AI comes into play. By exploiting meta-data on EV drivers' driving habits, charging behaviors, trips, etc., an AI agent could not only predict the charging behavior of EV drivers, but also the EVs' load profile on the power grid over time. This becomes very handy to the grid operator to manage the schedules of the EV drivers based on the forecasts from the AI agents. Further, AI could further be exploited to orchestrate the locations of EVCS to be deployed. By collecting readily available data on a population living in a specific area, as well as historical data of EV drivers, an AI agent could predict the percentage of the population that is more likely to purchase EVs along with the potential load profile. Thus, from the grid operator perspective, these predictions could be leveraged to plan the locations of EVCS to be deployed. Thus, the role of AI could be summarized in *(1) Load profile prediction to optimally deploy EVCS, (2) EV drivers' behavior forecast for better scheduling schemes*

On the industry side, the role of AI still serves the same purpose, and as such, there has been

few companies, start-ups that leveraged AI to improve the EV charging infrastructure. For instance, Oracle acquired Opower Inc. in 2016 gaining access to billions of data points on households' energy usage from 60 million customers across 100 utilities. Leveraging Oracle's deep learning framework, this rich dataset is used to forecast EV loads and inform power utilities so they would manage their power generation accordingly to accommodate for the load. Another interesting use case of AI is by a startup called GBatteries that demonstrated their patent in CES 2019. The company uses AI to speed up the charging process by collecting health indicators from the EV battery. These indicators are then analyzed and a decision is made determining whether the battery could be charged using the maximum power. The trade-off here is that charging at the maximum power leads to faster charging however, it comes on the expense of depleting the battery. Thus, by leveraging AI, a decision on the power level to be delivered to the EV battery is made.

In short, the power of AI revolves around detecting complex patterns and providing decisions/forecasts that could be mainly used by the power utility to better manage their power generation, or by EV drivers to speed up their charging.

3.4 Blockchain: For Secure Decentralized EV Charging

Blockchain is a disruptive technology that allows entities to perform transactions in a *(1) Distributed: all transaction history is distributed among all nodes in the network, (2) Decentralized: no central entity controlling the transactions, (3) Secure: through the use of Public Key Infrastructure (PKI)* environment. The basis of Blockchain is to allow different nodes/entities to communicate together in a trustless environment without the need to rely on a central entity to overlook these transactions. With such, the applicability of Blockchain could be extended from simply a distributed ledger, to include trading of digitized assets (Energy, money, etc.). The first application of Blockchain dates back to 2008 when Satoshi Nakamoto introduced the Bitcoin network as a way to transfer monetary value between different sources without the need for a bank. Later, Ethereum was born allowing the Blockchain technology to reach its true potential by allowing the creation of Decentralized App (dApps for short). With Ethereum, the concept of smart contracts was introduced which are pieces of software residing on the Blockchain network and automatically invoked when

specific clauses are met. With smart contracts, Blockchain provides an edge in creating decentralized economies for trading virtually any asset. An abstraction of a Blockchain network consists of three main layers:

- **Network Layer:** The network layer represents the communication protocol between the nodes in the network. Usually, the Blockchain network operates using Peer-to-Peer (P2P) protocols.

- **Consensus Layer:** The consensus layer is responsible for ensuring the validity of the data being shared in the Blockchain network. That is, when a transaction is issued and broadcast over the network, how to make sure that it is a valid transaction. For that, different consensus algorithms have been proposed with Proof of Work (PoW) and Proof of Stake (PoS) being the most famous mechanisms used. For scalability, specific nodes in the network known as miner/validators are responsible for performing the consensus algorithms. Further, depending on the implementation of the network, these validators/miners could be awarded with cryptocurrency for their contribution.

- **Transaction Layer:** The transaction layer is the last layer in the stack and its responsible for handling data being transacted in the network. Simply, it defines smart contracts and makes sure that they are properly invoked.

With such abstraction, Blockchain networks could be:

- **Public/Permissionless:** anyone can join the network and participate in the consensus/validation process.

- **Private/Permissioned:** only a set of authorized nodes can not only perform the validation process but also decide who joins the network, manage the network in terms of updates, etc.

Each implementation of the Blockchain network has its pros and cons. For instance, public Blockchain networks are the closest form of a decentralized, trustless environment that relies on its nodes to sustain itself. However, this comes at the expense of the speed due to a large number of participating nodes. On the contrary, private Blockchain networks are more scalable and faster networks, however, they give more control to the authorized nodes.

Within the context of EV charging, Blockchain networks could be the answer to the security and privacy problems facing the current infrastructure. Accordingly, there have been efforts from both the research and industry sectors to utilize Blockchain networks with EV charging. Similar to AI, we contextualize these efforts in Figure 3.4.

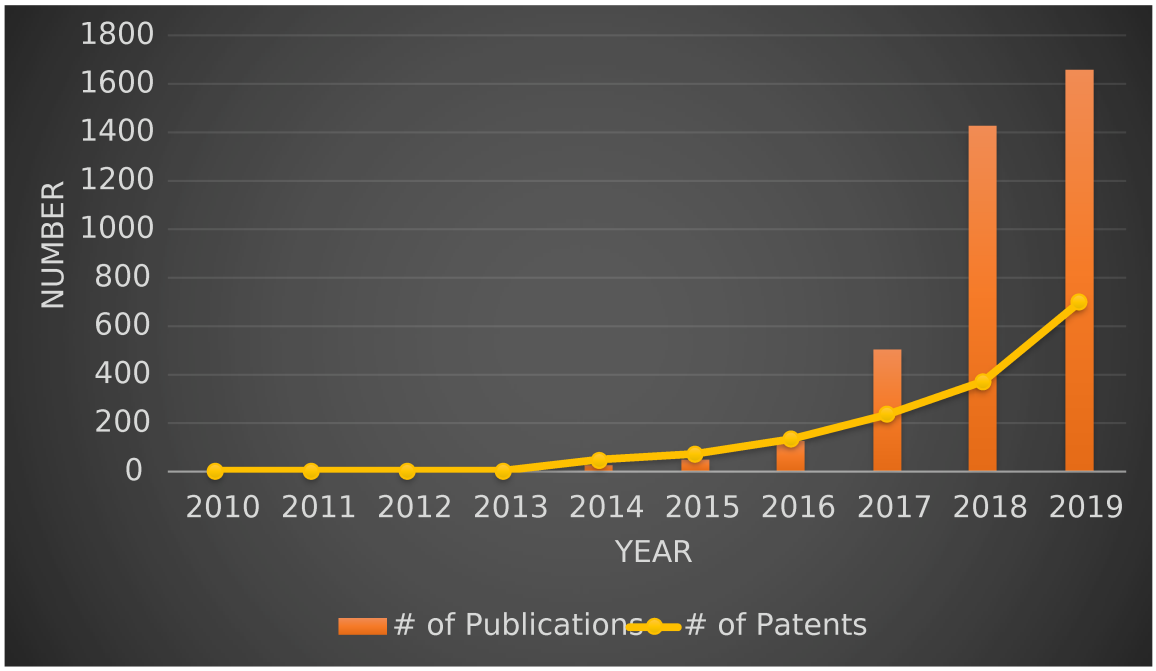


Figure 3.4: The Use of Blockchain within the EV charging environment in terms of publications and patents over the past decade

As shown in Figure 3.4, the number of publications and patents for Blockchain-enabled EV charging network started to see the light in 2014 followed by a huge increase by 2018 and 2019. To put these efforts in perspective, the early contributions were about digitizing energy by proposing P2P energy trading systems. Later, publications moved towards a Blockchain-enabled EV charging ecosystem that would allow the integration between smart grids and EVCSs to serve EV drivers. For instance, some research efforts focused on creating a Blockchain network to securely manage the energy trading between local communities generating energy and EVCSs. This scenario becomes advantageous as it would eliminate intermediaries (lower costs), and prevent malicious entities from misusing the system. Other work focused on creating a network of Blockchain networks composed of all entities participating in the charging infrastructure. [61, 62, 63]

On the industry side, the major role of Blockchain in the EV environment is to enable secure

energy trading by allowing homeowners to sell their energy (making their EVCS open to the public) to other EV drivers in a decentralized environment. Within this P2P energy trading context, different companies have taken initiatives to build Blockchain-enabled EV charging networks. For instance, Oxygen Initiative has extended already existing EV charging protocols (ISO-15118) and proposed a Blockchain network that enables either the utilities or any EVCS to offer pricing and grid conditions for EVs. Thus, in a sense, their network acts an auction house for the EVs allowing them to choose the best available options as well as giving them incentives if they choose to delay their charging to later times. The company believes that its system could further be extended to include the functionality of EV drivers selling energy back to the grid. Further, a company called Charg offers an Uber-like service, through the Ethereum network, for energy trading by allowing anyone to lease their EVCS to EV drivers in what they have called the Internet of Energy (IoE).

Thus, the key role of Blockchain resides in aiding EV drivers and home owners to trade energy securely with no intermediaries. This functionality could be easily extended to include EV drivers selling energy to the power grid as a way of peak shaving. Hence, Blockchain serves as an incentive for EV adoption as it would benefit both homeowners (making their EVCS public) and EV drivers (selling energy to the grid).

3.5 The Best of Both Worlds: Blockchain and AI

Based on the aforementioned discussion, AI plays a key role in managing the schedules of EVs and orchestrating their deployments through load profiles' forecast and charging behavior predictions. However, an AI-enabled charging system still relies on a central entity (power utility) to manage the transfer of energy. This scenario becomes particularly problematic when the security is taken into consideration. For instance, malicious entities can compromise EVCS and either cause disturbances to the power grid or simply steal energy or users' critical data. On the other hand, Blockchain aims at providing a secure, trustless, decentralized and distributed energy trading system. With such, this system could render intermediaries and central entities obsolete reducing unnecessary operational costs. Further, the Blockchain charging network could serve as an auction house where different energy suppliers (utility, private EVCS owners, etc.) could broadcast their

availabilities and prices over the network based on the grid and EVs conditions. However, the deployments of smart contracts in Blockchain lacks the flexibility to accommodate to the dynamic charging behavior of EV drivers and grid conditions. Thus, for a fully-fledged EV charging system, AI and Blockchain should complement each other.

One such scenario on the collaboration of AI and Blockchain is the work done in [64]. The authors proposed a Blockchain-enabled EV charging system where (1) EV drivers could charge their EVs from either the power grid, private EVCS owner, local communities, (2) drivers can discharge their EVs back to the grid to help reduce the load on the power grid. The authors then considered the optimization of the charging/discharging schedules through an adaptive algorithm to account for the change in EV charging demands.

Another scenario for the collaboration of AI and Blockchain is in [65] where the authors focused on the scalability of the Blockchain network itself rather than the schedules of EVs. Particularly, the authors leveraged deep learning to, based on EV data, maximize the transactional throughput while ensuring decentralization, latency and security of the system. This is particularly interesting as the proposed system is capable of changing its working mechanisms (block size, block dynamics, etc.) according to the dynamic changes in the environment.

On the industry side, a team in the Odyssey Hackathon, the Porsche Digital Lab, proposed a Blockchain-enabled charging environment backed with AI. The motive was similar to the aforementioned discussion, which involves reducing load on the grid, increasing user satisfaction and ensuring security. As a result, the team proposed an energy trading economy that allows local communities to lease their EVCSs, and EV drivers to sell back their energy. Further, the team introduced an AI agent to manage the schedules of EVs by predicting prices, availabilities and driving patterns.

3.6 Research Directions

Aside from existing work, the collaboration between AI and Blockchain goes beyond merely creating an open trading ecosystem for digitized assets. The true value for such collaboration prevails when considering the challenges they mitigate. In terms of security, Blockchain, indeed, provides a secure and immutable record of transactions through PKI and consensus algorithms. In fact,

by decentralizing and distributing the infrastructure, Blockchain mitigates one of the root causes of having a vulnerable charging ecosystem; multiple entry points. Particularly, with a decentralized system, the role CMS and power grid as managing entities would be rendered obsolete and would merely act as facilitators, reducing the threat landscape. Moreover, AI has held its ground in providing forecasts as well as detecting anomalies. Therefore, integrating AI with Blockchain paves the way for creating self-sustaining, self-correcting ecosystems. To put it in perspective, AI can be integrated within each layer of the Blockchain network providing different functionality at each layer. At the network layer, AI can be used as an added security layer to predict anomalies in the network and take action accordingly (isolating malicious nodes for instance). Further, at the consensus layer, AI can be used as a scalability measure to predict the system dynamics (network size, data frequency, etc.) and accordingly adjust the consensus mechanisms (block size, block generation time, etc.). Finally, AI can be used in the transaction layer to both detect anomalies, forecast the system dynamics, all of which would be used to adjust the smart contracts for better EV scheduling mechanisms. In principle, the integration of AI and Blockchain serves as the niche for self-correcting EV charging ecosystem.

While the research shows promising theoretical results, there is a need for further explorations. Specifically, the scalability and reliability of Blockchain within the EV charging networks need to be properly evaluated given the penetration rate of EVs. This can be further extended to develop new consensus algorithms that reduce the overhead in the network while considering the trade-offs in terms of security. Moreover, given the transparency in Blockchain transactions (all transactions are available and accessible), research directions in Zero-Knowledge Proofs (ZKP) and Homomorphic encryption are needed to solve this privacy issue. In addition, the use of federated learning within the Blockchain network is a rather interesting research direction that would aid in providing a fully-decentralized network with distributed AI nodes. Another way of decentralization is to abstract the EV charging network as a Multi-Agent System (MAS) with some agents responsible for data collection, AI calculations, block validation, etc. Thus, each agent can perform independently its allocated task Further, much of the work that integrated AI and Blockchain was on the theoretical side. However, there is much-needed real-world experimentations of such proposed systems to properly evaluate their performance. In addition, some research has been made on how to leverage

AI to detect new vulnerabilities, thus it would be interesting to explore the resilience of Blockchain and AI charging networks against demand-side IoT attacks (where an adversary compromise high wattage devices to cause disturbances to the grid), as well as new ones. A more interesting research direction is how to extend existing protocols (such as OCPP) to exploit both technologies for better security and energy management.

