# Cybersecurity for Electric Vehicle Fast-Charging Infrastructure

## Preprint

Anuj Sanghvi and Tony Markel

*National Renewable Energy Laboratory*

*Presented at the IEEE Transportation Electrification Conference and Expo (ITEC)*
*June 21-25, 2021*

**NREL is a national laboratory of the U.S. Department of Energy**
**Office of Energy Efficiency & Renewable Energy**
**Operated by the Alliance for Sustainable Energy, LLC**

**Conference Paper**
NREL/CP-5R00-75236
July 2021

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

# Cybersecurity for Electric Vehicle Fast-Charging Infrastructure

## Preprint

Anuj Sanghvi and Tony Markel

*National Renewable Energy Laboratory*

### Suggested Citation

Sanghvi, Anuj and Tony Markel. 2021. *Cybersecurity for Electric Vehicle Fast-Charging Infrastructure: Preprint*. Golden, CO: National Renewable Energy Laboratory. NREL/CP-5R00-75236. https://www.nrel.gov/docs/fy21osti/75236.pdf.

**NREL is a national laboratory of the U.S. Department of Energy**
**Office of Energy Efficiency & Renewable Energy**
**Operated by the Alliance for Sustainable Energy, LLC**

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

**Conference Paper**
NREL/CP-5R00-75236
July 2021

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

## NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Vehicle Technologies Office. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

*Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.*

NREL prints on paper that contains recycled content.

# Cybersecurity for Electric Vehicle Fast-Charging Infrastructure

Anuj Sanghvi Tony Markel
National Renewable Energy Laboratory
Denver, CO USA
Anuj.Sanghvi@nrel.gov Tony.Markel@nrel.gov

***Abstract*-The integration of electric vehicles (EVs) into electric grid operations can potentially leave the grid vulnerable to cyberattacks from both legacy and new equipment and protocols, including extreme fast-charging infrastructure. This paper introduces a co-simulation platform to perform cyber vulnerability analysis of EV charging infrastructure and its dependencies on communications and control systems. Grid impact scenarios through linkages to power system simulation tools such as OpenDSS and vehicle infrastructure-specific attack paths are discussed. An adaptive platform that assists with predicting and solving evolving cybersecurity challenges is demonstrated with a cyber-energy emulation that accelerates the analysis of cyberattacks and system behavior.**

## I. Introduction

Electric vehicle (EV) development and associated charging infrastructure are expected to advance rapidly. Thirty percent of all global vehicle sales may be EVs and hybrid EVs by 2025 [1], and they will rely on increasingly sophisticated strategies for grid integration. Next-generation EV charging infrastructure is expected to include interconnected renewable resources, such as photovoltaic (PV) arrays and battery storage systems, along with grid-edge devices. Although distributed energy resources (DERs) are useful in several ways, such as peak shaving at high demand times and backup supply for added resilience, the integration of vehicle charging and DERs could create more avenues for cyberattack. This paper examines potential cybersecurity challenges that could disrupt the grid through both legacy and new extreme fast-charging (xFC) EV infrastructure. The paper also introduces a Cyber-Energy Emulation (CEE) Platform that can simulate and visualize the consequences of an attack on power system devices, EV chargers, operators, and cloud servers.

## II. Current EV-Grid Connection and Risks for Cyberattacks

### A. Risks of Physical and Network Access to EVs

Cybersecurity assessments conducted on electric utilities across the United States demonstrate how legacy devices, communications protocols, and insecure applications can combine to form a weak cybersecurity posture [2], [3]. Physical and/or remote access to EV charging station components, including charge ports, power electronics, controllers, and local generation (e.g., PV and energy storage) could be paths to cause power fluctuations, leading to altered operations at the charging station, escalated privileges to administrative systems, exfiltration of financial information (including personally identifiable information), and reduced grid stability [4], [5]. One compromised EV supply equipment component can open the door to a variety of exploitable vulnerabilities [6]. Cloud computing and mobile application control have the potential to expand the threat surface to non-redupiation and firmware integrity challenges.

