A Security Perspective on Battery Systems of the Internet of Things

Article · April 2017

DOI: 10.1007/s41635-017-0007-0

6 authors, including:

Korosh Vatanparvar
University of California, Irvine
13 PUBLICATIONS **68** CITATIONS
SEE PROFILE

Atul Prasad Deb Nath
University of Florida
8 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Mohammad Abdullah Al Faruque
University of California, Irvine
80 PUBLICATIONS **734** CITATIONS
SEE PROFILE

J Hardw Syst Secur
DOI 10.1007/s41635-017-0007-0

A Security Perspective on Battery Systems of the Internet of Things

Anthony Bahadir Lopez[1] · Korosh Vatanparvar[1] · Atul Prasad Deb Nath[2] · Shuo Yang[2] · Swarup Bhunia[2] · Mohammad Abdullah Al Faruque[1]

Received: 21 March 2017 / Accepted: 20 April 2017

Abstract Battery (sub)systems are used in many systems (systems-of-systems) in the Internet of Things (IoT) ranging from everyday ones (e.g., mobile systems, home appliances, etc.) to safety-critical and/or mission-critical ones (e.g., electrical vehicles, unmanned aerial vehicles, autonomous underwater vehicles, etc.). As these systems become more interconnected with each other and their environments and batteries become more energy dense, the safety risks of using batteries increase. To guarantee effectiveness and prevent potential safety threats (i.e., failure, overheating, explosion), it is not only crucial to ensure that batteries are functioning correctly (via safety circuits and battery management system), but to also prevent security threats that specifically target the battery system from different parts of these systems. A security analysis is necessary for system manufacturers and users to understand what threats and solutions exist for battery system security. In this paper, we present a security perspective on battery systems, where we use a layered approach to analyze vulnerabilities, threats, and potential effects. We divide the battery system into the Physical, Battery Management System, and Application layers and use mobile systems and cyber-physical systems as case studies for IoT applications. We then highlight and discuss some existing solutions and mention the potential research directions on battery system security.

Keywords Battery · Mobile · Cyber-physical systems · Internet of things · Security · Survey

✉ Anthony Bahadir Lopez
anthl10@uci.edu

Korosh Vatanparvar
kvatanpa@uci.edu

Atul Prasad Deb Nath
atulprasad@ufl.edu

Shuo Yang
sy@ufl.edu

Swarup Bhunia
swarup@ece.ufl.edu

Mohammad Abdullah Al Faruque
alfaruqu@uci.edu

[1] University of California, Irvine, CA 92697, USA

[2] University of Florida, Gainesville, FL 32611, USA

1 Introduction

In our economy, batteries of all types play important roles to help drive various types of systems that are part of the Internet of Things (IoT). The IoT includes systems that are interconnected with each other and their environments via software, hardware, sensors, actuators, and network connectivity. Some examples of IoT include cyber-physical systems (CPS) and mobile systems. Mission-critical CPS used in transportation, manufacturing, power grid, military and more, all require batteries with high energy density and power density to ensure long-time safety and functionality. Mobile systems primarily require small, yet high energy density batteries that do not easily lose capacity for the satisfaction of consumers. The Li-Ion battery is one type of battery that fits these conditions and is garnering a huge amount of attention. According to the Department of Energy (DOE), by 2020, the global Li-Ion battery market is expected to quadruple [14]. It is even predicted that by 2024, the market for Electrical Vehicles will increase up to approximately $270 billion with an average price of $30 thousand.

Published online: 10 May 2017

Tesla alone is expected to consume over 2 billion highly efficient Li-Ion cells by the end of 2017 [26]. It will be a significant challenge in the near future to ensure that these and other types of batteries are trustworthy and functional.

These batteries are generally prone to thermal runway as a result of improper charging/discharging procedures, of defective materials, and/or of environmental effects. As battery manufacturers aim to pack more energy into smaller batteries, the risk and danger of using them increase. For this reason, safety circuits and battery management systems play particularly crucial roles in preventing such explosions. In addition to safety, however, certain security requirements must be guaranteed to users of battery-operated systems. These requirements include *confidentiality, integrity, availability*, and *authenticity* [6, 20]. In the case that an unexpected attack occurs, the system should also have detection, recovery, and resilience methods. Often, the battery is overlooked in the security analysis of these systems, but rather looked at in other types of system analysis (e.g., efficiency). This survey tries to address the lack of this battery security analysis by identifying and evaluating different attack vectors from different system layers. We call attacks that initiate from one layer and affect other layers: "cross-layer atttacks" as coined in [4]. The battery system is detailed in Fig. 1, where we abstract the system into three layers: the application layer, the battery management system (BMS) layer, and the physical layer. Since these different layers are all interconnected, the attackers can derive more sophisticated attack vectors from simpler ones.

