University Journal of Research: Computer Science and Applications

EVCS Under Siege: The Man-in-the-Middle Threat

Dr. Kashyap C. Patel[a], Dr. Sachinkumar Anandpal Goswami[b], Dr. Saurabh Dave[c], Dr. Ajaykumar Patel[d] and Bhargav Padhya[e]

[a]Assistant Professor, FCA, Ganpat University, Gujarat, India

[b]Assistant Professor, FCA, Ganpat University, Gujarat, India

[c]Pro Vice Chancellor, Ganpat University, Gujarat, India

[d]Associate Professor, FCA, Ganpat University, Gujarat, India

[e]Assistant Professor, FCA, Ganpat University, Gujarat, India

Corresponding Author Email: drkashyapcpatel@gmail.com

Abstract

Electric Vehicle Charging Stations (EVCS) are now a core part of urban infrastructure-a catalyst for sustainable transportation systems. In contrast, wireless connectivity exposed them to a variety of cybersecurity threats, of which the Man-in-the-Middle is a prominent threat. The key thrust of this research paper was the experimentation setup to highlight the vulnerabilities of EVCS against such attacks. We specified a comprehensive model of an EVCS, that encompassed a charging interface, power management systems, and communication protocols. We simulated a Rogue Access Point (Rogue AP) as an entry point to attack the EVCS network. It presented the attack model for how an attacker could catch and manipulate data between the charging station and users. We assessed the AI-driven methodology for man-in-the-middle attacks utilising machine learning techniques, aiming to compromise electric vehicle charging stations. This was also emphasised by the increasing complexity of cyber threats and the corresponding necessity for security measures. It will discuss the potential mitigation strategies for enhancing security in EVCS to counter MITM attacks such as robust encryption protocols, anomaly detection systems, and also user education programs. By discussing these results, this research shall contribute toward developing more resilient EVCS infrastructures to ensure safe, reliable, and versatile electric vehicle charging as urban areas up their embrace of electric vehicles.

Keywords: EVCS, Rogue Access Point, MiTM, EVCS security, AI driven MiTM, Drone

1. Introduction

The Electric Vehicle (EV) Charging Station market is expected to rise to a market size of USD 7.3 billion in 2024 and USD 12.1 billion by 2030, with growth at a Compound Annual Growth Rate (CAGR) of 8.8% during the forecast period from 2024 to 2030. China is the largest market for electric charging stations, and the study is covered under regions including China, Asia Pacific, Europe, North America, the Middle East, and the rest of the world. The market research report analyses the industry on various segments such as Level of Charging, Charging Service Type, Charge Point Operator, Charging Infrastructure Type, Charging Point Type, Installation Type, Connection Phase, Application, DC Fast Charging Type, Operation, and Region. Some of the notable companies that have been included in this report are ABB (Switzerland), BYD (China), Tesla (US), Schneider Electric (France), Tritium (Australia), Shell (UK), and Chargepoint (US) with 2023 as base year [1]. Electric mobility is one of the most promising global strategies toward decarbonizing the transport sector. In fact, India is one of the very few countries in the world that support the global EV30@30 campaign to drive 30% or more new vehicle sales to be electric by the year 2030 [2]. With the growing adoption of EVs, it is one crucial step toward connecting them with the urban infrastructure needed to support growing demand for charging. However, with the many uses of wireless connectivity to facilitate communication between users and charging interfaces as well as backend systems by these stations, it becomes vulnerable to a variety of forms of cybersecurity threats. Among these emerging threats is the possibility of a Man-in-the-Middle [3]-[8] attack that could compromise sensitive data and operate in the most disconcerting way, bringing operations to a halt. This paper presents experimental rigorous setups in a controlled lab environment to explore vulnerabilities to MITM [3]-[8] attacks against an EVCS [5] [25] [32]. This was demonstrated by constructing an end-to-end model of an EVCS that encompasses critical components, thus showing how attackers can exploit these weaknesses. The first phase of our research was on simulating a rogue access point [3]-[8], which compromised the EVCS [5] network. This is where interception and manipulation of data shared between the charging station and its users could be demonstrated. We take the experimentation a step ahead by including drone-based MITM attacks and demonstrate how drones can efficiently position themselves throughout the urban landscape to optimize their range and effect. In addition to the traditional methods, we extend our research by incorporating an AI-driven [12] [18] [36] [38] approach through MITM, wherein we make use of ML-based algorithms to parse and modify data on the fly after its interception. This novel method elucidates the constantly growing complexity of cyber threats while underlining the requirement for adaptive security measures to protect EVCS from possible breach. Thus, this research not only explores the vulnerabilities existing in EVCS networks but also addresses the prospects of mitigating strategies that can strengthen the security profile against MITM attacks. Thus, these issues are being used towards the aim of contributing valuable insights toward ensuring safety and reliability in charging electric vehicles [5] as cities continue to evolve into greener, more sustainable settings. [13] [14] [15] [25] [32]

