IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 18, Issue 2, Ser. I (Mar. – Apr. 2023), PP 39-46
www.iosrjournals.org

CYBERSECURITY MEASURES IN BATTERY ELECTRIC VEHICLES (Bi-Directional Charging)

Ankit Kumar Sahoo
IMT2018502
International Institute of Information Technology
Bangalore
Mentor - Prof. Roland E. Hass

Date of Submission: 01-05-2023 Date of Acceptance: 12-05-2023

I. INTRODUCTION

- Electric Vehicles are the new growing sector of the automobile industry in today's era. Electric vehicles (EVs) use electricity as their primary fuel or to improve the efficiency of conventional vehicle designs.
- Coming into existence in the mid-19th century, when electricity was introduced as a preferred method for motor vehicles propulsion, providing a fresh level of comfort and ease of operation.
- Internal combustion engines were the dominant propulsion methods for on-road automobiles like cars and trucks for almost a century.
- In the 21st century, EVs have seen a boost due to technological developments , increased attention on the usage of renewable energy and the potential reduction or the need to reduce transportation's impact on climate change and other environmental issues.
- As surveyed by The International Energy Agency, EVs sales may increase from 2% of global share in the year 2016 to 30% by 2030.

TYPES OF ELECTRIC VEHICLES
Hybrid Electric Vehicles (HEVs)
Plug-In Hybrid Electric Vehicles (PHEVs)
Battery Electric Vehicles (BEVs)

Low-emission vehicles that are powered by an internal combustion engine and an electric motor that uses energy stored in a battery, charged through regenerative braking. The ICE gets its energy from gasoline .

Similar to a HEV, but with a larger battery and electric motor. They have both gas tank and a charging port Which enables them to operate in an all-electric mode.

Powered completely and solely by an electric battery that is charged by plugging the vehicle into charging equipment. They always operate in an all-electric mode and have zero emissions.

BATTERY ELECTRIC VEHICLES (BEVs)

- BEVs do not have conventional engines but are driven solely by one or more electric motors powered by the energy stored in its batteries.

- All BEVs typically have shorter driving ranges per charge than comparable conventional vehicles have per tank of gasoline.

Key Components

1. All-electric auxiliary battery
2. Charging port
3. DC/DC converter
4. Electric traction motor
5. Onboard charger
6. Traction battery pack
7. Thermal system (for cooling)
8. Power electronics controller

CHARGING IN BEVs

- The batteries are charged by plugging the vehicle into an electric power source and can also be charged through regenerative braking.
- Regenerative braking - allows EVs to capture energy normally lost during braking by using the electric motor as a generator and storing that captured energy in the battery.
- Specifically, it comes down to two main considerations: WHERE it is being charged and HOW FAST it has to be charged.

Home Charging Public Charging

➢ Trickle Charge ➢ AC charging with a wallbox
- Standard 220 volt ○ 20-30 kW station
- 13-16 km/hour of charging
- 4-10 times faster than AC

➢ AC Household Charging household charging
- 230V outlet ➢ DC fast Chargers
- 3-4 times faster than trickle
- 45-60 kW Charge
- 20-80% of charge in just 40 minutes

TYPES OF CHARGERS

AC Connector Type	Power Ratings	Range/Hr charging	Voltage	Features
Type 1	~ 3.7 kW	12.5 miles	120 V	➔ No locking mechanism
	~ 7 kW	25 miles	230 V	➔ 5 pins and single phase only
Type 2	~ 3.7 kW	12.5 miles	120 V	➔ In-built locking mechanism
	~ 7 kW	25 miles	230 V	➔ Can carry 3 phase power
	22 - 43 kW	75 miles	400 V	➔ Most common on new cars

DC Connector Type	Power Ratings	Range/Hr charging	Voltage	Features
CHAdeMO	~ 50 kW	75 miles	400 V	➔ Original DC connector
	~ 100 kW	150 miles	500 V	➔ 4 pins
Combined CS (CCS)	~ 50 kW	75 miles	400 V	➔ High power
	~ 150 kW	225 miles	600 V	➔ 2 x 'Type 2' pins
	~ 300 kW	525 miles	900 V	➔ Most popular DC standard
Type 2 (TESLA)	~ 150 kW	225 miles	600 V	➔ Only Tesla superchargers
	~ 250 kW	375 miles	750 V	provide this type of DC fast charging.

