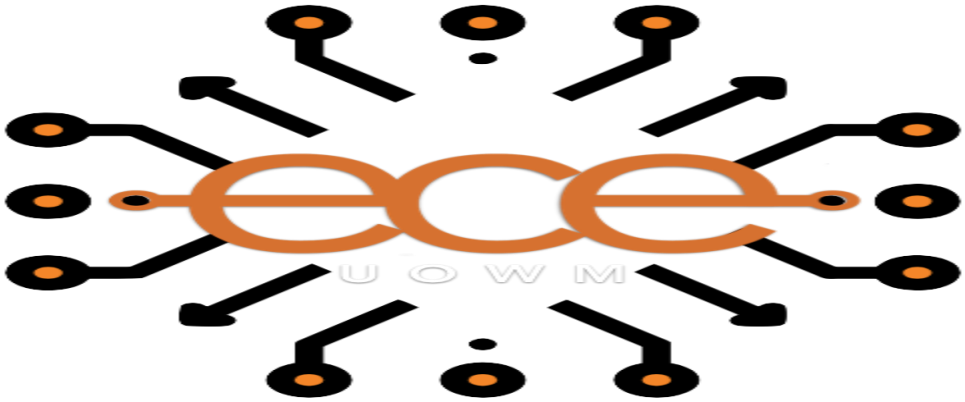


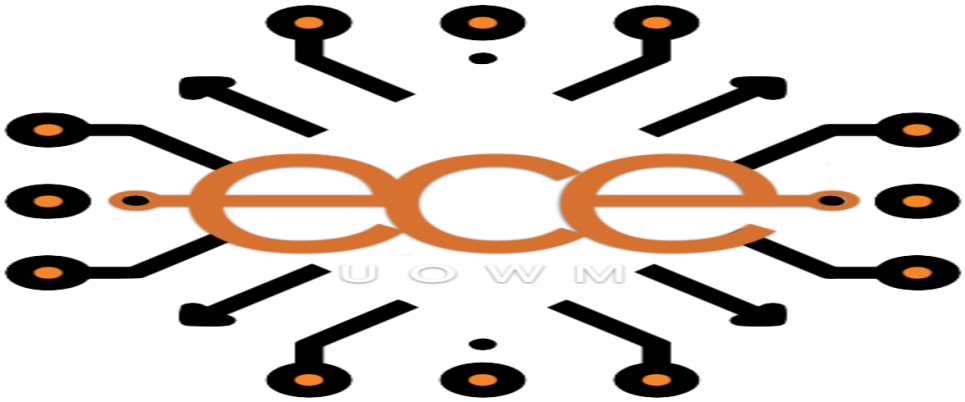
ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Τεχνικές ανίχνευσης και απόκρισης κυβερνοαπειλών για ηλεκτρικά οχήματα εξωτερικής τροφοδοσίας

ΠΑΝΑΓΙΩΤΗΣ ΚΟΥΡΤΖΕΛΛΗΣ 519

Επιβλέπων Καθηγητής: Επίκουρος Καθηγητής, Παναγιώτης Σαρηγιαννίδης

ΚΟΖΑΝΗ, ΙΟΥΛΙΟΣ 2020



DIPLOMA THESIS

Cyber threat Detection and Response Techniques for Plug-in Electrical Vehicles

PANAGIOTIS KOURTZELLIS 519

Supervisor: Assistant Professor, Panagiotis Sarigiannidis

KOZANI, JULY 2020

Δήλωση Πνευματικών Δικαιωμάτων

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1986 και τα άρθρα 2,4,6 παρ. 3 του Ν. 1256/1982, η παρούσα Διπλωματική Εργασία με τίτλο ΄΄ Cyber threat Detection and Response Techniques for Plug-in Electrical Vehicles ΄΄καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας και αναφέρονται ρητώς μέσα στο κείμενο που συνοδεύουν, και η οποία έχει εκπονηθεί στο Τμήμα Μηχανικών Πληροφορικής και Τηλεπικοινωνιών του Πανεπιστημίου Δυτικής Μακεδονίας, υπό την επίβλεψη του μέλους του Τμήματος κ. Σαριγιαννίδη Παναγιώτη, αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή / και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και μόνο.

Υπογραφή Φοιτητή:

Thanks

At the end of this dissertation, I would like to thank Prof. Panagiotis Sarigiannidis and the rest of the teaching staff for all the advice and help they have given me throughout its implementation.

I would also like to thank my friends Basilis, Dimitris, Jason and Stratos for their support over the years and last but most important I would like to thank my parents for always being there for me.

Abstract

One of the biggest problems of modern society is considered the air pollution, which has led to the discovery of alternative energy sources in combination with other factors, such as the reduction of natural resources due to their unbridled and uncontrolled exploitation. The interim solution of using catalysts to reduce pollution proved insufficient, because it simply limited the problem without leading to its final solution. The electric vehicle ensures zero emissions and frees users from dependence on liquid fuels, the sharp rise in prices and all kinds of shortages due to crises.

The various vehicles, on a case-by-case basis, are equipped with the corresponding fuels to power their engines from each of the refueling stations. Therefore, to charge electric vehicles, charging point stations are needed to supply electricity. Their supply, as mentioned, requires their connection to some kind of electricity network infrastructure. The large area of the electricity grid offers many options for potential charging facilities.

This thesis examines threats and cyber-attacks in the charging process and the targeting Battery Management System (BMS) and other parts of the car's electronics' system. More specifically, this thesis will examine whether the charging station hardware can be hacked in order to send these erroneous signals (either locally or remotely) and how the charging stations can be made tamper-proof and how cyber-attacks can be detected.

Charging Point Stations have many functions, such as, providing and controlling the energy to the Electric Vehicle (EV) using the Electric Vehicle Supply Equipment (EVSE) component, collecting the measurements from the meter for each charge of an Electric Vehicle, identifying and authorizing EV users via user authentication component, enabling remote capabilities (e.g., adjustment of the maximum current allowed by the Charge Point) to the Charge Point via the local Controller component over the Wide Area Network (WAN).

The protection of the European electric grid should become a priority for all the organization/entities that are getting engaged in the EV ecosystem. The output of this thesis is aiming at increasing the cyber security of a standard EV charging enterprise's platform through the integration of Machine Learning (ML) techniques for identifying anomalies in the charging patterns, and therefore minimize the exposure both enterprises' database and the stability of the electric grid. The thesis covers both the Information and Communications Technology (ICT) and the electric engineering domain on an effort towards increasing the cyber security on what is called Energy Internet.

In the implementation part of this thesis, we will use dataset in CSV format obtained from a standard EV charging enterprise's database to apply anomaly based algorithm, in order to discover if any abnormal functions of charging happens. For the smart charging abuse scenario, different evaluation methods will be applied in order to ensure high quality to the findings of the ML techniques. The applied evaluation methods will contain qualitative (visual inspection, manual investigation) metrics offering a validation framework wide enough to cover different aspects of cyber security in the area of EV smart charging.

Keywords:

- electric vehicles,
- electric vehicles smart charging,
- electric vehicle supply equipment,
- anomaly detection,
- machine learning

Table of Contents

Table of Figures

List of Tables

Chapter 1 - Introduction

1.1. Research Problem

The evolution of car and battery technology has now made electric propulsion a tangible reality, which is radically changing car data. Addressing the major environmental and economic challenges associated with climate change and dependence on fossil fuels creates new conditions for the automotive industry and for our daily lives. Electricity, like other alternative fuels, is constantly gaining ground [1].

The more electric vehicles expand and evolve, the more their refueling becomes a point of concern for drivers, a point of superiority over cars with internal combustion engines. The electricity grid ensures the widest possible availability of supply sources, while the technology makes charging electric vehicles in addition to being affordable and an extremely simple and easy process.

Main object of thesis is to examine threats and cyber-attacks in the charging process and the targeting BMS and other parts of the car's electrics' system. More specifically, a Plug-in Electric Vehicle communicates with and is controlled by a charging station. This means that if an attacker could intrude the software of the charging station, it might be possible to influence the charging behavior of the vehicle. Therefore, some threats and challenges arise in the security of smart charging of EVs:

• Disrupting the charging process by meddling with the Pulse Width Modulation - communication (PWM-communication) as prescribed by to the IEC61851-1:2017, which is supported by all charging stations.

• Disrupting the charging process and possibly gaining access to the BMS of the vehicle using the ISO/IEC15118 standard, this is to be expected as the future standard for electric vehicle communication.

Consequently, this thesis will investigate how tamper-safe Plug-in Electric Vehicles are when receiving erroneous signals:

• Whether the charging station hardware can be hacked in order to send these erroneous signals (either locally or remotely).

• How the charging stations can be made tamper-proof and how cyber-attacks can be detected.

1.2. Contribution of Thesis

The main contribution of this thesis is the new knowledge of examining possible threats and abuse of smart charging in Electrical Vehicles. In other words, applying specific algorithms in real collected database of a standard EV charging enterprise, to test the possible abnormal activity on the Charging Station can trigger designers and programmers of the networks of those smart Charging Stations, to reconsider the possible security issues that can arise, by third malevolent parties like industrial saboteurs.

Moreover, if algorithms can be applied in real time, then detection of such abnormalities during the process of smart charging could trigger an alarm that some abnormal activity is taking place, which then subsequently can give an insight to the developers, as to how can the cyber-attack be prevented adequately. This is more important than trying to solve the problem in later time, because the damage may very well be already done to the Charging Points and even worse to the Charging Stations and worst case scenario to the whole grid of the EV charging enterprise. Problems like these are easier to occur with the rapid increase of the Electrical Vehicles (EVs) distribution globally, so addressing this sooner is of great importance to all parties involved in their creation and usage.

1.3. Structure of Thesis

This thesis is divided into five main chapters. First chapter (current chapter) presents the main research problem and the main objectives. Second chapter, examines the concepts and main functions of EVs. In more detail, second chapter presents principles of operation of EVs, positive impacts of the introduction of the use of electric cars, smart Charging ways in Electrical Vehicles. Third chapter focuses on issues, vulnerabilities, threats and challenges of Smart Charging. More specifically, this chapter presents vulnerabilities in vehicle communication, possible attacks intervention in smart charging, and protocols that participate on smart charging function. Next, fourth chapter, presents an abuse scenario in smart charging station, and the implementation of anomaly based algorithm and data manipulation in order, such as “Isolation Forest” and “Standard Scaler” algorithm on data collected of charging cases, in order to conclude whether is possible to detect of abnormalities in smart charging function. Finally, conclusion chapter summarizes the most important findings of this research.

Chapter 2 - Electrical Vehicles

One of the biggest problems of modern society, air pollution, in combination with other factors such as the reduction of natural resources due to their unbridled and uncontrolled exploitation, has led to the discovery of alternative energy sources. In the spirit of the new data, vehicle manufacturers have been led to design and build electric vehicles. The intermediate solution of using catalysts to reduce pollution proved to be insufficient, because it simply limited the problem without leading to its final solution. The electric vehicle ensures zero emissions and frees users from dependence on liquid fuels, the vertical increase in their prices and any kind of shortages due to crises (e.g., Gulf War). Thus, ecological sensitivity, the realization that conventional vehicle pollutants are a major factor in air pollution and the knowledge that a clean environment is equivalent to quality of life have led the automotive industry to "listen" to new needs and adapt accordingly [2].

2.1. Principle of operation of an electric car

Electric cars simply depend on batteries. In this form, the mechanical parts of an electric car are very different from the parts of a car with an internal combustion engine. Electric battery cars usually have three main components, namely: the controller, the battery, and the electric motor. In an electric battery car, the accelerator pedal is connected to a potentiometer that measures the power the driver has applied to the pedal. The potentiometer then sends a signal to a controller telling him how much power the battery should give to the electric motor. The batteries used in electric cars are rechargeable and usually come in these forms or variants [3]:

- Nickel-Cadmium (NiCd)
- Lead-Acid (and adjustable lead acid valve or otherwise)
- Nickel Metal (NiMH)
- Metal Hydride

- (LiON) Lithium-ion polymers

The battery's energy output is measured in kilowatts per hours (KWh), which shows how much energy a battery is able to store or produce.

2.2. Electric vehicles

Vehicles belonging to this category operate exclusively using an electric motor, controlled by an electronic power converter. Electricity is provided by batteries, photovoltaic batteries or fuel cells. The electric car has zero carbon dioxide emissions as it moves. But if the electricity for charging the batteries comes from the conventional power grid, then carbon dioxide emissions are not significantly reduced. However, pollutants are concentrated and can be reduced by using filters in production stations. The biggest environmental benefit, however, is if electricity comes from alternative sources [4]. The autonomy of electric cars is generally lower than that of petrol cars. Typically with one charge an electric vehicle can cover a distance of 200-320 kilometers. Charging is a process that typically takes around 3-4 hours, which makes it difficult to cover long distances. A quick 80% charge can take half an hour. In an electric vehicle, the electric motor is the sole source of movement. In the electric vehicle industry, two types of engines have prevailed: the permanent brushless motor and the three-phase induction motor.

In “Prius” and “Civic” hybrid vehicles, the brushless motor solution has been chosen, while in purely electric vehicles, such as the high-performance Tesla Roadster, the inductor is used. Less common, and in lower power applications, is the use of DC, foreign or parallel excitation motors, while in the past such motors have been used in electric public transport.

2.3. Effect of the introduction of the use of electric cars

2.3.1. Energy consumption

It is common known, that electric cars have the advantage of thermal use in the city because they do not consume energy as long as they are stopped at the red signal. But how important is this advantage in mixed use? In most comparative studies, the kilometer-by-energy energy consumed by an electric car is about half that of a thermal car. However, these comparisons do not take into account the fact that the speed and all other conditions related to the comfort of the passengers are not the same in the two compared types of cars. In practice, the user of the electric car will be forced to drive at lower speeds and may not enjoy the comforts offered by the thermal car (e.g., air conditioning system and other electrical subsystems). Lower speeds have the effect of saving energy, reducing the number of accidents and reducing damage if they occur. Thus the effect of the application of electric cars on energy consumption will be positive on a short-term basis, although this advantage may long cease to have significant value in electricity consumption [4].