3.7 Conclusion

In this paper, we investigated the current deployments, protocols and infrastructure of the EV charging ecosystem. We identified two key challenges which are trading-off user satisfaction and grid operations and security and Privacy. For that, we evaluated, through collecting data on recent trends from research and industry, the use of AI to manage the schedules of EVs and help provision EVCSs. Similarly, we evaluated the role of Blockchain in securing the EV charging ecosystem and providing a trustless trading system that allows EVs, private EVCSs owner and power utilities to trade energies. It was shown that Blockchain can (1) help manage peak shaving by giving incentives to EV drivers to sell energy to the grid, (2) increase the satisfaction of EV drivers by allowing the selling of energy from private EVCSs owners and local communities, as well as lowering the costs by excluding intermediaries. While both on their own target some key challenges, a more-robust charging ecosystem requires the integration of AI and Blockchain. For that, we evaluated different use cases on how AI and Blockchain could be leveraged together to improve the charging ecosystem.

Chapter 4

An Anomaly Detection Engine for Securing the EV Charging Ecosystem with Blockchain and AI

4.1 Introduction

4.1.1 Motivation

Back in 1995, Clifford Stoll published an article in Newsweek titled "Why the Web won't be Nirvana" [66] dooming the fate of the Internet as an obsolete and speculative tool. One of the rather interesting quotes from the article was "...no computer network will change the way government works.". Fast-forward to a decade later, the Internet became not only an integral part of our lives but ironically a major influential tool on how governments work. Nowadays, the notion of the Internet extends from having two computers connected together, to millions of "things" capable of collecting, sharing and analyzing information, in what is known today as the IoT [7]. Thanks to advances in communication and computing technologies, the IoT paradigm enabled for services such as smart hospitals, smart transportation, smart factories, etc. that would, otherwise, be conceived as science fiction [6]. One particular service of interest is ITS and specifically EV and their charging infrastructure.

While the road to having fully driver-less smart vehicles is still ways behind from the finish line, EVs are considered a step in the right direction. To put it in perspective, the first EVs were introduced in the United States back in 2010 through the Chevy Volt and the Nissan Leaf. Due to many barriers including range limitations and outdated designs, EVs did not gain the appeal of the consumers. In the years that followed, major investments and incentives have been put in place causing a paradigm shift to the EV industry in terms of consumer adoption, public perception and technological developments. Nowadays, all car manufacturers have at least one EV model available to the consumers covering all their needs from economical and family SUVs to luxury and performance EVs [67]. With such penetration rate, the International Energy Agency (IEA) predicts that the number of EVs would reach 120 Million by 2030 [68]. Looking at the EV revolution and the sales forecasts, nothing would have been possible without the proper charging infrastructure.

The increasing demand on EVs over the past few years created a pressing need to procure the proper charging infrastructure for the EV drivers. This, in return, created a novel and lucrative business and research opportunity for both the industry and academia. To contextualize such an opportunity, the EVCS sales have witnessed almost 800% increase from 2012 to 2016 [69]. Hence, the business of the EVCS was booming in accord with the EV revolution to meet the drivers demand. Although EVCS sales were increasing each year, there is a set of barriers that needs to be addressed. One such barrier is the increasing gap between EVs and EVCS. According to the International Council of Clean Transportation (ICCT), given the forecasts for EV sales, there is still much infrastructure needed to meet such demands [69]. This in return raises some other issues, one of particular interests is the security of the EV charging infrastructure [18, 19].

4.1.2 Literature Review

Over the past few years, IoT has established a solid foothold in almost every field and sector. This paradigm shift from basic and human-dependent services to intelligent and human-machine integrated services, has transformed people's view on different aspects of technology in general and specifically on privacy and security. According to surveys by Mozilla, privacy is a major concern for IoT users [70]. From privacy and security labels [71], to lightweight security protocols [72], the literature is rich with security and privacy-preserving solutions targeted towards a more secure

IoT infrastructure. Going from generic IoT devices to application specific appliances, EVs and their charging infrastructure are no exception either. According to [73], the EV charging infrastructure is no stranger to security breaches and privacy concerns. With that, we broadly categorize the work in the literature targeted towards the security of EV charging infrastructure into:

Security Analysis

The opportunities that the EV industry brought forward did not only serve the consumers, but also opened the door for new and interesting research directions. With security being a major concern, lots of research efforts focused on analyzing the security of EV and their charging infrastructure. For instance, the authors in [73] provided a detailed assessment of the security of the EV charging ecosystem as a whole as well as the specific entities and protocols involved. On a different note, other works provided more vertical evaluation of the EV charging ecosystem by focusing on the protocols involved or the entities participating. On the protocol level, for example, the authors in [10] evaluated the security of the OCPP; an open source protocol for managing the communications between the EVCS and the CMS. Their findings included vulnerabilities in the protocol such as Man-in-The-Middle (MiTM) attacks. Another example for protocol analysis is [32] where the authors analyzed the security of the ISO-15118 protocol used for the Vehicle-2-Grid (V2G) communications. Similar to OCPP, it was concluded that ISO-15118 is vulnerable to DoS, MITM and jamming attacks. In a more practical implementation, the authors in [56] evaluated the physical layer security of the EV charging provisioned by ISO-15118. Among their conclusions, the authors found that an eavesdropper can recover almost all messages exchanged between the vehicle and the charger. On the infrastructure side, the authors from Kaspersky lab discovered, by analyzing the EVCS and reverse engineering their firmware, that they are vulnerable to many attacks including RCE [40]. While such vulnerabilities affect the operations of the EVCS and hence the adoption of EVs, they can have a much more devastating impact given the entities involved within the charging infrastructure. Specifically, an adversary can cause disturbances to the power grid by compromising a number of EVCS as shown in [19, 66].

Mitigation Strategies

By observing the security flaws in the EV charging ecosystem and the severeness of the vulnerabilities discovered, lots of research efforts has focused on the mitigation side. One of the more active field of research is developing more secure and privacy-preserving protocols for the EV charging ecosystem. Particularly, the authors in [74, 75, 76] proposed the use of Blockchain to secure the communication between EVs, EVCS and the CMS. Although the proposed system proved efficient in mitigating some of the threats such as DoS attacks, their scalability remains an issue towards their adoption. Other approaches [77, 78] followed a horizontal approach by proposing novel architectures for the charging infrastructure. In addition, some authors focused on securing the existing protocols (for example ISO-15118 and OCPP) against the discovered attacks [55, 79]. A different yet relevant mitigation strategies is leveraging machine learning and AI to detect anomalies in the smart meters values [80, 81, 82]. Such anomaly detection engines would facilitate detecting patterns and constructing normal profiles which would, in return, aid the power utility to detect malicious behaviors. However, to the best of our knowledge, no work has been done in detecting such anomalies in the context of the EV charging ecosystem and the attack scenario described.

4.1.3 Contribution

The majority of work in the literature focused on identifying the security threats and vulnerabilities in the EV charging infrastructure, providing novel abstractions of the ecosystem or developing new secure protocols or anomaly detection engines by leveraging tools such as Blockchain and AI. While such efforts provide guidelines for further explorations, this current work focuses on a more specific attack scenario and its mitigation. Particularly, we consider the demand-side IoT attack described in [46] within the context of EV charging. The IoT demand-side cyber attacks are nothing more but creating a botnet of compromised IoT devices to cause surge in power demands [46], with the ultimate goal of disturbing the power grid. Given the bidirectional power flow properties of EVs and the high power ratings of the EVCS, an adversary can launch a devastating cyber attack that cause disturbances to the power grid simply by compromising a number of EVCS and tampering

the schedules of EVs so they start charging/discharging simultaneously. Thus, unsecured and unmanaged EV charging can cause devastating impact on the more critical entities; power grid. To this end, we propose in this paper an anomaly detection engine that would enable early detection of such attack scenarios. Particularly, the main contributions are:

1. We propose an anomaly detection engine that collects EV charging schedules from the CMS of public networked charging stations. By collectively analyzing these schedules, the engine classifies whether these schedules are tampered with or not and thus, detecting a demand-side attack.

2. We perform simulations based on real-world data of the Irish public charging stations and power grid data. In addition, we evaluate our detection engine against different attack variations leveraging different types of learning algorithms (auto-encoders, distance-based and statistical algorithms). In essence, the proposed engine could detect mass behavioral change in the EV schedules, as well as subtle behavioral changes that could be leading to the attack. Further, the sensitivity of the detection could be easily tweaked allowing for detecting more complex attack variations.

3. In the case of private charging stations, we leverage Blockchain to provide an open energy trading architecture for the private EV charging infrastructure and its entities including EVCS, EVs and power utility. In principle, we define the participating nodes in the Blockchain network and their corresponding roles. Further, we explain how to provision the underlying transactions through smart contracts.

4. Thanks to the transparency of Blockchain networks, we exploit the public record of energy and data transactions as a feed to our AI engine. Essentially, the integration of the Blockchain public record of transactions and the AI engine provide a comprehensive solution for securing both public and private EVCS. Thus, anomalous behavior on both public AND private EVCS could be easily flagged by the interested entities (power grid in this case) to prevent the demand-side attack of occurring.

4.1.4 Outline

The remainder of the paper is organized as follows; we describe the EVCS demand-side attack scenario in Section 4.2. The detection strategies for public charging settings are discussed in Section 4.3. The experiments setup and the results are detailed in Section 4.4. Section 4.5 discusses the limitations of the proposed system and addresses its applicability for the private charging setting. Finally, we conclude in Section 4.6.

4.2 Attack Scenario

In order to better understand how critical the charging infrastructure is, it is essential to describe the targeted attack scenario. For that, we circle back to the idea of Distributed Denial of Service (DDoS) attacks within the context of IoT. In such attacks, an adversary compromises a number of IoT devices creating a botnet. By carefully instructing the bots within the botnet, the adversary can target websites, services, etc. as was seen in the Mirai Botnet attacks [83]. A novel variation of this attack scenario was proposed in [46] where the authors targeted the power grid by creating a Botnet of high-wattage IoT devices (smart heaters, refrigerators, etc.). With the EVCS being high wattage smart devices (7.2 kW for Level 2 chargers) in nature, this attack variation can be extended further to include creating a Botnet of EVCS and target the power grid causing blackouts [19]. With the inclusion of EVCS in such attack, its severity becomes more critical. This is due to the intrinsic characteristics of the EVCS including high wattage, ability for EVs to charge AND discharge to the power grid.

With the aforementioned discussion, we assume in this work an adversary with the ability to control a number of the EVCS available in the system. The validity of this assumption comes from the fact that the EVCS owners would control their EVCS in terms of availability, schedules and bookings through a web interface accessed by their credentials. This implementation is predominant in the OCPP which manages the communication between EVCS and the CMS. Thus, we assume that an adversary can compromise these credentials and thus take control over the EVCS. Once full control is achieved, we assume an adversary could apply different techniques with the goal of changing the schedules of the EV. An example of such techniques would be broadcasting low

prices to EV drivers from the compromised CMS. The idea here is that the adversary is allowing a large number of EVs to start the charging process at the same time. Consequently, if an adversary successfully changed the schedules of EVs making them start charging synchronously, he/she can cause frequency instability to the power grid, creating a similar effect to [46]. In addition, OCPP 2.0 supports the EV-Grid communication protocol (ISO-15118). With the recent advancement in ISO-15118 that would allow reverse power flow from EVs to the power grid, the attack becomes more severe. Particularly, if the adversary managed to get all EVs to be plugged-in, he/she can reverse the power flow causing a surge in supply or alternate cycles of charging and discharging, all of which would cause major disturbances to the power grid.

Given that the entry point of such attack is the EVCS and the end goal is disturbing the power grid, there needs to be an early detection mechanism that would allow the grid operator to take the required measures to mitigate it. However, given the different implementation of the EV charging infrastructure, we detail, in what follows, the detection strategies for both public and private charging. Particularly, we detail a generic anomaly detection engine for such attack scenario in a public charging setting. Further, we describe the challenges of leveraging such engine for private charging and propose some modifications accordingly.

4.3 Public Charging Detection Strategy

4.3.1 Deployment Structure

Before laying out the detection strategy, it is essential to describe the infrastructure considered. The EV charging infrastructure has different deployments depending on the locations, capabilities and modus operandi. According to Open Charge Map which is an open source map of charging stations, current EV charging systems could be grouped into the categories depicted in Figure 4.1.