The challenges at the physical layer are safety and security ones: *integrity, availability, authenticity*. Given the size of the battery market, it is no surprise that there are battery counterfeiters. Counterfeiters aim to profit from undermining the high quality battery market by creating their own low-quality batteries or reusing older ones. In addition to counterfeit, there exist replacement/swapping and tampering attacks that also breach the security requirements. Going up a layer, we find the BMS, which ranges from a simple system (only sensors) to a complex one (with sensors, models, and learning techniques). The BMS can estimate and predict the battery state to make decisions for functionality, efficiency, and safety. Unfortunately, we can also observe that there are potential security risks. If any malicious entity is able to gain direct or indirect control over a BMS, they will have the power to weaken or damage the overall system by controlling the battery-related protocols. The security concerns here correspond to *availability* and *integrity*. Lastly, the application layer may prove to be another avenue for attackers to gain access to the battery system. We use Cyber-Physical Systems (CPSs) and mobile systems as case studies for this layer and discuss the potential security risks of attackers leveraging software to directly or indirectly affect the battery, which in turn may negatively affect the system. The application layer of the battery system is susceptible to security attacks which affect the *availability*, *integrity*, and *confidentiality* of the overall system.

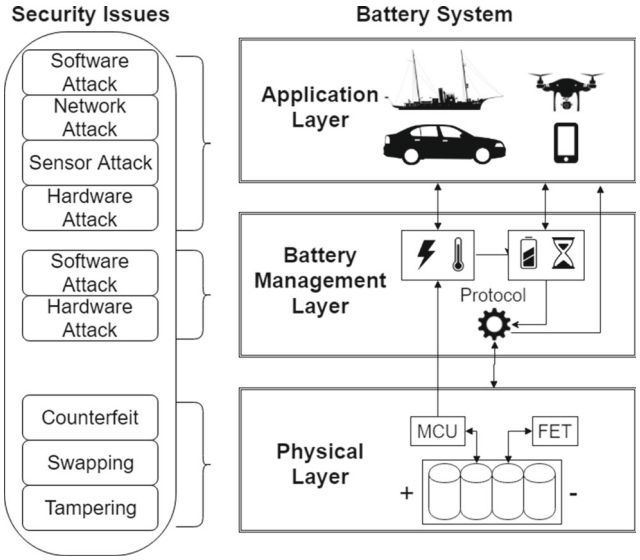

Fig. 1 Overview on battery system and security issues

This paper describes and evaluates the security issues of battery systems in IoT. The paper is organized as follows: Section 2 will discuss the potential attack vectors on the battery system within the physical layer, the BMS layer, and the application layer. We use cyber-physical and mobile systems as case studies for IoT applications. Section 3 will discuss approaches and challenges of related works on battery system security and safety. Additionally, we propose some solutions for some of the battery security issues discussed in this survey. Finally, we will wrap up the paper with some concluding remarks in Section 4.

2 Battery System Security Issues

2.1 Physical Layer

The physical layer of a battery system includes the battery cells, the surrounding circuitry, and the connections with the battery management system (BMS). The battery cells have certain limits (lower and upper voltage/current bounds) and demonstrate specific behavior towards different power requests. The BMS and the circuity components (e.g., fuses) are responsible for monitoring the battery cells and protecting them from overvoltage, undervoltage, overcurrent, overloading, and also overheating. See Fig. 2 for an abstracted model of the physical layer of a battery system.

The behavior of the battery cells can be modeled and described using an equivalent electric circuit model [33, 45,

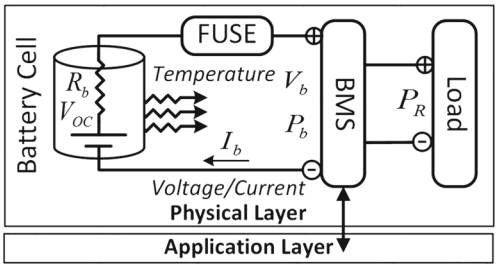

Fig. 2 Physical layer of battery system

57]; the battery cell is modeled as a variable-voltage power supply in series with an internal resistance. The ratio of the available charge to the battery capacity is represented by State-of-Charge (*SoC*) which changes over time as the battery is under utilization. The ratio of the battery's current condition to its ideal condition is represented by the State of Health (SoH) and measured with respect to one or many of the battery parameter. Open-circuit voltage (V_{OC}) of the battery (the variable voltage power supply) and the battery internal resistance (R_b) depend on the *SoC* value. Therefore, the current going through the battery (I_b) and the terminal voltage of the battery (V_b) significantly depends on the battery power (P_b) and the battery parameters. Moreover, the battery cells generate internal heat while charging or discharging which changes the battery temperature in a positive feedback manner. The heat generated is caused by the power loss due to internal resistance or the entropy change in the ions [27, 45]. The amount of the generated heat is also significantly dependent on the battery power and the battery parameters. It needs to be noted that the environment conditions such as ambient temperature and packaging heat dissipation factor influence this behavior as well.

Typically, the BMS implemented on a microcontroller unit utilizes the sensors connected to the battery cells in order to gather the values of the above-mentioned variables (e.g., current, voltage, and temperature). These values are then filtered out to remove the noise, for instance by using a Kalman filter [22], in order to estimate the battery state and prevent safety-threatening operations. However, the safe operation of the BMS and the battery system overall totally depends on having the right knowledge of the battery parameters. For instance, an unsafe operation may occur if the battery parameters such as control limits and modeling variables are different or get changed from what the BMS knows. This can happen by any attack on the battery which will be explained further.