Preliminary studies show that the use of small-scale electric cars does not cause serious problems in the balance of electricity supply, provided that their batteries will be charged during the night. However, this will not be the case if electric car users will be able to charge their batteries quickly during the day. The impact of this possibility should not be overlooked.

Each fast charging station can represent an installed capacity of 10 to 300 KW. Uncontrolled use of a large number of such stations can cause energy demand at unpredictably high levels and therefore require more power plants, perhaps even nuclear power plants that are not very popular today. In the case of a total replacement of thermal cars with electric ones, all the energy currently consumed for transport should be available in the form of electricity. In some cases, this energy accounts for 20 to 40% of the total en-

ergy consumed throughout the country. This will cause a desperately high need to build new power plants and may lead countries that have so far pursued a negative policy on the construction of nuclear power plants to revise their policy. One way to control the situation is to supply electric cars with special type of charging terminals and special charging systems (perhaps even inductive type, which are safer), so that it is not possible to connect to the usual type of household or industrial power receivers (sockets), but only with power receivers of a power supply system made exclusively for this use [5].

This network may provide electricity with a different and variable tariff depending on the availability of electricity. High charging voltages for relatively short periods of time will cost more. Low intensities during the night will cost a bit. We can thus avoid unwanted demand peaks. Citizens' mobility is increasing daily. In 10 to 30 years when the radius of electric cars will be similar to that of thermal cars, a million tourists who visit a neighboring country with their electric cars will easily be able to cause the collapse of their country's electricity distribution network hosts, unless, of course, all distribution networks are interconnected and supported [5].

2.3.2. Pollution and the greenhouse effect

The electric car is a "zero" pollution vehicle only locally in the area where it operates. If its batteries are charged with electricity generated by thermal power plants, then the problem of pollution is transferred elsewhere outside the city. But even so, it is technologically easier to tackle this problem worldwide. In addition, hydroelectric or geothermal power plants are not directly polluting. The same goes for solar power and under certain conditions nuclear power [3]. The total pollution from power plants depends on the percentage of the various energy sources used in each system and it varies from country to country. On a global scale, it is estimated that the widespread use of electric cars will reduce t Pollution both in the cities and as a whole will also reduce the greenhouse effect. Another cause of pollution is useless industrial products. Old cars belong to this

category. The numbers of cars sold annually show the magnitude of the problem. It is now necessary for cars to be recyclable. This must apply to electric cars as well, although a non-recyclable car made of non-recyclable synthetic materials may be lighter, more durable and more autonomous [4].

In traffic conditions and traffic accidents:

Traffic accidents are caused by three main causes:

1. The limited width of roads.

2. The need to impose speed limits to reduce the likelihood and severity of traffic accidents.

The irregular way in which drivers drive their cars (overtaking, etc.), due to the heterogeneity of the performance of these cars. The flow of traffic on our roads is comparable to the irregular flow of fluid mechanics. Mixing, in the same flow of traffic, vehicles with different performance (as in the case of thermal and electric cars) will not reduce traffic problems. It already exists, since thermal cars also differ significantly in performance [6].

Electric cars will be a new future product being designed. We now have the opportunity to impose standard performance data (e.g., all cars have the same top speed and the same acceleration). It is technically possible to extend this measure to thermal cars as well, using the electronic engine management system with which most of them are equipped. In this way, of course, the freedoms of car users are restricted, but the result will be favorable for them. Traffic will be smoother and traffic accidents will be reduced because overtaking and speeding will be reduced. Cars will drive on the roads almost like the wagons of the train trains. The measure is, of course, radical but justified by the many thousands of victims of road accidents each year. It is predicted that manufacturers will not support such a measure since the differences in the performance of cars are the dominant element of promotion and competition of their products. But there are many other

harmless properties at their disposal for the promotion of their products, such as e.g., the energy consumed per kilometer.

Many consumers will also oppose such measures. However, they must be convinced that improper use of the car is a danger to everyone's lives. Acceptance of general mandatory specifications that regulate the maximum speed of cars, as long as they are extended to thermal cars, will significantly reduce the differences in the performance of electric cars with those of thermal cars. It will also greatly facilitate the spread of electric cars.

2.4. Plug-in Electrical Vehicle

A Plug-in hybrid Electrical Vehicle (PHEV) is a hybrid vehicle with rechargeable batteries connecting the vehicle to a socket at an electrical source. The main components of an EV that are responsible for its operation are depicted below in Figure 1. Namely:

- **Battery:** In an electric drive vehicle, the auxiliary battery provides electricity to start the car before the traction battery is engaged and also powers vehicle accessories.

- **Charger:** Takes the incoming AC electricity supplied via the charge port and converts it to DC power for charging the traction battery. It monitors battery characteristics such as voltage, current, temperature, and state of charge while charging the pack.

- **Charge port:** The charge port allows the vehicle to connect to an external power supply in order to charge the traction battery pack.
- **Fuel storage (gasoline):** This tank stores gasoline on board the vehicle until it's needed by the engine.

- **Lightweighting materials:** Lightweighting usually refers to reduction of vehicle weight by substituting materials with a higher strength per weight than traditional materials. For example, when we replace heavier iron or steel parts with High Strength Steel (HSS), aluminum, magnesium or composite materials such as glass and carbon-fiber-reinforced polymers.

- **Power electronics controller:** This unit manages the flow of electrical energy delivered by the traction battery, controlling the speed of the electric traction motor and the torque it produces.

- **Electric traction motor:** Using power from the traction battery pack, this motor drives the vehicle's wheels. Some vehicles use motor generators that perform both the drive and regeneration functions.

- **Radiator:** This system maintains a proper operating temperature range of the engine, electric motor, power electronics, and other components.

- **Internal combustion engine:** In this configuration, fuel is injected into either the intake manifold or the combustion chamber, where it is combined with air, and the air/fuel mixture is ignited by the spark from a spark plug.

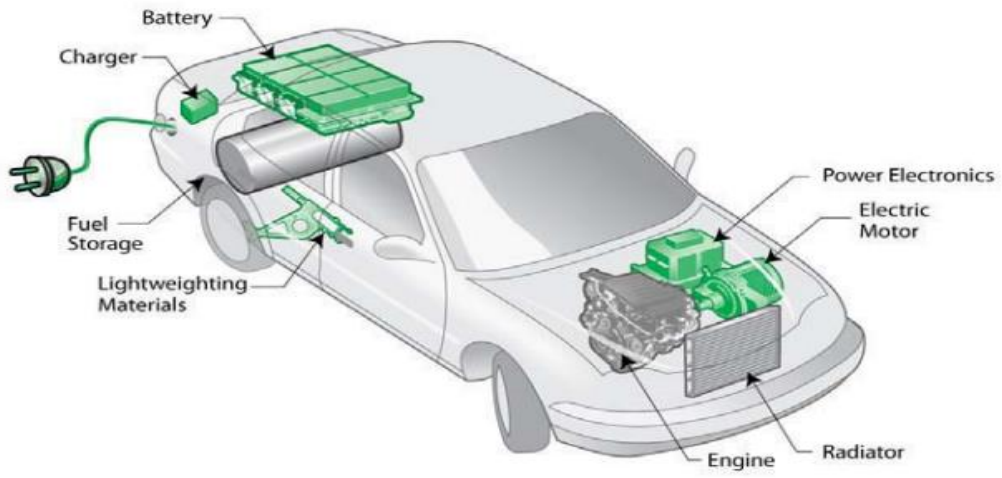


Figure 1- Parts of a plug-in Electrical Vehicle [7]

Hybrid plug-ins have the features of both conventional hybrid electric and purely electric vehicles. While PHEVs are expected in the form of passenger vehicles, they can also be commercially light trucks, business trucks, school buses, scooters and military vehicles. PHEVs are also referred to as “network-connected vehicles” or GO - HEVs in their conventional form. Compared to conventional cars, PHEVs can help reduce pollution and dependence on oil and reduce greenhouse gas emissions that lead to global warming. Plug-in hybrids do not use any natural fuel during their electrical operation, unless their batteries are recharged from Renewable Energy Sources. PHEVs have not yet entered mass production, but Toyota, General Motors and Ford have announced their intention to produce such vehicles.

Plug-in hybrids are the evolution of today's "fully" hybrid vehicles. A fully hybrid car has the ability to start and accelerate at low speeds without the use of the engine, with the battery being charged, however, exclusively by the engine and the power recovery system during braking. A plug-in hybrid works the same way but has a larger battery and gives the driver the option to charge it at home using a power source so he can only move his vehicle using electricity. Usually, the car will be charged at night, which will be

stationary for a long time. So PHEVs and HEVs use batteries powered by batteries and M.E.K., to save fuel, but PHEVs can further delay the use of fuel by charging the vehicle from home [6].

Moreover, plug-in hybrids have an advantage over purely electric vehicles in that their drivers do not have to worry about the possibility of "discharging" their vehicle. This is because when the battery is discharged, the plug-in vehicles operate like conventional ones and use their engine and power recovery system when braking to charge the battery and promote the vehicle. Because they use both an engine and an electric motor, PHEVs have smaller and cheaper battery packs than their purely electric vehicles. Today's hybrid commercial vehicles use, as mentioned, NiMH batteries, which can offer short distances with the exclusive use of electricity in the respective plug-in hybrids. For PHEVs, then, greater power storage and greater demands will be achieved with Lithium - ion (Li ion) battery technology, as expected.

2.5. Smart Charging in Electrical Vehicles

The electricity grid is in the middle of a mutation, a radical change, to harmonize with the needs of the sustainable economy. The 2020 European targets and the 2030 ones designed to reduce emissions increase the penetration of Renewable Energy Sources (RES) and improve the efficiency that enhances decentralized production, the use of storage systems and EVs. For the smooth operation of the new production and demand elements that arise, the electricity grid should become smarter.

Similarly, EU traffic is changing, bringing significant changes to meet the demand for environmentally friendly traffic. Electric traffic is constantly gaining ground as it has zero emissions, is quiet and 3 times more efficient than the corresponding petrol engines.

As the use of EV increases, the Electricity Distribution Networks will face local problems. Even at low levels of penetration, EV can easily overload the local network and alter the mains voltage, with negative effects on local consumers. Faced with this problem, the classic approach is through the construction of new lines and transformers, to meet the new demand. However, this approach is not the best financial solution and will burden network costs, creating a serious barrier to the penetration of electricity [8].

But there is another solution. What we call "smart charging". Smart charging includes the wise charge of EV batteries: charging them in a way that avoids overloading the network and in the future by offering support to the network in times of need and in a way that the EV battery will support the maximum intrusion of RES into the local network. Smart charging can offer multiple benefits to users, the grid and society as a whole:

1. Customer participation in smart charging is only possible if there are financial benefits to attracting them. Studies have shown that 90% of EV charging is done at the user's home or at work. With smart charging, users will be able to charge their car at home without differentiating the needs of their electrical installation. With this approach, users will be able to take advantage of low prices in the morning with low demand.

2. Smart charging gives EV the ability to be flexible loads scattered across the network, which can be used by the Network Operator in a way that meets the needs of the network and thus avoid costly network enhancements. Studies have shown that the electricity needs that arise if all traffic were electric (i.e., all cars moving today were electric) will be only 25% of the total energy consumed today by a country like Cyprus, to satisfy all needs of society / economy. With this finding, it is easy to conclude that the electric infrastructure, as it is today, could satisfy the entire additional load that will result in 100% of the traffic being electric, without the need for any amplification. This presupposes that the charging of EV will be done with smart management for the benefit of all [9].

3. Smart charging can offer sustainable electric propulsion with great benefits to society. The low cost of charging achieved through smart charging along with the efficiency of

electric cars will drastically reduce the use of primary energy, which will lead to a drastic reduction in emissions. With the flexibility offered by smart charging, the utilization of scattered RES systems is facilitated and allows for increased penetration with multiple benefits for all users.

All of the above can be done in the environment of developed operation of smart networks, which under the conditions of their development is imposed as soon as possible, with proper regulation and with a vision on the part of the Transmission and Distribution Network Administrators [9].

2.6. Ways of charging Electrical Vehicles

2.6.1. Method 1 - Slow charging from a common electrical outlet (single-phase, three-phase)

The vehicle is connected to the mains using common power receivers (usually 10 A) located in homes. In order to be able to use this charging method, the electrical installation of the house must meet all the safety requirements and there must be a grounding system as well as insurance devices, in order to protect against overload and protection against current leakage, which can still be caused inside the vehicle. This way of charging is the most common, thanks to the simplicity and cheap cost it requires, however it carries risks in case it is used incorrectly, and it is distinguished by many imitations. As for its misuse, it is important to note that although in most countries the existence of an escape relay is mandatory, several homes have older electrical installations without an escape relay, and it is usually difficult for the electric vehicle user to be aware of this. On the subject of the constraints encountered in this way of charging, these are:

-The available energy. In order to avoid overheating of the socket and cables, in case of using more hours than the allowable limit, and to avoid fire, the electric shock in case the electrical installation is outdated or the appropriate protection measures have not been taken.

-Energy management. If the socket that supplies the vehicle is not in a separate circuit or the total consumption exceeds the safety limit (usually 16 A), it will interrupt the circuit, interrupting the charging. The usual charging time is 10-15 hours and a 10 A circuit is usually used. Power receivers do not exceed 16 A-250 VAC although this is different in some countries (Figure 2).