With the variety of the deployments shown, addressing each deployment scenario would be rather challenging. Therefore, we broadly group the EVCS into either public and private stations. We refer to the public stations as networked charging stations that are deployed under the supervision of the power utility and are communicating with a CMSs. Based on this, there should exist a protocol that manages this communication. While some companies have their own proprietary

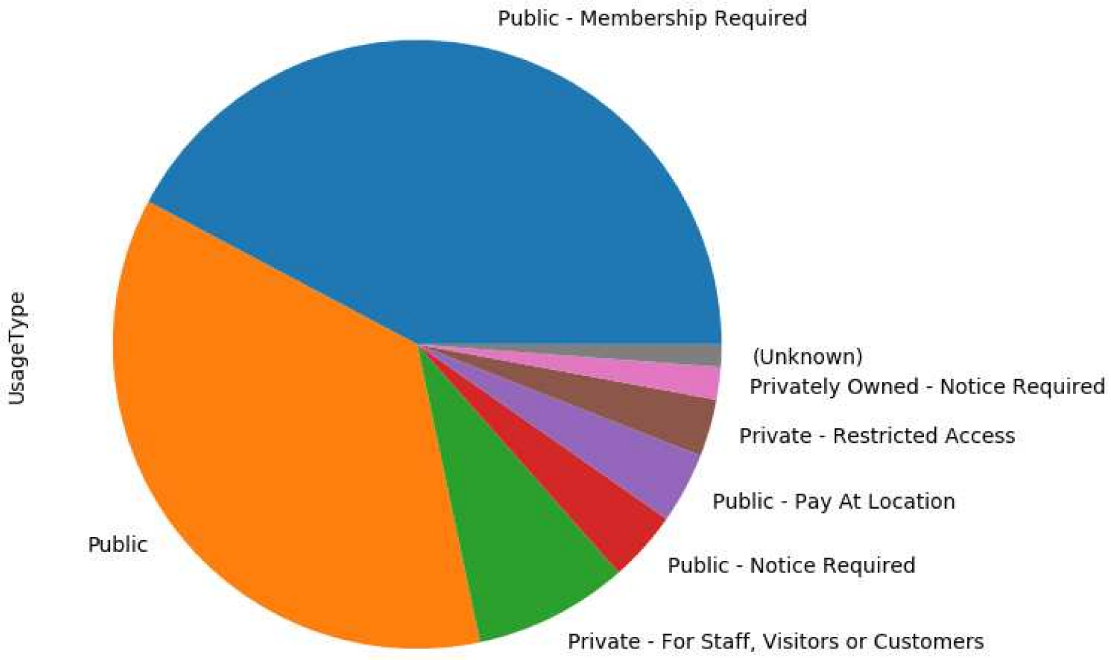


Figure 4.1: EVCS deployment types

protocols, we consider in our scenario that the communication is handled by OCPP as it is an open source protocol and used by one of the largest EV charging networks in the world (ChargePoint) [84]. On the other hand, we consider the private charging stations as stations in residential areas or business premises that only authorized users are allowed to use them. In addition, these stations are fully managed by their owners and the available data to the power utility is only the smart meters readings. Given the easier accessibility of data from the public EVCS, we first detail the anomaly detection engine for the public charging scenario.

With the considered infrastructure and threat model, the missing piece of the puzzle is the Anomaly Detection Engine. The purpose of the anomaly detection engine is to collect as much data as possible on EV charging processes, analyze them and provide analytics (warnings and alerts) to the power grid. Essentially, the anomaly detection engine would serve as a detection mechanism for the aforementioned attack. For that, we break down the design of the Anomaly Detection engine into:

ChargingProfile			
chargingProfileId	**100**		
stackLevel	**0**		
chargingProfilePurpose	**TxDefaultProfile**		
chargingProfileKind	**Recurring**		
recurrencyKind	**Daily**		
chargingSchedule	*(List of 1 ChargingSchedule elements)*		
	ChargingSchedule		
	duration	**86400 (= 24 hours)**	
	startSchedule	**2013-01-01T00:00Z**	
	chargingRateUnit	**W**	
	chargingSchedulePeriod	*(List of 3 ChargingSchedulePeriod elements)*	
		ChargingSchedulePeriod	
		startPeriod	**0 (=00:00)**
		limit	**11000**
		numberPhases	3
		startPeriod	**28800 (=08:00)**
		limit	**6000**
		numberPhases	3
		startPeriod	**72000 (=20:00)**
		limit	**11000**

Figure 4.2: OCPP 2.0 Charging Profile

4.3.2 Data Collection and Parsing

The first phase of anomaly detection is collecting data to be used in constructing "normal behavior profiles" that would serve as a benchmark to detect anomalies later. In order to properly define what a behavior profile is, we should note that the described attack relies on creating instantaneous surges in demand/supply. Thus, a normal profile that is based on load consumption (load profile) would result in late detection as the attack would have actually happened. Another crucial observation of the attack scenario is that an adversary has to change the schedules of EV drivers to be able to cause the surge. Thus, we define a behavior profile of EVCS as a profile of EV schedules. If any malicious scheduling events occur, they could be easily detected. As mentioned earlier, public EVCS are deployed under the supervision of the power utility. Thus, a utility can easily acquire EV schedules from the EVCS operators. However, due to the lack of public data on EV schedules, we utilize, in our work, load profile data of public EVCS and convert them to OCPP-compliant schedule (shown in Figure 4.2). For that, we:

- **Collect load profile data:** The load profile data was obtained from [85]. The data depicts the status of EVCS all over Ireland from the period of November 2016 to July 2019, collected over five-minute intervals. The status of the EVCS is represented as Out of Contact (OOC),

Out of Service (OOS), Partially Occupied (Part), Fully Occupied (Occ) or Unknown. The raw dataset contains more than $3GB$ of EVCS status from June 2018 to July 2019. Besides the status, the data contains the ID of the EVCS, the date and time of the status, the location in terms of latitude and magnitude, as well as physical address and the type of the station; Standard Type 2, CHAdeMO, CCS or FastAC.

- **Convert to schedules:** In order to change the collected data to OCPP schedules, some considerations were required to be taken care of. The first consideration is that the obtained data only shows the status of the EVCS, not the actual energy usage. As a result, it would be rather impossible to get the accurate energy used for each charging event especially that stations might have different charging ports. Thus, we replace the energy limit field in the OCPP schedule by the status. Another consideration is that the data contains usage status of the EVCS over five-minute intervals. As a result, we assume that the EVCS would send their schedules every five minutes to the detection engine. What this implies is that, every five minutes, there would be a schedule registered for each station.

To better visualize and process the collected data, we map the charging stations to the Ireland power grid buses. For that, we collect the Ireland power grid bus data from PyPsa-EUR [86], and map the EVCS to their closest bus. The result of this is a mapping of all EVCS mapped to 36 buses shown in Figure 4.3. The landmarks in the figure represents the starting location of the bus, and the heat-map represents the distribution of EVCS on each bus. Accordingly, to integrate the mapped buses to the data, we add a feature for each schedule to indicate the bus the EVCS is mapped to.

Another issue that was faced in the data collection phase is the lack of anomalous EV charging schedules. For that, we generate anomalous schedules according to two strategies:

- **Mass Changing of schedules:** The adversary changes the schedules of all compromised stations at once. For that, we select the three most, least and midst loaded buses and select the most and least occupied times of the day to be the target of the attack. In order to change the schedules, we choose all charging events scheduled two hours before and after the targeted times and reschedule them to the targeted time. An example of such anomaly is shown in Figure 4.4.