BI-DIRECTIONAL CHARGING

- Bidirectional charging allows us to not only charge the batteries of electric vehicles but to also take energy from car batteries and push it back to the power to help balance momentary spikes in electricity demand.
- To use the energy stored in the EV's battery to power your home or send it back to the grid, the DC electricity from the car must be converted back to AC electricity. That's done by a bi-directional charger, which looks similar to a regular home EV charger.
- Bi-directional chargers work in a similar way to solar inverters, and have a sensor to monitor the load of the house and how much power is being pumped in and out of the house. If the sensor detects that system voltage has been breached, the charger will switch off.
- Benefits:
  - Manage momentary spikes in electricity consumption
  - Reserve renewable energy and pull it back when exactly needed
  - Cost-effective EV charging method

BI-DIRECTIONAL CHARGING

- The first and foremost prerequisite for using a DC fast charger (bidirectional or not) is that the charger and the EV have compatible DC charging ports, as these are not standardised across OEMs, and are often offered as an expensive upgrade.
- Two other critical requirements for these chargers are that they must be galvanically isolated from the AC mains, and must cease operating as an inverter as an inverter upon loss of power.
- Another important requirement is that the charger operate at a very close proximity to the unity power factor (obtained when current and voltage are in phase, similar to a circuit containing only resistance).
- With an accelerated shift to using BEVs , batteries of EVs offer enormous potential in terms of using their vast storage capacity as a flexible solution to support the grid.
- There are two primary receivers of power from any BEV: the grid (V2G) and the electricity from a home or building (V2H).
- Bi-directional charging creates greater synergy between the clean transport sector and renewable energy sources, as the car batteries can store excess energy created by varied renewable sources, and then provide power to the grid or home when demand is high or energy production is low.

BI-DIRECTIONAL CHARGING

Problems to be solved :

V2G

- The smart grid controls vehicle charging and returns electricity to the grid.
- The transmission system operator may be willing to purchase electricity from customers at times of peak demand or to use the EV battery capacity for ancillary services such as balancing and frequency control.

V2B/V2H

- Vehicles supply supplemental power to the building or home.
- This does not directly affect grid performance but rather provides a back-up power supply.
- It can also help the vehicle owner to avoid demand charges or increase the usage share of power produced on-site by distributed generation.

CHARGING/DISCHARGING OF PEVs IN V2G

- In V2G systems, battery vehicles (BVs) or plug-in electric vehicles (PEVs) can be used as energy storage devices.
- The PEVs can choose to charge or discharge their batteries to maximize the performance and minimize the cost. However, since PEVs are mobile vehicles and the information about V2G systems is transmitted to the PEVs through wireless links, the V2G data communication is unreliable and vulnerable to cyber-attacks which can violate confidentiality, authenticity, integrity, and availability requirements of the data exchange in V2G systems.
- A number of cyber risks have emerged to the V2G systems.
- The majority of research works focus on mitigating the risks by protecting the systems and preventing adverse effects from the attacks.
- PEVs can act as an energy reserve. As such, PEVs are expected to potentially offer unprecedented benefits to the grid.

CHALLENGES OF V2G

- V2G communication systems are different from other existing communication systems in several ways, such as vehicle mobility, geographic location of the vehicle, charge and discharge operations, driving pattern, and limited communication range.
- In terms of security, authentication in the V2G network needs to be fast and efficient in order to support a large number of EVs expected to participate in dynamic charging/discharging.
- Confidential information, such as vehicle identity, vehicle type, charging and discharging time, and charging station identity (CSID), needs to be protected.
- Electric vehicles can communicate with the smart grid via distributed and/or centralized V2G networks for charging/discharging their batteries from/to the grid.
- Information exchanges over the V2G network controls physical components in the electric distribution grid. As a result, information or network security breaches may cause the malfunction and/or damage of critical power infrastructure.

PRIVACY AND SECURITY CONCERNS

Information Privacy: Referred to as the permissible use of information. To protect consumers' privacy, power utilities or third parties are responsible for implementing right to access policies that ensure consumers' information is accessed and used only for legitimate utility-related purposes.

Information Security: Commonly represented in terms of the confidentiality, integrity, and availability of information (CIA). It comprises practices and processes, such as encrypting the transmitted information between the charging station and the aggregator, thus ensuring that the information is protected against any unauthorized access.

Privacy Challenges

1. How to Keep a Vehicle's Identity and its Location Information Untraceable from the Aggregator?
2. How to Protect the Privacy of the Vehicle's Other Preferences?
3. What Information is Required for Billing?

