Research Paper E-ISSN NO : 2455-295X | VOLUME : 9 | ISSUE : 6 | SPECIAL ISSUE JUNE-2023

CONTEMPORARY ISSUES AND CHALLENGES OF THE ENVIRONMENT TO INTERRELATE THE SYSTEM OF EVs USING CYBERSECURITY

DR.J.PREETHA	PROFESSOR & HEAD , DEPARTMENT OF CYBER SECURITY, MUTHAYAMMAL ENGINEERING COLLEGE, RASIPURAM, INDIA -637408
DR.R.RAJKUMAR	ASSISTANT PROFESSOR, DEPARTMENT OF CIVIL ENGINEERING, PSG INSTITUTE OF TECHNOLOGY AND APPLIED RESEARCH, COIMBATORE, INDIA – 641062
S.SAHASRA	STUDENT, DEPARTMENT OF CYBER SECURITY, MUTHAYAMMAL ENGINEERING COLLEGE RASIPURAM, RASIPURAM, INDIA - 637408
G.SIBI	STUDENT, DEPARTMENT OF CIVIL ENGINEERING, PSG INSTITUTE OF TECHNOLOGY AND APPLIED RESEARCH, COIMBATORE, INDIA - 641062

ABSTRACT:

The popularity of electric vehicles (EVs) has been steadily increasing in recent years, with more and more consumers choosing to purchase these vehicles for their environmental and economic benefits. Electric vehicles (EVs) are becoming more prevalent on the roads, with their increasing popularity driven by the desire to reduce greenhouse gas emissions and dependence on fossil fuels. However, as with any new technology, EVs also pose new security risks, particularly with the increasing number of interconnected systems in the vehicle. This paper presents an overview of the cyber security threats faced by EVs, the challenges in securing these vehicles, and the solutions that are being developed to address these challenges. A comparison of different communication protocols used in EVs, highlighting their security features, is also presented.

KEYWORDS:

CYBER SECURITY, ELECTRIC VEHICLES [EV], COMMUNICATION PROTOCOLS, THREATS, CHALLENGES, SOLUTIONS.

INTRODUCTION

Electric vehicles (EVs) have gained significant attention in recent years due to their potential to reduce greenhouse gas emissions and dependence on fossil fuels. However, the increasing number of interconnected systems in EVs has led to new security risks, particularly cyber threats. EVs are complex systems that rely on multiple communication protocols to operate effectively, and the security of these protocols is critical to the safety and functionality of the vehicle. This paper provides an overview of the cyber security threats faced by EVs, the challenges in securing these vehicles, and the solutions that are being developed to address these challenges.

ELECTRIC VEHICLE CHARGING INFRASTRUCTURE:

There are a variety of ways that EVs can be charged, depending on the location and the specific needs of the driver.

As a result, charging infrastructure for EVs is designed for different applications and is of various types. EV chargers, also known as electric vehicle supply equipment (EVSE), come in different specifications and standards that vary from one country to another. These differences are based on the available EV models in the market and the characteristics of the electricity grid.

FIG 1: ELECTRIC VEHICLE

THE DIFFERENT TYPES OF EV CHARGING INFRASTRUCTURE INCLUDE:

1. Level 1 Charging: This type of charging involves plugging the vehicle into a standard 120-volt wall outlet. Level 1 charging is best suited for charging at home, as it is the slowest and can take up to 20 hours to fully charge an EV[12].

2. Level 2 Charging: This type of charging involves installing a charging station at home or a public charging station. Level 2 charging provides faster charging than Level 1, typically taking 4-8 hours to charge an EV fully.
3. DC Fast Charging: This type of charging is the fastest option and is available at public charging stations. DC fast charging can charge an EV to 80% in as little as 30 minutes, making it ideal for long-distance travel.

Electric Vehicle Supply Equipment (EVSE) is a crucial component of electric vehicle charging infrastructure. The EVSE is responsible for accessing power from the local electricity supply and using a wired connection and control system to safely charge electric vehicles.