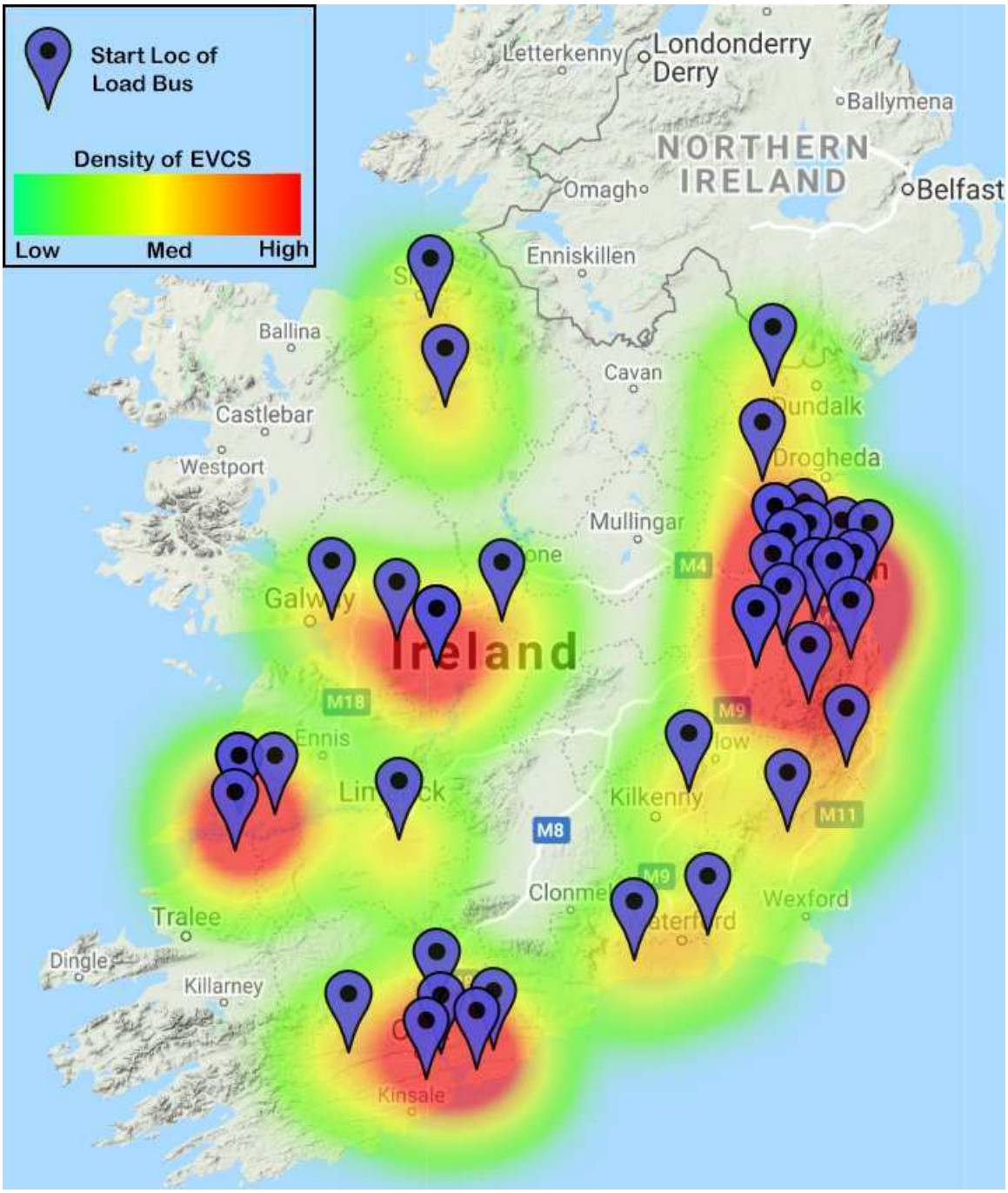


Figure 4.3: Distribution of EVCS and load buses in the Ireland power grid

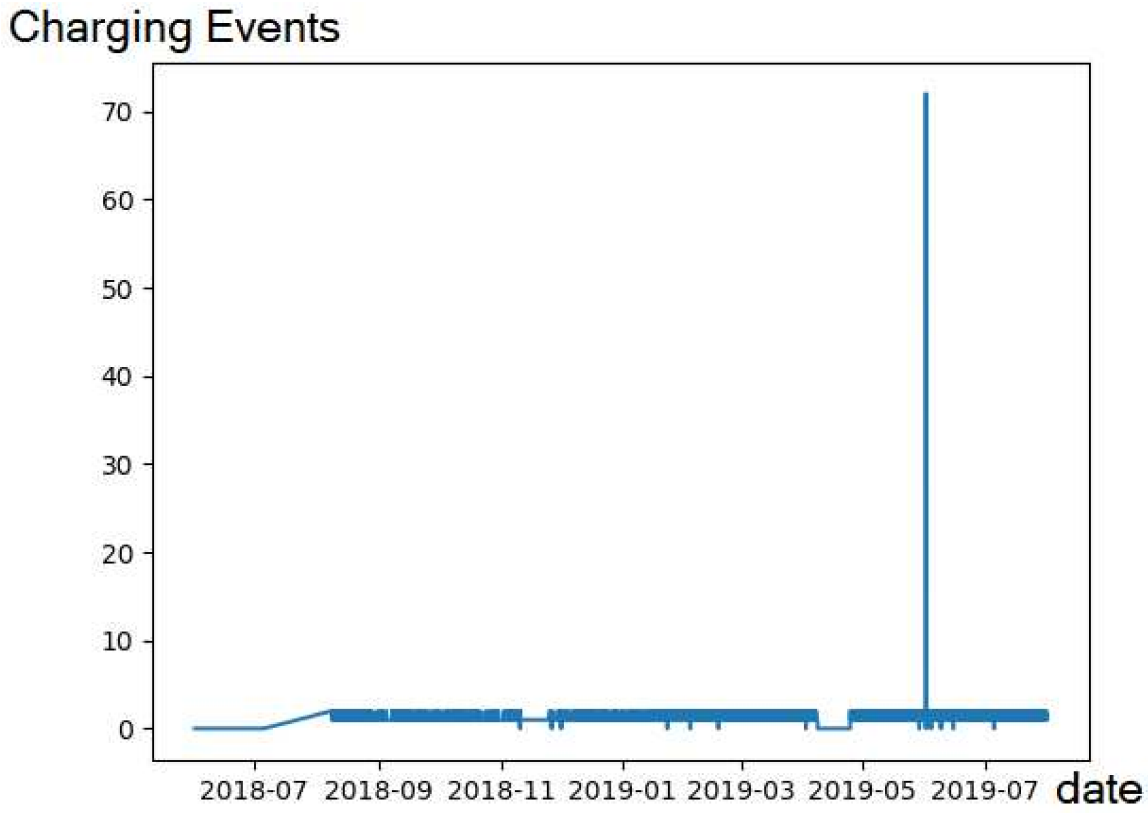


Figure 4.4: Mass changing schedules redistribution

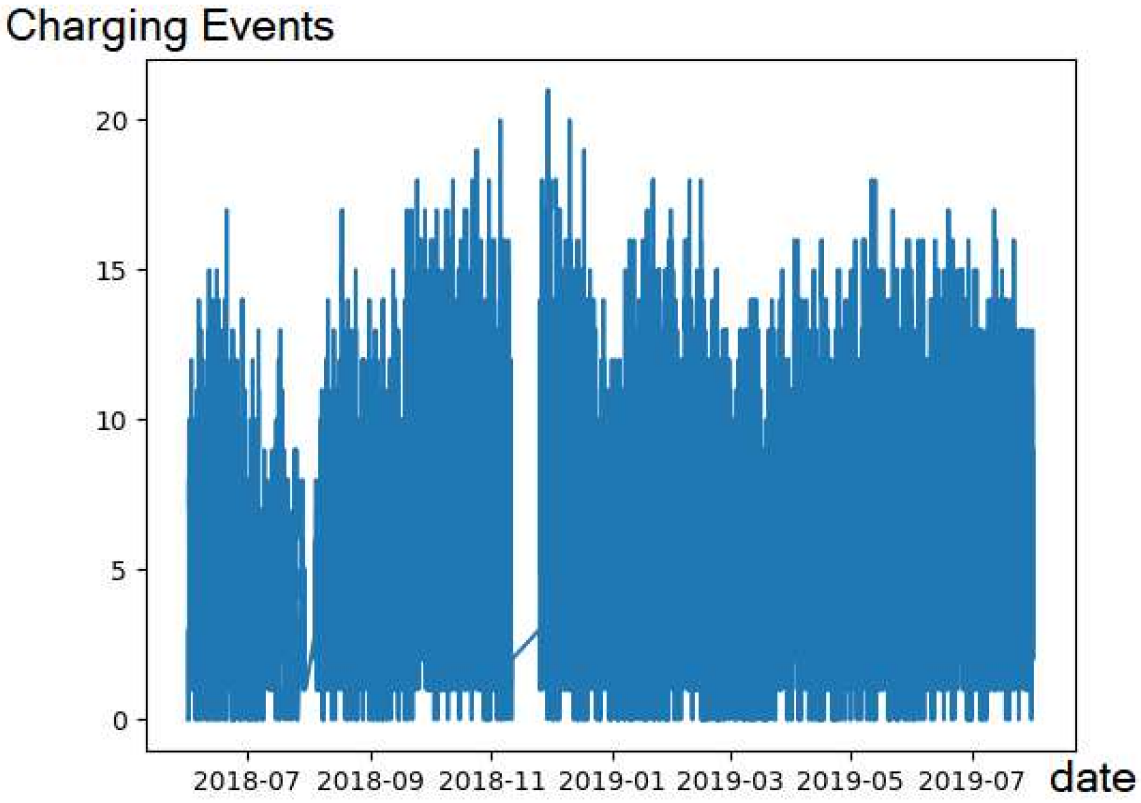


Figure 4.5: Subtle changing schedules distribution

- **Subtle Changing of schedules:** One thing to note is that converting load profiles to OCPP schedules does not truly reflect the actual schedule process. This is because some charging events might have been rescheduled from one day or hour to another or even cancelled. Hence, for the sake of adding more realization to the generated schedules, we highlight such rescheduling or cancellation by selecting a random set of charging events for each EVCS and either cancelling them, or moving them to another day/hour. Further, this subtle changing could be exploited by an adversary to cause more subtle disturbances to the charging of EVs so as to gradually increase the load, setting the stage for the more devastating attack. An example of such anomaly is shown in Figure 4.5.

By looking at Figures 4.4 and 4.5, it becomes clear that the mass changing could easily be detected using a simple threshold-based system. However, for a more stealth attack, the adversary would have to first change some schedules so as to alter the detection system by gradually increasing the load over time, and then performing the more devastating attack. These subtle changes in the

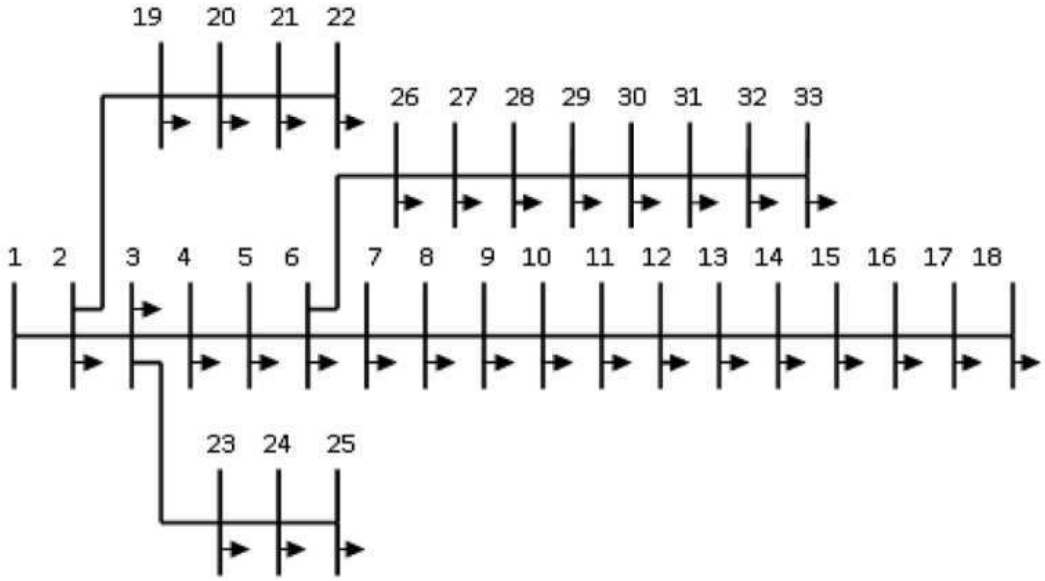


Figure 4.6: IEEE 33 Bus System Obtained from [1]

schedules would be hard to detect using threshold-based systems.

4.3.3 Impact of Added Anomalies on the Power Grid:

To give more realism to the added anomalies, we simulated their impact on a sample power grid. In particular, we simulated the IEEE 33 Bus system shown in 4.6 with the Irish Power Grid Load Data obtained from [87]. Due to the non availability of load profile data for the Irish power grid, we built a simple load profile for the buses by calculating the average hourly load profile from the period of March 2020 to April 2020. For simplicity, we distributed this load equally among the 33 buses.

With the load profile generated for each bus, we add the two kinds of aforementioned anomalies. For that, we choose one of the 36 buses and map its load profile to branch 1-2 in the IEEE 33 Bus system. Further, we select the targeted attack hour to be at $16:00$ in the case of the mass changing anomalies. We, then, run a time-series analysis on the grid system using GridCal in Python 3.7. Further, we assume that the acceptable voltage drop values are within 10%, and hence any drop of voltage below $0.9p.u$ would be considered critical. We demonstrate the impact of such anomalies in Figures 4.7, 4.8. One thing to note that we plotted only the impact on Bus 17 as it was shown that

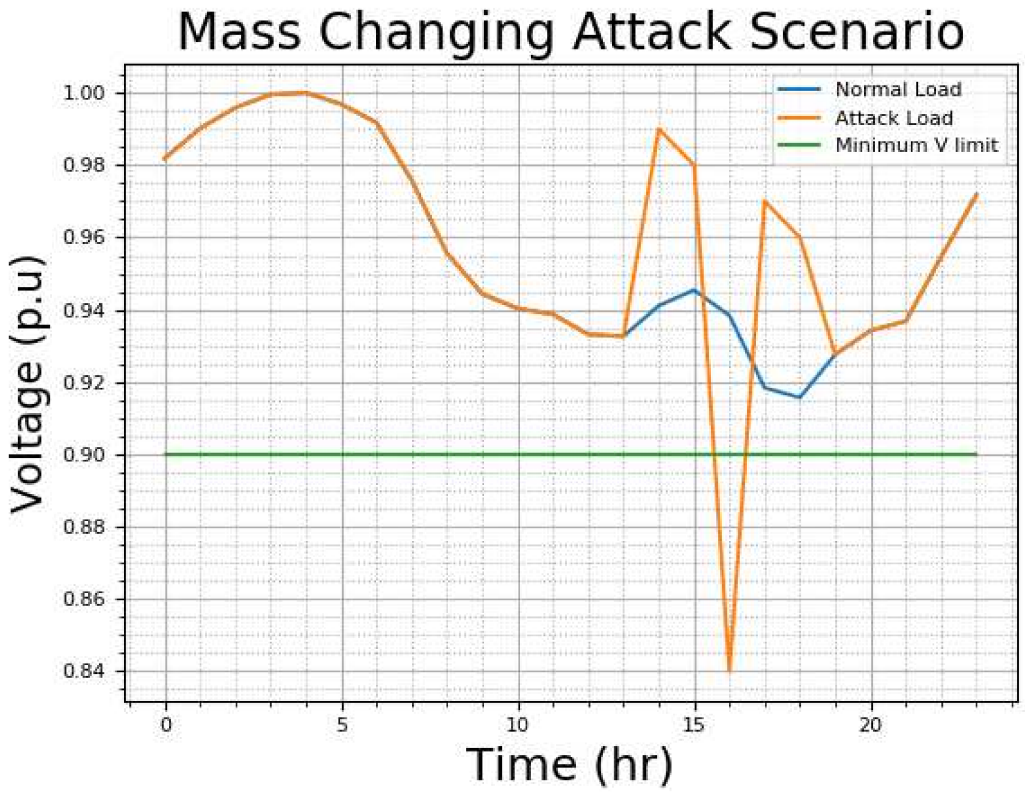


Figure 4.7: Impact of Mass Changing Anomaly on the IEEE Bus 17

it was the weakest bus in the whole network.

In the case of the mass changing, the targeted attack hour was at $16:00$, and as mentioned earlier, the adversary would need to change schedules two hours before and after the targeted hour. Thus, as can be seen from Figure 4.7, at time from $14:00$ to $16:00$ and $17:00$ to $18:00$, the voltage values have increased from their normal values as the load in the system has decreased. Further, at time $16:00$, the voltage values have dropped way below the minimum voltage limit to around $0.84p.u.$ This, if not handled properly, can have serious impact on the power grid. For instance, this attack can cause damage to the equipment and blackouts as well as elevated operational costs. Further, the critical voltage drop can cause line and cascading failures.

On the other hand, the subtle changing anomalies represents a more complex variation as demonstrated in Figure 4.8. At time $14:00$, the adversary starts rescheduling some part of the EVs to a later hour causing the voltage levels to drop slightly. Further, this trend continues, dropping the voltage every hour, till it falls below the minimum voltage level at time $20:00$. Although

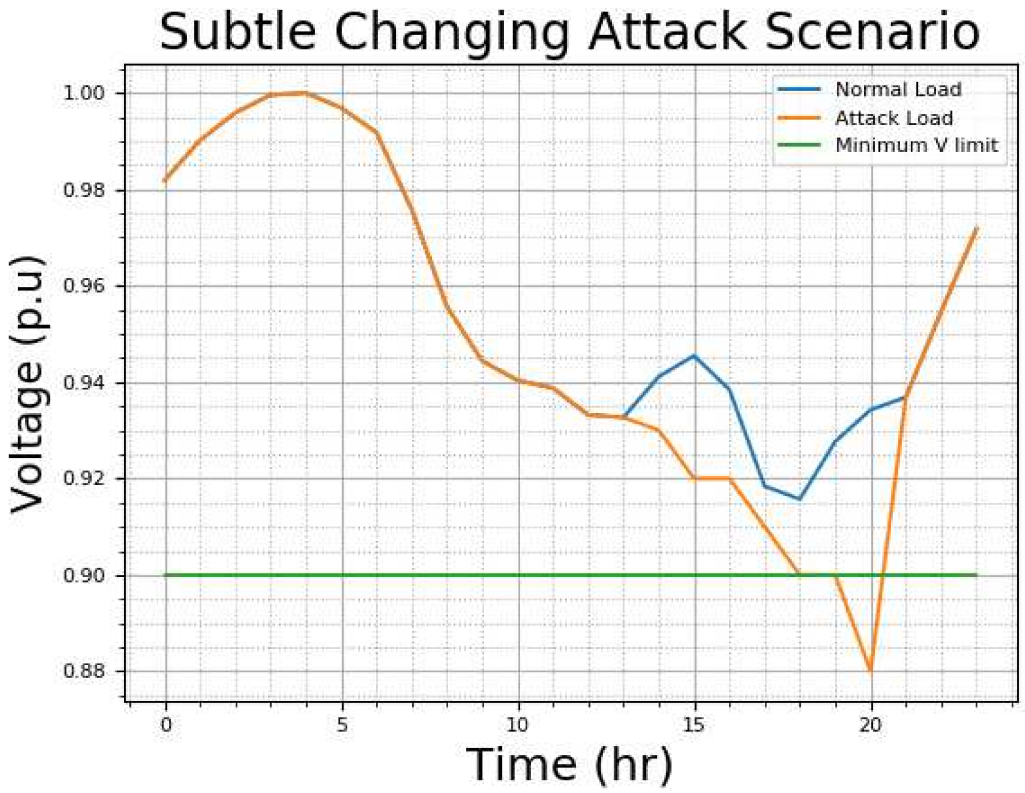


Figure 4.8: Impact of Subtle Changing Anomaly on the IEEE Bus 17

these demonstrated changes seems simple to detect, they allow the adversary to tamper the overall behavior of the EVCS profile data. Thus, over time, these subtle changes can cause a shift in the overall load profile of the EVCS. For instance, if this attack was carried out over an extended period (a couple of months), the "normal load profile" could shift from averaging at 0.97 to being 0.92 at $16:00$ due to these subtle changes over the months of the attack. This in return would make it difficult for a threshold system to simply detect these subtle changes.