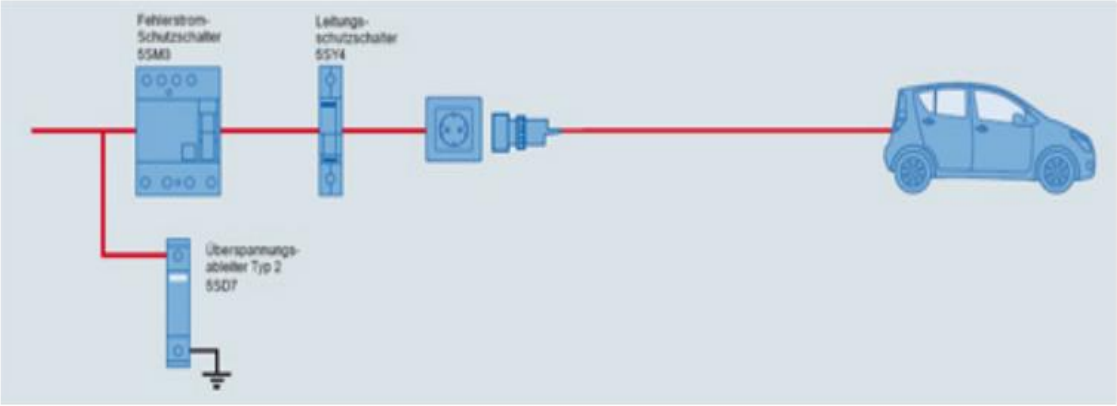


Figure 2- Charging according to Method 1: Slow charging from a common electrical outlet [10]

2.6.2. Method 2 - Slow charging from a common electrical outlet (single-phase, three-phase) with internal cable protection

The vehicle is connected to the mains using common power receivers as in the above case, the charging is done via single-phase or three-phase supply and ground pipe installation. However, this method provides additional protection by adding a control system inside the cable, which allows communication between the electric vehicle and the couple. Charging 2 was originally intended mainly for the US, but recently gained a lot of interest in Europe, with the aim of replacing Method 1. Nevertheless, in addition to the obvious disadvantage of having a control device inside the cable, the main disadvantage is the lack of protection of the coupler, one of the most likely fault points, by the control system. The charging time ranges from 3 to 8 hours (Figure 3).

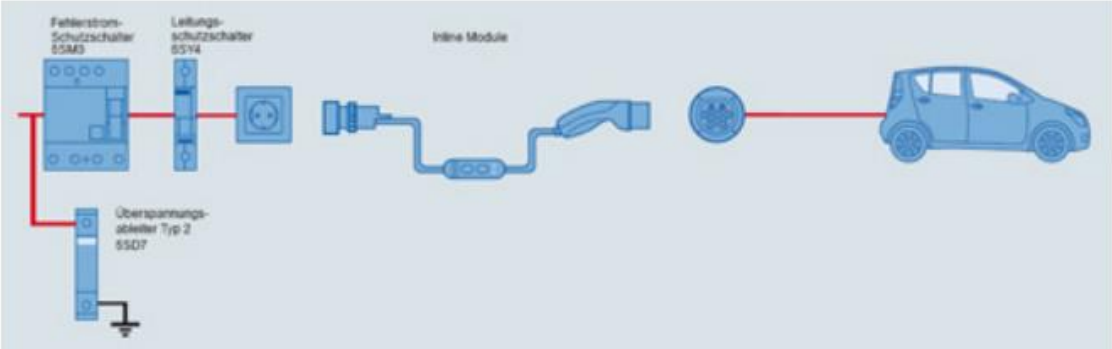


Figure 3- Charging according to method 2: Slow charging from a common electrical outlet (single-phase, three-phase) with internal cable protection [10]

2.6.3. Method3- Slow charging using a specific current receiver with an installed control and protection system.

The vehicle is connected directly to the mains via a socket of specific specifications and a separate circuit. This is the only way to charge the standard electrical installations. According to the international standard IEC 61851-1, the device / control system, between the supply equipment (i.e., the supply) and the electric vehicle, instructs the following functions [11]:

- Confirmation that the vehicle is properly connected
- Continuous control in case of power leakage
- Activate and deactivate the system
- Charging rate selection
- The control system is usually installed as an additional duct in the wiring of the charging cable, together with the phase, neutral, and ground. It therefore requires the use of special components.

It also allows the distribution of loads, so that the electrical appliances of the house operate during the charging of the vehicle or otherwise improve the charging time. Finally, pairs for this type of charging according to international standards require a range of control and signal nozzles at both ends of the cable, as seen below in detail in Figure 4.

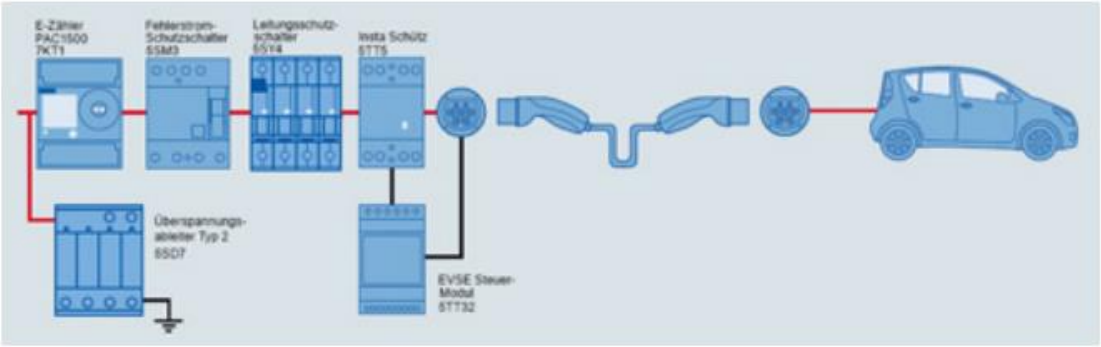


Figure 4- Charging according to method 3: Slow charging using a specific current receiver with an installed control and protection system. [10]

2.6.4. Method 4 - Fast charging using an external charger

This charging mode is related to the connection of the electric vehicle to the mains using an external charger that has a control and protection system installed. The alternating current of the network is converted to a continuous charging station and the plug type ensures that only if the vehicle fits, the connection can be made possible. Using fast charging with direct current, an intensity of up to 400 A is achieved [12].

2.6.5. Charging Levels

While in Europe the IEC 62196 standard is used, which separates charging modes to categorize charging equipment, in the United States charging modes are classified as Charging levels (Table 1).

Table 1- Charging times and the relevant requirements of the various charging levels

	Requirements	**Voltage (V) /Amber (A)**	**Time of charging**
LEVEL 1	------	120 / 13	7-8 hours
LEVEL 2	Special connection	240/32	3-4 hours
LEVEL 3	Special wiring and external charger	500/200	< 45 minutes

Level 1

The transfer of alternating current to the internal charger of the 120 Volt electric vehicle, either 15 A (using 12 A) or 20 A (using 16 A), through a common power socket, located either in homes or in commercial buildings in USA. However, because the power provided (maximum 1.44 kW) is insufficient, this results in prolonged charging times. So obviously, and it is an inefficient, but accessible and cheap option. At level 1, a new separate circuit is recommended as necessary to avoid overcharging. The charging equipment is installed inside the electric vehicle. While on the connection cable, a switch has been installed in case of power leakage.

Level 2

The transfer of alternating current to the internal charger of the electric vehicle, 208 to 240 Volts, single-phase or three-phase. The maximum current is set at 40 A. At this level, the equipment is divided into inductive and wired, to which reference has been made above. Regardless of the equipment, a separate circuit is required to charge the vehicle. Usually the charge ranges from 15 A, thus providing a maximum charging power of 3.3 kW.

Level 3

The transfer of direct current from an external charger to the electric vehicle. The maximum current intensity is set at 400 A. At this level, also known as Fast Charging, an external charger is used, installed on a three-phase 480 V AC circuit. The purpose of level 3 is to achieve a charge rate of 50% for a charge time of 10 to 15 minutes. Charging power ranges from 60 to 150 kW.

2.7. Charging Points/Stations

2.7.1. Charging Points for Electrical Vehicles

Faced with poor energy fossil fuels and the growing negative impact of climate change on society, many countries have launched national plans to reduce carbon emissions. In particular, the electrification of transport is considered to be one of the main ways to achieve a significant reduction in CO2 emissions. In recent years, electric cars have gained ground, and to this date, more than 180.000 of them have been developed worldwide. Despite this number corresponding to only 0.02% of all road vehicles, an ambitious goal of the countries is to have more than 20 million electric cars on the roads by 2020. In order to ensure the widespread development of electric cars it leads to significant reduction of CO2 emissions, it is important to be charged with energy use from renewable energy sources (e.g., wind, solar). [12].

Basically, in order for a smart network to work, they need to be developed to ensure the smooth integration of these sources into our energy systems. Electric cars could possibly help with energy storage when there is a surplus and supply power back to the grid when there is a demand for it. Indeed, the ability of electric cars to store energy while being used for transportation represents enormous potential for the development of energy systems [13].

On the one hand, since vehicles only drive for a small percentage of the day and a percentage of vehicles remain unused in parking spaces and given the fact that electric vehicles are equipped with large batteries, they could be used as storage devices when parking (process Vehicle-to-Grid (V2G)) and thus increase the energy storage capacity of the network. Indeed, there are studies that have shown that if a quarter of vehicles in the US were electric, this would double the current storage capacity of the network. On the other hand, since a large number of electric cars will need to be charged daily, if electric cars charge when needed, the network load may be overloaded. Grid-to-Vehicle (G2V) - in

real time, la taking into account the limitations of distribution networks within which electric cars must be charged.

In addition, electric car navigation systems must consider the ability of vehicles to recover energy when braking and / or when driving downhill and choosing routes that make full use of this capability. By doing so, it may be possible for vehicles to charge less frequently, thus maximizing energy efficiency, reducing costs for their owners, and minimizing the stresses they cause on power grids. In this context, a number of techniques and mechanisms for the management of electric vehicles, either individually or collectively, have been developed.

For example, some tissue and mobile-based applications have been developed to provide information to electric vehicle drivers about charging sites where charging time slots are available. In addition, original systems have been developed for energy-efficient routing, while new types of chargers that can fully charge an electric vehicle battery in less than an hour. Thus, while a number of developments have taken place in terms of physical infrastructure and technologies for electric vehicles, these may not be sufficient to manage the overcrowding of electric vehicles. Such problems will require algorithms involving a large number of heterogeneous entities (e.g., EV owners, charge point owners, network operators), each with its own goals, needs and motivations (e.g., energy for charging, maximize profit), while operating in highly dynamic environments (e.g., variable number of EVs, variable intent of drivers) and deal with a number of uncertainties (e.g., future arrival of vehicles, future energy demand, energy production from renewable sources) [13].

2.7.2. Charge point Infrastructure

The Charge Point has multiple other functions such as:

- Providing and controlling the energy to the EV using the EVSE component
- Collecting the measurements from the meter for each charge of an Electric Vehicle.
- Identifying and authorizing EV users via user authentication component
- Enabling remote capabilities (e.g., adjustment of the maximum current allowed by the Charge Point) to the Charge Point via the local Controller component over WAN.

Figure 5 illustrates the architecture of the EV Charging Systems that are in scope of this project.

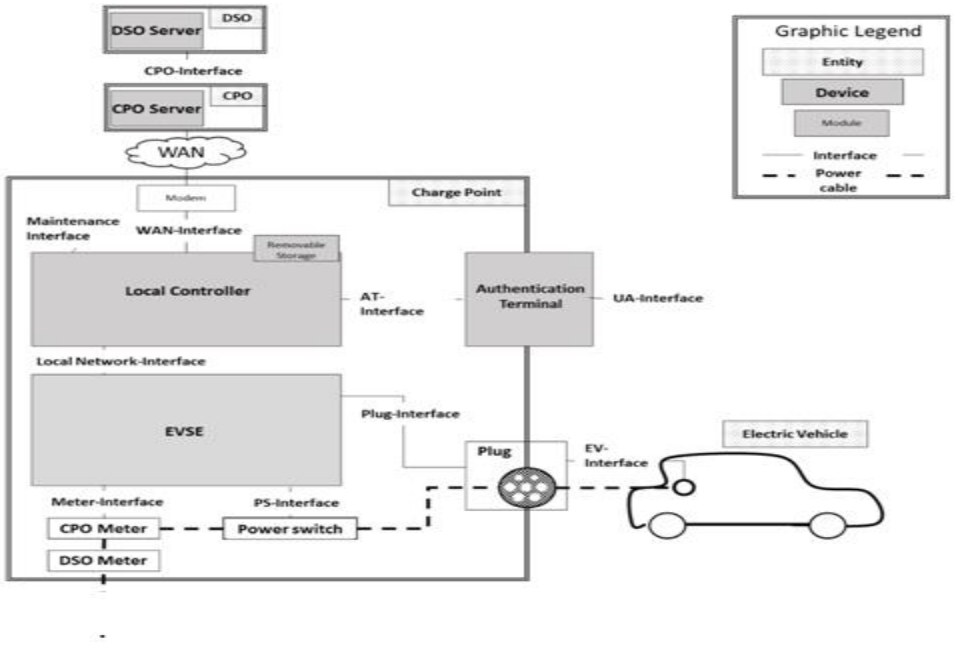


Figure 5- Charge Point System Architecture [14]

The externally reachable interfaces of the Charge Point are:

1. the WAN interface,
2. the Maintenance interface, and
3. the User Authentication (UA) interface

Note in particular that the internal interfaces in the Charge Point are not covered by security requirements. This reflects the current situation in which most of these interfaces use serial protocols with no security features. This exclusion of these interfaces implies that the inside of the Charge Point is a trusted environment: anyone with physical access to the internal systems can compromise the Charge Point. Physical security measures are implemented to prevent unauthorized access to the Charge Point internals.