2.1.1 Attack Model

The effects of supplying a counterfeit battery into a system can severely affect the *availability*, *integrity*, and *authenticity* of the system. It may also result in economic costs for both battery system manufacturers (due to warranty claims) and consumers (repairing/resupplying) [15]. This is due to not only a possible lack of safety circuitry in battery packs but also the cheap materials and manufacturing process used in making the counterfeit batteries [18, 29]. Counterfeiters also resell degraded batteries that are dangerous to use and more difficult to detect. The potential cost of using counterfeit batteries rises with lower quality authentication schemes (e.g., form factors, barcode, radio frequency identification), while the cost of preventing counterfeit batteries rises with higher quality authentication schemes (e.g., hashing, cryptography) [54]. Figure 3 depicts the counterfeit security issues.

Generally, a battery is manufactured and sent to the CPS manufacturer through shipping by third-party distributors. However, the received batteries on the CPS manufacturer side may not be authentic because a man-in-the-middle attacker replaced them, or the manufacturer deliberately sent fake batteries. The attack model involves an attacker who wishes to modify the authentic battery or replace it with counterfeit at any stage in the supply chain, to either profit from selling cheaper batteries, or to intentionally put others at risk. A real-case scenario occurred when a Simi Valley CEO sold counterfeit batteries worth more than $2.6 million to the U.S. Department of Defense, who used them in the critical systems on submarines and aircraft carriers [53]. Because the batteries had been covered with counterfeit labels of the approved manufacturers and had spoofed form factors, they were used before eventually being detected. In another example, in 2009, the customs authorities from an airport in Germany found counterfeit mobile phone batteries branded as Siemens, despite Siemens stopping its mobile phone business many years ago. These batteries turned out to have no protection circuitry and were easily ignitable if they came into contact with water [15]. There have been several incidents that indicate the risks of using either counterfeit or faulty batteries: The Samsung Galaxy 7 case [11]; cellphones bursting into flames [28, 52]; battery explosions in self-balancing scooters known as "hoverboards" [35]; Li-Ion batteries catching on fire in Boeing 787 Dreamliner [37]; and a Tesla car catching on fire

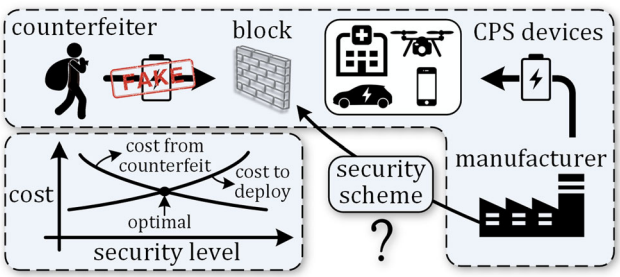

Fig. 3 Counterfeit security issues

within just 5 min of being used [3]. In some of these incidents, the sources state that it is unknown whether or not the batteries were counterfeit. This provides additional motivation to determine the authenticity of batteries to prevent such scenarios.

Another attack may occur during offline or runtime (when the user is using a battery-operated system) where an attacker could tamper with the safety circuitry on the battery pack and/or replace existing batteries with lower-quality/faulty ones to cause system failures. An example would be replacing batteries in systems to cause inefficiency, missed deadlines or safety risks. An attacker could even replace backup batteries used for emergency situations (e.g., during power outage). Researchers on unmanned aerial vehicles (UAVs) are looking toward automated battery replacement to expand UAV operation in areas too risky for humans [50]. However, with less human-in-the-loop interaction in the battery supply chain, there is a potential vulnerability where enemies or other attackers can replace batteries at the battery supply location. In another case, if attackers can capture a UAV by making it appear that it fell down due to a glitch (such as in the Iran-U.S. RQ-170 incident in 2011), they may be able to replace the UAV's battery or tamper with its battery pack circuit before releasing it again. The battery swapping threat also exists for the electrical vehicle and electric scooter. Electrical vehicle (Tesla) and scooter (Gogoro) manufacturers are planning to create battery swapping stations to help ease range anxiety issues for users [59]. On top of rechargeable battery systems, it needs to be noted that the threat model also includes battery swapping for longer-lasting non-rechargeable battery systems in IoT devices. Such a threat exists if we assume that the attacker has a sufficient level of physical access to the battery during system runtime. The attacker may then be able to replace an IoT device's battery with a shorter-lasting one or a defective one. As these systems are generally expected to last a long time to ensure a high level of availability for many systems, the battery swapping attack could cause a major breach in availability and cause a "domino effect" on the availability of other dependent systems. It is clear that if a legitimate battery was swapped, the security of the system and the safety of the user may be seriously threatened. We can generalize the attack model for counterfeit, replacement, and tampering as shown in Fig. 4.

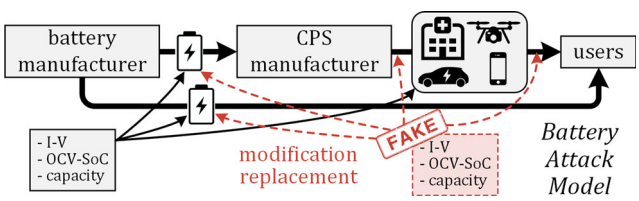

Fig. 4 Abstract attack model on batteries

2.2 Battery Management System Layer

The BMS can be any system that manages the battery [2]. As discussed, batteries are sensitive to overcharging and deep discharging because they may damage the battery, therefore shortening its lifetime and even causing hazardous situations. This requires the adoption of a proper BMS to maintain the states of each cell of the battery within its safe and reliable operating range. In addition to its primary functionality of battery protection, a BMS should estimate the battery status in order to predict the actual amount of energy that can still be delivered to the load [9]. The system could be electronic systems, mechanical systems, or any possible device and technology. The battery could be a single cell, battery module, or battery pack, and it could be rechargeable or non-rechargeable. The system could manage the battery by monitoring the battery, estimating the battery state, protecting the battery, reporting the data, balancing it, etc. [30]. A BMS can include any of the following functions [2]: monitoring, protecting, estimating, maximizing, reporting the battery state to users, and/or external devices.