Further, one thing to note from these graphs is that we assume that attack has already happened and the grid operator is just observing these events. Thus, as mentioned earlier, the key element in the detection engine is to rely on the collected schedules other than the load profile data, as the latter would means late detection.

4.3.4 Feature Engineering

Before feeding the dataset to the machine learning algorithm, some feature engineering is required. Particularly, we formulate the dataset as a uni-variate time series. Initially, the dataset contains the following features: Date, Time, EVCS ID, EVCS location, EVCS Type, Status, Mapped Bus. The feature engineering is done as follows:

- **Remove Redundant Features:** Ultimately, the adversary would target EVCS located on a specific bus. Thus, we remove the EVCS location and ID as the mapped bus feature would be indicative of both location and ID for our purposes. In addition, Date and Time features are merged into timestamp of the format $(dd - mm - yyyhh : mm : ss)$. In addition, for a more meaningful representation of the status, we map the status values to 0 for out of service or out of contact, 1 for partially occupied and 2 for fully occupied.

- **Remove Unwanted Features:** Due to the limited information regarding the EVCS, the only informative feature is the EVCS type. However, due to the lack of the energy usage of the EVCS, this feature did not provide much knowledge about the EVCS, and hence was dropped.

- **Splitting:** Up to this point, the dataset contained Date, Time, Mapped Bus and Status features. As previously mentioned, for an effective attack, specific buses should be targeted. Thus, we split the dataset into 36 chunks, each counting EVCS data mapped to the 36 buses in the Ireland grid.

- **Aggregation:** The last step of the feature engineering is to aggregate the data. Thus, for each of the 36 chunks of data, we group the data by the timestamp feature and aggregate over the sum of the status.

The final dataset after this phase is 36 chunks (for each of the 36 buses), each containing the timestamp (five minute intervals), the total number of charging events scheduled at this timestamp, and 1000 anomalous schedules.

4.3.5 Learning Algorithm

There exist many algorithms that could be used for anomaly detection, from supervised and semi-supervised to self and unsupervised algorithms. Although supervised algorithms would typically yield higher accuracies, in a real world setting, labeled data is more often considered an asset. Thus, to give more realism to the problem, we do not label our dataset and hence we opt to use unsupervised learning algorithms. In particular, we choose four different learning algorithms:

- **Seasonal ESD:** The seasonal Extreme Studentized Deviate algorithm was developed in Twitter [88]. It represents a statistical approach for automatically detecting contextual anomalies. The algorithm relies on decomposing the time series into seasonal and trend components, and applying Median Absolute Deviation (MAD) to detect anomalies.

- **One Class SVM:** The One Class Support Vector Machine (OCSVM) algorithm was developed in [89]. The idea behind OCSVM is to model the dataset by a function that is positive for high density points and negative for lower density points. With that, the function can differentiate between anomalous and non-anomalous data due to their different densities.

- **Isolation Forests:** The Isolation Forest algorithm [90] has been widely used for detecting anomalies. In essence, it randomly selects a feature and split the dataset according to a split value. By recursively splitting the dataset, the anomalies are isolated as they would have different feature values from the rest of the dataset.

- **LSTM:** The LSTM is a type of auto-encoder that learns a decompressed representation of input sequence [91]. In the context of anomaly detection, LSTM networks tries to reconstruct the input data with a reconstruction error for each data point. Thus, if the reconstruction error exceeds a specific threshold, the data point is flagged as anomaly.

These algorithms were specifically chosen as they cover a wide array of anomaly detection approaches. For instance, the SESD algorithm follows a statistical approach, while the LSTM is an auto-encoder. Further, some algorithms are better suited for point-anomalies detection (OCSVM), while others proved superior in detecting contextual anomalies (SESD).

4.4 Experimental Evaluation

After performing the data collection and processing, we performed different experiments to evaluate the anomaly detection engine and determine the best algorithm to use. All data collection, processing and learning algorithms has been implemented in Python 3.7. The LSTM model was implemented using Keras library, while the Isolation Forests and OCSVM were implemented using Sklearn library. Finally, the SESD was implemented using the SESD Python library. Further, each of the algorithms used required a set of parameters, these are shown in Table 4.1.

Algorithm	Parameters	Description	Value
SESD	periodicity	How periodic the data is	yearly
	hybrid	Use the seasonal hybrid ESD (more robust)	True
	max anomalies	An upper bound for the number of anomalies in the data	10000
	threshold	Threshold at which a point is considered an anomaly	[0.1, 0.01, 0.001]
OCSVM	kernel	The type of kernel to be used (linear, poly, rbf)	rbf
	contamination	Percentage of anomalies in the data	[0.1, 0.01, 0.001]
Isolation Forest	contamination	Percentage of anomalies in the data	[0.1, 0.01, 0.001]
LSTM	depth	The number of LSTM layers in the netwrok	5
	neurons/layer	The number of hidden neurons in each layer	50
	threshold	Threshold at which a point is considered an anomaly	[0.1, 0.01, 0.001]

Table 4.1: Models parameters

As shown in the table, each model has a different set of parameters. However, the threshold/contamination model was present in all three models. As a result, we use this parameter to tweak the performance of each model. For that, we perform three different experiments, each with a different threshold/contamination value $[0.1, 0.01, 0.001]$. In what follow we present the results for each of the models. The full results for each threshold values are found in Tables 4.2, 4.3 and 4.4.

4.4.1 Threshold = 0.1

The results for the threshold value = 0.1 are depicted in Figure 4.9. As can be seen from the Figure, this specific threshold value resulted in high detection accuracy across all algorithms. In particular, the percentages of true alerts was above 93% for all algorithms. Further, the highest accuracy was achieved using the LSTM algorithm detecting all anomalies introduced in the data. The second highest accuracy is seen in the OCSVM with a value of 96.1%. The IF algorithm has the lowest accuracy with a value of 93.5%. On the other hand, the relatively high threshold value

resulted in high false alert values. The worst performance was of the OCSVM algorithm with more than 1500 false alerts. Further, the LSTM algorithm resulted in the lowest rates of false alerts with a value of 535, which is considered relatively high compared to the number of actual anomalies.

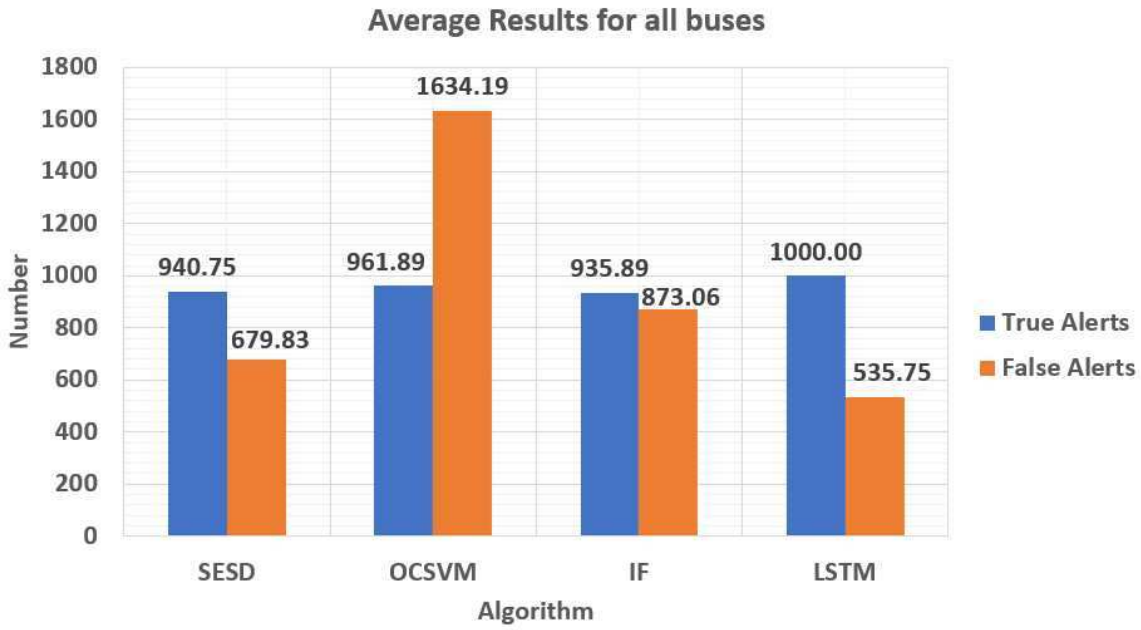


Figure 4.9: Average results for all buses for threshold = 0.1

4.4.2 Threshold = 0.01

The results have improved by dropping the threshold from 0.1 to 0.01 as depicted in Figure 4.10. As illustrated, the number of false alerts has dropped significantly across all algorithms. The LSTM false detection values has dropped by more than 70%. In addition, the SESD algorithm overall performance improved in terms of false alerts, with a slight drop of almost 4% in the true alerts rate. The IF algorithm also has a similar performance to the SESD algorithm with just 0.5% difference between the two algorithms. By closely observing the results for this threshold value, it was clear that all the mass changing anomalies were correctly flagged. Further, most of the subtle anomalies were also flagged by almost all algorithms. However, the OCSVM flagged a number of data points that, when taking out of context of the EVCS schedule, would be considered as anomalies. The reason behind this is that the OCSVM does not necessarily detect contextual anomalies, unlike the LSTM or SESD algorithms that address seasonality and context. This threshold yielded the best

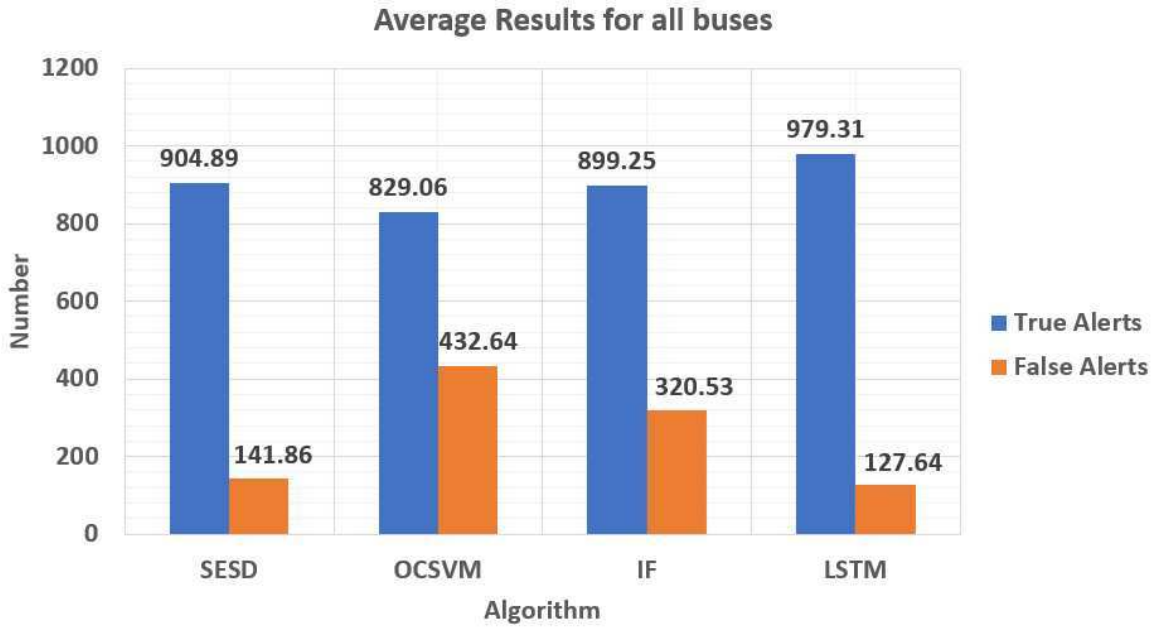


Figure 4.10: Average results for all buses for threshold = 0.01

results overall in terms of high accuracy and low number of alerts.

4.4.3 Threshold = 0.001

The purpose of experimenting with such a low threshold is to test how effective the algorithms are in detecting the mass changing anomalies. The results are depicted in Figure 4.11. As expected, the number of false alerts have dramatically dropped to below 100 for all algorithms. Moreover, the true alert rates has also dropped by almost 50% for all algorithms. The majority of the detected anomalies were mass changing anomalies for all buses, with just a few of the subtle changing anomalies.

Based on the experimental evaluations, the LSTM appeared to produce the best results among all the algorithms, followed by the SESD. Further, the use of the threshold proved to be useful in adding a degree of flexibility to the detection engine. Particularly, a low threshold could be used to detect the more subtle behavioral changes. However, this would be traded-off with the high rate of false alerts. Overall, the proposed engine proved effective in detecting both variations of behavioral change. In what follows, we detail the modifications required for the proposed engine to be applicable on both private and public EVCS.