One of the essential features of an EVSE control system is its ability to provide various functions, such as user authentication, authorization for charging, information recording and exchange for

Vehicle Segment	Battery Capacity (kWh)	Battery Voltage (V)
Micro EV	5-15	200-400
City EV	15-30	200-400
Compact EV	30-40	200-400
Mid-Size EV	40-60	300-500
Full-Size EV	60-100	300-500
Luxury EV	60-100+	300-500+

TABLE 1: ELECTRIC VEHICLE BATTERY CAPACITY & VOLTAGE

network management, and data privacy and security. It is recommended that EVSEs with at least basic control and management functions be used for all charging purposes to ensure safety and efficiency.

Conductive charging, which involves plug-in (wired) charging, is the most widely used charging technology. The requirements of EVSEs for conductive charging depend on factors such as vehicle type, battery capacity, charging methods, and power ratings. This means that the charging infrastructure needed for an electric car will depend on the specific vehicle and its charging needs.

The charging requirements for electric vehicles (EVs) are determined by the specifications of the EV batteries. Power must be supplied to the battery at the right voltage and current levels to allow for charging. The typical capacity and voltage of EV batteries vary among the different EV segments, as shown in the table below.

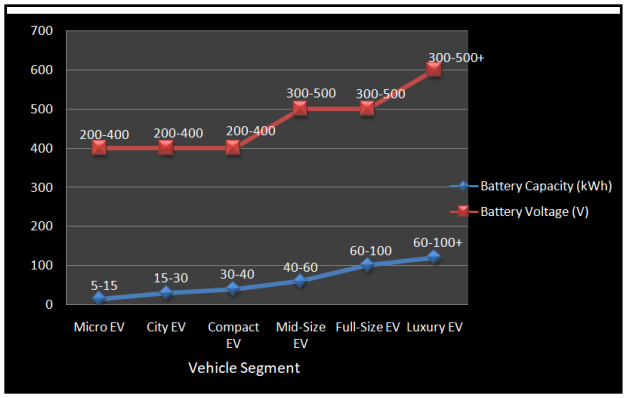

FIG 2: GRAPH OF ELECTRIC VEHICLE BATTERY CAPACITY & VOLTAGE

As can be seen in the table, the battery capacity and voltage of EVs varies significantly depending on the vehicle segment. Micro and City EVs typically have smaller battery capacities and lower voltage requirements, while Luxury EVs have larger battery capacities and higher voltage requirements.

ELECTRIC VEHICLE CHARGING METHOD:

Charging an electric vehicle (EV) involves supplying direct current (DC) to the battery pack. However, most electricity distribution systems supply alternating current (AC) power, which means that a converter is required to provide DC power to the battery. Conductive charging can be either AC or DC, and the charging infrastructure required for each type of charging is different[12].

In the case of AC charging, an AC electric vehicle supply equipment (EVSE) is used to deliver AC power to the onboard charger of the EV. The onboard charger then converts the AC power to DC, which is stored in the battery. The AC EVSE typically has a lower power output and is suitable for charging at home or in public areas where longer charging times are possible.

In the case of DC charging, a DC EVSE is used to convert the power externally and supply DC power directly to the battery, bypassing the onboard charger. DC EVSEs typically have a higher power output and are designed for fast charging[7].

AC and DC charging for electric vehicles (EVs) are further classified into four charging modes, each with its own set of specifications and requirements. Modes 1-3 pertain to AC charging, while Mode 4 pertains to DC charging.

Modes 1 and 2 are applicable for connecting an EV to a standard socket outlet, utilizing a cable and plug. However, Mode 1, also known as dumb charging, does not permit any communication between the EV and the electric vehicle supply equipment (EVSE) and its use is not recommended. On the other hand, the portable cable used in Mode 2 has an inbuilt protection and control capability, making it suitable for home charging[12].