2.2.1 BMS Functions

Battery management is mandatory for Li-ion batteries to ensure energy availability and lifetime, and the safety of the energy storage system. To do these, a BMS must at least do the following [2]: Prevent overvoltage/undervoltage; prevent overheating; prevent low temperatures; and prevent the overcharging/undercharging. The basic framework of software and hardware in the BMS is shown in Fig. 5 [30]. The

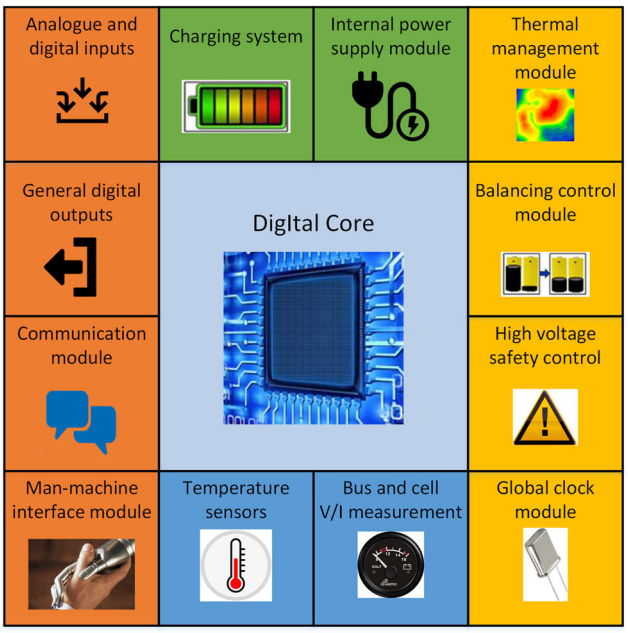

Fig. 5 Framework of software and hardware of BMS

BMS would have inputs such as a main circuit current sensor and a voltage sensor to measure the main current and voltage; temperature sensors to measure the temperature of the cells, the temperature outside the battery box, and maybe also the temperature at the battery coolant inlet and outlet; general analog inputs from sensors of specific applications; and general digital inputs like charging allowed/banned, etc.

The BMS would have outputs to modules such as a thermal management module (including a fan and/or electric heater), a balancing module (including a capacitor with switch array and dissipation resistance) to do the battery equalization, voltage safety management (including a main circuit contactor and battery module contactor), general digital outputs (e.g., display of battery status, charging indicator, failure alarm), and a communication module. Also, the BMS would have the internal power supply module and global clock module, and it may have the charging system and man-machine interface module.

2.2.2 Attack Model

The BMS is a combinational structure of hardware and software that interacts with the application layer, and affects and controls the battery system's physical layer with state estimation/prediction, parameter detection, safety control, charge control, battery equalization, information storage, and so on. It makes the BMS a powerful tool, which if vulnerable, could be used by adversaries to attain valuable information and control all BMS functions, including ignoring critical battery conditions and tolerating high voltages and currents, to damage the battery and even to ignite a fire [41]. Actually, without proper protection on the safety and security of the BMS, the more functional a BMS is, the more vulnerable a battery system could be, as the adversary can manipulate more behavior of the battery and get more information.

The BMS hardware is comprised of sensors, actuators, and controllers. Integrated circuit (IC) counterfeiting and/or tampering can happen in many phases of the BMS supply chain, including IC manufacturing, system manufacturing and integration. They may affect the availability, integrity, and authenticity of the battery system in different ways. For instance, degraded ICs that are recycled, remarked, out-of-spec, or defective will not only lead to economic loss but also cause functional downgrading and even system damage [19]. Tampering can either be on the die level ("hardware Trojan"') or package level. The malicious or affected circuitry due to tampering can act as a silicon time bomb where the BMS will start behaving differently (such as draining or aging the battery) under certain conditions, or act as a backdoor where secret information from the system can be sent out to an adversary.

The BMS software is comprised of the programs in the controllers and firmware in all the ICs. The software of a BMS can be tampered either during IC manufacturing or system integration. Given simplistic security measures such as a deterministic password, an attacker can gain direct access to the BMS's firmware [32]. Moreover, cross-layer attacks initiated from the application layer can affect the BMS layer, which makes it possible to replace the BMS software remotely through Bluetooth, Wi-Fi, etc. In attacks targeting availability, malicious software could be injected to change the normal behavior of battery and control the charging, equalization of the battery, etc. In attacks targeting confidentiality, critical data stored in the BMS, such as SOC, SOH, accumulated charge, and so on, can leak to the adversary due to malware inserted in BMS. Attackers can leverage the BMS functionalities to conduct more sophisticated attacks, as shown in the following section.