2. Literature Review

Charge manipulation attacks (CMAs) on smart EV charging stations modify the EV aggregator's demand by manipulating charging session information. The paper calculates CMAs' economic impact on day-ahead and real-time energy market EV aggregators. It also presents an unsupervised deep learning-based mechanism to detect CMAs by monitoring EV charging parameters, exposing smart charging risks and the need for monitoring tools [19]. The authors present "Brokenwire," a novel attack on the Combined Charging System (CCS), a popular DC quick charging system for EVs. The attack affects vehicle-charger control communication, aborting charging sessions. It can be done remotely from afar using off-the-shelf radio technology, disrupting automobiles or fleets silently and simultaneously. The study shows the attack's effectiveness in real-world circumstances and suggests mitigation methods [40]. This research introduces "EVExchange," an attack that allows an adversary to steal energy during V2G (car-to-Grid) connection by charging their own car while the victim pays. If reverse charging is enabled, the attacker can benefit by selling the victim's car's electricity while depleting the battery. The authors used virtual and physical testbeds to evaluate the assault and suggest a lightweight ISO 15118 protocol change with a distance bounding mechanism as a countermeasure [41]. The research examines charger-EV communication mechanisms and finds that the SAE J1772 charging control protocol lacks authenticity protection. The authors suggest "ChargeX," an attack that manipulates EV charger charging states or rates to interrupt charging schedules, cause DoS, or degrade battery performance. They create and test numerous assault techniques on public and home chargers to prove their efficacy and generalization [42]. The research analyses EV user interface, network connection, and terminal maintenance weaknesses and dangers to understand EV adoption and charging alternatives. The authors identify cyberattacks, including various attack modes, using the STRIDE threat model and suggest secure coding, tamper detection sensors, network segmentation, intrusion detection systems, and role-based access control mechanisms to secure

EV charging systems [43]. In a smart grid, Man-in-the-Middle (MiTM) attacks allow outsiders to eavesdrop or impersonate devices, resulting in misleading data or command injections that can jeopardize power system operations. The authors build and implement multi-stage MiTM incursions in a cyber-physical power system testbed to show how they can trigger physical events. For stealthy attacks, they provide detection strategies based on intrusion detection system and network monitoring tool warnings [44]. This study explores power plant Modbus protocol vulnerabilities to cyberattacks that threaten energy infrastructure. The authors develop a real-time cyber-physical systems testbed to assess smart power grid network vulnerabilities. They analyze the system's response to a Modbus protocol Man-in-the-Middle attack and offer a cybersecurity approach to address network weaknesses and deploy effective countermeasures [45].

Electric Vehicle Charging Stations face major cybersecurity concerns, notably Man-in-the-Middle (MiTM) attacks, according to the studied literature. These attacks can cause energy waste, financial losses, and chargeable service disruptions. The investigations emphasize the need for protocol upgrades, intrusion detection technologies, and continual monitoring to protect the EV charging infrastructure.

3. Setup the smart EVCS at lab

The smart EVCS model will help researchers understand real-time operations and responses. Current, voltage, and temperature will be monitored in the smart electric vehicle charging station. Through an LCD panel and web interface, the system provides real-time, overcurrent prevention, and smart grid integration [2] [18] [19] [20] [28] [30] [33] [39]. This EVCS configuration offers Wi-Fi remote control and monitoring for dynamic load balancing and grid management. The sensors and microcontrollers give hands-on IoT, electronics, and smart energy experience [2] [15] [17] [23] [24] [26] [27] [29].

3.1 Components for set up

This comprehensive Smart EV Charging Station design provides a solid foundation for learning IoT, renewable energy, and smart grid [18]-[20]. It creates a project from these modules and technologies, providing real experience in electronics, programming, and system integration.

The following table 1 describes the components list and their functionalities.

Table 1. Components list

Component Type	Specific Component
Microcontroller	Arduino Uno or Raspberry Pi
Charging Station	Type 2 Charging Unit (or simulator)
Sensors	ACS712 (Current), ZMPT101B (Voltage), DS18B20 (Temperature), PZEM-004T (Energy Meter, optional)
User Interface	16x2 LCD Display, Buttons, LED Indicators
Connectivity	ESP8266 or ESP32 (Wi-Fi Module)
Power Management	Relay Module, Fuse, Circuit Breaker (optional)
Resistors & Capacitors	4.7kΩ Pull-up Resistor, 0.1 µF Decoupling Capacitor
Miscellaneous	Breadboard, Jumper Wires, PCB

3.2 Components for circuit diagram

Design Smart EVCS schematic in Fritzing or Tinkercad. Connect the ACS712 current, ZMPT101B voltage, and DS18B20 temperature sensors to A0 and digital pin 2, respectively. We can use a 4.7kΩ pull-up resistor. The LCD display has normal wiring, the relay module is on digital pin 8, and the Wi-Fi module (ESP8266/ESP 32) has suitable connection pins.

The following table 2 describes the components list and their functionalities for connection.

Table 2. Components list for circuit diagram

Components	Connection
Current Sensor (ACS712)	Connected to Arduino's A0
Voltage Sensor (ZMPT101B)	Connected to Arduino's A1
Temperature Sensor (DS18B20)	Connected to Digital Pin 2 with a 4.7kΩ pull-up resistor
LCD Display	Connected according to standard wiring
Relay Module	Connected to Digital Pin 8
Wi-Fi Module (ESP8266) / ESP32	Connected to appropriate communication pins, ESP32 has built-in Bluetooth capacity with more GPIO pins

3.3 Software set up

This software displays current, voltage, and temperature on a real-time electric vehicle charging station. Additionally, it includes overcurrent protection, disconnecting the charging station if unsafe current levels are detected. The LCD screen displays all these crucial parameters, which are switched off to the charging relay as needed, and the readings update every second for real-time decision-making. This configuration is described as below [2] [15] [17] [23] [24] [26] [27] [29].