PRIVACY AND SECURITY CONCERNS

Security Challenges

1. What if a vehicle misbehaves?
2. Is There a Linkability Issue?
3. What if an Adversary Performs Attacks?
4. Impersonation Attack:
5. Replay and Injection Attack:
6. Redirection Attack:
7. Known Key Attack:
8. Repudiation Attack:
9. Flood-Based DoS Attack:

Privacy Objectives

1. Identity Anonymity
2. Vehicle Untraceability
3. Forward Privacy

SMART CHARGING MANAGEMENT SYSTEM

- In concept, a smart charging management system (SCMS) optimizes the charging of plug-in vehicles (PEVs) and provides various grid services including voltage control, frequency regulation, peak shaving, renewable energy integration support, spinning reserve, and emergency demand response.
- These functionalities largely depend upon data collected from various entities such as PEVs, electric vehicle supply equipment (EVSE), service providers, and utilities.
- SCMS can be susceptible to both cyber and physical threats (e.g. man-in-the-middle attack, data intrigued attack, denial of charging, physical-attack) due to interactions of and interdependencies between cyber and physical components.

CYBERATTACKS IN SCMS

A. False Data Injection Attack PEV - charging/discharging data throughout the grid are collected with the help of smart measuring devices, installed at charging stations.

B. Man-in-the-Middle Attack - an attacker intercepts and manipulates data that are communicated between various parties. Through MITM, an attacker can also cause intentional overcharging/discharging of PEV batteries causing damage to PEV and its batteries.

C. Denial-of-Service Attack - causes the unavailability of network service to intended users as a result of an attacker's action to jam and overload the network.

D. Malware Injection via EVSEs - Due to the publicly available nature of Electric Vehicle Supply Equipments(EVSEs), especially, at public charging stations are susceptible to malware injections. The malware injected EVSEs can cause theft of several sensitive information such as payment information, personal information, charging time, payment amounts, etc.

E. Physical Attack - A compromised PEV or EVSE is a potential personal safety concern and grid network concern. The coordinated charging events could cause widespread disruption of the power grid.

SECURE SMART V2G NETWORK

There are five main goals of cybersecurity in smart grids:

1. Authentication: The V2G network must provide mutual authentication between the vehicles and the aggregator and/or the registration authority. This process helps protect the network against redirection and impersonation attacks.The system verifies that the credentials provided by the user are correct or not.
2. Authorization: The user is authenticated when he provides the correct credentials. Now, the user becomes authorized to use the services and to transmit and receive data packets. In an unencrypted authentication process, credential inserted by the users are exposed to the attacker, and later, the attacker uses the credentials and pretends to be an authorized user.

SECURE SMART V2G NETWORK

Confidentiality: There is an abundance of sensitive data circulating throughout the smart grid network. Private information must be secret or hidden in order to provide confidentiality to the transmitted information. Encryption is used to provide confidentiality to the messages.

Integrity: This protects the recipient against data tampering by ensuring that the data is not changed or corrupted during transmission. For each sent message, it is required to verify whether any violation has taken place during message transmission.

Availability: Availability ensures that whenever user requires resources or/and data, they are always available. There are various factors that can affect the availability such as fault at the data center, but in terms of cybersecurity, it is affected by cyber attacks such as denial of service (DoS) attack.

SECURE SMART CHARGING

A newly proposed system architecture that involves charging stations, EVs, charging or discharging at a station, aggregators, communication servers at different locations and one or more authentication servers in the network, includes a scheme with various security and privacy features, such as:

1) Anonymous authentication and fine-grained access control
2) Anonymous signatures
3) Information confidentiality and message integrity
4) Remote attestation
5) Payment system in the V2G network

Payment Systems in a V2G Network

- The V2G payment system should be very efficient and secure, and able to authenticate involved parties many times in a day to support smart charging and discharging.
- Smart charging allows a vehicle owner to charge and discharge its vehicle's battery based on inputs, such as how long he wants to charge, what battery level he wishes to keep for the next day, after what battery level he wants to earn profit by discharging battery, and so on.

CYBER ATTACKS - examples

- Stuxnet (a worm) Cyber Attack – crippled the Iranian Nuclear Program
  - Started somewhere around 2007 when and Iranian nuclear engineer plugged his laptop into a secure computer network in the enrichment complex.
  - Weeks later the centrifuges began to spin wildly and tore themselves to pieces, causing massive destruction in Natanz nuclear facility.
  - Sent false info to scientists who tried searching for issues, and showed them that all the systems were functioning properly.
  - This was done by targeting the hardware suppliers and putting the worm in their electronic devices
- Car Cyberattacks and challenges
  - Playing with windows, speedometer, engine malfunction, indicators were part of the test.
  - Most cars are vulnerable to cyber invasion.
  - Due to mobile applications, car thieves can gain unauthorized entry to the vehicle.
  - Manipulation of safety aspects like cruise control, steering and braking systems.
  - Vulnerabilities in the third-party supply chain.
  - Stealing financial features involving payment for fuels, tolls, and subscriptions.