2.3 Application Layer

Attack Classification In battery security, the attacks can be broadly classified based on the security objectives and action characteristics. Similarly, the mobile battery and cyber-physical system attacks via the application layer can be classified into three categories depending on the adversary's intention to damage or disrupt availability, integrity, and confidentiality of the critical functions and information within the system. The various types of battery attacks include overcharging, draining, information leaking, and illegally modifying user sensitive information exchanged by data network, mobile and cyber-physical system applications, and the battery management system.

- **Attacks on Availability:** Attacks targeting availability are also called denial of service attacks. The action characteristics of these attacks include attempts to disrupt the battery service availability of the system which may lead to detrimental effects on the system.
- **Attacks on Integrity:** The action characteristics of attacks on integrity include deliberate attempts to modify or disrupt the device battery functionality or information exchanged by data networks, battery management systems, and the system.
- **Attacks on Confidentiality:** This kind of attacks can be defined as the attempts to leak unauthorized information about the user or the overall system through attacks on the battery system.

2.3.1 Cyber-Physical System Applications

CPSs have been used in many applications such as the smart grid, autonomous automobile systems, medical monitoring, process control systems, robotics systems, and automatic avionics. Due to the interconnection between the cyber and physical layers, CPSs are more vulnerable than traditionally

isolated computer systems. A novel type of attack as a result of this interconnection is the "cross-layer attack," as mentioned earlier. This type of attack can start from one layer and propagate to another layer. Meaning that "cross-layer attacks" can be more sophisticated, difficult to detect, and more dangerous.

In this section, we will focus on taking a look on the security of battery-operated Cyber-Physical Systems. These systems are constantly in motion and have processing capabilities for highly interacting with the physical environment in a feedback manner to control certain functions. They highly depend on batteries to perform their autonomous, mission-critical, and/or safety-critical functions. These systems require high-quality batteries with strict constraints, such as high energy density, and accurate BMSs to ensure that the batteries will not fail or cause catastrophe in their runtime environments, which could lead to financial loss, physical damage, and even human injuries or casualties. Some examples of these systems include electrical vehicles (EVs), solar-powered management systems (SPMS), unmanned aerial vehicles (UAV), and autonomous underwater vehicles (AUV), and spacecraft systems. Because each system is uniquely designed for different application purposes, it is apparent that they have both unique and common battery system security challenges.

Attacks Targeting Availability EVs carry a large amount of batteries packed together to sustain varying demands over time and to guarantee a sufficient driving range for consumers [55, 56]. An EV can have BMSs at the cell, the module, and the pack levels. These BMSs are then connected with each other via an internal controller area network (CAN) bus and with external electronic control units (ECUs) of the vehicle via an external CAN bus. ECUs are connected with each other via different intra-network protocols and technologies (e.g., MOST, LIN, CAN, FlexRay and Ethernet designed for various objectives (e.g., safety, efficiency, etc) (Fig. 6).

With access to the intra-network, it turns out that it is highly viable for an attacker to exploit and conduct a wide variety of attacks on the automotive system. Additionally, they can perform most of the BMS-layer attacks (Section 2.2) on battery systems. The intranetwork can be accessible to attackers via malware or malicious websites that applications may stumble upon through different communication mediums, such as telematics, dynamic short range communication (DSRC) used in vehicle to vehicle or vehicle to infrastructure communication (V2X), Bluetooth, Wi-Fi, and USB cable [10]. However, it can be possible to implement indirect attacks on the battery system via unique application layer features, such as by disabling the regenerative braking system or by altering the heating-ventilation-air-conditioning (HVAC) system without the passenger noticing. These attacks end up draining the batteries and therefore affect their availability, and in turn, affect the EV availability to the users. Another sophisticated attack may include draining the EV battery by spoofing sensor information sent to ECUs via the intranetwork [23]. Such information (e.g., the GPS location, proximity data, velocity and relative velocity, tire pressure, etc.) is crucial to the efficiency and safety guarantees that EVs should provide [1, 58].

Besides causing the EV to waste critical resources, an attacker can spoof critical information to cause the battery-operated CPSs to draw out more power from the battery and cause deep discharge. Deep discharge in certain instances can lead to a battery with a heavily degraded capacity or even a battery left in a dangerous state (e.g., broken separator). Both conditions could eventually lead to thermal runway and explosion [17]. As a result, this attack can be either categorized as an availability or denial-of-service (DoS) attack, with potential consequences of causing damage or severely injuring humans. It goes without saying, but future autonomous vehicles may experience similar security vulnerabilities as EVs, especially with high levels of autonomous processing units and interconnectivity in the application layer (see software-defined batteries for heterogenous battery systems such as EVs and mobile systems proposed by Microsoft, Tesla, University of Massachusetts Amherst, and Columbia University [5]). Already,

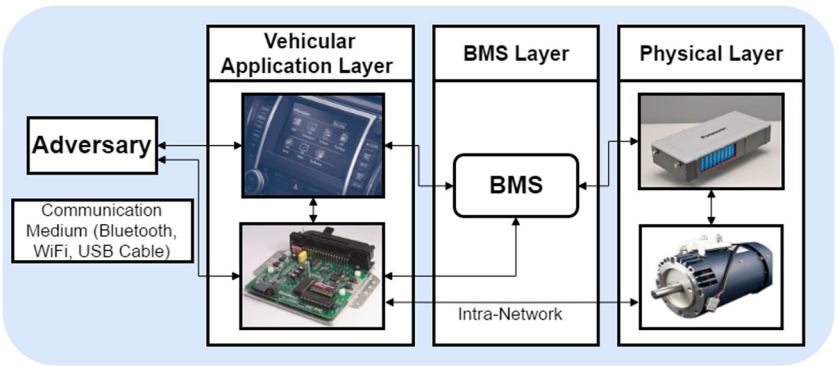

Fig. 6 Abstracted battery system attack model on electrical vehicle

researchers have expressed their concerns over the importance of securing EV battery systems [42].