Hardware Configuration - sensor and control pins:

- Current sensor connected to analog pin A0
- Voltage sensor connected to analog pin A1
- Relay module connected to digital pin 8
- One-wire temperature sensor bus on digital pin 2
- Set maximum allowable current to 10.0A

Peripheral Initialization:

- Configure LCD display using pins 12 (RS), 11 (E), and 5-2 (D4-D7)
- Initialize one-wire communication protocol for temperature sensors

- Prepare Dallas Temperature sensor library for reading temperature data

Setup Routine:

- Initialize 16x2 LCD display with proper column/row configuration
- Configure relay pin as output device controller
- Establish serial communication at 9600 baud for debugging
- Start temperature sensor interface
- Ensure relay starts in OFF state (safety precaution)

Main Operation Loop

Sensor Readings:

- Measure current using analog-to-digital conversion (0-5V scaling)
- Measure voltage using similar ADC conversion
- Request and retrieve temperature data from DS18B20 sensor

Safety Protection

Implement overcurrent detection:

- If current exceeds 10A threshold: Disable relay output, Display "Overcurrent!" warning on LCD
- Else maintain relay activation

User Feedback:

- First LCD line: Show real-time current (A) and voltage (V)
- Second LCD line: Display temperature (°C) or overcurrent warning
- Refresh display every 1 second

Timing Control:

- Maintain 1-second interval between measurement cycles

3.4 Web Interface / Web Server set up

This is to set up a web server for remote monitoring and operation of the Electric Vehicle Charging Station (EVCS). This server will then use AJAX or Web Sockets to provide real-time charge, voltage, and current data without page reloads. Secure connectivity, user identification, and data logging make the EVCS more efficient and user-friendly. Yes, Flask (Python) or Node.js will be used to create the web server, ensuring smooth interaction and system management.

3.5 Smart Grid Integration

User engagement and payment simulation at smart EVCS can be improved by using an RFID-based or mobile app interface for authentication and processing payments. Arduino or Raspberry Pi can control simple payment verification systems, which are easy to use. Cloud data logging and IoT functionalities must also be used. An MQTT broker or RESTful API can log charging data like voltage, current, and time to the cloud. Then, a dashboard displays this data in real time to remotely monitor the charging station's operation and usage [2] [18] – [20] [23] [28] [30] [33] [39].

After setting up and demonstrating the Smart EVCS model, security implementation and testing will begin. This is possible by using a Rogue AP-based MITM attack against the system. The goal is to simulate a security compromise in user-EVCS communication.

4. Exploring the vulnerabilities of smart EVCS via Rogue AP base MITM

With the advent of electric cars, the technological designs of smart EVCS have become highly important. High-end technologies dependent on wireless communication are present here to facilitate easy charging at these centers. However, as the systems become integrated, so do their vulnerabilities, especially malicious attacks. Among these, Rogue AP based MITM attack is of the highest concern. Severely, this attack can compromise the integrity and security of the data in the charging infrastructure of both the users. [5] [18] [24] [25] [27] [31] [32]

- Weak Authentication Protocols

Many EVCS operate with antiquated or base authentication protocols. Such systems are pretty vulnerable to spoofing [5] [18] [24] [25] [27] [31] [32]. Some common vulnerabilities are:

Weak Passwords: Poor passwords that can be easily predicted.

No 2FA: The absence of a secondary authentication step makes it quite easy for an attacker to gain unauthorized entry [5] [18] [24] [25] [27] [31] [32].

- Unencrypted Communication Unencrypted communications pose a significant risk:

Plain Text Data Transmission: This can expose sensitive data to attackers in case it's not encrypted like in the case of TLS/SSL [5] [18] [24] [25] [27] [31] [32].

Vulnerability to Packet Sniffing: Tools such as Wireshark can capture unencrypted data packets hence sensitive information being transmitted is exposed [5] [18] [24] [25] [27] [31] [32].

- End-User Awareness and Education [24] [25] [27] [32].

The ignorance of the end-users leads to its major cause since;

Network Security: Most users do not know any danger in surfing through public networks they don't even know what their own network looks like [5] [18] [24] [25] [27] [31] [32].

User Finding Networks: Normally users connect to available networks without validating whether it's a legal or illegal service [5] [18] [24] [25] [27] [31] [32].

- Inadequate Security Practices by EVCS Operators

Outdated Software: Charging stations may operate on outdated firmware, lacking the essential security patches [5] [18] [24] [25] [27] [31] [32].

Limited Monitoring: A significant number of EVCS lack adequate monitoring systems to detect unauthorized access or anomalous activity [5] [18] [24] [25] [27] [31] [32].

There is a strong call for the implementation of robust security measures. Lack of proper authentication, inadequate encryption, user awareness, and operational security practices need to improve in order to enhance the security posture of the EVCS [5] [18] [24] [25] [27] [31] [32].

4.1 Rogue AP based MITM for Smart EVCS

To simulate and evaluate a Rogue Access Point-based Man-in-the-Middle attack on the Electric Vehicle Charging Station model, in which a hostile actor Rogue AP intercepts communications between the EVCS and authorised network users.

The requirements for installing an EVCS for testing and simulation are relatively high. On the hardware side, the Raspberry Pi or Arduino will act as the controller for the EVCS, while a Wi-Fi adapter (which might be built into the Raspberry Pi) is required to connect the station to the network. The simulation of the attacker's device can be obtained using a laptop or a PC. Another Wi-Fi adapter must be set up on the attacking device to set up the rogue access point. Furthermore, a battery or a power supply should be obtained to simulate the EV battery connected to the charging station. The EVCS software needs to be implemented on the Raspberry Pi or Arduino for charging, sensor measurement, and Wi-Fi communication [8]. The rogue AP software package may include aircrack-ng, ettercap, or hostapd [8] for configuring a rogue AP and starting MITM attacks. In addition, SSLStrip or Bettercap can be used during the attack to intercept and manipulate traffic, and while carrying out the attack, Wireshark will be useful in analysing and monitoring network traffic. The following table outlines the prerequisites for setting up Rogue AP in network [3]-[8] [12]-[15] [18] [25]–[27] [30] [31] [32] [39].