Vendor clouds have access to hundreds of chargers, and if compromised, can scale the attack surface exponentially. The high power and voltage levels of xFC infrastructure (e.g., 400 kW at 1000-V DC) increase the hazards and ability to impact the grid and vehicles more than lower-power charging systems. Legacy communications systems and protocols could also put EV infrastructure at risk of cyberattacks requiring a robust patch management process. Communications networks link EVs and chargers to several stakeholders—including charging station operators, grid operators, vendors/manufacturers, and aggregators—who have both physical and network access to share information for control, monitoring, and analytics [7]. Information in these networks that is vulnerable to compromise includes the state of charge, charging duration, payment information, electricity price, and load control [8]. Analyzing and prioritizing these interconnections risks could help address cybersecurity related to data leakage and manipulation.

### B. Risks of xFC Cyber-Physical Architecture for EVs

Fig. 1 introduces a notional depiction of the communications nodes used in current and future xFC infrastructure. It also denotes the variety of standards and protocols currently in use. Fig. 1 brings awareness to the breadth of entry pathways to the system that could potentially provide access and manipulation, leading to system disruption. The figure attempts to resolve the complexities of DERs, connections to legacy grid components and vendor clouds, charging network operators, and aggregators, with some interactions feeding into advanced distribution management system platforms. Insecure implementation of protocols with legacy systems make the next generation of xFC infrastructure susceptible to cyberattacks. xFC and existing DC charging methods require critical communications between an EV and the charging infrastructure to coordinate charging voltage and current settings. Unlike AC charging, this communication creates a potential vulnerability because the onboard charge controller must communicate important battery constraints to the offboard battery charger for control action.

