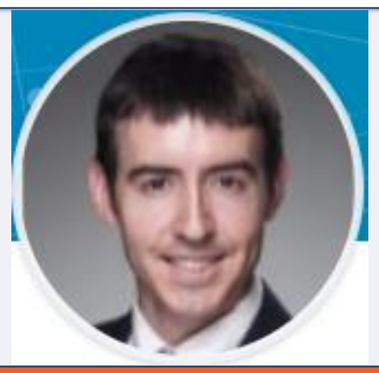
Detection of malicious cyber-attacks in EV charging system

Gabriel Hurtado, Paulina Salinas, Patrick Saenz, Dr. Guenevere Chen

The University of Texas at San Antonio, San Antonio TX, 78249



Name: *Gabriel Hurtado*
Status: *Junior, undergraduate student*
Department: *EE/CE*
Area of Study: *Cybersecurity*
USDA/UTSA Mentor(s): *Dr. Guenevere Chen*

WeARE Research Area

This research is focused on cybersecurity, which is based on the efforts to ensure that the availability, confidentiality, and integrity of all types of information. It has been shown that civil society, numerous industries, and governments across the world are in agreement that information and communications technologies (ICTs) are a unique and functioning ecosystem and a shared resource and common good [1]. Thus, a sustainable approach must be used, where everyone's interactions with ICTs are deliberate and well understood, and act to protect and respect this digital ecosystem for future use.

Motivation or Background

The threat of electronic cyber attacks are ubiquitous, especially where electronic devices are embedded within networks, and this embedded design aspect is a key component to electric vehicles (EVs). Specifically, EV battery packs are especially vulnerable to these malicious attacks due to distinctive risks associated with them. For instance, battery management systems (BMS) could have faulty components, such as a voltage regulator, which this component if subjected to a cyber attacks could lead to overcharging or undercharging [2]. These attacks could lead to damage to auxiliary components through internal shorts from overdischarge, by decreasing the lifespan of the battery significantly, or even endanger the life of the occupant by triggering thermal (fire) events [3] (Fig.1). Other possible cyber attacks can include denial of service (Dos) attacks, which can disrupt the battery service availability and lead to disruptions of the regenerative braking system, or attacks on integrity and confidentiality, which can modify or disrupt the battery functionality or leak unauthorized information about the occupant of the EV [4]. This experiment and methodology will contribute in building the foundational knowledge and principles of EV cybersecurity, which will be crucial in the near future.

Objectives

1. Develop intrusion detection system using deep learning and machine learning in order to effectively detect and monitor cyber attacks, determine the importance of cybersecurity when analyzing charging systems, batteries and electric vehicles. We also want to conduct a test bed vulnerability assessment of level 2 charging system to securely control activity in electric vehicles when examining battery charging techniques.
2. Monitor onboard charger CAN BUS message by hacking predefined Battery Management System (BMS) control message. Understand the methodology behind the electric vehicle charging system to recognize vulnerability, cyber attacks, and specific problems compromising authenticity and functionality.

Methodology

Our methods focus on using the Controller Area Network (CAN) bus system, which contains a protocol for serial communications that supports real-time control of electronics control units (ECUs) in EVs. Our testbed, shown in Fig. 2., contains an EV charger that is connected to a CALB 100Ah battery, which represents a EV battery. A battery management system (BMS) is connected between these two devices, and this device will monitor the CAN bus packets, or messages that are sent between the BMS and the battery.

CAN packets consist mainly of an identifier and data, and each packet can be classified as either normal or diagnostic. The packet contains either 11 or 29 bits, depending on if they contain a basic or extended identifier respectively (Fig. 3) [5]. In this figure, the IDE bit is classified as either a low (dominant) or high (recessive), which is used to identify a 11 or 29 bit identifier. Using the python-can library, our main method will be to monitor the CAN, and then interact with the CAN bus. By doing so, we will then maliciously alter the control field of CAN packets to either overcharge or undercharge the battery. Throughout this process, we will monitor the voltage and current in the battery using the BMS and record this information.

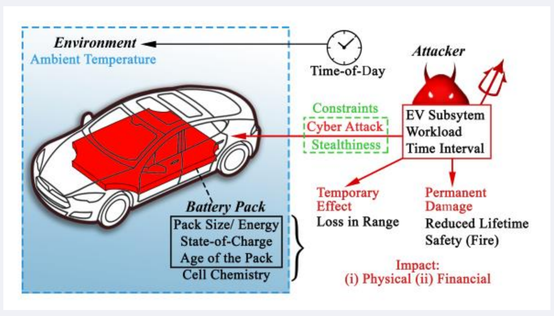


Fig. 1
Illustration showing the financial or physical impact of cyberattacks on EVs [2].

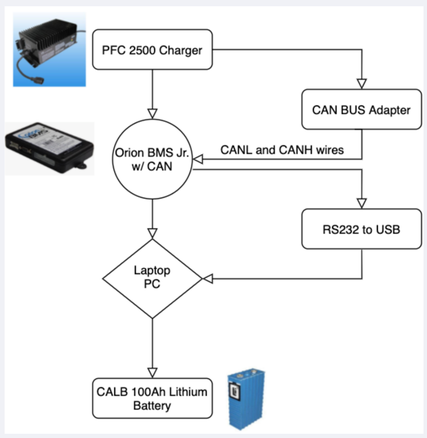
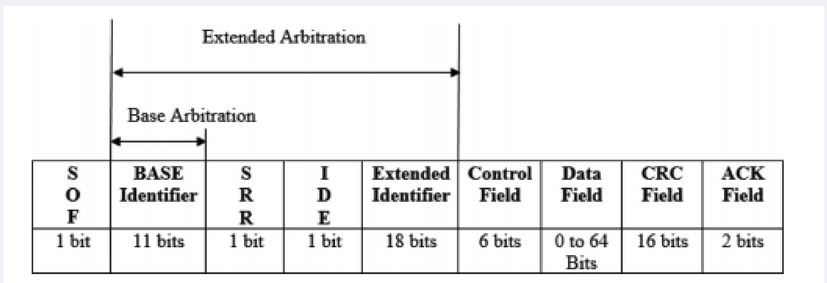


Fig. 2
The testbed for the EV battery cyberattack detection system.