The Charge Point System Architecture references various items in the Graphic legend:

- An **Entity** represents a main part of the EV charging system.
- A **Device** identifies the component included in the EV charging system. A device is can contain Modules and can have Interfaces to communicate with other devices.
- A **Module** identifies the physical part of the Device where important functionalities are to be found.
- An **Interface** defines the communication link between two Devices

Chapter 3 - Threats and Challenges of Smart Charging

3.1. Vulnerabilities in vehicle communication

Vulnerabilities within vehicular communications lead to four vehicular cyber security challenges, which are described by [15]:

- Limited connectivity: Though the external connectivity of vehicles is increasing, most vehicles do not yet have the capability to update their software through Over-the-Air (OTA) updates, which would enable vehicles to always be protected against the latest cyber-attacks. Even as OTA updates become more standard, vehicles will also be at risk of malfunctions due to incomplete updates.
- Limited computational performance: Vehicular computational performance is generally limited, as compared to the computational performance of a computer. This limitation exists because vehicles have a longer lifetime and must endure higher temperatures and vibrations than the average PC or laptop. As a result of their computational disadvantage, vehicles are more likely to be hacked than computers. The limited computational performance of vehicles will also mean that some vehicular cyber security solutions will have too high an overhead to be implemented.
- Unpredictable attack scenarios and threats: A vehicular architecture can be infiltrated through many different entry-points, including vehicular databases, remote communication technologies, and vehicular parts. New attacks are continually being developed, which means that automakers will find it difficult to predict where hackers will strike next. An unsecured product manufactured by Original Equipment Manufacturers (OEMs) can provide hackers with additional entry-points into a vehicle.
- Critical risk for driver's or passenger's lives: Even if just a few sensors are misinformed or only a small number of illegitimate messages are sent, a vehicle could

experience malfunctions that place the lives of drivers, passengers, and pedestrians at risk.

3.2. Threats and Attacks in Charging of electric Vehicles

Many attacks on electric vehicle charging within a smart grid environment have been identified [18] and find that EV charging is susceptible to masquerading, tampering, eavesdropping, and denial of service attacks, in addition to privacy concerns and charging thievery. Fries and Falk [19] discuss EV charging susceptibility to eavesdropping, man-in-the-middle and tampering attacks on the payment price and the amount of energy that the meter believes the EV has received. They also discuss the potential for malicious software within the vehicle to affect a charging station, or a compromised charging station to affect an EV.

Threats targeting vehicular communications can be understood through the three layer Autonomous Vehicular Sensing Communication Control (AutoVSCC) framework. Smart Charging may put into risk the reliability and security of the power network, as neither the charging stations have deployed security mechanisms for identifying and preventing security threats and attacks, nor the Distribution System Operator's (DSO) have implemented security mechanisms for mitigating potential disturbance of the network due to a break-down (or a hack) of the smart charging stations [18]. Smart charging is complex system which requires the orchestration of a number of services such as metering and payment for energy, communication between the EV battery management system and the charge point, followed by a communication mechanism between the CP and a central management system, and finally the establishment of a communication channel between the CS and energy suppliers (DSO, Transmission System Operators (TSO), smart girds, etc.). Having in mind that the services are offered from different entities, this complex

communication schemes creates an environment susceptible to a number of security threats on different levels [17].

The co-existence of an electrical system monitored and controlled from an ICT infrastructure is an open challenge due to the heterogeneity of the cyber-physical systems that are get engaged that require the standardization of protocols and the implementation of two primary interfaces, one for electricity and another for the management of the system. In the case of the smart charging scenario, the ICT system is related to the status, authorization, metering, and billing of the EV that interact with the system [20].

A higher level depiction of the entities that are getting engaged in the smart-charging use case are depicted in Figure 6. The DSO is responsible for the distribution of the electric power and ensures the functionality of the electricity network, the CPO takes care of the customer-end services (authentication, billing, etc.) alongside with the management of the charging points, the Electro Mobility Service Providers (eMSP) is responsible for setting the billing mechanism, the CP acts as the open gate to the system, and eventually the EV which is the end-user to the infrastructure. The roles/entities of the smart-charge use case that are described briefly above are presented in the form of a table (Table 2), provide a more detailed description about their functionalities.

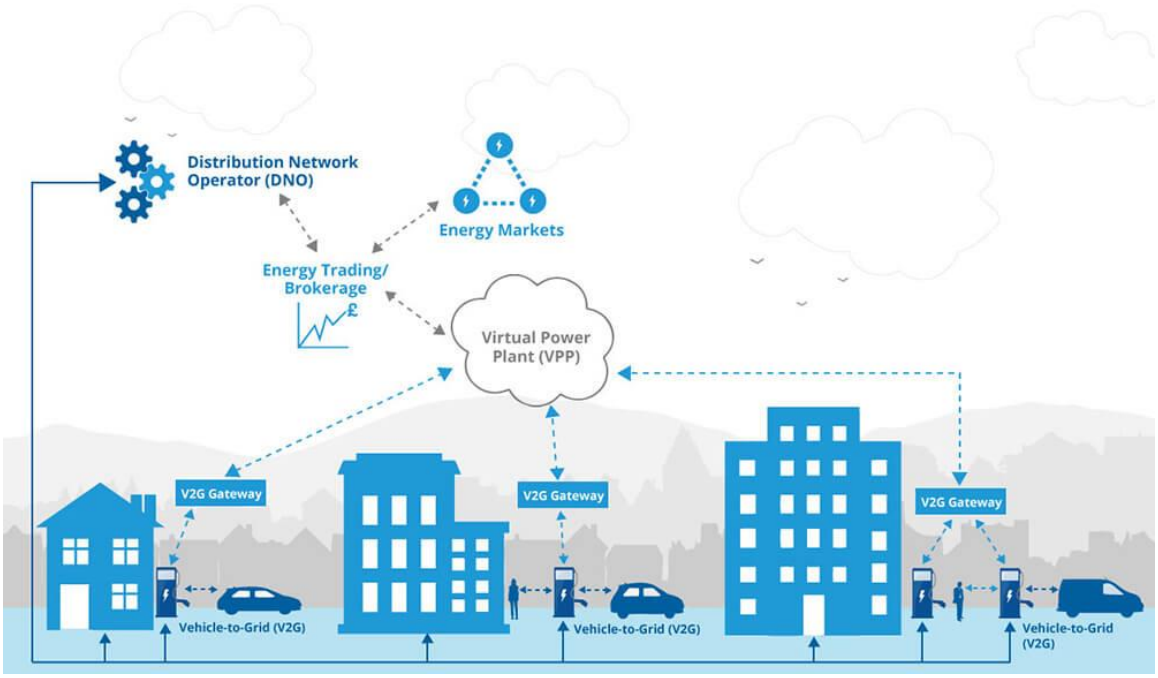


Figure 6- A high level depiction of the entities getting engaged in the smart charge scenario [21]

Table 2- A high level depiction of the entities getting engaged in the smart charge scenario

Entity	Description
Distribution System Operator - DSO	The distribution system operator (DSO) manages electrical grid. The DSO does not produce electric power but does however ensure that it is transported from the power station to the place where it is needed. The most important task of the DSO is to maintain a stable, reliable and well-functioning electricity network.
Electro Mobility Service Providers - eMSP	An eMSP is a market role that offers charging services to EV drivers. An eMSP provides value by enabling access to a variety of charge points around a geographic area, usually in the form of a charge card. This means the EMSP is responsible to set up contracts with customers (owners of EV cars) and for managing customer information and billing.
Charge Point Operator - CPO	The CPO is responsible for the management, maintenance and operation of the charging stations (both technical and administrative). The role of CPO can be segmented into: 1. Responsibility for administrative operation (e.g., access, roaming, billing to eMSP etc.) and 2. Responsibility for technical maintenance, which is often done by the manufacturer. CPOs play a very important role in the EV market as they are responsible for bridging the gap between the enti-

	ties managing and maintaining the physical electrical network – the DSOs – and all other entities: the energy providers, the customers and the eMSPs.
Charging Point – CP	Charge Points are devices where EVs get charged. Each CP contains at least one meter per socket (Measuring Instruments Directive meter (MID meter)) owned and controlled by the CPO. This CPO meter is connected to the energy socket through which the EV gets charged and is used to measure the energy consumed by the EV. Each CS also includes a Local Controller (LC) with a connection (e.g.: General Packet Radio Services (GPRS) or wire connection) to the back-office of the CPO. Among other things (e.g.: remote updates), such connection is used to authenticate the customer (EV owner) at the CPO.
Electric Vehicle - EV	Gets charged through a CP. In many cases a vehicle will charge to its maximum capacity, but the vehicle can always determine its own charging profile within the range available

3.3. Protocols that participate on smart charging

3.3.1. IEC 61851-1

Different charging topologies need to be considered for conductive AC- and DC-based dedicated charging equipment. Such EV charging equipment is defined in the IEC 61851 standards series (Figure 7). The first part describes general requirements for conductive charging systems. It applies to on-board and off-board AC and DC charging equipment and also to any additional services on the vehicle which may require electrical power when connected to the supply network. It defines four different charging modes starting from slow charging using household-type socket outlets to fast charging using an external charger. It also defines characteristics and operating conditions of the supply device and the connection to the vehicle as well as the operator's and third parties electrical safety [23].

IEC 61851-1 specifically defines a safety-related low level signaling process based on a Pulse Width Modulation (PWM) signal indicating various EV connection states, supported charge currents and communication means. The PWM signal provides means for handling time critical state changes, some of them even with respect to individual safety. Hence, IEC 61851-1 is a cross-cutting standard in terms of the previously mentioned domains, dealing with charging topologies, safety and communication (on a signaling level).

3.3.2. IEC 61140 - Safety

In terms of safety requirements for EV charging infrastructures, IEC 61140 defines common aspects for the installation and equipment of electrical assemblies in order to ensure protection of persons and animals against electric shocks (Figure 7). It is intended to provide the fundamental principles and requirements which are common to electrical installations, systems and equipment or necessary for their co-ordination. Closely related to IEC 61140, IEC 60529 defines the degrees of protection which must be provided by enclosures of electric equipment. Extending the scope of these rather general safety standards, IEC 60364-7-722 particularly defines safety requirements for supply equipment of EVs in own voltage electrical installations. It furthermore also covers safety requirement for reverse energy flow from the EV back to public grid infrastructures. The work on this part of the standard is still in progress [24].

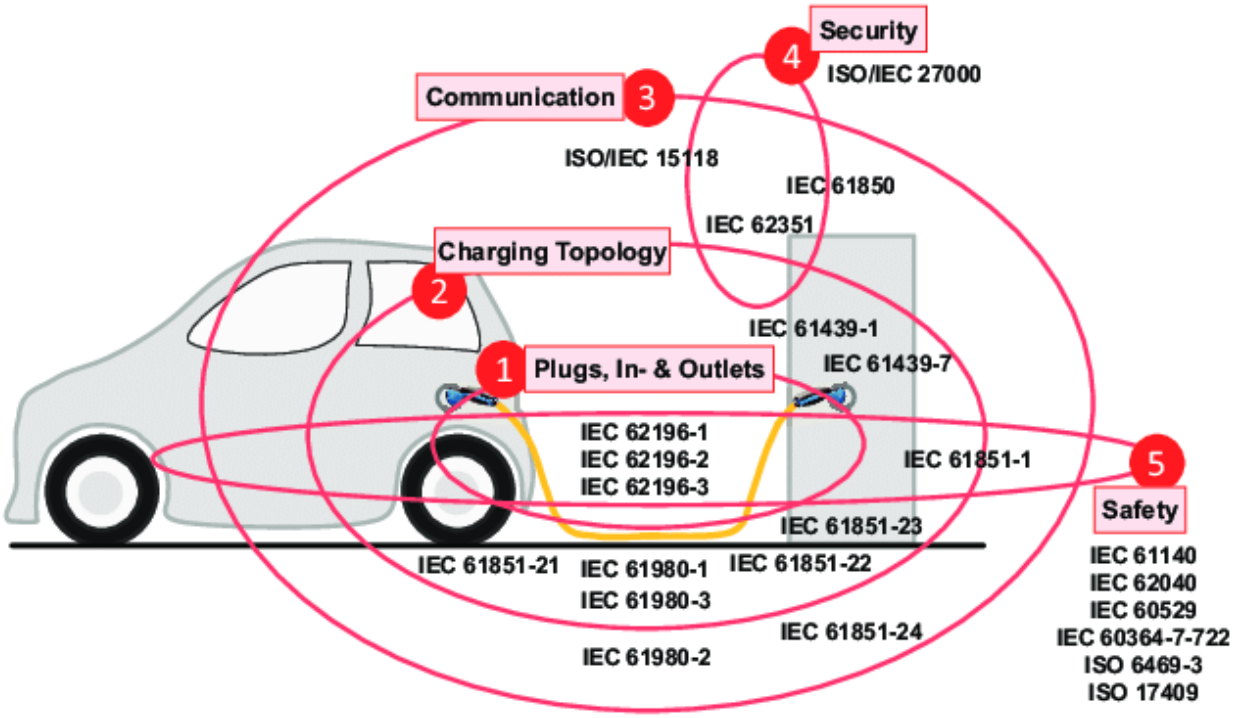


Figure 7- Protocols that participate on smart charging of an Electrical Vehicle [23]

Smart Charging Abuse

A cloud-based back office of a Charge Point Operator (CPO) communicates with a charge point via the Open Charge Point Protocol (OCPP). This standard is supported by more than 97% of the connected charging stations worldwide. The charge capacity of a charging station can be set from the cloud by means of OCPP requests. Version 1.6 and 2.0 of this protocol support smart charging. This means that one platform can connect to a wide range of charging stations and still be able to provide smart charging services to all of them.

The charging station then in turn communicates with the charging station via the IEC 61851 protocol (for high speed DC charging other standards are used, but these are usually not used for smart charging).