Modes 3 and 4 provide a separate charger device to supply power to the EV, and have improved control systems. These modes are typically used for commercial or public

charging. Mode 3 is also known as smart charging and allows communication between the EV and the EVSE, enabling features such as user authentication, authorization for charging, and data exchange for network management. Mode 4 is used for DC fast charging and allows for higher power output, making it suitable for charging stations along highways and other locations where quick charging is needed.

FIG 3: ELECTRIC VEHICLE CHARGING

GROWTH OF INDIAN EV INDUSTRY (OVER 10 YEARS):

The Indian electric vehicle (EV) industry has witnessed significant growth over the past decade. Here are some key factors and developments that have contributed to this growth:

1. Government Initiatives: The Indian government has implemented various policies and initiatives to promote the adoption of electric vehicles. This includes the Faster Adoption and Manufacturing of Electric Vehicles (FAME) scheme, which provides financial incentives for EV buyers, subsidies for manufacturers, and support for charging infrastructure development.
2. Charging Infrastructure: The establishment of a robust charging infrastructure network is crucial for the widespread adoption of electric vehicles. Over the past decade, there has been a significant increase in the number of public and private charging stations across the country, making it easier for EV owners to charge their vehicles
3. Increased Consumer Awareness: There has been a growing awareness among consumers about the environmental benefits of electric vehicles, such as reduced carbon emissions and lower air pollution. This awareness, coupled with government campaigns and incentives, has encouraged more people to consider electric vehicles as a viable transportation option.
4. Expansion of EV Models: Several automakers have introduced electric vehicle models in the Indian market over the past decade. This includes both domestic and international manufacturers, offering a range of electric cars, two-wheelers, and commercial vehicles. The availability of a wider variety of EV options has contributed to increased consumer interest and adoption

Year	2-wheelers	3-wheelers	4-wheelers	Buses	Goods carriers	Total
2013	1,989	36	374	1	43	2,443
2014	1,678	12	481	3	20	2,194
2015	1,454	5,399	678	3	19	7,553
2016	1,459	46,561	621	4	54	48,699
2017	1,523	82,238	820	17	533	85,131
2018	16,572	1,08,289	988	49	657	1,26,555
2019	29,756	1,31,375	847	468	53	1,62,499
2020	28,632	88,227	3,179	88	13	1,20,139
2021	1,53,523	1,53,679	12,112	1,177	1,084	3,21,575
2022	6,22,337	3,37,335	37,792	1,932	453	9,99,849
Total	8,58,923	9,53,151	52,898	3742	2,929	18,76,637

TABLE 2: GROWTH OF INDIAN EV INDUSTRY(OVER 10 YEARS)

CYBERSECURITY THREATS TO ELECTRIC VEHICLES:

One of the primary cybersecurity threats to EVs is the potential for unauthorized access to the vehicle's electronic systems. This could be achieved through a variety of means, such as by exploiting vulnerabilities in the vehicle's software or by using wireless connections to gain access to the vehicle's control systems. Once an attacker gains access to the vehicle's electronic systems, they could potentially take control of the vehicle's operations, disable safety features, or access sensitive information.

Another potential cyber security threat to EVs is the possibility of a denial-of-service attack. This type of attack involves overwhelming the vehicle's electronic systems with data requests, causing the system to crash or become unresponsive. In an EV, a denial-of-service attack could cause the vehicle to stall or become completely unresponsive, putting the driver and passengers at risk.

Finally, EVs are also vulnerable to malware and other types of malicious software. Malware could be introduced to the vehicle's electronic systems through a variety of means, such as by connecting an infected USB drive or through a wireless connection. Once installed, malware could be used to steal sensitive information, disrupt the vehicle's operations, or cause other types of damage[9].

RISKS OF CYBER ATTACKS ON ELECTRIC VEHICLES:

The risks associated with a successful cyber attack on an EV are significant. For example, an attacker who gains access to the vehicle's electronic systems could take control of the vehicle's operations, potentially causing an accident or other dangerous situation. Additionally, an attacker could access sensitive information about the driver or passengers, such as location data or personal identification information. This could be used for identity theft or other malicious purposes.