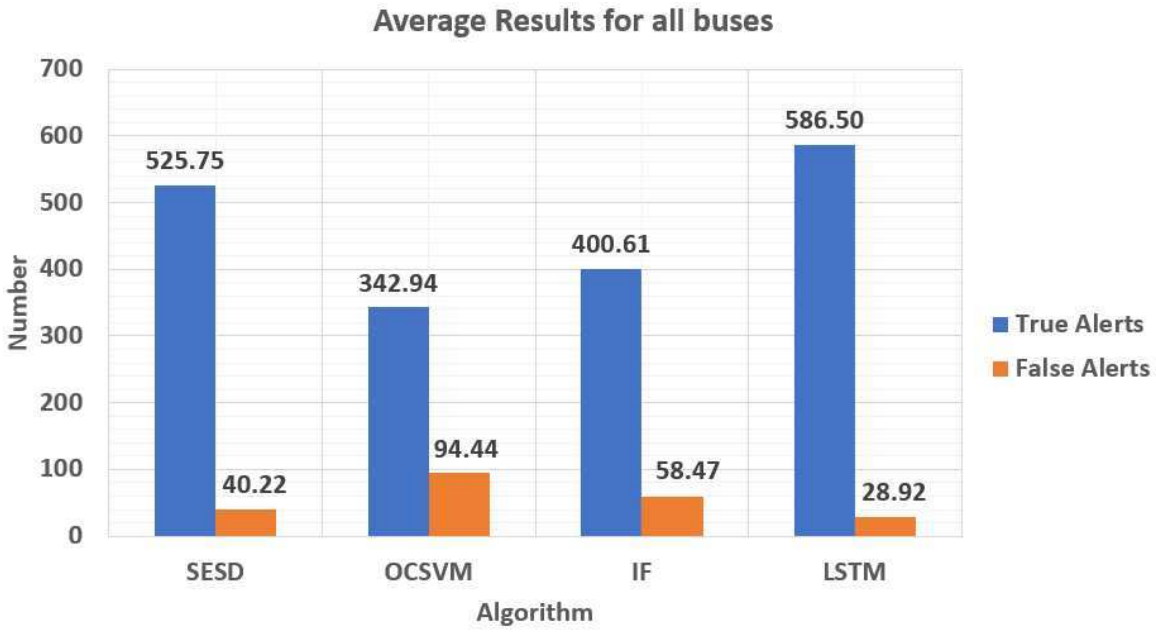


Figure 4.11: Average results for all buses for threshold = 0.001

4.5 Private Charging Detection Strategy

4.5.1 Scenario

Within the realm of EV charging, the recipe for an efficient and functional system relies on the entities participating in the system and the environment at which these entities operate within. To this end, we depict our considered system in Figure 4.12. In our abstraction of the EV charging infrastructure, we consider a residential area consisting of multiple homes. For a more realistic representation, we assume that EVs and EVCS are distributed among these homes. For instance, some homes may contain one or more EVs while others may contain none. Similarly, some homeowners may own one or more EVCS. Further, we assume that the energy provider have deployed some public EVCS at different locations in the neighborhood. In addition, we consider that both EVs and EVCS participate in an open energy trading network. In other words, homeowners, who own EVCS, can rent out their privately-owned charging stations to be used by EV drivers in return for profit [92]. Thus, EV drivers have the option to charge their vehicles at the public or private EVCS.

Such open energy trading system would require mutual trust between the different entities. For example, EV drivers need to trust the owners of the private EVCS as to supply the amount of energy

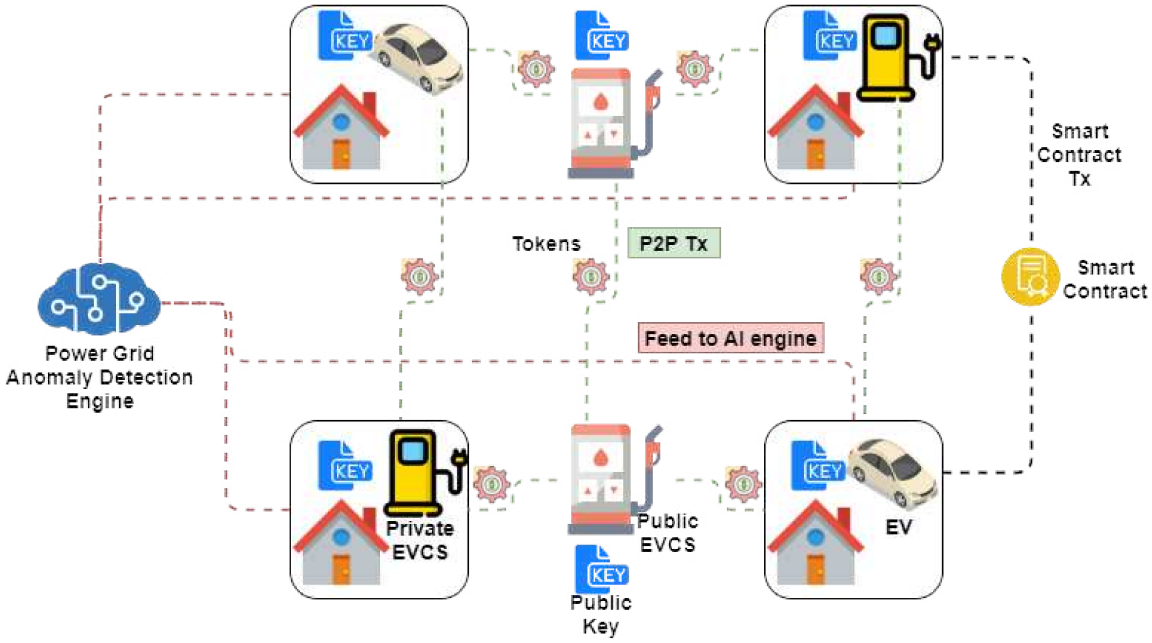


Figure 4.12: Proposed Blockchain Network

required to charge their vehicles. Similarly, the owners of the private EVCS need to guarantee that the EV drivers that utilize their stations would pay the associated charging fees. Typically, in order to build this trust, there is a central entity (a central management system, station operator, etc.) that records these transactions (energy supplied, fees payment, etc.). Thus, in case of conflict, the central entity would review the transactions and resolve the conflict accordingly. However, involving a central entity has two major drawback. The first one is the possibility of the central entity being compromised or biased towards a specific entity. The other drawback is the added cost coupled with the operations of the central entity. On the other side of the spectrum, a decentralized system reduces the risk of the whole system being compromised by compromising the central entity, as well as, cut on the operational cost. For these particular reasons, we provision this open energy trading system with Blockchain. For that, we consider each of EVs and EVCS (both public and private) to be nodes in the Blockchain network and design a simple Blockchain network. For better illustration, we break down the Blockchain network design into:

Initialization

Initially, no nodes are available in the network. Each entity would then need to register in the network.The registration phase entails that the registering entity be assigned a private/public key pair. The public IP address would be the unique identifier for the node. Upon registration, the owner of the EVCS (public and private) broadcast their availabilities in terms of dates, location and times and price of energy $(\$/kW)$. Thanks to the immutability property of Blockchain, these prices and availability records can not be tampered with by an adversary; only the owners of the stations can modify these records.

Booking and Charging

Given that such system should enable the trading of digitized assets, we consider that the energy and money transactions are encapsulated within smart contracts. Particularly, when an EV owner needs to charge his/her vehicle, he/she can look up at the available stations along with their prices and locations. The user can then choose to charge at either the public or private EVCS based on his preference. Once a driver has chosen a station, a smart contract is issued between the EV owner and the EVCS including the ID of both of them, price of the charging $(\$)$ (which is determined by the chosen EVCS), the date and time of the charging $(dd-mm-yyyy\ hh:mm:ss)$, the amount of energy required to charge (kW) and the duration of the charge (s). Along with the smart contract, money is transfered from the EV driver's wallet to the smart contract. When an EV is plugged into the EVCS, the smart contract is invoked by checking the ID of the EV along with the data and time of the charging. If those match the conditions on the smart contract, the charging process starts for the duration specified in the contract. Once the charging process is completed, the smart contract transfers to the EVCS the agreed upon fee. In the case of an incomplete charging process (either entities decided to stop the charging process), the smart contract calculates the amount of used energy and pays the EVCS the corresponding fee. The remaining balance in the contract is then refunded back to the driver. The logic of the booking and charging processes is detailed in Figure 4.13.

The outlined Blockchain network allows decentralized operations of registration and booking

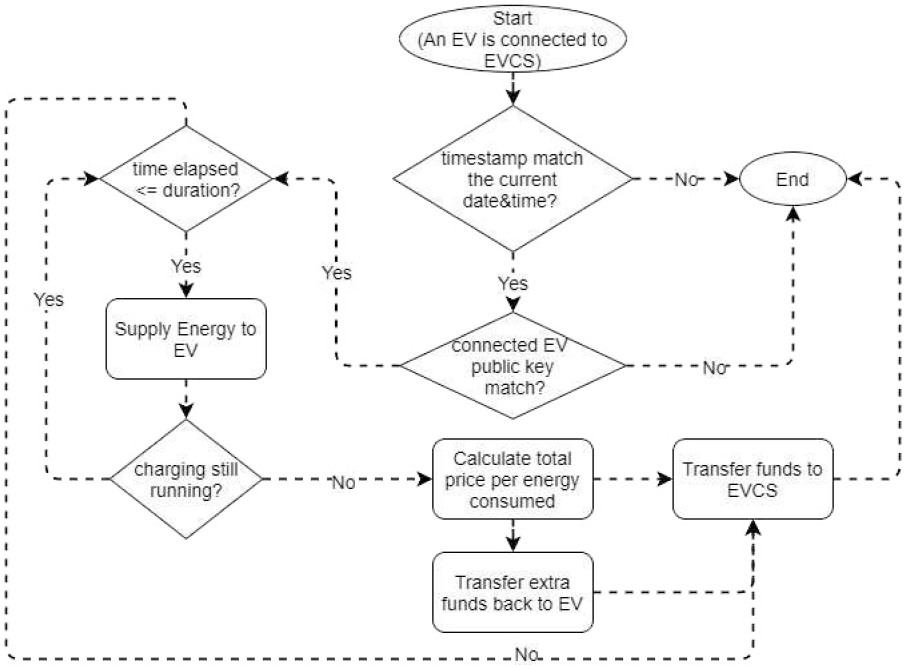


Figure 4.13: Smart Contract Flowchart

of EVCS and the charging of EVs. This in itself serves as incentives for homeowners to purchase EVCS as they can gain money by renting them out to EV drivers. Beside the decentralization aspect, the transparency offered by the Blockchain network allows interested entities to pull the public records of transactions corresponding to a snapshot of time. Hence, the Blockchain network would also serve as a data aggregation network for the EV charging and EVCS load behavior. As a case in point, the power utility could periodically pull the transactions issued in the Blockchain network and leverage them to create load profiles for EVs and EVCS that could then be used for better energy management at the power utility. In our scenario, we build up on that case and consider the power utility to be the interested entity in the public record of transactions. Specifically, we assume that the power utility is running the anomaly detection engine described above with its feed being the transactions record in the Blockchain network.

4.6 Conclusion

In this work, we exploited different machine learning algorithms to detect the rising demand-side EVCS attacks. We obtained real-world data on the Irish public EVCS load profiles and power

grid and introduced two types of artificial anomalies in the dataset. By mapping the EVCS to the Irish load buses, the dataset was split into 36 chunks and fed to four different anomaly detection algorithms (SESD, OCSVM, IF and LSTM). Through experimenting with different threshold values, LSTM and SESD performed the best in terms of detecting the actual anomalies and resulting in a low number of false alerts. From there, we abstracted and detailed how this anomaly detection engine could be also leveraged within the context of private EVCS through the use of Blockchain networks.