Practical Approach:

The scenario is designed for a lab setup where we create and execute a Rogue AP-based Man-MITM attack targeting Smart EVCS. The objective is to demonstrate the vulnerability of EVCS to wireless-based attacks, which can lead to data interception, manipulation, and even control of the charging infrastructure [2]-[9] [32].

1. Smart EVCS Network Installation

Step 1: Set up a test bed Wi-Fi network using either a real Access Point or an emulated Access Point.

SSID: *EVCS_Network*

Encryption: *WPA2*

Step 2: Connect the Smart EVCS units to the *EVCS_Network*.

Most of the Smart EVCS devices are equipped with Wi-Fi and send/ receive information from backend systems or mobile apps.

For example, a client device like an electric vehicle or an application in a smartphone would connect over Wi-Fi to charging stations and access the system for billing and monitoring purposes.

2. Creating the Rogue AP

Step 1: Configure a Rogue Access Point using airbase-ng or hostapd on a Kali Linux machine.

Objective: Broadcast the same SSID (*EVCS_Network*) to trick the EVCS devices and clients into connecting to the rogue AP instead of the legitimate network.

Tool setup:

airbase-ng -e EVCS_Network -c 6 wlan0mon or hostapd rogueap.conf

rogueap.conf will contain:

interface=wlan0

```
ssid=EVCS_Network
hw_mode=g
channel=6
macaddr_acl=0
auth_algs=1
wpa=2
wpa_key_mgmt=WPA-PSK
wpa_passphrase=EVCS_passphrase
```

Step 2: Enable IP forwarding and set up a NAT rule using iptables to route traffic between interfaces (rogue AP and legitimate network).

```
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -o wlan1 -j MASQUERADE
iptables -A FORWARD -i wlan0 -o wlan1 -j ACCEPT
```

Step 3: Run dnsmasq to deliver DHCP and DNS services to the associated Smart EVCS and clients.

This guarantees that devices linking to the Rogue AP get valid IP addresses and DNS resolution.

3. MITM Set up

Step 1: Use arpspoof to poison the ARP cache of the EVCS, causing it to send traffic through the attacker machine (Rogue AP).

```
arpspoof -i wlan0 -t [EVCS_IP] -r [Gateway_IP]
```

Step 2: Use sslstrip to downgrade HTTPS traffic to HTTP, making it easier to seize sensitive data.

```
sslstrip -l 8080
```

Step 3: Configure ettercap or mitmproxy to complete packet interference and manipulation.

Ettercap: Can intercept and log traffic, providing a full MITM experience.

```
ettercap -Tq -M arp:remote /[EVCS_IP]/ /[Gateway_IP]/
```

mitmproxy: A more modern proxy tool for intercepting and inspecting HTTPS traffic.

```
mitmproxy --mode transparent --showhost
```

4. Monitoring and Exploitation

Step 1: Utilise Wireshark to record network traffic and discern essential data, including authentication credentials, directives transmitted to the EVCS, or payment information.

```
wireshark -i wlan0
```

Step 2: Examine the communication to see if sensitive data, including payment information or control commands, is susceptible to interception.

If the EVCS system employs inadequate encryption or lacks it entirely, sensitive data, including billing information and EV instructions, can be readily accessed.

Step 3: Optionally, alter traffic in real-time. For instance, if the EVCS interacts with an application for billing purposes, adjust the communication to vary the charging cost or time.

5. Post-Attack Activities

Step 1: Disengage the EVCS and client from the unauthorised access point to prevent detection.

Step 2: Eliminate all logs or evidence of the unauthorised access point on the network.

Step 3: Record discoveries and traffic for analysis, particularly if this laboratory pertains to a penetration testing engagement.

6. Operating System

Kali Linux: The predominant operating system for penetration testing, equipped with essential tools for rogue access point and man-in-the-middle attacks.

7. Potential Attack Outcomes

Data Interception: Acquire sensitive information such as credentials, payment details, or session data.

Traffic Manipulation: Modify communications between the EVCS and client, potentially impacting invoicing or electric vehicle charging. Overwhelm the EVCS by transmitting faulty packets or by maintaining its disconnection from the authorised network.

The following figure describes the outline structured of MITM attack through Rogue AP on Smart EVCS

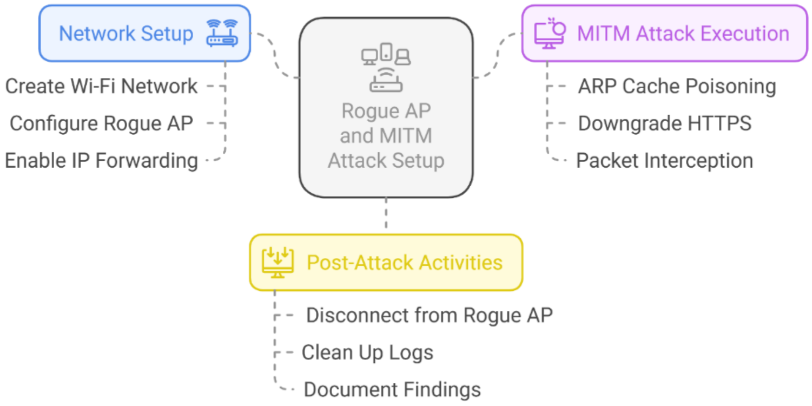

Figure 1. MITM attack through Rogue AP on Smart EVCS

The following image (Fig.1) depicts a real time scenario to perform NITM on an EVCS. The attacker hides the Rogue AP into the car and the other one is mounted on ceiling and performs a MITM and intercept the communication between the car and the station. The attacker can take control over, or manipulate the charging process of the vehicle, because the message says, "Your Car is Hacked". This captures security vulnerabilities in public EVCS infrastructure [5] [8] [17].