Finally, a successful cyber attack on an EV could also have economic implications. For example, if a denial-of-service attack were to occur, the vehicle could become unusable, resulting in lost productivity and revenue.

EVs face a range of cyber security threats, including hacking, malware, and phishing attacks. Hackers can gain unauthorized access to the vehicle's systems, allowing them to control various components of the vehicle, including the brakes, steering, and acceleration. Malware, such as viruses and Trojans, can be introduced to the vehicle's systems through various means, such as USB drives or over-the-air updates. Phishing attacks can target vehicle owners, tricking them into providing sensitive information or downloading malicious software.

Researchers at the University of Georgia also found that an attack on an EV through a charging station could affect not only the charging station itself but also the vehicle control system as well as any infrastructure connected to it[3].

The number of suppliers that are involved with the development of electric vehicles combined with sophisticated control systems, more communication, ECUs and code leaves a wide attack surface that can be breached through multiple entry points. The entire ecosystem surrounding the vehicle—the charging station and power grid—can also pose a cybersecurity concern[3].

Some safety concerns are that electric charging stations are being developed quickly and are connected to both the internet and the vehicle, which leaves an enormous opportunity for hackers to access vehicles, homes, businesses and even the power grid—potentially creating a blackout in an entire city.

CYBER ATTACKS ON ELECTRIC VEHICLES AND CHARGING STATIONS:

1. **USB ports :**

   USB ports on charging stations could also be used for malicious intent that could directly affect driver privacy[11]. Through a simple flash drive, logs and data can be copied to the drive, giving attackers not only the data on the OCPP server itself, but also confidential information on users of the charging point, allowing attackers to copy their ID numbers or even track their location

FIG 4: CHARGING PORT

2. **MALWARE AND RANSOMWARE ATTACKS:**

   Malicious software can infect an electric vehicle's onboard computer or the charging station's control system, potentially allowing the attacker to control or shut down the vehicle or station. In some cases, attackers may demand payment to release the control of the systems back to the owner[10].

3. **Password Attacks:**

   Weak passwords and security practices can make charging stations and electric vehicles vulnerable to password attacks. Attackers may use brute-force or phishing techniques to steal passwords and gain access to the systems.

4. **Physical Security Breaches:**

   Cyber attacks are not limited to the virtual world. A physical security breach, such as tampering with a charging station or an electric vehicle's wiring, can also cause damage or even harm to individuals[10].

5. **Data Theft:**

   Charging stations and electric vehicles collect a vast amount of data, including personal information and location data. Attackers can target this data to commit identity theft or use it for other nefarious purposes.

6. **GPS Spoofing:**

   GPS spoofing involves the manipulation of GPS signals to change the location of a vehicle. This type of attack can be used to mislead electric vehicle drivers and potentially cause damage or accidents.

CONSEQUENCES OF CYBER ATTACKS ON ELECTRIC VEHICLES:

Cyber attacks on electric vehicles can have serious consequences, including loss of control over the vehicle, data compromise, and reputational damage.

LOSS OF CONTROL:

Cyber attacks on electric vehicles can allow hackers to take control of the vehicle's electronic systems, potentially causing physical harm to the driver, passengers, and other road users. For example, hackers could remotely disable the brakes or steering system, causing the driver to lose control of the vehicle. They could also take control of the accelerator, potentially causing the vehicle to accelerate uncontrollably, putting everyone in the vehicle and on the road at risk.

DATA COMPROMISE:

Electric vehicles are equipped with numerous sensors and communication systems that gather and transmit data about the vehicle's performance, usage, and location. If a cybercriminal gains access to this data, they could compromise the privacy and security of the vehicle's occupants. They could potentially use the data for fraudulent purposes, such as identity theft, or sell it on the

dark web, where it could be used for targeted advertising or other malicious activities.