S O F	BASE Identifier	S R R	I D E	Extended Identifier	Control Field	Data Field	CRC Field	ACK Field
1 bit	11 bits	1 bit	1 bit	18 bits	6 bits	0 to 64 Bits	16 bits	2 bits

Fig. 3
Data frame of CAN packet [5].

Results

Given that this is an ongoing research project, this section will be based on previous but similar work in this research field. The results that will be analyzed will be the battery specifications, such as overcharging or undercharging, due to the fact that the CAN bus messages from the BMS to the battery will be altered using a simulated cyber attack. Therefore, during an overcharge, the real-time voltage and current readings should be increased, hence during the cyber attack the power consumption level of the battery should be relatively increased during this event.

For an undercharge attack, the results should be opposite, such that the power consumption levels from the battery should be decreased during this event. The overcharge and undercharge results should be similar to previous work where a denial of service (DoS) cyber attack was initiated on a Programmable Logic Controller (PLC), and the power consumption level were recorded in normal operations and during a DoS attack. Given the nature of DoS attack, which bombards the PLC unit with large amounts of diagnostic nod requests to read a block information, as a result the resources of the unit were exhausted and rendered the device unusable. Power consumption were increased during this event when compared with normal operations [6].

That being so, the results for this study would be similar to previous work in this field.

Literature Review

This field of research is vastly expanding and there have been numerous studies that are similar to the current experiment. In Lopez et al, the focus was also cyber attacks on the BMS, but in this case, battery parameters were modified such as control limits from what the BMS knows [7]. Also, BMS software was replaced remotely through Bluetooth or Wifi. This paper also focused on using DoS attacks to disable the regenerative braking system, or altering the HVAC system without the passenger noticing. Another study used two separate "Smart" attacks from a smartphone on the EV charging system. The 1st was a battery charge request while the user is not in the vehicle during the battery charging process, and the second was an AC-turn on request when the user is not in the vehicle and does not consider whether the vehicle is in the battery charging process. Both of these attacks were designed to drain power from the battery (Fig 4.) [8].

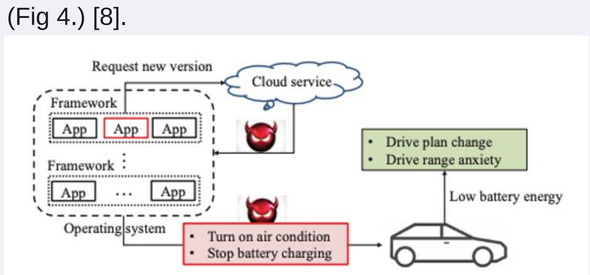


Fig. 4. *Simulated battery attack on EV batteries through a smartphone [8].*

Future Plans

The future plans for this project include the addition of more batteries that we could use either in series or parallel. This will be done to change the voltage and current side of the battery portion of the test bed. Also, with the BMS system, we could also build a custom battery, since the input voltage is adjustable.

Acknowledgments

This work is supported by the USDA National Institute of Food and Agriculture, Interdisciplinary Hands-on Research Traineeship and Extension Experiential Learning in Bioenergy/Natural Resources/Economics/Rural project, U-GREAT (UnderGraduate Research, Education And Training) program (2016-67032-24984).

References

1) RSA Ebook, 2017 *Consumer Cybersecurity Confidence Index*, at 2, www.rsa.com/content
2) S. Sripad, S. Kulandiaivel, et al, "Vulnerabilities of Electric Vehicle Battery Packs to Cyberattacks," *2010 Cryptography and Security*, Dept. of Mechanical Engineering, Carnegie Mellon University
3) Y. Fraiji, L. Ben Azzouz, W. Trojet and L. A. Saidane, "Cyber security issues of Internet of electric vehicles," *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, Barcelona, 2018, pp. 1-6.
4) Anthony Bahadir Lopez et al., "A security Perspective on Battery Systems of the Internet of Things," *Advanced Integrated Cyber-Physical Systems Lab,* University of California Irvine
5) L. Pan, X. Zheng, H.X. Chen, et al., "Cyber Security attacks to modern vehicular systems,"*2017 Journal of Information Security and Applications*, pp. 90-100.
6) Q. Chen, C. Calhoun, S. Sykes, et al. "Towards a Cyber Defense Framework for SCADA Systems Based on Power Consumption Monitoring," *2017 Hawaii International Conference on System Sciences*.
7) 1.A. Lopez, K. Vatanparvar, A. Nath, S. Yang, S. Bhunia, M. Faruque, "A Security perspective on Battery Systems of the Internet of Things," *2017 J. Hardware and Systems Security*, Volume 1, Issue 2, pg. 188-199.
8) 1.L. Kang, H. Shen, "Preventing battery attacks on electrical vehicles based on data-driven behavior modeling," *2019 ICCPS*, pg. 35-46.