True Alerts					False Alerts				
Bus ID	**SESD**	**OCSVM**	**IF**	**LSTM**	**Bus ID**	**SESD**	**OCSVM**	**IF**	**LSTM**
1	1000	1000	1000	1000	**1**	100	3017	698	241
2	922	1000	0	1000	**2**	1000	2383	1422	643
3	997	1000	1000	1000	**3**	400	843	585	34
4	1000	1000	1000	1000	**4**	426	1162	722	243
5	1000	1000	1000	1000	**5**	400	462	1015	534
6	1000	1000	1000	1000	**6**	300	235	781	631
7	1000	1000	1000	1000	**7**	643	359	928	363
8	1000	1000	1000	1000	**8**	532	2730	231	756
9	0	1000	692	1000	**9**	643	4651	435	453
10	1000	1000	1000	1000	**10**	843	434	1099	342
11	1000	1000	1000	1000	**11**	934	432	922	645
12	1000	1000	1000	1000	**12**	532	3876	600	764
13	999	1000	1000	1000	**13**	1992	291	1014	452
14	1000	1000	1000	1000	**14**	1244	1719	1106	353
15	1000	1000	1000	1000	**15**	1721	3225	819	765
16	1000	1000	1000	1000	**16**	443	421	813	745
17	1000	628	1000	1000	**17**	532	452	452	242
18	1000	1000	1000	1000	**18**	875	1249	1721	453
19	986	1000	1000	1000	**19**	453	3125	1082	756
20	1000	1000	1000	1000	**20**	75	506	884	678
21	1000	1000	1000	1000	**21**	653	2482	569	342
22	1000	1000	1000	1000	**22**	782	1653	762	230
23	1000	1000	1000	1000	**23**	354	892	1093	534
24	969	1000	1000	1000	**24**	854	354	713	657
25	1000	1000	1000	1000	**25**	689	512	1872	901
26	1000	1000	1000	1000	**26**	843	243	862	423
27	1000	0	0	1000	**27**	357	1242	1921	653
28	0	1000	1000	1000	**28**	753	782	991	564
29	994	1000	1000	1000	**29**	325	7218	979	234
30	1000	1000	1000	1000	**30**	246	1562	630	867
31	1000	1000	1000	1000	**31**	201	781	862	436
32	1000	1000	1000	1000	**32**	805	310	733	1034
33	1000	1000	1000	1000	**33**	1289	6187	787	345
34	1000	1000	1000	1000	**34**	241	1031	337	645
35	1000	1000	1000	1000	**35**	463	402	403	876
36	1000	1000	1000	1000	**36**	1531	1608	587	453
Mean	940.75	961.8888889	935.8888889	1000	**Mean**	679.8333333	1634.194444	873.0555556	535.75

Table 4.2: Detailed Results for threshold = 0.1

True Alerts					False Alerts				
Bus ID	**SESD**	**OCSVM**	**IF**	**LSTM**	**Bus ID**	**SESD**	**OCSVM**	**IF**	**LSTM**
1	1000	900	943	1000	**1**	20	1003	210	85
2	900	932	0	994	**2**	302	950	649	102
3	950	1000	1000	1000	**3**	85	302	350	0
4	1000	513	1000	1000	**4**	100	305	381	82
5	1000	432	1000	974	**5**	105	158	492	143
6	1000	841	1000	1000	**6**	96	68	204	203
7	1000	1000	1000	979	**7**	201	90	495	98
8	1000	340	1000	1000	**8**	103	872	99	81
9	932	1000	894	942	**9**	90	904	183	97
10	854	843	1000	1000	**10**	301	105	385	78
11	810	1000	1000	923	**11**	298	235	471	142
12	1000	536	1000	1000	**12**	185	1032	132	142
13	912	389	603	990	**13**	502	40	389	192
14	1000	942	1000	1000	**14**	305	320	482	93
15	1000	1000	849	982	**15**	230	783	218	124
16	1000	1000	1000	1000	**16**	80	329	325	152
17	1000	634	1000	847	**17**	129	193	182	93
18	600	610	1000	1000	**18**	231	535	392	132
19	970	1000	879	894	**19**	70	974	472	144
20	1000	1000	1000	1000	**20**	0	281	163	212
21	400	473	1000	986	**21**	123	789	99	70
22	847	1000	1000	1000	**22**	144	284	345	79
23	1000	1000	1000	1000	**23**	50	202	427	132
24	968	1000	1000	1000	**24**	90	93	348	198
25	400	1000	792	978	**25**	103	184	461	293
26	859	1000	1000	1000	**26**	184	212	242	87
27	1000	0	0	1000	**27**	40	301	247	102
28	310	1000	1000	995	**28**	100	183	532	146
29	872	943	1000	1000	**29**	48	1632	500	75
30	1000	832	1000	1000	**30**	97	200	134	252
31	1000	823	1000	973	**31**	40	174	276	184
32	1000	1000	823	1000	**32**	201	40	388	213
33	992	863	807	910	**33**	183	984	462	60
34	1000	1000	1000	899	**34**	99	213	89	123
35	1000	1000	1000	1000	**35**	69	202	192	126
36	1000	1000	783	989	**36**	103	403	123	60
Mean	904.8889	829.0556	899.25	979.3056	**Mean**	141.8611	432.6389	320.5278	127.6389

Table 4.3: Detailed Results for threshold = 0.01

True Alerts					False Alerts				
Bus ID	**SESD**	**OCSVM**	**IF**	**LSTM**	**Bus ID**	**SESD**	**OCSVM**	**IF**	**LSTM**
1	592	341	452	623	**1**	0	45	92	0
2	452	318	0	429	**2**	94	100	75	12
3	423	423	632	599	**3**	12	68	12	0
4	873	192	579	798	**4**	0	89	23	0
5	619	100	598	432	**5**	73	31	41	24
6	832	90	689	499	**6**	81	34	68	32
7	642	582	412	371	**7**	74	52	41	21
8	875	68	482	752	**8**	85	121	0	19
9	642	502	294	681	**9**	23	131	76	15
10	513	204	589	488	**10**	99	47	98	2
11	579	398	587	471	**11**	86	98	99	5
12	782	283	399	572	**12**	63	293	41	23
13	763	97	192	531	**13**	42	0	81	34
14	681	384	423	464	**14**	45	93	24	6
15	752	475	253	467	**15**	86	211	52	34
16	681	572	467	699	**16**	10	94	92	152
17	753	192	584	323	**17**	31	99	62	3
18	284	107	485	785	**18**	57	121	99	31
19	513	592	182	479	**19**	14	123	112	39
20	499	498	523	542	**20**	0	98	87	28
21	90	103	578	451	**21**	83	62	0	0
22	201	399	509	682	**22**	74	94	87	0
23	631	475	402	654	**23**	0	45	97	43
24	402	512	389	651	**24**	21	0	63	59
25	192	394	129	655	**25**	24	31	100	79
26	351	384	298	652	**26**	47	58	52	41
27	412	0	0	763	**27**	0	90	69	28
28	70	593	293	601	**28**	21	84	123	35
29	127	204	379	611	**29**	0	392	91	0
30	469	200	489	652	**30**	72	74	12	73
31	591	184	462	589	**31**	0	42	24	73
32	496	593	124	712	**32**	23	0	46	56
33	472	124	203	653	**33**	21	213	52	0
34	591	592	578	431	**34**	26	82	0	51
35	483	489	639	699	**35**	38	87	9	23
36	599	682	128	653	**36**	23	98	5	0
Mean	525.75	342.9444	400.6111	586.5	**Mean**	40.22222	94.44444	58.47222	28.91667

Table 4.4: Detailed Results for threshold = 0.001

Chapter 5

Conclusion & Future Work

5.1 Conclusion

With their integration with almost every aspect of our lives, IoT services promise a seamless experience that would facilitate the users' lives. From smart homes and smart cars to smart factories and smart cities, the IoT paradigm is bringing novel services that was thought of as science fiction a couples of years back. However, for the IoT to reach is full potential, different sectors should overlap to provide a new set of services for a truly connected world. One area where such an overlap prevails is in the EVs and their charging infrastructure. Despite their penetration rate and promising forecasts, Evs are still facing major obstacles towards their adoption, one of which is the availability of their charging infrastructure. This growing need of procuring a well-developed charging infrastructure necessitates major investments in terms of both monetary and intellectual assets. With such, different companies - from startups (ex: ChargePoint) to Fortune 500 companies (Schneider Electric) have started manufacturing and deploying EVCS all over the world, as well as going a step further and embracing the IoT paradigm by provisioning smart EVCSs. While smart EVCSs bring EV charging a step closer to its perceived potential, they present themselves a fertile attack surface for adversaries that could render the whole infrastructure obsolete.

In this thesis, we provided a comprehensive analysis of the security of EVCS. In particular, in Chapter 2, we surveyed the state-of-the-art deployments, protocols and participating entities and observed two key concerns; the lack of standardization and multiple points of entry. In light of

these two concerns, we demonstrated a multi-stage network attack that would allow an adversary to disturb the power grid. Specifically, we leveraged Internet scanning tools (Shodan and Censys) to locate the IP addresses and ports of EVCSs. Once a dataset was collected, a brute-force attack was performed in order to gain root access to the devices. Surprisingly, some EVCSs from major manufacturer displayed the password in plain text in web interface of the device. While accessing the devices allowed us to download all devices' logs, restrict user access, download the firmware, one of the rather interesting features was the ability to remotely control the device and change the users' charging schedules. From there, a coordinated attack was simulated in which an adversary controlling a number of EVCSs within a geographical area creates a traffic bottleneck by tampering the schedules of the users forcing them to start charging at the same time instant. Once an adversary creates a bottleneck of EV drivers charging simultaneously, he/she can cause major disturbances on the power grid. By simulating three different variations of the attack; sudden demand surge, sudden supply surge and alternating attack, it was concluded that these variations can cause frequency instability which in return can cause severe impacts on the power grid such as equipment damage, cascading failures and blackouts.

It, thus, becomes evident that the security of the EV charging infrastructure is critical as it bridges different services between different sectors; transportation and energy sectors. In efforts to improve the current charging infrastructure and particularly addressing the aforementioned concerns, we provided a systematic evaluation of current solutions leveraging both Artificial Intelligence (AI) and Blockchain technologies over the past 10 years in Chapter 3. It was concluded that AI is a promising solution to the optimal charging schedules by collecting data of EV drivers and providing forecasts that would help operators better improve their deployments of EVCS. Further, AI could be used a cyber-security measure by detecting anomalies in the charging network. On the other hand, Blockchain provides a benchmark for a fully decentralized, distributed and secure charging infrastructure. Particularly, Blockchain can provide an open energy trading ecosystem where different entities (for example power grid operators, smart communities, EVs) can trade energy without the need for a centralized entity. This in return would cut on operating costs and increase EV adoption by giving incentives to EV drivers.

While both technologies target specific issues, the integration of both technologies opens the

horizon for novel functionalities for the charging ecosystem. Accordingly, in Chapter 4, we expanded on the roles of both AI and Blockchain in mitigating the attack described in Chapter 2. We proposed an anomaly detection engine that leverage different learning mechanisms (auto-encoders and statistical-based) to detect anomalous EV schedules. Through extensive simulations, it was concluded that the proposed system is effective in early detecting the proposed attack by flagging anomalous schedules while offering enough flexibility to tweak its sensitivity. In addition, we further explored a re-envisioning of the whole EV charging infrastructure by leveraging Blockchain. It was concluded that the integration of Blockchain with the proposed anomaly detection engine can be effective in securing the EV charging infrastructure on both public and private fronts.

5.2 Future Work

This thesis opens the door for some interesting research directions. One such work is to further expand on the idea of integrating AI and Blockchain and provide an extensive analysis on the feasibility of such integration within the context EV charging ecosystem. The premise here is that Blockchain adds lots of computation workload in the network. Thus, the evaluation would need to assess whether this computation workload is acceptable or not, and further provide solutions to reduce such overhead. In addition, one could study how AI could be used to create a dynamic Blockchain network. While this work was introduced in the literature as shown in Chapter 3, a more analytical approach is needed. Another interesting direction is to study the firmware of the EVCS to discover more vulnerabilities. Although some work has already been done in this direction as shown in Chapter 4, a more comprehensive study on the different firmware used by different manufacture would offer great insights on the vulnerabilities of the EVCS. On a different note, one can focus on the security of EVs and how they can be exploited to disturb the power grid. For instance, it was shown in multiple research that EVs could be hijacked remotely over the Internet. Thus, one can explore the different attacks that an adversary can do to disturb the power grid or the charging infrastructure. Finally, one rather interesting direction is to follow the same footsteps of this work and apply it to a different kind of IoT devices. For instance, one can study the security of the medical IoT devices (MRI machines, PET Scanners) and determine if they can disturb the power grid.

Bibliography

[1] P. Meera and S. Hemamalini, "Optimal siting of distributed generators in a distribution network using artificial immune system," *International Journal of Electrical and Computer Engineering*, vol. 7, no. 2, p. 641, 2017.

[2] L. Baumer, "Forecasts for 1907," *The Punch*, vol. 131, dec 1906.

[3] M. Campbell-Kelly and D. D. Garcia-Swartz, "The history of the internet: the missing narratives," *Journal of Information Technology*, vol. 28, no. 1, pp. 18–33, 2013.

[4] B. M. Leiner, V. G. Cerf, D. D. Clark, R. E. Kahn, L. Kleinrock, D. C. Lynch, J. Postel, L. G. Roberts, and S. Wolff, "A brief history of the internet," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 5, pp. 22–31, 2009.

[5] P. Corcoran, "The internet of things: why now, and what's next?," *IEEE consumer electronics magazine*, vol. 5, no. 1, pp. 63–68, 2015.

[6] N. Kherraf, S. Sharafeddine, C. M. Assi, and A. Ghrayeb, "Latency and reliability-aware workload assignment in iot networks with mobile edge clouds," *IEEE Transactions on Network and Service Management*, vol. 16, no. 4, pp. 1435–1449, 2019.

[7] N. Kherraf, H. A. Alameddine, S. Sharafeddine, C. Assi, and A. Ghrayeb, "Optimized provisioning of edge computing resources with heterogeneous workload in iot networks," *IEEE Transactions on Network and Service Management*, 2019.

[8] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[9] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[10] C. Alcaraz, J. Lopez, and S. Wolthusen, "OCPP protocol: Security threats and challenges," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2452–2459, 2017.

[11] I. Lee and K. Lee, "The internet of things (iot): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[12] E. Global, "outlook 2018," *International Energy Agency*, pp. 1–71, 2018.

[13] D. Hall, M. Moultak, and N. Lutsey, "Electric vehicle capitals of the world: Demonstrating the path to electric drive. the international council on clean transportation (icct), march," *Global-EV-Capitals_White-Paper_06032017_vF. pdf*, 2017.

[14] Y. Zhang, J. Chen, L. Cai, and J. Pan, "Expanding ev charging networks considering transportation pattern and power supply limit," *IEEE Transactions on Smart Grid*, 2019.

[15] Y. Wu, A. Ravey, D. Chrenko, and A. Miraoui, "Demand side energy management of ev charging stations by approximate dynamic programming," *Energy Conversion and Management*, vol. 196, pp. 878–890, 2019.