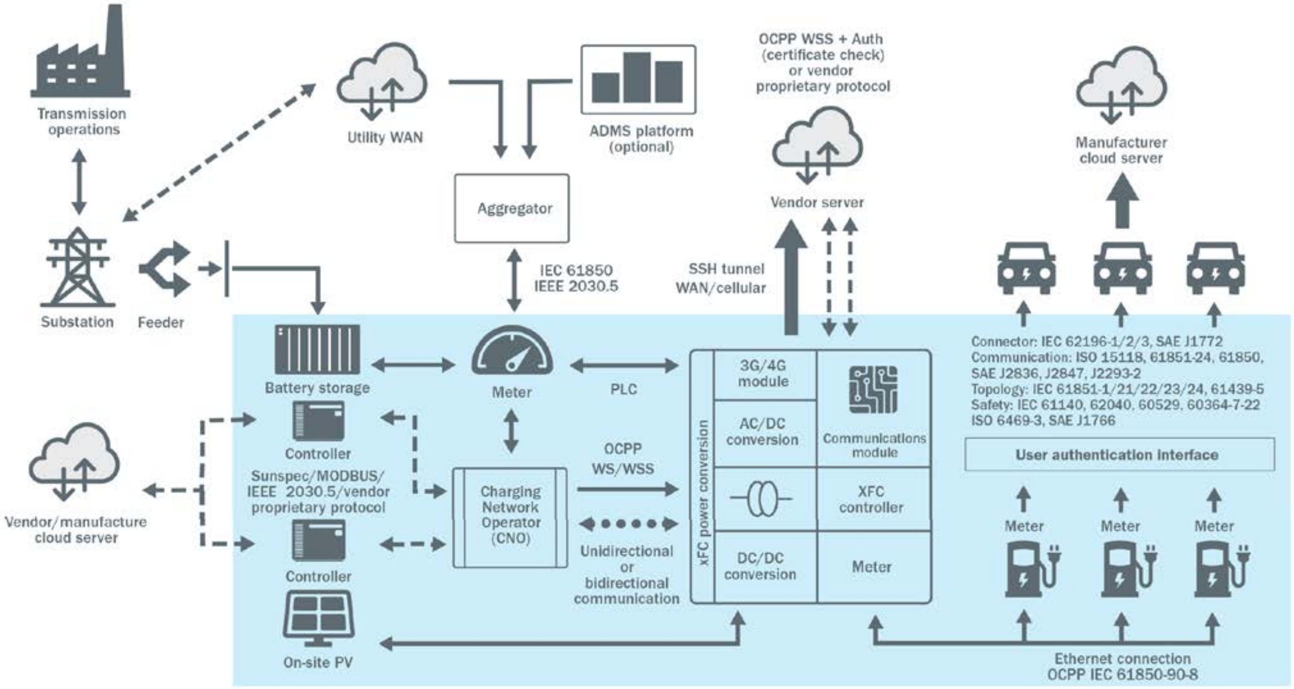

Transmission operations
Utility WAN
ADMS platform (optional)
OCPP WSS + Auth (certificate check) or vendor proprietary protocol
Manufacturer cloud server
Aggregator
Vendor server
Substation
Feeder
IEC 61850
IEEE 2030.5
SSH tunnel WAN/cellular
Connector: IEC 62196-1/2/3, SAE J1772
Communication: ISO 15118, 61851-24, 61850, SAE J2836, J2847, J2293-2
Topology: IEC 61851-1/21/22/23/24, 61439-5
Safety: IEC 61140, 62040, 60529, 60364-7-22
ISO 6469-3, SAE J1766
Battery storage
Meter
PLC
3G/4G module
AC/DC conversion
Communications module
xFC power conversion
XFC controller
DC/DC conversion
Meter
User authentication interface
Controller
Sunspec/MODBUS/ IEEE 2030.5/vendor proprietary protocol
Charging Network Operator (CNO)
OCPP WS/WSS
Unidirectional or bidirectional communication
Vendor/manufacture cloud server
Controller
Meter
Meter
Meter
On-site PV
Ethernet connection OCPP IEC 61850-90-8

Fig. 1. Through industry engagement, this communications architecture figure was developed to identify the majority of specific communications standards, interconnections, control elements, and connections to the grid of an xFC infrastructure [9].

## III. A Power and Communications Co-simulation and Emulation Platform

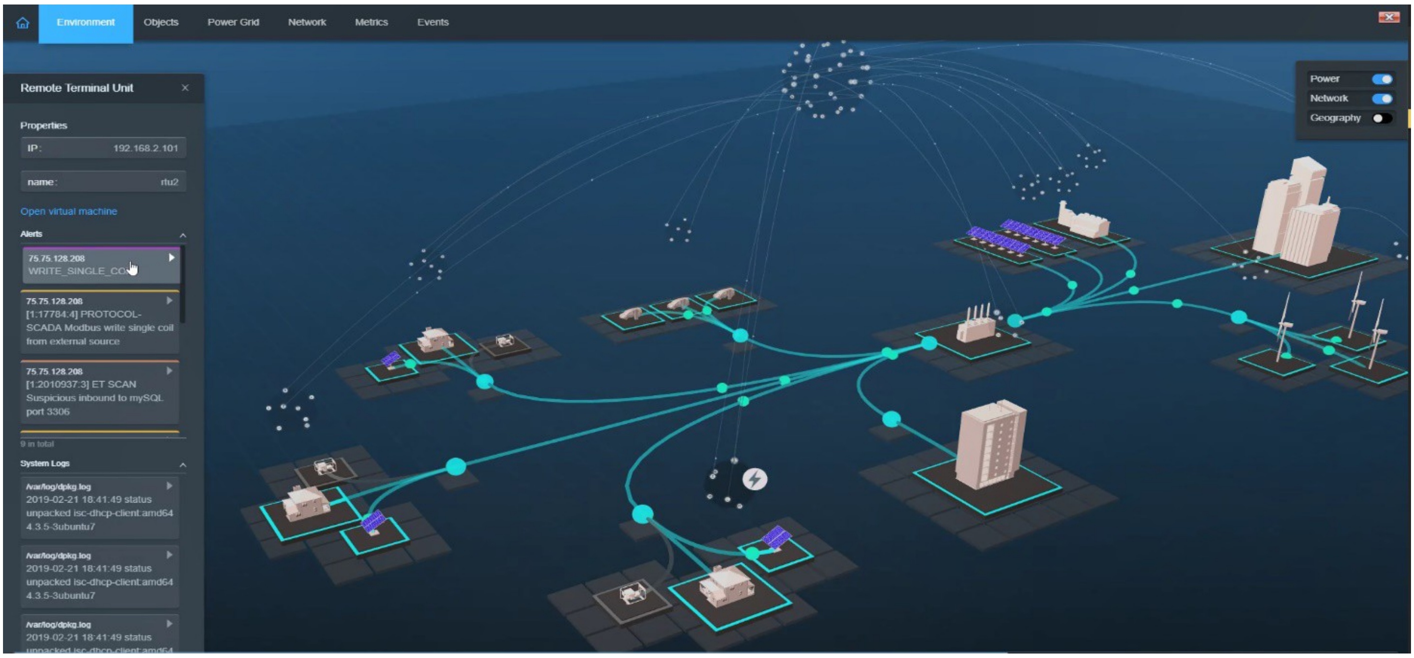
The National Renewable Energy Laboratory (NREL) staff has designed the CEE Platform, a unique, open-source set of technologies, to capture both the power system and networking components of an EV charging infrastructure interacting with the grid as well as DERs that could be manipulated to cause a system disturbance.