The solar power management system (SPMS) has become vulnerable to novel security threats due to the integration of modern digital circuitry, advanced metering infrastructure (AMI), home energy management systems (HEMS), advanced communication modules, etc. The increased number of applications of solar powered systems include unmanned cars and aerial vehicles, autonomous cyber-physical systems to smart homes, gadgets, and home appliances. For instance, the latest home solar panel available in the market, named Solpad [47], comes along with communication features like Internet Hotspot and works with Solcontrol [48], an added feature to individually monitor and control the charging and discharging pattern of gadgets and appliances like smart phones, tablets, LED lights, drones, TVs, laptops, refrigerators, etc. The increased accessibility of the solar power system increases the vulnerabilities as well.

The microcontroller in solar power management systems can be a potential target of the adversary for availability attacks. In most cases, the microcontroller is utilized as a charge controller of the battery module [44]. If the adversary can maliciously modify the functionality of the microcontroller by inserting Trojans and malware, the operation and security of the battery system will be in jeopardy. Disrupting the communication between the sensors and microcontroller can result in battery exhaustion and denial-of-service attack scenarios [8]. The adversary might physically tamper the microcontroller or sensors to disrupt the availability and functionality of the battery module.

UAV and AUV battery systems are potentially vulnerable to attacks from the application layer via remote access to the communication module or indirectly via the system's sensors. One possible attack would be to spoof critical sensor information to cause battery exhaustion. Because they are battery-dependent and autonomous, the sensor information for these systems may be arguably more critical for their functionalities than other CPSs. For instance, the GPS location, temperature, speed, acceleration, and localization features are all critical factors for these systems to succeed in their missions. Sensors have already been shown to be vulnerable to spoofing in UAVs [13, 21]. In some cases, unique features for each system can also be exploited to cause severe consequences. For example, AUVs use "dead reckoning" to estimate one's position while diving, but if its Doppler velocity log (DVL) is providing spoofed information by an attacker, the overhead can be significant and potentially cause the battery to fail and the system to be lost forever. Gathering and processing DVL data is already an energy and computation intensive procedure [60]. Another case would be spoofing the underwater current information to covertly drain the AUV batteries.

Attacks Targeting Integrity and Confidentiality Attacks that target the integrity and confidentiality of a system can also be done via the application layer of battery-operated CPSs. These attacks can focus on stealthily forging data of the battery to confuse the system or the user, or by obtaining critical information about the system or the user via the behavior of the battery. For example, supposing an attacker has access to the history of the EV battery usage (achievable by having access to the On-Board Unit or the BMS via the intra-network), the attacker can extract critical information such as the driver's habits and location. However, with knowledge of the habits and location of a driver, an attacker can eventually conduct a bigger breach in the driver's privacy. On the other hand, an attacker can use the access of the CAN bus of the EV to do an integrity attack by displaying incorrect information about the battery state (e.g., SoC and SoH) to the user. As a result, the consequences for this attack could be that the attacker unknowingly damages the vehicle or ends up stranded in the middle of a trip with a discharged or unusable battery.

For SPMS, another potential threat can be malicious hardware modification of the circuit schematic during fabrication, which can trigger an attack on the battery system during runtime. Yang et al. [61] demonstrated such an attack via an analog Trojan, which can be as minute as one gate and hard to detect as tests unlikely trigger sequences for activation. The malicious circuit is designed to fully charge a capacitor by siphoning charge from adjacent wires and further exploit the capacitor to change the value of a target flip-flop. The premise of such attacks is not limited to the microcontroller and these attacks can be designed to exploit analog circuitry of the solar power system and cause security issues for the battery. These novel vulnerabilities require to be addressed with proper security measures to ensure safe and reliable operations of solar powered battery management systems.

2.3.2 Mobile Applications

The omnipresence of mobile data services and applications expose mobile device batteries to novel security risks. The attackers can exploit unique vulnerabilities in mobile networks, applications, device resources, and network interconnectivity. As battery security challenges mostly arise from cyber-physical attacks launched in conjunction with malicious applications, it is essential to comprehend the potential risks of batteries emanating from the application layer. In general, the attacks via mobile applications are orchestrated by exploiting multiple layers of a mobile device and the communication network. An illustration of possible attacks on mobile battery spanning over multiple layers of communication network, mobile applications, and device resources is depicted by Fig. 7. For instance, if the