SMART GRID

- The Smart Grid with the integration of advanced technologies such as communication and advance computing power is anticipated to offer enhancement in efficiency, reliability, and availability.
- The world is transitioning from the conventional grid to the smart grid at a rapid pace. Innovation always comes with some flaws; such is the case with a smart grid.
- Furthermore, the Smart Grid provides infrastructure which is integrated with two-way communication and electricity flows.
- The Smart Grid is an organized technology where its inheritance the legacy power generation techniques which use natural gas, fossil fuel, coal as well as uses renewable sources of energy, such as wind turbines and solar power.
- A smart grid integrates the traditional electrical power grid with information and communication technologies (ICT). Such integration empowers the electrical utility providers and consumers to improve the efficiency and the availability of the power system while constantly monitoring, controlling, and managing the demands of customers

SMART GRID

- The Smart Grid is known to provide well-organized power distribution and consumption to a network of smart devices, transformer sand machines.
- Due to the heterogeneous communication architecture of smart grids, it is quite a challenge to design sophisticated and robust security mechanisms that can be easily deployed to protect communications among different layers of the smart grid-infrastructure

SECURITY RISKS IN SMART GRID

The smart grid connects with multiple domains using different protocols, making it vulnerable to numerous cyberattacks. There are many risks that Smart Grids can potentially obtain, and these could not only affect the organizations but will also affect regular customers.

There are mainly two kinds of attacks:

Passive attacks - are those in which no harm to the data is done, but the attacker only monitors the data. These are classified into two categories :

- ❏ eavesdropping attack
- ❏ traffic analysis attacks.

Active attacks - are more dangerous compared to passive attacks, as the attacker modifies the data or stops the receiver from receiving the data. These include masquerade attacks, replay attack, false data attack, and denial of service attacks.

SECURITY RISKS IN SMART GRID

- The eavesdropping attacks is when the attacker can see the data packets shared between sender and the receiver. However, the attacker does not modifies the data.
- Traffic analysis attack is another kind of passive attack in which the attacks continuously monitors and analyzes the traffic between the sender and the receiver.
- The replay attack is when the attacker and sender both send the data to the receiver; this confuses the receiver in differentiating between real data by sender and the data routed through the attacker.
- In the masquerade attack, the sender is idle, but the receiver keeps receiving data from the attacker.
- The false data injection attack in when the data do not come to the receiver directly from the sender instead the receiver receives the modified data from the attacker. However, both the sender and the receiver are unaware about the modification done by the attacker.
- Denial of service attack is a kind of attack in which attacker does not target the sender or receiver but the data server.

SECURITY RISKS IN SMART GRID

The major causes that make the smart grid vulnerable to cyberattacks are as follows:

Increased installation of intelligent electronic devices (IEDs):

a. As the number of devices in the network rises, the number of attack sites for attackers increases as well.
b. Even if the security of a single point is compromised, the entire network system would be impacted.

Installation of third-party components:

a. Third-party components that are not advised by experts increase the network's vulnerability to cyberattack.

b. These devices may be infected with trojans, which can then infect other devices on the network.

SECURITY RISKS IN SMART GRID

Inadequate personnel training:

a. Proper training is necessary to operate any technology.

b. When staff are not sufficiently taught, they might easily fall victim to phishing attempts.

Using Internet protocols:

a. Not all protocols are secure when it comes to data transmission.

b. Certain protocols transfer data in an unencrypted format.

c. As a result, they are easy candidates for data extraction via man in the middle attacks.

Maintenance:

a. While the primary goal of maintenance is to keep things functioning properly, it can become a vector for cyberattacks at times.

b. While doing maintenance, operators often disable the security system to conduct testing.

SOLUTIONS FOR A SMART GRID

Practically some security risks ideally need security solution to protect against vulnerabilities and regarding network security in Smart Grids, the networks are the most vulnerable against threats and risks.

- Encryption: Encryption is the process of taking some information (your data) and scrambling it so that it can't be read. When you connect to the internet using a VPN your connection is what becomes encrypted, which means that if cyber criminals were to intercept the stream of your data, all they would get is gibberish code.
- Remote access VPN: The Remote access VPN uses a public network such as the internet to provide access to organizations' private network. The users will use mobile devices or desktop using the VPN gateway for access after providing authentication.