### A. *ØMQ and protobuf*

Researchers use a ZeroMQ (ØMQ) + publish/subscribe model and protobuf to simulate power systems and emulate networks for cyber analysis and testing. In the context of the virtualized environment, message queues are used for inter-process communications that enable the transfer of control, content, or data.

- ØMQ is a high-performance, asynchronous messaging library for applications that require concurrent processes to run. The ØMQ sockets represent a many-to-many connection between end points and require messaging patterns such as request/reply, publish/subscribe, push/pull, and exclusive pair. Specifically of interest here is the message pattern of publish/subscribe, in which the message sender has no knowledge of the receiver; this message pattern categorizes published messages into classes. Similarly, a subscriber expresses interest in one or more classes and only receives messages from classes without the knowledge of the publisher or sender of the message. The ØMQ library application programming interface is designed to represent these sockets [10]. This library provides various functions such as (a) ØMQ Context, which keeps the list of sockets and manages the asynchronous I/O threads and internal queries; (b) ØMQ Messages, which are discrete units of data passed between applications or components of the same application; and (c) ØMQ Sockets, which present an abstraction of an asynchronous message queue with the exact queuing semantics [11]. Depending on functions of the end points, they either publish or subscribe to messages that are handled by the ØMQ sockets.

- Protobuf is a protocol buffer core technology, described as a language- and platform-neutral, extensible way of serializing structured data for use in communication protocols [12]. In our approach, protocol buffers are used in developing programs that communicate with each other over a wire. Although ØMQ provides a connection for Device A to Device B, structured data in a defined format of protobuf are added to that connection to send messages [12]. This combination provides a reliable backbone for the overlying technologies to interact.



Remote Terminal Unit

Properties

IP: 192.168.2.101

name: rtu2

Open virtual machine

Alerts

```
75.75.128.208
WRITE_SINGLE_CO

75.75.128.208
[1:17784:4] PROTOCOL-SCADA Modbus write single coil from external source

75.75.128.208
[1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306
```

9 in total

System Logs

```
/var/log/dpkg.log
2019-02-21 18:41:49 status unpacked isc-dhcp-client:amd64 4.3.5-3ubuntu7

/var/log/dpkg.log
2019-02-21 18:41:49 status unpacked isc-dhcp-client:amd64 4.3.5-3ubuntu7

/var/log/dpkg.log
2019-02-21 18:41:49 status
unpacked isc-dhcp-client:amd64
```

Fig. 2. NREL's Cyber-Energy Emulation Platform. The green lines denote power flow exchanges of OpenDSS, and the white lines above them represent communications between virtual nodes in minimega.

### B. *minimega*

The devices within an electric grid can be emulated using virtual machines that run programs similar to the applications found in an industrial control system device [13]. These devices are emulated inside virtual machines and can communicate with each other via sockets and virtual networks. The publisher/subscriber [14] model or broker/provider model can be used to provide communications between virtual machines and other platforms, such as the open-source Distributed Systems Simulator (Open DSS). Minimega was developed by Sandia National Laboratories to emulate a network of devices with a power layer represented within OpenDSS. Virtualization in this case provides the ability to represent and simulate a system from a very small scale (10 nodes) to an extremely large scale (thousands to millions of nodes) with the assumption of adequate computational power.