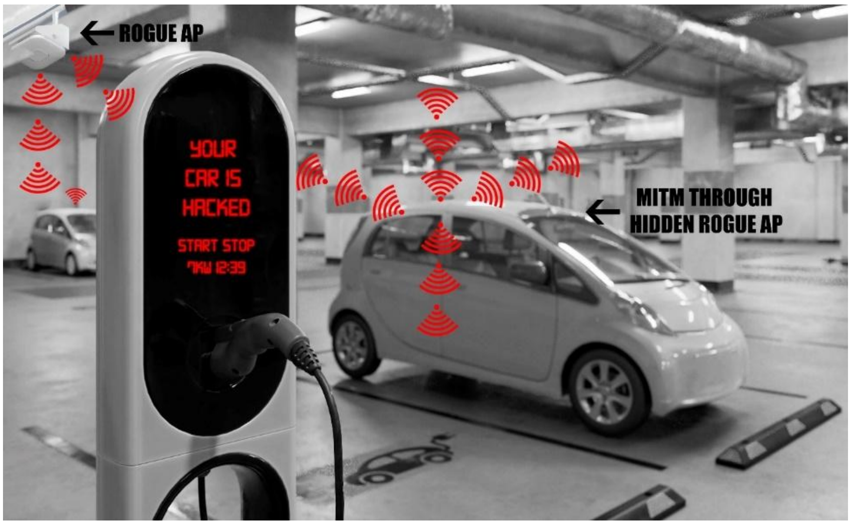

Figure 2. Real Time Scenario of MITM through Rogue AP

4.2 Consequences of Rogue AP based MITM on Smart EVCS

An MITM attack on an EVCS can have extensive and severe effects. It poses a major danger of financial fraud due to overcharging, undercharging, or theft of customer billing information for unauthorized activities. Since users rely on uninterrupted charging, halted, delayed, or changed charging sessions may disrupt operations. This would also damage the infrastructure since the improper power or charging time could damage the EVCS units or the automobiles under charging. Data theft is an attacker's top concern. They can take sensitive user data like credit card numbers, login credentials, and vehicle status, leading to identity theft or fraud. Finally, if such an attack goes public, it damages the EVCS provider or network's reputation, which could hurt business operations and client retention [5] [8] [11]-[14] [17] - [19] [21] [27].

Thus, Rogue AP based MITM attack against a smart EVCS may cause catastrophic damaging information theft, operational manipulations, and financial frauds. It will be a very disrupting kind of attack for both the users and the infrastructure provider, thus determining the importance of having strong security inside smart charging networks.

4.3 Use case: Ai powered MITM through Rogue AP on Smart EVCS

Next-level cyber risks include AI-powered MITM attacks on Smart EVCS via Rogue APs. AI can now adapt and optimize automated attacks, making data theft and operation manipulation easier and harder to detect. The methodologies, tools, technologies, AI basic fundamentals, and pseudocode for an AI-powered MITM on Smart EVCS using a Rogue AP are explained in full here. The following AI scenario greatly impacts Smart EVCS [16] [19] [22] [34] [35] [37].

Rogue AP-based MITM attacks can intercept and manipulate Smart EVCS, mobile apps, backend servers, and linked vehicles' network connection. By incorporating Artificial Intelligence (AI) into this assault, the opponent acquires the capability to:

- Automate the capture of critical information [16] [19] [22] [34] [35] [37].
- Evaluate and modify the assault in real-time [16] [19] [22] [34] [35] [37].
- Alter traffic to introduce harmful directives [16] [19] [22] [34] [35] [37].
- Avoid detection by network security measures, including Intrusion Detection Systems (IDS) [10] [28] [34] [35] [37].

This AI-driven assault focusses on the network layer of the EVCS infrastructure, leveraging its wireless communication protocols and backend interactions to impair functioning or seize control of charging sessions.

Use case:

A simulated MITM attack could show how AI could identify and alter traffic in real time, disrupting Smart EVCS operations. Attackers could disrupt services or exploit financial flaws by modifying sensitive commands or payment data. An attacker creates a Rogue AP and a Smart EVCS that employees or users may connect to. This lets the attacker intercept and alter EV, charging station, and backend network traffic [16] [19] [22] [26] [31] [34] [35] [37] [39].

It uses AI to detect sensitive packets including payment data, authentication tokens, and possibly "startCharging" or "stopCharging" control signals. All these packets can be changed in real time to make money, interrupt charging, or sabotage vehicles.