SOLUTIONS FOR A SMART GRID

- Malware Protection: The Smart Grid requires Malware Protection because the Embedded system and the General-purpose systems which are connected to the Smart Grid needed to be secured and protected from cyber-attacks. The Embedded system requires a manufactures key which can be used to secure the product for software validation.
- Network Security: The Virtual Private Network (VPN) provides additional security while using the public network, such as the Internet. The (VPN) uses a variety of security methods such as encryption and protecting any data transmitted across the network as the data may be at risk when using the public network infrastructure.

SOLUTIONS FOR A SMART GRID

- Authentication: Maintaining authentication and control access are the main concern where the identity should be verified via strong authentication mechanisms. In order to implement the authentication, an "implicit deny policy" is possibly valuable when accessing the network.
  - By using the policy, it offers security solutions for the organization and using the implicit deny policy it can be beneficial because the individual users will have different permission which grants individual users' specific permissions where the Manager can see all the additional data related to projects whereas the staff has limited access of data.
- IPS & IDS: Network Intrusion Prevention System (IPS) and Network Intrusion Detection System (IDS) technologies. Intrusion prevention systems continuously monitor your network, looking for possible malicious incidents and capturing information about them.

GRID INTEGRATION OF EVs AND ITS IMPACT

- Integration of electric vehicles (EV) with the grid is essential for acceleration of EV adoption in India.
- Increase in EV penetration will inevitably demand an increase in the number of EV charging stations.
- E-mobility is a deep confluence between the transport and power sector and therefore integration of EV charging infrastructure with distribution grids creates both challenges and opportunities for the conventional power sector.
- The key challenges faced in integrating EV charging infrastructure with the grid are:

- Voltage Stability Issues
- Phase Imbalance
- Increase in Peak Load
- Overloading
- Power Losses
- Power Quality
- Impact on Reliability

GRID INTEGRATION OF EVs AND ITS IMPACT

- Although the primary application of an EV charger is to charge up the EV to satisfy the EV user's transportation needs, EVs can potentially perform a range of grid support services by controlling the charging of EV or by allowing bidirectional flow of power.
- The controllable nature of EV charging makes them ideal for providing ancillary services. Different strategies can be utilized for these ancillary services provisions.
- From the perspectives of transmission system operators and the distribution operators, EVs can be utilized as a mobile storage unit to benefit the different grid operators.

USE CASES OF BI-DIRECTIONAL CHARGING

https://www.bable-smartcities.eu/explore/use-cases/use-case/useCase/vehicle-to-x-v2x-charging-for-electric-vehicles.html

Challenge / Goal

In Barcelona and other municipalities of Catalonia, several measures have been implemented in order to promote e-mobility and facilitate a growth of Electric Vehicle usage in the region. Within the GrowSmarter project, Endesa Energía has installed five fast charging stations for Electric Vehicles in Barcelona to achieve this goal. However, charging batteries for a rapidly expanding fleet of electric vehicles will soon become a major challenge for our grids due to limited grid capacity.

Solution

Vehicle-to-Everything (V2X) applications has focused on the combination of Vehicle-to-Building (V2B) services with Vehicle-to-Grid (V2G) renewable energy generation in buildings. An energy management system optimizes the operation of V2G chargers, PV module and energy storage by communicating in real time and sending set points to the controllable elements.

In Barcelona, Endesa has installed six V2X Endesa chargers in an Endesa Building with Distributed Energy Resources (DER) including a PV Plant, a storage system, chargers (normal, fast and V2X) and a Demand Management System (DMS). The V2X bidirectional Endesa charger uses CHAdeMO protocol. It is designed to provide energy to the vehicle, the grid or to a house using different grid applications such as Time shift, Power balancing and Power quality support.

USE CASES OF BI-DIRECTIONAL CHARGING

https://www.bable-smartcities.eu/explore/use-cases/use-case/useCase/the-parker-project-v2g-servic es.html

Challenge / Goal

The aim of the Parker project was to validate that series-produced electric vehicles as part of a company fleet can support the power grid with V2G services. Ultimately supporting the use of renewable energy while earning money through grid services.

Solution

The project utilized a number of contemporary electric vehicles and V2G DC chargers provided by its industrial partners and used them to carry out a number of tests and demonstrations in PowerLabDK - an experimental platform for power system research.

Further, the project partnered with the world's first commercial pilot (the Frederiksberg Forsyning V2G hub) where electric vehicles provided grid services.

The project used the above assets to investigate three key topics: grid applications, grid readiness as well as scalability and replicability.