### C. *Running the CEE Platform*

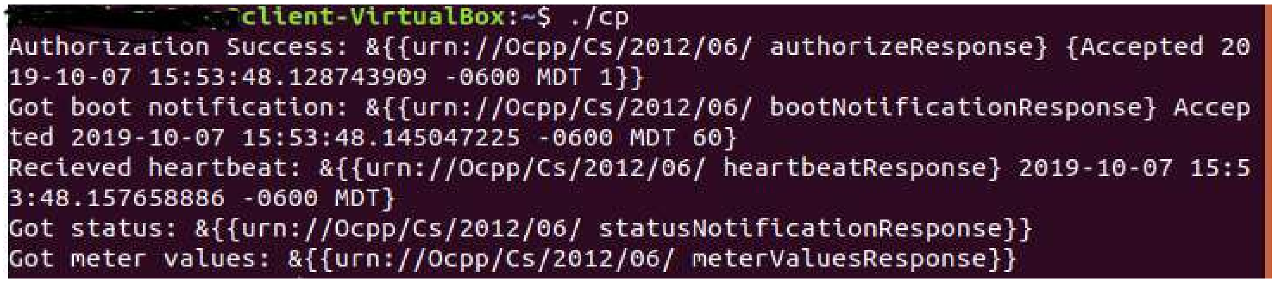
Fig. 2 is a Web-browser-based, visual 3D representation of communications and power flow layers. ØMQ's messaging bus and protobuf's data structure, along with minimega, come together at this application-level interface to visualize consequences of attacks on electric power systems. The CEE Platform uses OpenDSS models to simulate grid operations. Details of charging stations that have PV arrays on-site, combined with battery storage to act as backup or a peak-shaving resource, are the current focus of the CEE Platform enhancements, along with infrastructure-specific threats. Simulated power systems devices can then be tested for cyber analysis, along with EV chargers, operators, and manufacturer cloud servers running firmware and applications, which are implemented using standard protocols [2].

### D. *Real-Time Attack Analysis and Test Cases*

Within the CEE Platform, the key research focus is a cyberattack on the communications medium between the charger and central energy management system. A commonly used communications method for EV infrastructure interoperability is the Open Charge Point Protocol (OCPP), an open-application layer protocol defined to enable multivendor charger communications.

The OCPP communication can be implemented as a client-server model, with a charger or charge point as the client and a central management system as the server. Simulating OCPP communications is a way to understand and explore potential outcomes to message manipulation. Multiple messages within the protocol are initiated either by the charger or by the central system [15].

Fig. 3 depicts the operation of a simulated charge point and the messages it sends/receives. Using a Go implementation of the OCPP1.5 and OCPP1.6J [16], a basic OCPP client-server model was built to exchange OCPP messages. This basic setup can be used for cyber tests, such as man-in-the-middle or denial-of-service attacks, by manipulating data in transit or by spoofing the identity of either the client or the server [17].



```
[redacted]client-VirtualBox:~$ ./cp
Authorization Success: &{{urn://Ocpp/Cs/2012/06/ authorizeResponse} {Accepted 20
19-10-07 15:53:48.128743909 -0600 MDT 1}}
Got boot notification: &{{urn://Ocpp/Cs/2012/06/ bootNotificationResponse} Accep
ted 2019-10-07 15:53:48.145047225 -0600 MDT 60}
Recieved heartbeat: &{{urn://Ocpp/Cs/2012/06/ heartbeatResponse} 2019-10-07 15:5
3:48.157658886 -0600 MDT}
Got status: &{{urn://Ocpp/Cs/2012/06/ statusNotificationResponse}}
Got meter values: &{{urn://Ocpp/Cs/2012/06/ meterValuesResponse}}
```

Fig. 3. Simulated OCPP client or charge point with message exchanges. Examples of messages received from the server or central system are Authorization, Boot Notification, Heartbeat, Status, and Meter Values.

Even though the OCPP implementation of each manufacturer will have a different method of deployment, the purpose of this experimental setup is to focus initially on the threats associated with an OCPP architecture [18]. Combining the central management system and charge point communications with the CEE Platform's power systems communications introduces a novel platform to test risks and the resilience of the future xFC system. Further revisions to the system representations could address standard protocols, including OCPP and ISO 15118, along with proprietary approaches. The ability to visualize and analyze consequences of responses caused by anomalies to cyber-physical systems through cyber events presents a path toward a more secure and resilient charging infrastructure.

## IV. Conclusions and Implications

Billions of dollars are expected to be invested during the coming decade to implement EV charging infrastructure, much of which will likely support xFC rates in the 350-kW range [19]. These stations could include on-site PV and energy storage to aid with demand charge mitigation and enhance station value proposition as the EV market matures over time. This paper described a robust emulation environment, including its foundational components: minimega, ØMQ, protobuf, OpenDSS, and the innovative CEE Platform. Initial work on EV infrastructure is simple in representation; however, the platform enables scalability to address future analytic needs along with safety and interoperability. The work presented here considers attacks on the OCPP communications pathway. Future studies will address vulnerabilities in additional protocols, including Modbus, Controller Area Network, and Distributed Networking Protocol 3. Continued research of cybersecurity hardening and resilience strategies for an expansive EV charging infrastructure will be critical for continued EV market development.