There are a few important observations to be made here:

- Via OCPP, the maximum charge rate for a charge point/socket can be set for a specific period.
- The charge point imposes this maximum on the EV.
- The EV can choose its own charge rate, as long as it is below the maximum.

It is therefore *not possible* to set a specific charge rate for an electric vehicle, only the maximum charge rate can be set.

There are currently around 20.000 charging stations connected to a standard EV charging enterprise. On average, a charging station can charge at around 11 kW. This means that someone with access has control over charging stations with a combined capacity of around 220 MW, equal to the power output of a medium-sized power plant. It is expected that around 200,000 charging stations will be connected in 5 years, which corresponds to a potential capacity of around 2 GW. Simultaneous switching on or off of all these charging stations can lead to a pan-European blackout.

The protection of the European electric grid should become a priority for all the organization/entities that are getting engaged in the EV ecosystem. The output of this scenario is aiming at increasing the cyber-security of a standard EV charging enterprise's platform through the integration of ML techniques for identifying anomalies in the charging patterns, and therefore minimize the exposure both enterprises' database and the stability of the electric grid. The scenario covers both the ICT and the electric engineering domain on an effort towards increasing the cyber security on what is called Energy Internet [22].

Chapter 4 - Smart Charging Scenario: Algorithms

4.1. Algorithms

4.1.1. Isolation Forest

Isolation Forest utilizes the concept of isolation to detect anomalies in the dataset. It takes advantage of two quantitative properties that anomalies have:

- Anomalies are the minority, consisting of fewer instances, and
- They have feature values which are very different from those of normal instances.

These two characteristics make anomalies susceptible to isolation, meaning that they are more likely to be isolated from other instances when the dataset is randomly partitioned. This algorithm works by recursively randomly partitioning the dataset until it reaches a particular depth or isolates a point. To represent the partitions, it uses a special kind of Binary Search Tree (BST), called iTree.

The idea is that anomalies, since they lay further from the rest observations, will require a lower number of random dataset partitions to become isolated, whereas normal observations will need a higher number, as they are close to other normal points. This translates to respectively shorter and longer path lengths (or distances from the root node) in each iTree. The anomaly score that is inferred for an example during the evaluation stage is based on this path length value. For example, in Figure 8, we can see that point xo requires on average fewer “cuts” to be isolated, than point xi . The model of Isolation Forest is composed of an ensemble of iTrees. Each iTree is built on a subsample of the original dataset. The use of subsamples has some very useful properties. Each subsample is formed by randomly picking instances from the whole dataset without replacement.

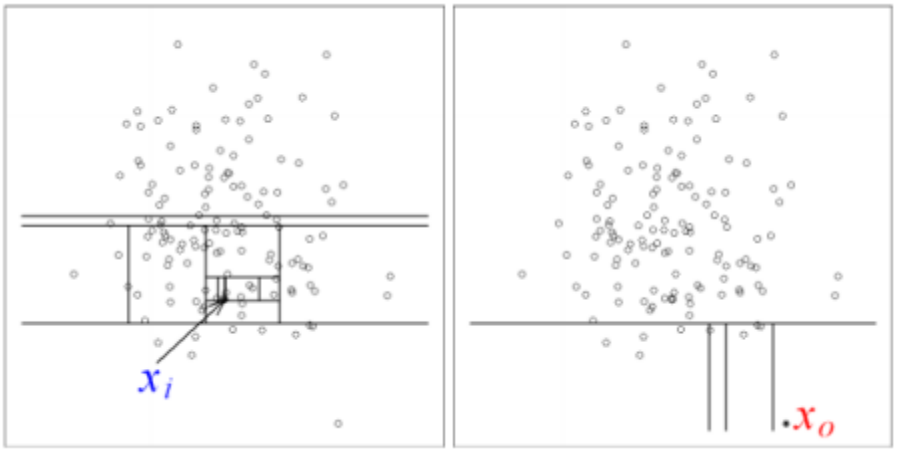


Figure 8- Isolation Forest anomaly score

The anomaly score for a data point is the average value of the path lengths acquired by "passing" the data point from each iTree this approach often causes a high computational complexity for data of higher dimensionality, and, because the model is optimized to profile normal points, and not to detect anomalies, it often ends up with too many false positives, or few true positives (not to mention that most of the times a labeled dataset is mandatory for the training phase). Isolation Forest is different from such algorithms because its model isolates anomalous instances instead of profiling the normal ones, requires no labeled dataset (it is an unsupervised algorithm) and is also robust when applied at data with high dimensionality.

Moreover, most distance-based and density-based methods do not handle the effects of swamping and masking well, having poor performance in such cases. Swamping is the when normal instances are too close to anomalies, causing them to get incorrectly flagged, and masking is the situation in which too many similar anomalies form a small cluster, concealing their presence. Isolation Forest alleviates the effects of these two situations by operating on random subsamples of the original dataset.

4.1.2. Anomaly Detection

Anomaly detection refers to the problem of finding patterns in a set of data that do not agree with the expected behavior. Extreme pricing detection has a variety of applications such as credit card fraud detection, security fraud detection, security and medical care systems, and even military systems for detecting hostile activities. The importance of extreme price detection stems from the fact that extreme data values translate into important information in a wide range of application areas.

The first attempts to detect extreme values date back to 1970, when researchers tried to elicit erroneous measurements from their data to ensure that the data matched best with the proposed models [23]. Detection of anomalies or extreme prices has been researched in the field of statistics since the beginning of the 19th century. Over the years, a wide variety of techniques have been developed in various fields of research. Many of them have been created for more specific applications while others are more general. There are also cases where, although a technique has been developed for a specific problem, it is then applied to areas that were not originally intended.

Types of extreme anomalies

Point anomalies

We encounter these extreme values if an object in the data (a point) shows a different behavior from the rest of the data. Although it is the most easily detectable type of extreme value, an important problem is the appropriate measure of the deviation of one point from the rest. In Figure 9, we see an example of extreme point values, where it is clear that the two points that are in a circle and have been named V1 are much further away from the set of points V2 and are characterized as extreme values [24]. As an example from real life let's talk about credit cards. We assume that all the data refers to the transactions of an individual and more specifically to the amounts spent per transaction.

A transaction in which the amount allocated is much larger than the average normal spent by that particular individual is characterized as a point extreme value.

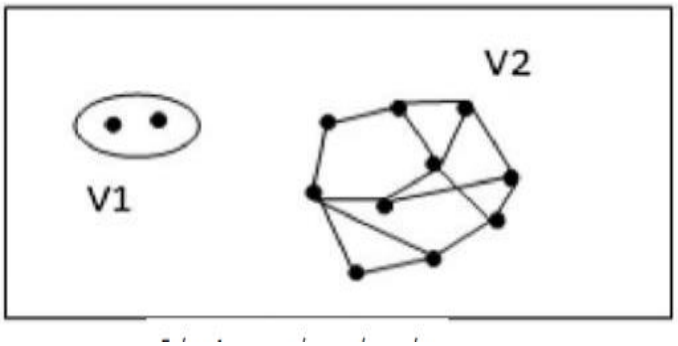


Figure 9- Extreme point values (anomalies) [25]

Environmental values related to contextual anomalies

This type, we find it if one point of the data deviates significantly from the rest in a particular environment, and only in that. The concept of environment arises from the structure of data and is part of the wording of the problem. Each fact is defined on the basis of two characteristics.

A) The environmental characteristics, e.g., those that determine the environment and

B) The behavioral characteristics, e.g., those that determine the points that are outside the specific environment. [26]

Collective extreme anomalies: This type of extreme value refers to a set of data, which as a group, show a different behavior from the general set of data, while as independent units may not be extreme values. In Figure 10, we see an example of a collective extreme value. In the cardiogram, while the values that are in red alone are not an extreme value, as a set of values they differ from the usual and are characterized as abnormal. [26]

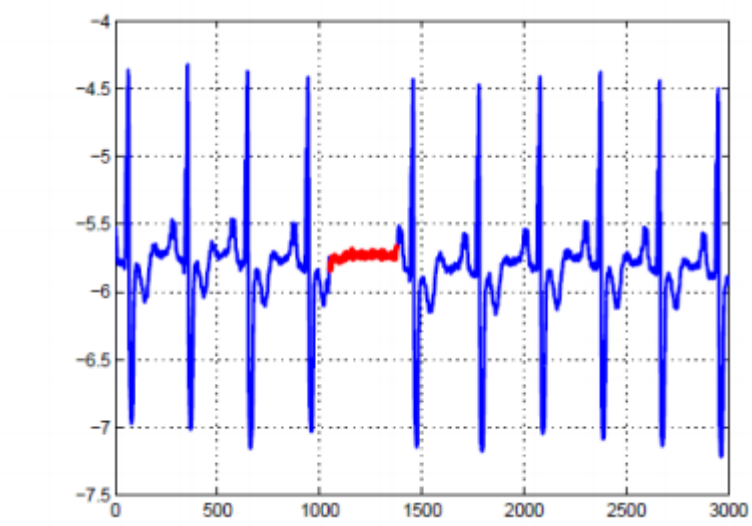


Figure 10- Collective anomaly corresponding to an Atrial [27]

4.2. Ways to operate extreme price detection techniques

Supervised problems

Supervised problems are those that the computer does not solve on its own. That is, the computer is given a set of data, and there is the human factor, which tells the computer how to sort this data. The behavior of the data, whether normal or not, should be predetermined. This can be done in two ways, either by saying what is normal and anything that does not go with it is considered an extreme value, or by determining what is

abnormal and anything that is contrary to it is considered normal. This technique requires the human factor to know all possible extreme values or that it can be considered normal in the data, something that is not so feasible since the goal is for the computer to be able to detect extreme values on its own. Theoretically, this type of methodology provides a better detection of extreme values as there is access to more information, but keeping accurate data labels is a major challenge that rejects this theory. [28]

Unsupervised

In unattended techniques, there is no pre-classification by the human factor, and the computer must detect for itself that there are extreme values, if of course they exist. In these methods, it is assumed that data that behaves normally often follow a pattern, while extreme values do not behave in this way. However, this assumption is not always correct as there are cases where the similarity is not enough to determine the regularity or not of some data as in the case of collectively extreme values. That is why this technique is often ineffective and leads to wrong extreme values.

Semi-supervised

This kind of approach is something between the two previous ones. It is used when from all the data, there are a few that have been pre-characterized as normal. Based on this, we try to characterize what is left. This approach essentially sets a limit to normalcy, where a given value is called an extreme value if it is outside it and normal if it is within it.

Chapter 5 - Methodology - Data Analysis

This chapter presents the methodology process that will be applied in dataset that contain real recorded charging processes, which took place during 2018 and 2019. Main concept of the implementation is to examine possible threats and cyber-attacks on smart charging network that used by charging point stations, where electrical vehicles are connected in other to be charged.

5.1. Research Questions

As mentioned before, in charging process, an attacker could exploit vulnerabilities of the network of a charging station and affect the behavior of the charging process in plug-in electrical vehicles that are connected. Therefore, the main object of thesis is to examine threats and detect cyber-attacks in the charging process. In this scenario, a Plug-in Electric Plug-in Electric Vehicle communicates with and is controlled by a charging station. Consequently, the specific research questions arise:

a) Whether the charging station hardware can be hacked in order to send these erroneous signals (either locally or remotely)
b) How the charging stations can be made tamper-proof and how cyber-attacks can be detected

In order to answer the above research questions, it is necessary to run specific anomaly detection test, using isolation forest algorithm and other data manipulation. Consequently, if a charging process behaves abnormally, in other words, if a connected Electrical Vehicle requests high voltage, could. Therefore, it is crucial for the charging station owner to monitor, manage, and restrict the use of their devices remotely to optimize energy consumption. Otherwise, the smart network of the charging station might break down.

5.2. Data for the scenario

In the context of this thesis, we used a dataset in CSV format. This dataset contains Charge Detail Records with the following columns (Table 3). For better view and accuracy in the anomalies that will show in the results, the EV charging dataset will be comprised of millions of charge sessions hosted on a cloud platform dating back to 2012. The database consists of different tables, each one of them representing a unique entity in the EV scenario, namely: the Charge Points, the Charge Detail Records (CDRs), the Connections and the Meter Values (MVs).

Table 3 - Charge Detail Records (CDRs),

Column	Data type	Description
ID	PK, int	ID for CDR
Duration	Nvarchar (50)	Duration of session
Volume	Nvarchar (50)	Volume in kWh
AuthenticationId	Nvarchar (50)	Unique charge card ID
ChargePoint_ID	FK, int	Unique Charge Point ID
ConnectorId	Nvarchar(255)	ChargePoint Connector Identifier
dStart	datetime	Session start time
dEnd	datetime	Session end time

Table “Charge Detail Records (CDRs)” (Table 3) ,describes the necessary details of each charging attempt such as the duration and the volume, but it also includes features from other tables as foreign key in order to express the correlation with the other entities of the grid. Therefore, every record to the database includes the unique ID of the charge card used by the EV driver, and the unique ID of the charging station. The features of duration, volume and session start/end time have the highest value for the Artificial Intelligence (AI) algorithms, as they can offer a useful insight for the pattern of a charging session.

Artificial Intelligence and Machine Learning are nowadays two very interchangeable words. They are not quite the same thing, but the perception that they are can sometimes lead to some confusion.

- Artificial Intelligence is the broader concept of machines being able to carry out tasks in a way that we would consider “smart”.
- Machine Learning is a current application of AI based around the idea that we should really just be able to give machines access to data and let them learn for themselves.

Our purpose in this implementation is to run some algorithms, in order to see if smart charging system can secure the enterprise’s grid, and to prevent potential blackouts in the EU’s electrical grid. In the scenario of the smart charging abuse, different users are synchronized (either on purpose either unintentionally) and proceed timely in connection/disconnection actions, causing an unexpected load to the electrical grid. Such actions can be prevented if AI/ML techniques are integrated into the EV charging enterprise’s software.