REPUTATIONAL DAMAGE:

Cyber attacks on electric vehicles can also have a significant impact on the reputation of the vehicle manufacturer. If a cyber attack on a vehicle is widely publicized, it can damage the manufacturer's reputation and erode consumer trust in their products. This can have significant financial implications for the manufacturer and damage their ability to sell their vehicles.

ECONOMIC COSTS:

Cyber attacks on electric vehicles can also result in significant economic costs. In addition to the potential costs of repairing or replacing damaged vehicles, cyber attacks can also result in lost revenue for vehicle manufacturers, particularly if consumers become hesitant to purchase their products.

In summary, cyber attacks on electric vehicles can have severe consequences, including loss of control over the vehicle, data compromise, reputational damage, and economic costs. It is therefore essential that appropriate cyber security measures are implemented to protect electric vehicles from cyber threats.

The increasing connectivity and digitalization of electric vehicles have raised concerns about their cyber security. Cyber security in electric vehicles refers to the measures and techniques used to protect the vehicles and their components from cyber-attacks, unauthorized access, data theft, and other cyber threats.

Electric vehicles are complex systems that rely on a range of components and networks to operate. These components and networks include the battery management system, the vehicle controller, the charging system, the infotainment system, and the communication systems that connect the vehicle to external networks. Each of these components presents potential attack vectors for cybercriminals.

The potential risks and threats that electric vehicles face include remote control of the vehicle, data theft or manipulation, hacking of the vehicle's firmware or software, and denial of service attacks. If any of these attacks were successful, they could cause physical harm to the driver, passengers, or other road users, or compromise sensitive personal data.

To address these risks, cyber security in electric vehicles requires a multi-layered approach that incorporates both hardware and software solutions. Hardware solutions include secure hardware modules, secure communication protocols, and secure key management systems. Software solutions, on the other hand, involve secure firmware, software updates, and intrusion detection and prevention systems. Additionally, cyber security in electric vehicles requires strong user authentication and access control measures[2].

CHALLENGES IN SECURING EVS:

Securing EVs is a complex task due to the numerous interconnected systems that make up the vehicle. EVs rely on various communication protocols to operate, including Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay, and Ethernet. However, many of these protocols have limited security features, making them vulnerable to cyber attacks. Additionally, the open architecture of EVs makes them more susceptible to attacks as there are more points of entry for cyber criminals[9][8].

SOLUTIONS FOR CYBER SECURITY IN EVS:

To address the cyber security challenges faced by EVs, a range of solutions are being developed. One such solution is the use of secure communication protocols, such as FlexRay and Ethernet, which offer more robust security features. Other solutions include the development of secure over-the-air update mechanisms, the implementation of secure boot processes, and the use of intrusion detection[5] and prevention systems.

There are a number of countermeasures that can be used to protect EVs from cyber threats. These include:

1. Encryption: Encryption can be used to protect sensitive information that is transmitted wirelessly, such as vehicle location data or driver identification information.
2. Firewalls: Firewalls can be used to prevent unauthorized access to the vehicle's electronic systems. This can help prevent malware from being introduced to the vehicle's systems and can also prevent attackers from taking control of the vehicle.
3. Intrusion Detection Systems: Intrusion detection systems can be used to monitor the vehicle's electronic systems for signs of unauthorized access or other suspicious activity. This can help detect and prevent cyber attacks before they are able to cause significant damage. Intrusion detection systems can be used to detect cyber attacks on electric vehicles in real-time[5]. These systems use advanced machine learning algorithms to analyze the behavior of the vehicle's electronic systems and identify any anomalous behavior that may indicate a cyber attack[1]. Once an intrusion is detected, the system can automatically take action to mitigate the attack.
4. Over-the-Air (OTA) Updates: OTA updates can be used to ensure that electric vehicles are running the latest software and firmware, which are more secure and less vulnerable to cyber attacks. OTA updates can be used to patch vulnerabilities in the vehicle's software or firmware, as well as to update security protocols and settings.
5. Multi-Layered Authentication: Multi-layered authentication can be used to prevent unauthorized access to the vehicle's electronic

systems. This can include using biometric authentication, such as facial recognition or fingerprint scanning, in addition to traditional password-based authentication[2].