We showed real-time Rogue AP setup in the legitimate network above. When a device connects to this Rogue AP, the attacker will relay all EVCS-cloud or local backend server connection, allowing traffic eavesdropping and manipulation. Below is the rest of the scenario:

Network Traffic Sniffing

- The attacker uses a packet sniffer such as Wireshark or tcpdump to capture the traffic exchanged between the EV and the charging station [16] [19] [22] [26] [31] [34] [35] [37] [39].
- The goal here is to:

Identify the specific packets such as payment authorization, charging commands, or session management tokens [2] [5] [6] [16] [19] [22] [26] [31] [34] [35] [37] [39].

Analyze this traffic using AI and automate it [2] [16] [19] [22] [26] [31] [34] [35] [37] [39].

AI-Based Traffic Categorization

Using AI-based tools, the attacker will now begin real-time auto-classification of the packets to obtain sensitive information. This can be done by:

- Machine Learning Model: The model learns to identify traffic patterns that correspond with payment data, charging commands, or session tokens [5] [6] [16] [19] [22] [26] [31] [34] [35] [37] [39].
- The size of the packet, protocol type, destination port, and payload data may be characteristics that make sensitive packets different from general traffic. For example, payment transactions differ from HTTP requests [5] [6] [16] [19] [22] [26] [31] [34] [35] [37] [39].

Sensitive packets have been recognized. In this case, the attacker manipulates the data in.

- Charging Commands: AI can detect "startCharging" and sends it as "stopCharging," and the car will not charge at all.
- Payment Data: AI recognizes the packet holding the amount to charge and changes the amount owed (for instance, from $10 to $1).

- Authentication Tokens: AI detects tokens for sessions and stores them for use in subsequent functions in order to provide access to control over the session for charging.

In Real Time Packet Manipulation:

After the identification of the sensitive packets by the attacker, they manipulate those packets in real time. Some examples of this are:

- Billing Fraud: Modify the payment packet to reduce the billing amount from perhaps $20 to $1 and pay to charge your car at almost no cost [5] [6] [16] [19] [22] [26] [31] [34] [35] [37] [39].
- Charging Sabotage Control: Find a charging command in a packet and change it to "stopCharging". This prevents allowing the EV to charge or generates additional disruptions [5] [6] [16] [19] [22] [26] [31] [34] [35] [37] [39].
- Session Hijacking: The attacker uses captured session tokens to hijack an ongoing session and impersonate the user, remotely assuming control of the charging process [5] [6] [16] [19] [22] [26] [31] [34] [35] [37] [39].

Session Hijacking for Further Exploitation

An attacker can use the session tokens (captured by AI):

- Controlling User Accounts: Obtain unauthorized access to user accounts to initiate or pause charging sessions, change billing preference or view personal data stored in the backend. [5] [6] [16] [19] [22] [26] [31] [34] [35] [37] [39]
- Compromise Charging Stations: The attacks may execute malicious commands directly on the EVCS infrastructure, with the intention of damaging or simply making the station inoperable. [5] [6] [16] [19] [22] [26] [31] [34] [35] [37] [39]

Here's a small program simulating an AI-powered Man-in-the-Middle (MITM) attack on an Electric Vehicle Charging Station (EVCS). This program is intended for educational purposes only and demonstrates how AI could be used to classify and manipulate network traffic. The example focuses on recognizing a specific "startCharging" command and altering it to "stopCharging" in real-time, showcasing how AI could be used for packet manipulation.

The AI model automatically classifies the sensitive data, and the attacker will manually define how to manipulate that data once detected.

5. Future Enhancement and Mitigation Activities

As AP and AI-powered MITM attacks are advanced, several potential security improvements to protect EVCS, as well as their communications, are enumerated as follows:

AI-Powered IDSs:

Use AI and machine learning to detect anomalous traffic patterns and rogue AP behavior, making stealthy MITM attacks smarter [5] [6] [16] [19] [22] [26] [28] [31] [34] [35] [37] [39].

Dynamic Certificate Pinning:

Only trusted servers must be contacted by EVs and EVCS, utilizing pinned SSL/TLS certificates, ensuring that rogue AP or untrusted sources will not be able to connect [5] [6] [16] [19] [22] [26] [28] [31] [34] [35] [37] [39].

Behavior-Based Device Authentication:

Analyze user and device behavior to detect anomalies and prevent suspicious behavior, for example unauthorized connection or session hijacking [5] [6] [16] [19] [22] [26] [28] [31] [34] [35] [37] [39].

Quantum-Resistant Encryption:

Deploy encryption algorithms, which are resistant against quantum computing attacks, to protect communications of the EVCS from future AI-driven decryption attempts [5] [6] [16] [19] [22] [26] [28] [31] [34] [35] [37] [39].

Wireless Spectrum Monitoring & AP Fingerprinting:

RF fingerprinting shall continuously monitor the wireless spectrum of all devices to identify and prevent rogue APs whose function is to masquerade as legitimate networks [5] [6] [16] [19] [22] [26] [28] [31] [34] [35] [37] [39].

Mutual Multi-Factor Authentication:

EVs paired with a charging station must render mutual multi-factor authentication, thus eliminating any unauthorized access and connection [5] [6] [16] [19] [22] [26] [28] [31] [34] [35] [37] [39].

Blockchain-Based Authentication:

Leaning on blockchain as a foundation, make an authentication system that is distributed and tamper-proof, so it is the devices and also the EVCS that interact securely in the most transparent way.

Real-Time Packet Integrity Verification:

Introduce cryptographic signatures to the packets flowing in the network so that any changes occurring during transmission are rejected and not accepted [5] [6] [16] [19] [22] [26] [28] [31] [34] [35] [37] [39].