The dataset in CSV format, which has been collected from an EV charging enterprise since 2012, can be used as a starting point for getting an insight of the charging stations’ behaviour, extracting the attributes of a “normal” charging action and identifying suspicious actions as outliers.

An outlier is an observation that lies an abnormal distance from other values in a random sample from a population. In a sense, this definition leaves it up to the analyst (or a consensus process) to decide what will be considered abnormal. Before abnormal observations can be singled out, it is necessary to characterize normal observations. In very large samplings of data, some data points will be further away from the sample mean than what is deemed reasonable. This can be due to incidental systematic error or flaws in the theory that generated an assumed family of probability distributions, or it may be that some observations are far from the center of the data. Outlier points can therefore indicate faulty data, erroneous procedures, or areas where a certain theory might not be valid. However, in large samples, a small number of outliers is to be expected (and not due to any anomalous condition). Outliers should be investigated carefully. Often they contain valuable information about the process under investigation or the data gathering and recording process.

5.3. Finding abnormal charging processes

Isolation Forest

Returns the anomaly score of each sample using the Isolation Forest algorithm

The Isolation Forest 'isolates' observations by randomly selecting a feature and then randomly selecting a split value between the maximum and minimum values of the selected feature Since recursive partitioning can be represented by a tree structure, the number of splitting required to isolate a sample is equivalent to the path length from the root node to the terminating node This path length, averaged over a forest of such random trees, is a measure of normality and our decision function.

In order to discover abnormal charging processes, isolation Forest algorithm will be applied on dataset (described previously). Isolation forest gives us the opportunity to detect possibly abnormal requests of high voltage power for a plugged-in Electrical Vehicle.

Using isolation forest algorithm, we can group charging processes into two main categories:

a) Charging processes that behave normally (expected behaviour)

b) Charging processes that shows unusual behaviour and should be investigated further. For example, we can detect a charging process, where an Electrical Vehicle EV requests a greater amount of power, or a specific car(s) is/are charged on a different station(s) from the usual ones.

Therefore, in this implementation, we have to discover possible "Anomalies". Anomalies are data patterns that have different data characteristics from normal instances. The detection of anomalies has significant relevance and often provides critical actionable information in various application domains. For example, anomalies in credit card trans-

actions could signify fraudulent use of credit cards. An anomalous spot in an astronomy image could indicate the discovery of a new star. An unusual computer network traffic pattern could stand for an unauthorized access. These applications demand anomaly detection algorithms with high detection performance and fast execution.

StandardScaler

Alongside with the isolation Forest algorithm we will also apply on the dataset the Standard Scaler algorithm.

Standard Scaler standardizes features by removing the mean and scaling to unit variance.

The standard score of a sample x is calculated as: z = (x - u) / s, where u is the mean of the training samples or zero if with_mean=False, and s is the standard deviation of the training samples or one if with_std=False.

Centering and scaling happen independently on each feature by computing the relevant statistics on the samples in the training set. Mean and standard deviation are then stored to be used on later data using transform.

Standardization of a dataset is a common requirement for many machine learning estimators: they might behave badly if the individual features do not more or less look like standard normally distributed data (e.g., Gaussian with 0 mean and unit variance). In practice we often ignore the shape of the distribution and just transform the data to center it by removing the mean value of each feature, then scale it by dividing non-constant features by their standard deviation.

Chapter 6 - Results of Implementation

6.1. Tools and Programs Used

In order to run tests in the records of the EV charging enterprise's database 2018, we used Python language, which is a very powerful tool in data analysis, Anaconda environment, where we ran the code and Jupyter Notebook (Figure 11).

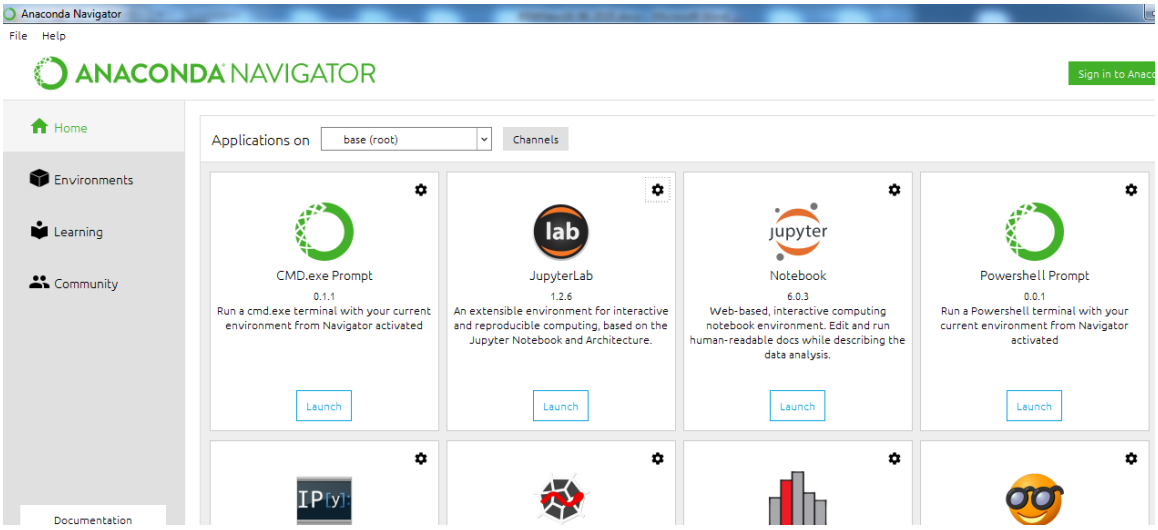


Figure 11- Anaconda program

6.1.1. Anaconda

Anaconda Enterprise enables developers and data scientists to access cutting-edge technology and use their preferred tools and packages without sacrificing security. Anaconda is a Python distribution. A Python distribution provides the Python interpreter, together with a set of Python packages and sometimes other related tools, such as editors. The main advantages of Anaconda distribution includes:

• NumPy, SciPy, Matplotlib and Biopython

• Spyder

• Jupyter Notebook

6.1.2. Jupyter

The Jupyter Notebook is an interactive programming environment, in which you can combine Python code and execution results with annotations, equations, figures, inks, etc. The Jupyter Notebook will run in the internet browser of our computer and does not require internet access, it will access to our local files via the browser interface. Notebooks are similar to Word documents and we can edit them interactively in the internet browser. Notebooks are saved in its own format with the '.ipynb' extension, but can be also downloaded as PDFs, HTML pages or Python code.

6.1.3. Necessary Python libraries

For scientific computing and computational modeling, we need additional collections of Python modules called libraries or packages. They are not part of the Python standard distribution. These allow us, for example, to create plots, operate on matrices, and use advanced numerical methods:

- **NumPy** (NUMeric Python): matrices and linear algebra
- **SciPy** (SCIentific Python): many numerical routines
- **Matplotlib** (PLOTting Library): creating plots of data

- **Pandas**: Pandas is built on top of the NumPy package, meaning a lot of the structure of NumPy is used or replicated in Pandas. Data in pandas is often used to feed statistical analysis in SciPy, plotting functions from Matplotlib, and machine earning algorithms in Scikit-learn.

6.2. Code implementation

Isolation.py contains the necessary code, in order to run isolation method and find possible anomalies for the charging processes that have been recorded in the dataset of the EV charging enterprise. Anomalies are data patterns that have different data characteristics from normal instances. The detection of anomalies has significant relevance and often provides critical actionable information in various application domains. For example, anomalies in credit card transactions could signify fraudulent use of credit cards. An anomalous spot in an astronomy image could indicate the discovery of a new star. An unusual computer network traffic pattern could stand for an unauthorized access. These applications demand anomaly detection algorithms with high detection performance and fast execution.

The Isolation Forest ‘isolates’ observations by randomly selecting a feature and then randomly selecting a split value between the maximum and minimum values of the selected feature. Since recursive partitioning can be represented by a tree structure, the number of splitting required to isolate a sample is equivalent to the path length from the root node to the terminating node. This path length, averaged over a forest of such random trees, is a measure of normality and our decision function.

In this implementation, we use Isolation method to isolate normal and abnormal charging processes. For this purpose, we selected “Duration” as the characteristic in order to test if there is unusual time for the EV to be charged. Time was converted into seconds in order to compare and isolate the results.

Explanation of code

Implemented code is presented above. First of all, it is necessary to ink our project with the appropriate libraries:

```
import numpy as np # linear algebra


import pandas as pd # data processing, CSV file I/O (e.g., pd.read_csv)
```

Next, we define a function named “convert”. This function was used in order to convert time format into seconds. In csv dataset duration a charging process is formatted like “10:08:00”. Consequently, this function take as parameter time duration and returns in main program, total seconds.

```
def time_convert(x):
    h,m,s = map(int,x.split(':'))
    return (h*60+m)*60+s
```

In main program, first of all we read CSV file. The necessary code is:

```
df=pd.read_csv("cdr2020h.csv")
df.head()
```

Next, we define the columns that we want to plot in diagrams. More specifically, we selected:

- ID (id of charging process)
- VOLUME (Voltage power for EV)
- Duration (Duration of time that recorded in the specific charging process)

The data above is for a use case at a charging process that was recorded in the EV charging enterprise's database. We have to identify first, if there is an anomaly at a use case level. Then for better action ability we drill down to individual metrics and identify anomalies in them.

Creation of Pivot on the data frame, in order to create a data frame with all metrics at a **date level.**

```
metrics_df=pd.pivot_table(df,values='Volume',index='ID',columns='Duration')
metrics_df.head()
metrics_df.reset_index(inplace=True)
```

Level the multi-index pivot data frame and treat na with 0:

```
metrics_df.fillna(0,inplace=True)
metrics_df.head()
metrics_df.columns
```

Define isolation forest and specify parameters.

Algorithm parameters used in code:

1. **n_estimatorsint**, default=100
   The number of base estimators in the ensemble.

2. **max_samples**"auto", int or float, default="auto"
   The number of samples to draw from X to train each base estimator.
   - If int, then draw max_samples samples.
   - If float, then draw max_samples * X.shape[0] samples.
   - If "auto", then max_samples=min(256, n_samples).

   If max_samples is larger than the number of samples provided, all samples will be used for all trees (no sampling).

3. **max_features** int or float, default=1.0
   The number of features to draw from X to train each base estimator.
   - If int, then draw max_features features.
   - If float, then draw max_features * X.shape[1] features.

4. **bootstrap** bool, default=False
   If True, individual trees are fit on random subsets of the training data sampled with replacement. If False, sampling without replacement is performed.

5. **n_jobsint**, default=None
   The number of jobs to run in parallel for both fit and predict. None means 1 unless in a joblib.parallel_backend context. -1 means using all processors.
   See Glossary for more details.

6. **random_state** int or RandomState, default=None
   Controls the pseudo-randomness of the selection of the feature and split values for each branching step and each tree in the forest.

   Pass an int for reproducible results across multiple function calls. See Glossary.

7. **verboseint**, default=0
   Controls the verbosity of the tree building process.

Isolation forest tries to separate each point in the data. In case of 2D it randomly creates a line and tries to single out a point. Here an anomalous point could be separated in few steps while normal points which are closer could take significantly more steps to be segregated. Using sklearn's Isolation Forest here as it is a small dataset with few months of data, while recently h2o's isolation forest is also available which is more scalable on high volume datasets would be worth exploring.

Next, as long as we have imported isolation forest library, we gave the appropriate parameters for built-in function Isolation Forest:

```
clf=IsolationForest(n_estimators=100, max_samples='auto', \
max_features=1.0, bootstrap=False, n_jobs=-1, random_state=42, verbose=0)
```

A sudden spike or dip in a metric is an anomalous behavior and both the cases needs attention. Detection of anomaly can be solved by supervised earning algorithms if we have information on anomalous behavior before modeling, but initially without feedback it's difficult to identify those points. So we model this as an unsupervised problem using algorithms like Isolation Forest, One class SVM and STM. Here we are identifying anomalies using isolation forest.