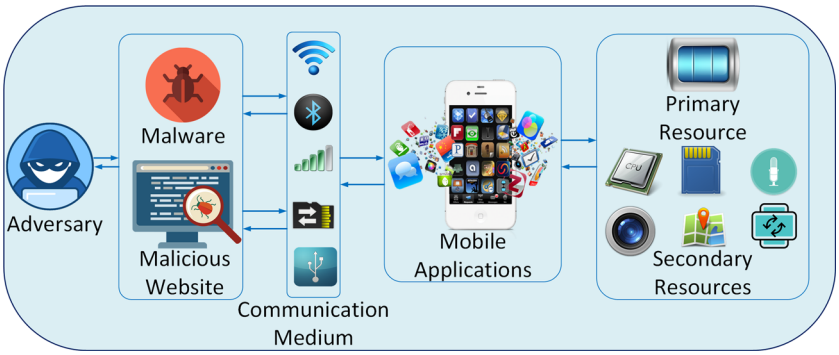

Fig. 7 Abstracted battery system attack model on mobile device

adversary launches a benign looking malware that is downloaded by the users unknowingly via Wi-Fi, Bluetooth or the other mediums, the malware can deliberately and secretively exploit the battery power (deemed as primary resource in context of battery security) or other resources like processor, storage, camera, microphone, GPS, accelerometer, etc. to disrupt the proper functionality of the device's battery system.

In this section, an overview of the threats and vulnerabilities of mobile battery security is provided. The mobile application attacks are categorized into general classes at first. Then, the potential threats of the attacks are analyzed via case studies available in the literature.

Attacks Targeting Availability As the primary security goal of any device is to maintain availability of reliable services, we first investigate the application layer vulnerabilities to availability attacks. Any disruption in service availability of the mobile devices will severely degrade the communication capability of users and further impair the operation of mobile devices. Many types of battery exhaustion DoS attacks have been designed by researchers over the past years to imitate adversaries and analyze the effects on the device under attack. The notion of battery exhaustion by a variant of DoS attack, named sleep deprivation torture attack, was first introduced by Stajano et al. [49].

DoS attacks on general purpose mobile computers were first demonstrated by Martin et al. [31]. The authors classified sleep deprivation attacks into three different categories: *Service request attacks, benign power attacks, and malignant power attacks*. Service request power attacks aim at placing repeated network service requests with intentionally misplaced information to keep the device under attack occupied authenticating or servicing the request. Benign power attacks focus on executing valid energy-hungry tasks for an indefinite time. Malignant power attacks attempt an unauthorized security breach and alteration of the operating system kernel or application binary code to increase energy consumption during execution.

Multimedia messages (MMS) and the insecure interaction between cellular data networks and the Internet can be exploited to launch an attack on mobile battery systems. Racic et al. [40] introduced a two-stage battery exhaustion attack by exploiting an insecure cellular data service. In the first stage of the attack model, the adversary compiles a hit list of potential targets comprising cell phone numbers, device models, and IP addresses through MMS notification messages. Once the information is obtained, the attacker starts sending periodical User Datagram Protocol (UDP) packets through the exploitation of Packet Data Protocol (PDP) context retention and the paging channels. The unique features of the attack include stealthy exploitation of the cellular network vulnerability and a quick battery drainage due to increased power consumption of up to 22%.

Flooding the mobile devices with spam contents by exploiting the Wi-Fi and Bluetooth protocols can also lead to the overconsumption of power and battery exhaustion. The ramification of battery exhaustion attacks launched via IEEE 802.11 Wi-Fi, IEEE 802.15.1 Bluetooth, and a combination of both mediums are analyzed by Moyers et al. [34]. They performed extensive tests on the effects of Bluetooth and Wi-Fi attacks on the battery lifetime of mobile devices. The Wi-Fi attacks included a Ping flood, an ACK flood, and a SYN flood. The Wi-Fi attacks demonstrated an approximate 10 to 12% faster rate of battery depletion under attack compared to an idle state. The Ping of Death, BlueSmack, BlueSpam, and Blueper floods are selected to demonstrate the effect of Bluetooth attacks on battery exhaustion. The battery lifetime reduction due these Bluetooth attacks varied from 8 to 17%.

Apart from the single attack vectors via Wi-Fi or Bluetooth mediums, blended attacks are also tested with an intention to inflict quicker battery depletion of the target device. The impact of blended attacks on mobile device are recorded till the Wi-Fi NICs become unresponsive. The full battery drain period is extrapolated based on the acquired data. Two different blended attacks are

demonstrated including BlueSYN Flod and PingBlender flood. BlueSYN Flood attack is a combination of BlueSmack and Syn Flood. Similarly, PingBlender attacks combines the ping flood attack of wifi and Bluetooth medium. The attacks demonstrated an accelerated battery depletion rate of up to 18.5%.

Sleep disorder bugs in mobile devices can be misused by an adversary to maliciously exhaust battery power of the targeted system. Jindal et al. [25] proposed a taxonomy of sleep disorder bugs and category of time critical sections which are deemed as the primary cause of sleep disorder bugs in mobile applications, framework services, and the android kernel. Exploitation of multimedia contents to drain the device battery can be another novel attack premise for attackers. Multimedia based DoS attacks on android device batteries were introduced by Fiore et al. [16].

Attacks Targeting Integrity and Confidentiality The attacks targeting integrity and confidentiality of battery security can originate in and propagate through applications, the cellular data network, and Internet. The primary intentions of such attacks are obtaining and/or illegally modifying critical information about the users and devices through exploitation of the mobile battery system. Compared to DoS attacks, the attacks on integrity and confidentiality can be considered less brute-force and more sophisticated. These attacks attempt to stealthily fabricate or obtain user and device sensitive information exchanged between the device and its BMS.

