IEEE Internet of Things Journal, vol.12, no.19, pp.39689-39700, October, 2025.

MitM Attack to Electric Vehicle AC Chargers

J. Jarauta Gastelu; R. Gesteira Miñarro; J. Matanza Domingo; R. Palacios Hielscher; G. López López

Abstract-

This paper explores a Man-in-the-Middle (MitM) attack targeting AC charging points for electric vehicles (EVs), demonstrating the ability to covertly control the vehicle’s charging process without detection by either the charging station or the vehicle. The attack was conducted successfully in both controlled laboratory environments and real-world settings, exposing vulnerabilities in the communication protocols between the charging station and the vehicle. By intercepting and manipulating the communication, an attacker can adjust the charging rate, reducing, increasing, or halting the charging process altogether. This not only affects individual vehicles but could have a broader impact on the electrical grid, especially as the use of high-power EV chargers continues to grow. With the rapid increase in electric vehicle adoption worldwide, the potential for synchronized attacks on multiple charging points presents a significant risk to grid stability, from local affections to higher widespread impacts. This research then underscores the need for stronger cybersecurity measures to protect the charging infrastructure and prevent large-scale disruptions to energy systems.

Index Terms- Electric Vehicles, AC Charging, Man-in-the Middle, Cybersecurity

Citation:
Jarauta Gastelu, J.; Gesteira-Miñarro, R.; Matanza, J.; Palacios, R.; López, G. "MitM Attack to Electric Vehicle AC Chargers", IEEE Internet of Things Journal, vol.12, no.19, pp.39689-39700, October, 2025.