Now here we have metrics on which we have classified anomalies based on isolation forest algorithm. We will try to visualize the results and check if the classification makes sense. Next, we normalize and fit the metrics to a PCA to reduce the number of dimensions and then plot them in 3D highlighting the anomalies.

```
import matplotlib.pyplot as plt
from sklearn.decomposition import PCA
```

```
    from sklearn.preprocessing import StandardScaler
    from mpl_toolkits.mplot3d import Axes3D
    pca = PCA(n_components=3)  # Reduce to k=3 dimensions
    scaler = StandardScaler()
    #normalize the metrics
    X = scaler.fit_transform(metrics_df[to_model_columns])
    X_reduce = pca.fit_transform(X)

    fig = plt.figure()
    ax = fig.add_subplot(111, projection='3d')
    ax.set_zlabel("x_composite_3")

    # Plot the compressed data points
    ax.scatter(X_reduce[:, 0], X_reduce[:, 1], zs=X_reduce[:, 2], s=4, w=1,
abel="inliers",c="green")

    # Plot x's for the ground truth outliers
    ax.scatter(X_reduce[outlier_index,0],X_reduce[outlier_index,1],
X_reduce[outlier_index,2],
               w=2, s=60, marker="x", c="red", abel="outliers")
    ax.legend(
```

Now as we see at the 3D point the anomaly points are mostly wider from the cluster of normal points, but the 2D point will help us to judge even better. Let's try plotting the same fed to a PCA reduced to 2 dimensions.

```
from sklearn.decomposition import PCA
pca = PCA(2)
pca.fit(metrics_df[to_model_columns])
res=pd.DataFrame(pca.transform(metrics_df[to_model_columns]))
Z = np.array(res)
figsize=(12, 7)
plt.figure(figsize=figsize)
plt.title("IsolationForest")
plt.contourf( Z, cmap=plt.cm.Blues_r)
b1 = plt.scatter(res[0], res[1], c='blue',
                 s=40,label="normal points")

b1 = plt.scatter(res.iloc[outlier_index,0],res.iloc[outlier_index,1], c='red',
                 s=40,  edgecolor="red",label="predicted outliers")
plt.legend(loc="upper right")
plt.show()
```

```
# Input data files are available in the "../input/" directory.
# For example, running this (by clicking run or pressing Shift+Enter) will list the files in the
import warnings
warnings.filterwarnings('ignore')
import os


def time_convert(x):
    h,m,s = map(int,x.split(':'))
    return (h*60+m)*60+s

df=pd.read_csv("cdr2018.csv")
df.head()

metrics_df=pd.pivot_table(df,values='Volume',index='ID',columns='Duration')
metrics_df.head()

metrics_df.reset_index(inplace=True)
metrics_df.fillna(0,inplace=True)
metrics_df.head()

metrics_df.columns

to_model_columns=metrics_df.columns[1:20]

from sklearn.ensemble import IsolationForest
clf=IsolationForest(n_estimators=100, max_samples='auto', \
                        max_features=1.0, bootstrap=False, n_jobs=-1, random_state=42, verbose=0)
clf.fit(metrics_df[to_model_columns])
pred = clf.predict(metrics_df[to_model_columns])
metrics_df['anomaly']=pred
outliers=metrics_df.loc[metrics_df['anomaly']==-1]
outlier_index=list(outliers.index)
#print(outlier_index)
```

```
#Find the number of anomalies and normal points here points classified -1 are anomalous
print(metrics_df['anomaly'].value_counts())
import matplotlib.pyplot as plt
from sklearn.decomposition import PCA
from sklearn.preprocessing import StandardScaler
from mpl_toolkits.mplot3d import Axes3D
pca = PCA(n_components=3)  # Reduce to k=3 dimensions
```

```
scaler = StandardScaler()
#normalize the metrics
X = scaler.fit_transform(metrics_df[to_model_columns])
X_reduce = pca.fit_transform(X)

fig = plt.figure()
ax = fig.add_subplot(111, projection='3d')
ax.set_zlabel("x_composite_3")

# Plot the compressed data points
ax.scatter(X_reduce[:, 0], X_reduce[:, 1], zs=X_reduce[:, 2], s=4, lw=1, label="inliers",c="green")

# Plot x's for the ground truth outliers
ax.scatter(X_reduce[outlier_index,0],X_reduce[outlier_index,1], X_reduce[outlier_index,2],
           lw=2, s=60, marker="x", c="red", label="outliers")
ax.legend()
plt.show()

from sklearn.decomposition import PCA
pca = PCA(2)
pca.fit(metrics_df[to_model_columns])
res=pd.DataFrame(pca.transform(metrics_df[to_model_columns]))
Z = np.array(res)
figsize=(12, 7)
plt.figure(figsize=figsize)
plt.title("IsolationForest")
plt.contourf( Z, cmap=plt.cm.Blues_r)
b1 = plt.scatter(res[0], res[1], c='blue',
                 s=40,label="normal points")

b1 = plt.scatter(res.iloc[outlier_index,0],res.iloc[outlier_index,1], c='red',
                 s=40,  edgecolor="red",label="predicted outliers")
plt.legend(loc="upper right")
plt.show()
```

6.3. Evaluation

6.3.1. Dataset of 2018

Running the python code on the dataset of the charging records of 2018, we take the following result and plots (Figure 12 and Figure 13):

```
 1    1997
-1       2
Name: anomaly, dtype: int64
```

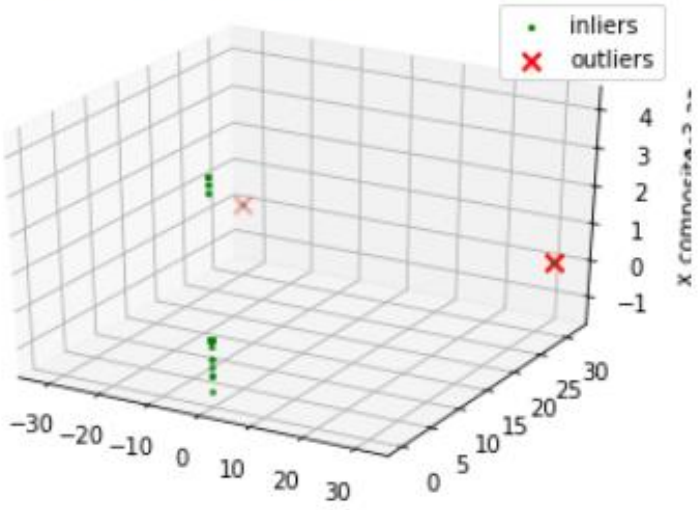


Figure 12- Isolation Forest Dataset 2018 results in three dimensional view showing charging anomalies

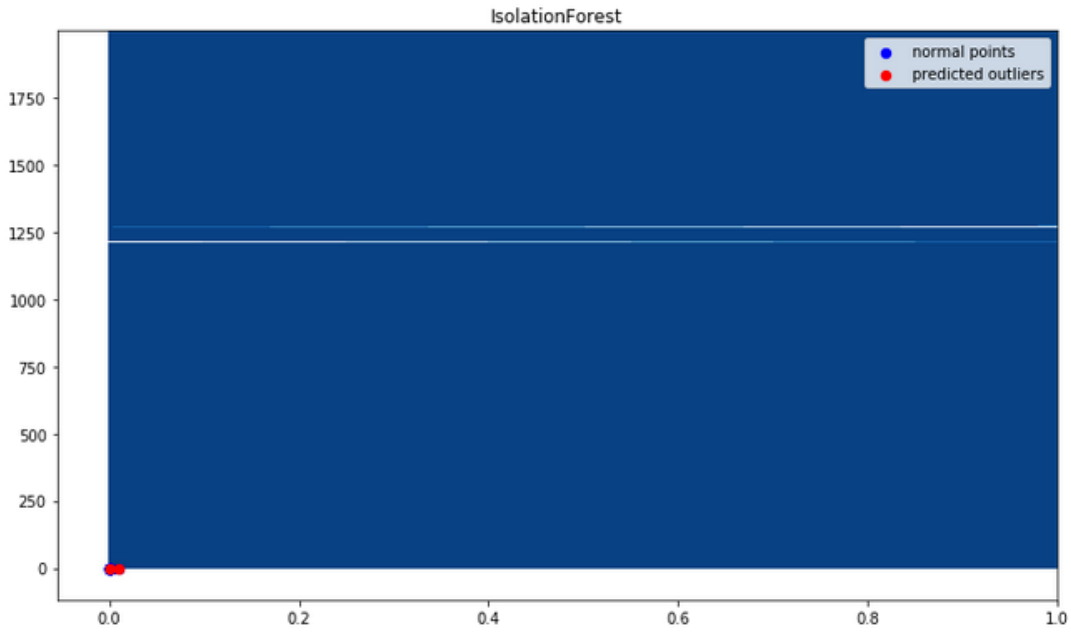


Figure 13- Isolation Forest Dataset 2018 results in two dimensional view showing charging anomalies

We can conclude that two of 1999 charging processes behave abnormally. This means most probably someone has tempered the system to exploit it for his/her benefit or even wanted to damage it. This information could be important for the appropriate function for a charging station. Consequently, Charging Stations might implement real-time anomaly detection programs, in order to monitor and control the power of the smart network, and to detect if an electrical Vehicle's smart charging process behaves abnormally. Upon such implementations, new ways to prevent the cyber-attacks will arise, further securing the charging grid, which is our ultimate goal.

6.3.2. Dataset of 2019

Running the above code on dataset of charging records of 2019 (2614 total charging processes), we take the following result and plot (Figure 14):

```
1    2614
Name: anomaly, dtype: int64
```

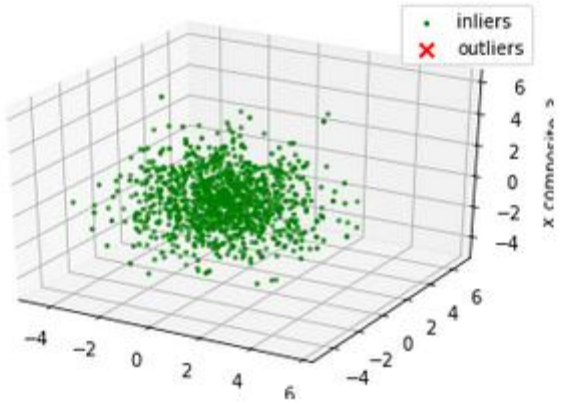


Figure 14- Isolation Forest Dataset 2019 results in three dimensional view showing charging anomalies

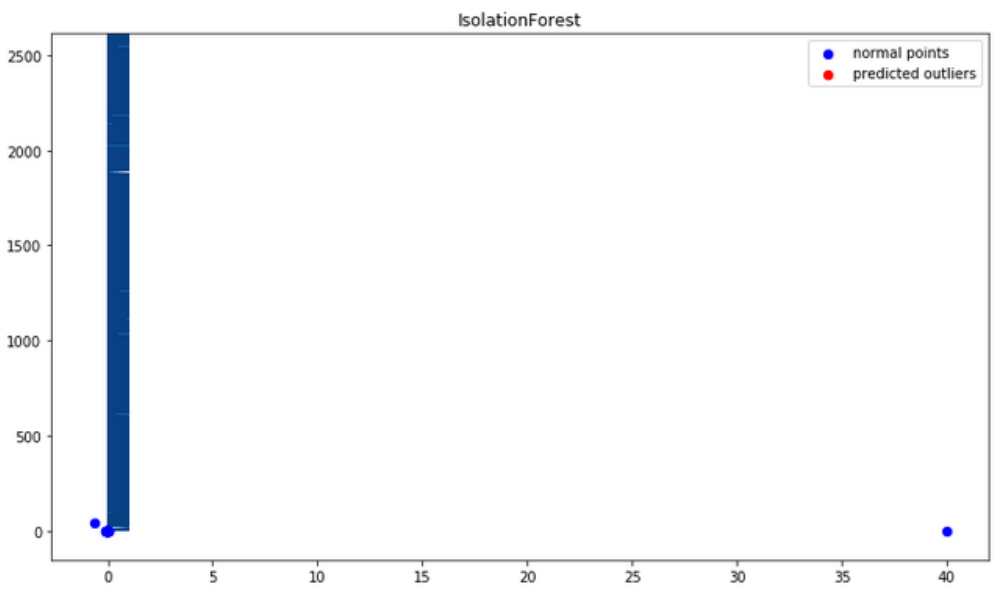


Figure 15- Isolation Forest Dataset 2019 results in two dimensional view showing charging anomalies

As we can see from the two graphs that were produced by our algorithm in this particular set of data no outliers, where detected, which means no abuse was done to our charging process. This is the optimal function of a Charging Station in a daily basis, where the car can power itself with proper dosage and safety protocols that prevent it from damaging its electronics from the charging. Something, like that is also crucial as less maintenance is needed and less energy is wasted, which is good for the state of the environment.

6.3.3. Dataset of 2020

After running the python program on dataset of charging records (9161 total charging processes) that were recorded in 2020, it seems that there is no detected abnormal behavior, as Figure 16 presents.

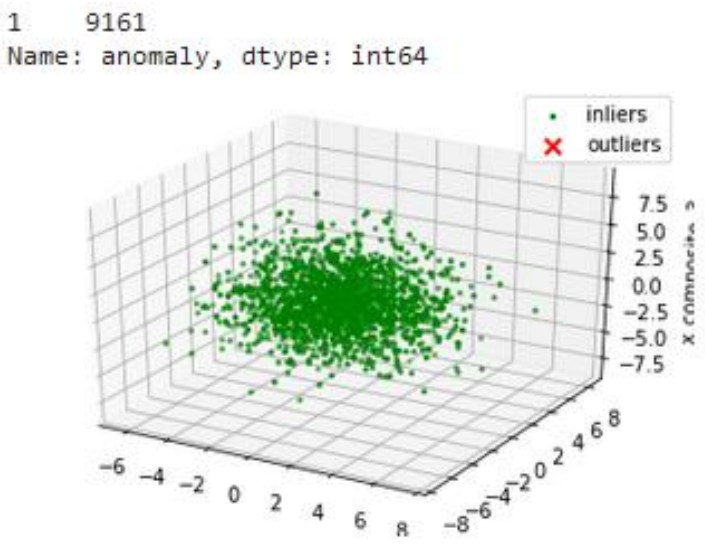


Figure 16- Isolation Forest Dataset 2020 results in three dimensional view showing charging anomalies

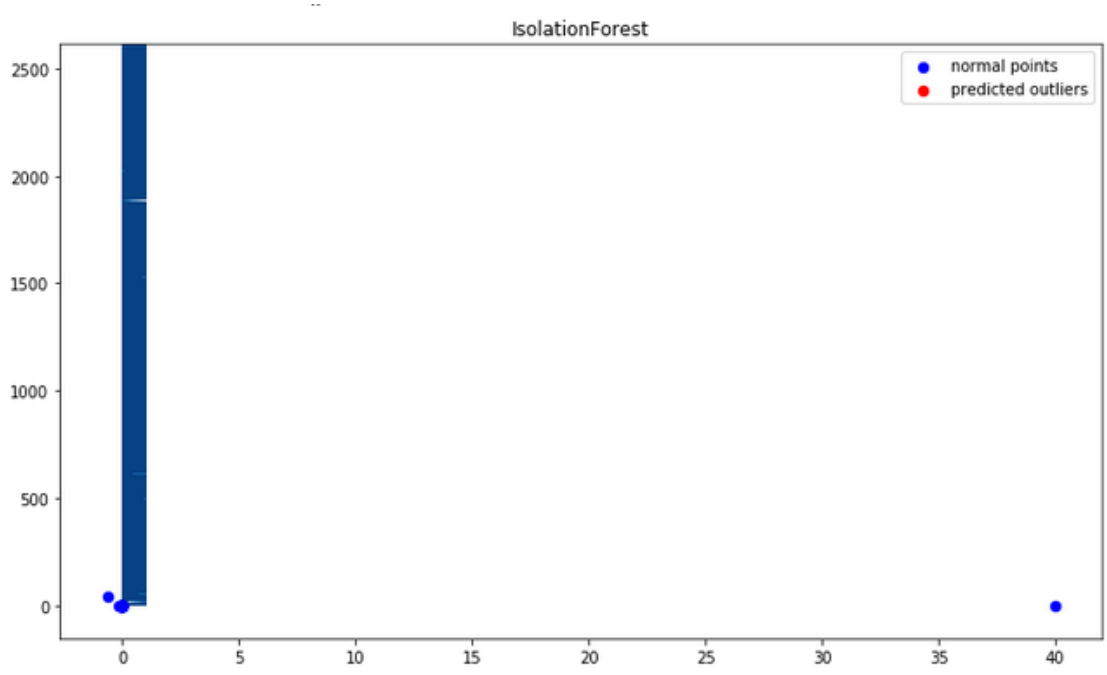


Figure 17- Isolation Forest Dataset 2020 results in two dimensional view showing charging anomalies

Since both datasets of 2019 and 2020 did not find any anomalies, we conclude that cyber-attacks to Charging stations are not very common however from the dataset of 2018, we can see that they are not nonexistent either. Probably if the algorithmic anomaly detection code inspected more processes, the results would be even more conclusive upon the scale of these attacks. Constant surveillance of the Charging Stations is very important in order for the detection of those spikes too be more efficient.