Network Segmentation and Isolation:

Critical operations of an EVCS are isolated into separated network segments, and chances of attacking surfaces are reduced since the access is limited. Rogue AP and AI-based MITM attacks in the future on the EVCS systems become much more complicated [5] [6] [16] [19] [22] [26] [28] [31] [34] [35] [37] [39].

6. Conclusion

This study examines the growing need for EVCS in urban infrastructure and cybersecurity concerns, particularly MITM attacks and Rogue Access Points. It provides real experiments on how an attacker might intercept and manipulate user-EVCS communication. AI automates and optimises MITM attacks, increasing their threat level, according to the research. Since the conclusion emphasises the necessity for better encryption, anomaly detection, and user awareness to prevent these cybersecurity attacks, this is especially true. This research develops more resilient EVCS infrastructures to provide security and better integration into the smart urban ecosystem through rigorous testing and simulation attacks. Naturally, this research calls for immediate mitigation of these cyber vulnerabilities to protect the developing electric vehicle sector and its infrastructure.

References

1. Yahoo! (n.d.). Ev charging station market worth $12.1 billion by 2030 – exclusive report by MarketsandMarketsTM. Yahoo! Finance. https://finance.yahoo.com/news/ev-charging-station-market-worth-233000480.html

2.Electric vehicle charging infrastructure ... (n.d.). https://www.niti.gov.in/sites/default/files/202108/HandbookforEVChargingInfrastructureImplementation081221.pdf

3. Patel, K. C., & Patel, A. (2022, November). Rogue access point: The WLAN threat. In 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 943-950). IEEE.

4. Patel, K. C., & Patel, A. (2022, March). Taxonomy and future threat of rogue access point for wireless network. In 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 679-688). IEEE.

5. Patel, K. C., & Goswami, S. A. (2024). Rogue Access Points: A Critical Threat to Electric Vehicle Charging Station Security. COMPUTER, 24(7).

6. Patel, Dr. K. C. (2024). International Journal of Scientific Research in computer science, engineering and information technology. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(3), 632–643. https://doi.org/10.32628/ijsrcseit

7. Patel, Dr. K. C. (2022). RECOGNITION OF ROGUE ACCESS POINTS USING A MACHINE LEARNING APPROACH. INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS - IJCRT (IJCRT.ORG), 10(12), C663–C672. https://ijcrt.org/papers/IJCRT2212283.pdf

8. Chaitanyakumar, P. K. An Experimental Study and Novel Approach for Detection and Suppression of Rogue Access Point in Wlan.

9. Purohit, S., & Govindarasu, M. (2024, July). FL-EVCS: Federated Learning based Anomaly Detection for EV Charging Ecosystem. In 2024 33rd International Conference on Computer Communications and Networks (ICCCN) (pp. 1-9). IEEE.

10. ElKashlan, M., Aslan, H., Said Elsayed, M., Jurcut, A. D., & Azer, M. A. (2023). Intrusion detection for electric vehicle charging systems (evcs). Algorithms, 16(2), 75.

11. Attanasio, L., Conti, M., Donadel, D., & Turrin, F. (2021, May). MiniV2G: an electric vehicle charging emulator. In Proceedings of the 7th ACM on Cyber-Physical System Security Workshop (pp. 65-73).

12. MEKKAOUI, K. (2024). Enhancing V2G Network Security: A Novel Cockroach Behavior-Based Machine Learning Classifier to Mitigate MitM and DoS Attacks. Advances in Electrical & Computer Engineering, 24(2).

13. Aljohani, T., & Almutairi, A. (2024). A comprehensive survey of cyberattacks on EVs: Research domains, attacks, defensive mechanisms, and verification methods. Defence Technology.

14. Nasr, T. (2021). Large-Scale Study of Internet-Connected Electric Vehicle Charging Station Management Systems: Discovery, Security Analysis and Mitigation (Doctoral dissertation, Concordia University).

15. Dehrouyeh, Fatemeh, Li Yang, Firouz Badrkhani Ajaei, and Abdallah Shami. "On TinyML and Cybersecurity: Electric Vehicle Charging Infrastructure Use Case." arXiv preprint arXiv:2404.16894 (2024).

16. Basnet, M. (2022). Deep Learning-Powered Computational Intelligence for Cyber-Attacks Detection and Mitigation in 5G-Enabled Electric Vehicle Charging Station. The University of Memphis.

17. ElHussini, H. (2020). The Count of EV Charging: Attacking, Mitigating and Re-envisioning the Infrastructure (Doctoral dissertation, Concordia University).

18. Ojha, N. K., Pandita, A., & Vaish, A. (2024). Cyber-security challenges for artificial intelligence-empowered electric vehicles—analysis and current status. Artificial Intelligence-Empowered Modern Electric Vehicles in Smart Grid Systems, 317-346.

19. Jahangir, H., Lakshminarayana, S., & Poor, H. V. (2024). Charge Manipulation Attacks Against Smart Electric Vehicle Charging Stations and Deep Learning-based Detection Mechanisms. IEEE Transactions on Smart Grid.

20. Developing a Security Metric for Assessing the Power Grid's Posture Against Attacks From EV Charging Ecosystem

21. Nasr, T., Torabi, S., Bou-Harb, E., Fachkha, C., & Assi, C. (2022). Power jacking your station: In-depth security analysis of electric vehicle charging station management systems. Computers & Security, 112, 102511.

22. Basnet, M., & Ali, M. H. (2021). Exploring cybersecurity issues in 5G enabled electric vehicle charging station with deep learning. IET Generation, Transmission & Distribution, 15(24), 3435-3449.