[16] Y. Zhao, H. Huang, X. Chen, B. Zhang, Y. Zhang, Y. Jin, Q. Zhang, L. Cheng, and Y. Chen, "Charging load allocation strategy of ev charging station considering charging mode," *World Electric Vehicle Journal*, vol. 10, no. 2, p. 47, 2019.

[17] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "Smart electric vehicle charging: Security analysis," in *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, pp. 1–6, IEEE, 2013.

[18] R. M. Pratt and T. E. Carroll, "Vehicle charging infrastructure security," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–5, IEEE, 2019.

[19] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles+ grid data: Is a new cyberattack vector viable?," *arXiv preprint arXiv:1907.08283*, 2019.

[20] G. S. Morrison, "Threats and mitigation of ddos cyberattacks against the us power grid via ev charging," 2018.

[21] IEA, "Global ev outlook 2019," tech. rep., IEA, 2019.

[22] W. YS and C. KT, "Battery sizing for plug-in hybrid electric vehicles," *Journal of Asian Electric Vehicles*, vol. 4, no. 2, pp. 899–904, 2006.

[23] C. Thomas, "Fuel cell and battery electric vehicles compared," *international journal of hydrogen energy*, vol. 34, no. 15, pp. 6005–6020, 2009.

[24] A. Muir and J. Lopatto, "Final report on the august 14, 2003 blackout in the united states and canada: causes and recommendations," 2004.

[25] U. O. Handbook-Glossary, "european network of transmission system operators for electricity.[online] 2004."

[26] I. Rahman, P. M. Vasant, B. S. M. Singh, M. Abdullah-Al-Wadud, and N. Adnan, "Review of recent trends in optimization techniques for plug-in hybrid, and electric vehicle charging infrastructures," *Renewable and Sustainable Energy Reviews*, vol. 58, pp. 1039–1047, 2016.

[27] R. J. Flores, B. P. Shaffer, and J. Brouwer, "Electricity costs for an electric vehicle fueling station with level 3 charging," *Applied energy*, vol. 169, pp. 813–830, 2016.

[28] G. Joos, M. De Freige, and M. Dubois, "Design and simulation of a fast charging station for phev/ev batteries," in *2010 IEEE Electrical Power & Energy Conference*, pp. 1–5, IEEE, 2010.

[29] J. Y. Yong, V. K. Ramachandaramurthy, K. M. Tan, and N. Mithulananthan, "A review on the state-of-the-art technologies of electric vehicle, its impacts and prospects," *Renewable and Sustainable Energy Reviews*, vol. 49, pp. 365–385, 2015.

[30] A. Foley, I. Winning, and B. Ó. Gallachóir, "State-of-the-art in electric vehicle charging infrastructure," in *2010 IEEE Vehicle Power and Propulsion Conference*, pp. 1–6, IEEE, 2010.

[31] A. Briones, J. Francfort, P. Heitmann, M. Schey, S. Schey, and J. Smart, "Vehicle-to-grid (v2g) power flow regulations and building codes review by the avta," *Idaho National Lab., Idaho Falls, ID, USA*, 2012.

[32] K. Bao, H. Valev, M. Wagner, and H. Schmeck, "A threat analysis of the vehicle-to-grid charging protocol iso 15118," *Computer Science-Research and Development*, vol. 33, no. 1-2, pp. 3–12, 2018.

[33] A. Heinrich and M. Schwaiger, "Iso 15118–charging communication between plug-in electric vehicles and charging infrastructure," in *Grid Integration of Electric Mobility*, pp. 213–227, Springer, 2017.

[34] T. Anegawa, "Characteristics of chademo quick charging system," *World Electric Vehicle Journal*, vol. 4, no. 4, pp. 818–822, 2010.

[35] O. C. Alliance, "Open charge point protocol 2.0," *Open Charge Alliance*, 2014.

[36] OCPP, "Ocpp 2.0 part 2: Specification," tech. rep., OCPP, 2018.

[37] O. C. P. Interface, "Open charge point interface (ocpi)," 2018.

[38] Open Charge Map, "The global public registry of electric vehicle charging locations," 2018.

[39] K. Harnett, B. Harris, D. Chin, G. Watson, *et al.*, "DOE/DHS/DOT Volpe Technical Meeting on Electric Vehicle and Charging Station Cybersecurity Report," tech. rep., John A. Volpe National Transportation Systems Center (US), 2018.

[40] Y. Ryabova, "Don't be sure charging your electric car is secure enough," jan 2018.

[41] H. Booth, "Draft nistir 8138, vulnerability description ontology (vdo)," 2016.

[42] D. Skylar, "Chargepoint home security research," tech. rep., Kaspersky Lab Security Services, 2018.

[43] T. Spring, "Critical bug patched in schneider electric vehicle charging station," nov 2018.

[44] A. Bhardwaj, A. Sharma, V. Mangat, K. Kumar, and R. Vig, "Experimental analysis of ddos attacks on openstack cloud platform," in *Proceedings of 2nd International Conference on Communication, Computing and Networking*, pp. 3–13, Springer, 2019.

[45] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, *et al.*, "Understanding the mirai botnet," in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, pp. 1093–1110, 2017.

[46] S. Soltan, P. Mittal, and H. V. Poor, "Blackiot: Iot botnet of high wattage devices can disrupt the power grid," in *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pp. 15–32, 2018.

[47] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, "A coordinated multi-switch attack for cascading failures in smart grid," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1183–1195, 2014.

[48] A. K. Farraj and D. Kundur, "On using energy storage systems in switching attacks that destabilize smart grid systems," in *2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pp. 1–5, IEEE, 2015.

[49] P. Corporation, "Power world corporation homepage," Feb 2020.

[50] O. Erdinc, N. G. Paterakis, T. D. Mendes, A. G. Bakirtzis, and J. P. Catalão, "Smart household operation considering bi-directional ev and ess utilization by real-time pricing-based dr," *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1281–1291, 2014.

[51] R. Jarvis and P. Moses, "Smart grid congestion caused by plug-in electric vehicle charging," in *2019 IEEE Texas Power and Energy Conference (TPEC)*, pp. 1–5, IEEE, 2019.

[52] A. Khan, S. Memon, and T. P. Sattar, "Analyzing integrated renewable energy and smart-grid systems to improve voltage quality and harmonic distortion losses at electric-vehicle charging stations," *IEEE Access*, vol. 6, pp. 26404–26415, 2018.

[53] R. Gottumukkala, R. Merchant, A. Tauzin, K. Leon, A. Roche, and P. Darby, "Cyber-physical system security of vehicle charging stations," in *2019 IEEE Green Technologies Conference (GreenTech)*, pp. 1–5, IEEE, 2019.

[54] Y. Fraiji, L. B. Azzouz, W. Trojet, and L. A. Saidane, "Cyber security issues of internet of electric vehicles," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, IEEE, 2018.

[55] J. E. Rubio, C. Alcaraz, and J. Lopez, "Addressing security in ocpp: Protection against man-in-the-middle attacks," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–5, IEEE, 2018.

[56] R. Baker and I. Martinovic, "Losing the car keys: Wireless phy-layer insecurity in {EV} charging," in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pp. 407–424, 2019.

[57] T. M. Bojan, U. R. Kumar, and V. M. Bojan, "An internet of things based intelligent transportation system," in *2014 IEEE International Conference on Vehicular Electronics and Safety*, pp. 174–179, 2014.

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

[59] T. Bunsen, P. Cazzola, M. Gorner, L. Paoli, S. Scheffer, R. Schuitmaker, J. Tattini, and J. Teter, "Global ev outlook 2018: Towards cross-modal electrification," 2019.

[60] P. Hertzke, N. Müller, S. Schenk, and T. Wu, "The global electric-vehicle market is amped up and on the rise," *McKinsey Cent. Futur. Mobil.*, pp. 1–8, 2018.

[61] Y. Wang, Z. Su, Q. Xu, T. Yang, and N. Zhang, "A novel charging scheme for electric vehicles with smart communities in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 8487–8501, 2019.

[62] T. Jiang, H. Fang, and H. Wang, "Blockchain-based internet of vehicles: Distributed network architecture and performance analysis," *IEEE Internet of Things Journal*, 2018.

[63] Y. Wang, Z. Su, and N. Zhang, "Bsis: Blockchain based secure incentive scheme for energy delivery in vehicular energy network," *IEEE Transactions on Industrial Informatics*, 2019.

[64] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25657–25665, 2018.

[65] M. Liu, Y. Teng, F. R. Yu, V. C. Leung, and M. Song, "Deep reinforcement learning based performance optimization in blockchain-enabled internet of vehicle," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2019.

[66] C. Stoll, "Why the web won't be nirvana," *News week, np Retrieved from http://www. news week. com/clifford-stoll-why-web-wont-be-nirva na-185306*, 1995.

[67] S. Carley, S. Siddiki, and S. Nicholson-Crotty, "Evolution of plug-in electric vehicle demand: Assessing consumer perceptions and intent to purchase over time," *Transportation Research Part D: Transport and Environment*, vol. 70, pp. 94–111, 2019.

[68] É. Latulippe, K. Mo, *et al.*, "Outlook for electric vehicles and implications for the oil market," tech. rep., Bank of Canada, 2019.

[69] M. Nicholas, D. Hall, and N. Lutsey, "Quantifying the electric vehicle charging infrastructure gap across us markets," *The International Council on Clean Transportation*, pp. 4–14, 2019.

[70] J. Caltrider, "fascinating things we learned when we asked the world "how connected are you?"," 10.

[71] P. Emami-Naeini, Y. Agarwal, L. F. Cranor, and H. Hibshi, "Ask the experts: What should be on an iot privacy and security label?," *arXiv preprint arXiv:2002.04631*, 2020.

[72] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Lsb: A lightweight scalable blockchain for iot security and privacy," *arXiv preprint arXiv:1712.02969*, 2017.

[73] J. Antoun, M. E. Kabir, B. Moussa, R. Atallah, and C. Assi, "A detailed security assessment of the ev charging ecosystem," *IEEE Network*, 2020.

[74] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet of Things Journal*, 2018.

[75] H. Liu, Y. Zhang, S. Zheng, and Y. Li, "Electric vehicle power trading mechanism based on blockchain and smart contract in v2g network," *IEEE Access*, vol. 7, pp. 160546–160558, 2019.

[76] M. Kim, K. Park, S. Yu, J. Lee, Y. Park, S.-W. Lee, and B. Chung, "A secure charging system for electric vehicles based on blockchain," *Sensors*, vol. 19, no. 13, p. 3028, 2019.

[77] A. C.-F. Chan and J. Zhou, "A secure, intelligent electric vehicle ecosystem for safe integration with the smart grid," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 3367–3376, 2015.

[78] K. Shuaib, E. Barka, J. A. Abdella, F. Sallabi, M. Abdel-Hafez, and A. Al-Fuqaha, "Secure plug-in electric vehicle (pev) charging in a smart grid network," *Energies*, vol. 10, no. 7, p. 1024, 2017.

[79] S. Lee, Y. Park, H. Lim, and T. Shon, "Study on analysis of security vulnerabilities and countermeasures in iso/iec 15118 based electric vehicle charging technology," in *2014 International conference on IT convergence and security (ICITCS)*, pp. 1–4, IEEE, 2014.

[80] T. Streubel, C. Kattmann, A. Eisenmann, and K. Rudion, "Detection and monitoring of supraharmonic anomalies of an electric vehicle charging station," in *2019 IEEE Milan PowerTech*, pp. 1–5, IEEE, 2019.

[81] L. Zhang, L. Wan, Y. Xiao, S. Li, and C. Zhu, "Anomaly detection method of smart meters data based on gmm-lda clustering feature learning and pso support vector machine," in *2019 IEEE Sustainable Power and Energy Conference (iSPEC)*, pp. 2407–2412, IEEE, 2019.

[82] S. W. Yen, S. Morris, M. A. Ezra, and T. J. Huat, "Effect of smart meter data collection frequency in an early detection of shorter-duration voltage anomalies in smart grids," *International Journal of Electrical Power & Energy Systems*, vol. 109, pp. 1–8, 2019.

[83] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[84] ChargePoint, "Chargepoint adopts ocpp for its charging stations." https://www.chargepoint.com/about/news/chargepoint-adopts-ocpp-its-charging-stations/.

[85] J. Burkill, "Irish electric vehicle charge point status datasets," oct 2017.

[86] J. Hörsch, F. Hofmann, D. Schlachtberger, and T. Brown, "Pypsa-eur: An open optimisation model of the european transmission system," *Energy strategy reviews*, vol. 22, pp. 207–215, 2018.

[87] EirGrid, "Eirgrid's smart grid dashboard energy & system data from the all-island power system.," apr 2020.

[88] J. Hochenbaum, O. S. Vallis, and A. Kejariwal, "Automatic anomaly detection in the cloud via statistical learning," *arXiv preprint arXiv:1704.07706*, 2017.

[89] B. Schölkopf, R. C. Williamson, A. J. Smola, J. Shawe-Taylor, and J. C. Platt, "Support vector method for novelty detection," in *Advances in neural information processing systems*, pp. 582–588, 2000.

[90] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in *2008 Eighth IEEE International Conference on Data Mining*, pp. 413–422, IEEE, 2008.

[91] F. A. Gers, J. Schmidhuber, and F. Cummins, "Learning to forget: Continual prediction with lstm," 1999.

[92] C. Coin, "Charg ev charging station white paper," white paper, Charg Coin, 2017. Available Online at: https://chgcoin.org/white-paper/.