6.4. Discussion of implementing

The diagrams that were generated from running tests above show the number of splits required to isolate a normal point and an anomaly. Splits, represented through blue lines, and happen at random on a random attribute and in the process building a decision

tree. The number of splits determines the level at which the isolation happened and will be used to generate the anomaly score.

The process is repeated multiple times and we note the isolation level for each point/instance. Once the iterations are over, we generate an anomaly score for each point/instance, suggesting its likeliness to be an anomaly. The score is a function of the average level at which the point was isolated. The red points on the basis of the score, are labeled as anomalies.

The process of tree construction is repeated multiple times and each time we pick a random sub-sample and construct the tree. There are no strict rules to determine the number of iterations, but in general, we could say the more the merrier. The sub-sampling count is also a parameter and could change depending on the data set.

Every anomaly detection algorithm has to score its data points/instances and quantify the confidence the algorithm has on its potential anomalies. The generated anomaly score has to be bounded and comparable. In Isolation Forest, that fact that anomalies always stay closer to the root, becomes our guiding and defining insight that will help us build a scoring function.

The isolation forest algorithm thrives on sub-sampled data and does not need to build the tree from the entire data set; it works well with sub-sampled data. While constructing the tree, we need not build tree taller than a valued defined (very cheap to compute), making it low on memory footprint. Since the algorithm does not depend on computationally expensive operations like distance or density calculation, it executes really fast. The training stage has a linear time complexity with a low constant and hence could be used in a real-time online system.

Therefore, extracting and isolating abnormal values, charging processes that behave with abnormal power (volume) might easily be detected.

Conclusions & Future Work

This Thesis examined threats and cyber-attacks in the charging process and the targeting BMS and other parts of the car's electronics' system. The main advantage of the electric vehicles is its contribution to the reduction of air pollution, most of which is due to the pollution of conventional vehicles. Electric vehicles have virtually zero pollution, causing minimal air pollution and zero pollution of the moving space. In a recent measurement it appears that the electric vehicles are 98% cleaner than the conventional. Other advantages are the reduced air pollution, a phenomenon that makes the atmosphere of modern cities unbearable. The electric vehicles are essentially silent compared to vehicles with internal combustion engines. They are more reliable than conventional vehicles. Also, they are easier to build because the electric motors are very simple in their structure, compared to internal combustion engines. Since it is powered by electronic power converters, which are easily controlled electronically, water is usually not required for cooling and does not use filters or oil, so it does not present problems caused by low ambient temperature. Finally, an electric car consumes energy only when it is moving. When not moving e.g., stops at traffic lights or heavy traffic jams, does not consume energy.

A Plug-in Electric Plug-in Electric Vehicle communicates with and is controlled by a charging station. Charging Stations play an important role and they multiple other functions such as providing and controlling the energy to the EV using the Electric Vehicle Supply Equipment (EVSE) component, collecting the measurements from the meter for each charge of an Electric Vehicle, identifying and authorizing EV users via user authentication component. Moreover, charging stations enable remote capabilities (e.g., adjustment of the maximum current allowed by the Charge Point) to the Charge Point via the Local Controller component over WAN. The main contribution of this thesis is to give new knowledge of examining possible threats and abuse of smart charging in Electrical Vehicles. In other words, applying specific algorithms in real collected database of a standard EV charging enterprise, to test possible abnormal activity on the charging sta-

tion can trigger designers and programmers of the networks of smart charging Station, to reconsider the security issues. Moreover, if algorithms can be applied in real time, then detection of abnormalities during smart charging could trigger an alarm that some abnormal activity is taking place.

Many attacks on electric vehicle charging within a smart grid environment have been identified. EV charging is susceptible to masquerading, tampering, eavesdropping, and denial of service attacks, in addition to privacy concerns and charging. Charging can be attacked by methods of eavesdropping, man-in-the-middle and tampering attacks on the payment price and the amount of energy that the meter believes the EV has received. They also discuss the potential for malicious software within the vehicle to affect a charging station, or a compromised charging station to affect an EV.

This means that if an attacker could intrude the software of the charging station, it might be possible to influence the charging behavior of the vehicle. This Thesis examined whether the charging station hardware can be hacked in order to send these erroneous signals (either locally or remotely) and how the charging stations can be made tamper-proof and how cyber-attacks can be detected. Using Isolation Forest Algorithm and python language, we presented a fully functioned program, giving as input charging processes, obtained by a standard EV charging enterprice's database and as output we isolated, abnormal charging processes. In this case an abnormal charging process is the situation, where an electric vehicle requests high volume of power.

To conclude, there are some possible ways for charge stations, on order to detect abnormal situations in charging processes of Electrical Vehicles. In this thesis, isolation forest seems to be useful in order to test the charging processes that requests high voltage of power. Therefore, charging stations network could trigger an alarm in order to investigate an abnormal situation, possibly a cyber-attack.

References

1. Yosra, Fraiji & Azzouz, Lamia & Trojet, Wassim & Saidane, Leila. (2018). Cyber security issues of Internet of electric vehicles. 1-6. 10.1109/WCNC.2018.8377181.

2. Li, Yanmei & Ha, Ningning & Li, Tingting. (2019). Research on Carbon Emissions of Electric Vehicles throughout the Life Cycle Assessment Taking into Vehicle Weight and Grid Mix Composition. Energies. 12. 3612. 10.3390/en12193612.

3. Acharya, Shree & Choi, Kyung-Ho & Wi, Young-Min & Lee, Jaehee. (2018). Smart Charging for Grid-Connected Electric Vehicles to Provide Regulation Service. Journal of the Korean Institute of Illuminating and Electrical Installation Engineers. 32. 32-39. 10.5207/JIEIE.2018.32.1.032.

4. Fauzan, Ts Dr Mohd Faizal & Feng, S. & Zureel, M. & Sinidol, B. & Wong, D. & Jian, G.. (2019). A REVIEW ON CHALLENGES AND OPPORTUNITIES OF ELECTRIC VEHICLES (EVS). Journal of Mechanical Engineering Research & Developments. 42. 130-137. 10.26480/jmerd.04.2019.130.137.

5. Hajebrahimi, Ali & Kamwa, Innocent. (2018). A Novel Approach for Plug-in Electric Vehicle Planning and Electricity Load Management in Presence of a Clean Disruptive Technology. Energy. 158. 10.1016/j.energy.2018.06.085.

6. Xiang, Yue & Hu, Shuai & Youbo, Liu & Zhang, Xin & Liu, Ji. (2018). Electric Vehicles in Smart Grid: A Survey on Charging Load Modelling. IET Smart Grid. 2. 10.1049/iet-stg.2018.0053.

7. Igbinovia, Famous & Fandi, Ghaeth & Mahmoud, Rateb & Tlustý, Josef. (2016). A Review of Electric Vehicles Emissions and its Smart Charging Techniques Influence on Power Distribution Grid. Journal of Engineering Science and Technology Review. 9. 80-85. 10.25103/jestr.093.12.

8. Martinenas, Sergejus & Pedersen, Anders Bro & Marinelli, Mattia & Andersen, Peter & Træholt, Chresten. (2015). Electric vehicle smart charging using dynamic price signal. 2014 IEEE International Electric Vehicle Conference, IEVC 2014. 10.1109/IEVC.2014.7056150.

9. Parkinson, Simon & Ward, Paul & Wilson, Kyle & Miller, Jonathan. (2017). Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. IEEE Transactions on Intelligent Transportation Systems. 1-18. 10.1109/TITS.2017.2665968.

10. https://www.vreg.be/sites/default/files/uploads/siemens.pdf

11. Hanauer, Dieter. (2018). Mode 2 Charging—Testing and Certification for International Market Access. World Electric Vehicle Journal. 9. 26. 10.3390/wevj9020026.

12. Borges, J. & Ioakimidis, Christos & Ferrão, Paulo. (2010). Fast charging stations for electric vehicles infrastructure. WIT Transactions on Ecology and the Environment. 130. 275-284. 10.2495/ISLANDS100241.

13. Lopes, Joao Abel & Soares, Filipe & Almeida, Pedro & Moreira da Silva, M.. (2009). Smart Charging Strategies for Electric Vehicles: Enhancing Grid Performance and Maximizing the Use of Variable Renewable Energy Resources.

14. https://www.smartgrid-forums.com/wp-content/uploads/2018/06/11.-SmartSec-Europe-2016-ENCS-Michael-John.pdf

15. Ferreira, João & Monteiro, Vitor & Afonso, J.L. & Silva, Antonio. (2011). Smart electric vehicle charging system. 758 - 763. 10.1109/IVS.2011.5940579.

16. Afonso, J.L. & Ferreira, João & Monteiro, Vitor & Silva, Antonio. (2013). Smart Electric Vehicle Charging System.

17. H. Onishi Paradigm change of vehicle cyber security 4th International Conference on Cyber Conflict (2012), pp. 381-391

18. M.A. Mustafa, N. Zhang, G. Kalogridis, Z. Fan Smart electric vehicle charging: security analysis IEEE PES Innovative Smart Grid Technologies Conference (2013)

19. S. Fries, R. Falk Electric vehicle charging infrastructure-security considerations and approaches INTERNET 2012: the Fourth International Conference on Evolving Internet (2012), pp. 58-64

20. Clairand, Jean-Michel & Rodríguez-García, Javier & Alvarez, C.. (2018). Smart Charging for Electric Vehicle Aggregators considering Users' Preferences. IEEE Access. PP. 1-1. 10.1109/ACCESS.2018.2872725.

21. Twentyman J. (2018). Smart energy: Why vehicle-to-grid technology is on the move, Internet of Business, April 2018, https://internetofbusiness.com/smart-energy-why-vehicle-to-grid-technology-is-on-the-move/

22. Antoun, Joseph & Kabir, Mohammad & Moussa, Bassam & Atallah, Ribal & Assi, Chadi. (2020). A Detailed Security Assessment of the EV Charging Ecosystem. IEEE Network. PP. 1-8. 10.1109/MNET.001.1900348.

23. Schmutzler, Jens & Andersen, Claus & Wietfeld, Christian. (2013). Evaluation of OCPP and IEC 61850 for smart charging electric vehicles. 1-12. 10.1109/EVS.2013.6914751.

24. K. Wang *et al*., "A Survey on Energy Internet: Architecture, Approach, and Emerging Technologies," in *IEEE Systems Journal*, vol. 12, no. 3, pp. 2403-2416, Sept. 2018.

25. Zamini, Mohamad & Hasheminejad, Seyed Mohammad Hossein. (2019). A comprehensive survey of anomaly detection in banking, wireless sensor networks, social networks, and healthcare. Intelligent Decision Technologies.

26. Jing, Wentao & Yan, Yadan & Kim, Inhi & Sarvi, Majid. (2016). Electric vehicles: A review of network modelling and future research needs. Advances in Mechanical Engineering. 8. 10.1177/1687814015627981.

27. Chandola, Varun & Banerjee, Arindam & Kumar, Vipin. (2009). Anomaly Detection: A Survey. ACM Comput. Surv. 41. 10.1145/1541880.1541882.

28. Kong, Peng-Yong & Karagiannidis, George. (2016). Charging Schemes for Plug-In Hybrid Electric Vehicles in Smart Grid: A Survey. IEEE Access. 4. 6846-6875. 10.1109/ACCESS.2016.2614689.

29. Garcia-Villalobos, Javier & Zamora, I. & Martín, J.I. & Asensio, F.J. & Aperribay, V.. (2014). Plug-in electric vehicles in electric distribution networks: A review of smart charging approaches. Renewable and Sustainable Energy Reviews. 38. 717-731. 10.1016/j.rser.2014.07.040.

30. Brown, Kenneth. (2013). Electric vehicle supply equipment; a safety device. 1-5. 10.1109/ITEC.2013.6573505.

31. Yuan, Kai & Sun, Chongbo & Song, Yi & Xue, Zhenyu & Wu, Zhili & Gao, Shuang & Xu, Jing. (2017). Electric vehicle smart charging network under the energy internet framework. 1-5. 10.1109/EI2.2017.8245431.