## References

[1] "Driving into 2025: The future of electric vehicles," JPMorgan, October 10, 2018. [Online]. Available: https://www.jpmorgan.com/global/research/electric-vehicles.

[2] "Cybersecurity for the future electric grid," National Renewable Energy Laboratory, Golden, CO, USA, 2019. [Online]. Available: https://www.nrel.gov/docs/fy19osti/73906.pdf.

[3] M. Martin and Michael Ingram, "Guide to cybersecurity, resilience, and reliability for small and under-resourced utilities," National Renewable Energy Laboratory, Golden, CO, USA, Tech. Rep., 2017. [Online]. Available: https://www.nrel.gov/docs/fy17osti/67669.pdf.

[4] A. McIntyre, "Renewable systems interconnection study: Cybersecurity analysis," Sandia National Laboratories, Albuquerque, NM, USA, 2008.

[5] K. H. S. G. J. B. Cabell Hodge, "https://www.iea.org/tcep/transport/electricvehicles/," NREL, 2019.

[6] C. Carryl, M. Ilyas, I. Mahgoub and M. Rathod, "The PEV security challenges to the smart grid: Analysis of threats and mitigation strategies," *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, Las Vegas, NV, 2013, pp. 300-305.

[7] A. D. Wellisch, J. Lenz, A. Faschingbauer, R. Pöschl, and S. Kunze, "Vehicle-to-grid AC charging station: An approach for smart charging development," *13th IFAC and IEEE Conference on Programmable Devices and Embedded Systems*, 2015, pp. 55-69, doi: https://doi.org/10.1016/j.ifacol.2015.07.007.

[8] "Enabling fast charging: A technology gap assessment," Office of Energy Efficiency and Renewable Energy, 2017. [Online]. Available: 10.2172/1416167.

[9] H. Chaudhry and T. Bohn, "Security concerns of a plug-in vehicle," *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, Washington, DC, 2012, pp. 1-6.

[10] "zmq." http://api.zeromq.org/4-2:zmq (accessed Mar. 19, 2020).

[11] "ZeroMQ." https://zeromq.org/ (accessed Mar. 19, 2020).

[12] "Protocol buffers." Google. https://developers.google.com/protocol-buffers/ (accessed Mar. 19, 2020).

[13] "minimega: A distributed VM management tool." https://minimega.org/articles/usage.article (accessed Mar. 19, 2020).

[14] "Publish/subscribe pattern." *Wikipedia*. https://en.wikipedia.org/wiki/Publish%E2%80%93subscribe_pattern (accessed Mar. 19, 2020).

[15] "Open charge point protocol 1.6." Open Charge Alliance. https://www.openchargealliance.org/protocols/ocpp-16/ (accessed Mar. 19, 2020).

[16] "go-ocpp." Github.com. 2019. https://github.com/eduhenke/go-ocpp (accessed Mar. 19, 2020).

[17] S. Ahmed and F. M. Dow, "Electric vehicle technology as an exploit for cyber attacks on the next generation of electric power systems," *2016 4th International Conference on Control Engineering & Information Technology (CEIT)*, Hammamet, 2016, pp. 1-5.

[18] C. Alcaraz, J. Lopez and S. Wolthusen, "OCPP protocol: Security threats and challenges," in *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2452-2459, Sept. 2017.

[19] J. Teter, P. Le Feuvre, M. Gorner, and S. Scheffer, "Electric vehicles: Tracking clean energy progress," IEA, 2019, [Online]. Available: https://www.iea.org/tcep/transport/electricvehicles/.

[20] C. Hille, and M. Allhoff, "EV charging: Mapping out the cybersecurity threats and solutions for grid and charging infrastructure," P3 Group, 2018, [Online]. Available: https://www.smartgrid-forums.com/wp-content/uploads/2018/06/EV-Charging-Mapping-out-the-Cyber-security-threats-and-solutions-for-grids-and-charging-infrastructure-Chistian-Hill-.pdf.