6. Hardware-Based Security: Hardware-based security can be used to prevent cyber attacks on the vehicle's electronic systems. This can include using secure microcontrollers and hardware security modules (HSMs) to store sensitive data and perform cryptographic operations.

CONCLUSION:

Indeed, cyber security is crucial to ensure a safe environment for electric vehicles and the people who use them. The growing popularity of electric vehicles highlights the need for increased attention to cyber security to prevent potential cyber attacks. As the use of EVs becomes more prevalent, the risks associated with cyber attacks are increasing. Cyber criminals can gain unauthorized access to a vehicle's systems and control its components, including the brakes, steering, and acceleration. Such unauthorized access can put the lives of vehicle occupants and others on the road at risk. The interconnected nature of these vehicles presents new security risks, and it is critical to ensure the safety and functionality of these systems. By implementing secure communication protocols, developing secure update mechanisms, and collaborating among stakeholders, we can work towards a safer environment for electric vehicles and ensure the safety of people on the roads.

REFERENCES

1. Cyber security in Connected and Automated Vehicles: A Comprehensive Overview by the US Department of Transportation (2018)

2. Cyber security and Privacy for Connected Vehicles: Overview and Future Research Directions by S. Seshadri et al. in Proceedings of the IEEE (2016)

3. Roy Fridman Forbes Councils Member Forbes Technology Council COUNCIL POST retrieved from: https://www.forbes.com/sites/forbestechcouncil/2022/10/19/the-importance-of-cybersecurity-in-fueling-the-electric-vehicle-revolution/?sh=3dfcf0be5994

4. A review of cyber security in connected and automated vehicles by J. Seo et al. in Computer Networks (2017)

5. Sajjad Abedi, Ata Arvani and Reza Jamalzadeh. Cyber Security of Plug-in Electric Vehicles in Smart Grids: Application of Intrusion Detection Methods. Retrieved from: https://www.researchgate.net/publication/278655187_Cyber_Security_of_Plug-in_Electric_Vehicles_in_Smart_Grids_Application_of_Intrusion_Detection_Methods

6. Securing Cyber Physical Systems by S. Basu et al. in Communications of the ACM (2015)

7. Anuj Sanghvi; Tony Markel Cyber security for Electric Vehicle Fast-Charging Infrastructure. 2021 IEEE Transportation Electrification Conference & Expo (ITEC)

8. A Survey of Cyber security Challenges in Smart Vehicles by Y. Chen et al. in IEEE Internet of Things Journal (2019)

9. Cyber security for Electric Vehicles: Threats, Challenges, and Solutions by T. A. Alharbi et al. in IEEE Access (2021)

10. Alessandro Brighente, Member, IEEE, Mauro Conti, Fellow, IEEE, Denis Donadel, Raadha Poovendran, Fellow, IEEE, Federico Turrin, and Jianying Zhou, Senior Member, IEEE, Electric Vehicles Security and Privacy: Challenges, Solutions, and Future Needs. Retrieved from: https://www.researchgate.net/publication/367050012_Electric_Vehicles_Security_and_Privacy_Challenges_Solutions_and_Future_Needs

11. oded yarkoni, The Increasing Need for Electric Vehicle Cyber Security. Retrieved from: https://upstream.auto/blog/the-hidden-cyber-risks-of-electric-vehicles/

12. HANDBOOK of ELECTRIC VEHICLE CHARGING INFRASTRUCTURE IMPLEMENTATION. Retrieved from: https://www.niti.gov.in/sites/default/files/2021-08/HandbookforEVChargingInfrastructureImplementation081221.pdf