23. Purohit, S., & Govindarasu, M. (2023, November). Cybersecurity Investment Analysis for Electric Vehicle Charging Infrastructures. In 2023 Resilience Week (RWS) (pp. 1-6). IEEE.

24. Sarieddine, K., Sayed, M. A., Torabi, S., Attallah, R., Jafarigiv, D., Assi, C., & Debbabi, M. (2024, July). Uncovering Covert Attacks on EV Charging Infrastructure: How OCPP Backend Vulnerabilities Could Compromise Your System. In Proceedings of the 19th ACM Asia Conference on Computer and Communications Security (pp. 977-989).

25. Hamdare, S., Kaiwartya, O., Aljaidi, M., Jugran, M., Cao, Y., Kumar, S., ... & Lloret, J. (2023). Cybersecurity risk analysis of electric vehicles charging stations. Sensors, 23(15), 6716.

26. Sarieddine, K. (2024). Bolstering EV Charging Ecosystem Infrastructure Resilience and Unraveling Threats-A Comprehensive Study (Doctoral dissertation, Concordia University).

27. Skarga-Bandurova, I., Kotsiuba, I., & Biloborodova, T. (2022, December). Cyber security of electric vehicle charging infrastructure: Open issues and recommendations. In 2022 IEEE International Conference on Big Data (Big Data) (pp. 3099-3106). IEEE.

28. Mekkaoui, K., Mekour, M., & Teggar, H. (2024). Securing Vehicle-to-Grid Networks: A Bio-Inspired Intrusion Detection System. Scientia Iranica.

29. Islam, S., Badsha, S., Sengupta, S., Khalil, I., & Atiquzzaman, M. (2022). An intelligent privacy preservation scheme for ev charging infrastructure. IEEE Transactions on Industrial Informatics, 19(2), 1238-1247.

30. Ahalawat, A., Adepu, S., & Gardiner, J. (2022, October). Security threats in electric vehicle charging. In 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) (pp. 399-404). IEEE.

31. Basnet, M., & Ali, M. H. (2023, July). Deep-Learning-Powered Cyber-Attacks Mitigation Strategy in the EV Charging Infrastructure. In 2023 IEEE Power & Energy Society General Meeting (PESGM) (pp. 1-5). IEEE.

32. Zografopoulos, I., Hatziargyriou, N. D., & Konstantinou, C. (2023). Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. IEEE Systems Journal.

33. Sayed, M. A., Ghafouri, M., Debbabi, M., & Assi, C. (2022, July). Dynamic load altering EV attacks against power grid frequency control. In 2022 IEEE Power & Energy Society General Meeting (PESGM) (pp. 1-5). IEEE.

34. Bibi, I., Akhunzada, A., & Kumar, N. (2022). Deep AI-powered cyber threat analysis in IIoT. IEEE Internet of Things Journal, 10(9), 7749-7760.

35. Gürfidan, R., Ersoy, M., & Kilim, O. (2022, May). AI-powered cyber attacks threats and measures. In The International Conference on Artificial Intelligence and Applied Mathematics in Engineering (pp. 434-444). Cham: Springer International Publishing.

36. Mehra, A., & Badotra, S. (2021, October). Artificial Intelligence Enabled Cyber Security. In 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC) (pp. 572-575). IEEE.

37. Marshell, M. J., & Jeyaraj, K. A. (2024, August). Securing Vehicle-to-Everything (V2X) Communication in AI-Empowered Electric Vehicles. In 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) (pp. 151-158). IEEE.

38. Dhiman, D., Bisht, A., Thakur, G., & Garg, A. (2025). Artificial Intelligence and Machine Learning-Enabled Cybersecurity Tools and Techniques. In Advanced Techniques and Applications of Cybersecurity and Forensics (pp. 35-56). Chapman and Hall/CRC.

39. Cai, M., Wu, Z., & Zhang, J. (2014, November). Research and prevention of rogue ap based mitm in wireless network. In 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (pp. 538-542). IEEE.

40. Köhler, S., Baker, R., Strohmeier, M., & Martinovic, I. (2022). Brokenwire: Wireless disruption of ccs electric vehicle charging. arXiv preprint arXiv:2202.02104.

41. Conti, M., Donadel, D., Poovendran, R., & Turrin, F. (2022, September). Evexchange: A relay attack on electric vehicle charging system. In European Symposium on Research in Computer Security (pp. 488-508). Cham: Springer International Publishing.

42. Zhou, C., Yan, Q., Yu, Z., Dixit, E., Zhang, N., Zeng, H., & Ghanhdari, A. S. (2023). ChargeX: Exploring State Switching Attack on Electric Vehicle Charging Systems. arXiv preprint arXiv:2305.08037.

43. Ganesan, S., Patel, D. K., & Chokhalingam, R. (2024). Security of Electric Vehicle Charging Stations. International Journal of Electrical and Computer Engineering Research, 4(4), 1-7.

44. Wlazlo, P., Sahu, A., Mao, Z., Huang, H., Goulart, A., Davis, K., & Zonouz, S. (2021). Man-in-the-middle attacks and defence in a power system cyber-physical testbed. IET Cyber-Physical Systems: Theory & Applications, 6(3), 164-177.

45. Banik, S., Banik, T., Hossain, S. M., & Saha, S. K. (2023, June). Implementing man-in-the-middle attack to investigate network vulnerabilities in smart grid test-bed. In 2023 IEEE World AI IoT Congress (AIIoT) (pp. 0345-0351). IEEE.