As incidents of mobile phone battery explosions have been reported in several occasions, it can be assumed that the adversary might try to explode the battery in an attempt to injure the user and damage the device [11, 52]. Poorly made or counterfeit batteries can get overheated during regular mode of operation and result in an explosion. In context of mobile applications, if the adversary can disable the safety precaution of the BMS against overheating and overcharging, it is possible to cause an explosion or fire by the mobile battery. The attacker can attempt such an attack by corrupting or breaching the battery firmware of the device and disrupting the proper communication between the device operating system and battery management system.

The novel security threats to user confidentiality via mobile battery system attacks are highlighted by Olejnik et al. [39]. They have demonstrated a novel approach of generating a fingerprinting vector of the user by exploiting the HTML5 battery status APIs of common web browsers. In the attack model, the adversary obtains information about the battery's SoC and charge/discharge time readouts by exploiting the web scripts. The information is further utilized to identify users visiting the same website or other websites containing a similar web script. Also, the websites can reconstruct the user identifiers. Thus, the users can be identified and tracked over the Internet.

Taxonomy of Battery System Attacks We have provided Fig. 8 to summarize the various types of attacks on battery systems that we discussed. Each attack may target one or more layers and has a set of action characteristics that are manifested into the system. An adversary may exploit one or more of the following mediums to perform their attacks: physical access, sensors, software/hardware, and communication channels.

3 Existing and Proposed Solutions

3.1 Existing Solutions

Physical and BMS Layers Down to the physical layer, there are traditional safety circuits used to prevent the battery or the overall system to go into an unstable state. However, it can be observed that such safety circuits can be tampered with in counterfeit battery packs. For battery counterfeit, some solutions are form factors, barcoding, radio frequency identification (RFID), and hashing/cryptography (e.g., SHA-1/HMAC, KEELOQ, XTEA) [54]. Evidently, the form factors, barcoding, RFID, and (some) cryptographic solutions suffer from lack of entropy and therefore are typically easily replicated. On the other hand, although stronger cryptographic solutions can potentially solve these problems, typically their inputs are deterministic (simple keys from the manufacturer of the battery) and therefore

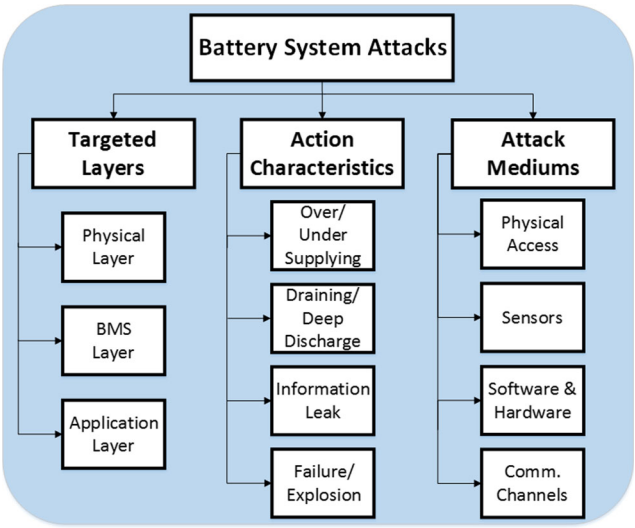

Fig. 8 Taxonomy of battery system attacks

may lead to a lack of security [32, 38]. Furthermore, they can add a non-trivial cost to the battery pack [12].

Application Layer Many intrusion detection methodologies have been developed over the years to detect and thwart battery exhaustion DoS attacks on mobile computers and smart phones. Nash et al. [36] developed an intrusion detection system (IDS) Framework to mitigate the impact of battery depletion DoS attacks in mobile devices and laptops. Jacoby et al. [24] proposed a battery-based intrusion detection system (B-BID) to prevent the exploitation of battery power via DoS attacks. Moyers et al. [34] developed a hybrid scheme named multi-vector portable intrusion detection system (MVP-IDS) that monitors the host-based device instantaneous current (IC) and traffic signatures. The framework recognizes any significant change in the instantaneous current of the device and correlates it to the anomaly or increase in Wi-Fi or Bluetooth traffic

3.2 Future Directions

Existing solutions for physical battery safety typically deal with identifying or predicting the state of the battery on the BMS to take safety precautionary measures. These solutions include both diagnostic and prognostic approaches, e.g., with Kalman filter, particle filter, neural networks, parametric modeling, mapping, etc. [43]. We believe that through the use of the diagnostic and prognostic approaches on the BMS, it may be possible to derive a cost-effective and secure authentication solution for the physical security of the battery. Specifically, it may be possible to derive a unique signature from the battery's physical features to authenticate the battery to detect/prevent counterfeit, swapping, and tampering. There are several sources which suggest that each battery has unique features [7, 46], but there are no related works on using them for the purpose of authentication. There is also a strong necessity to prevent IC counterfeit/tampering to secure the system. This is a huge research area and out of the scope of this survey. For this reason, we point readers to [19, 51] for more information on IC security.

Application layer security should incorporate features to prevent both static and dynamic attacks. To address the static attacks (i.e. the attempts to maliciously modify installed operating system properties and applications), authentication and secure operation verification of executable code and applications is required. As for dynamic attacks that attempt to maliciously inject malwares or run contents from an insecure source, the security methods should be capable of detecting anomalous deviation in operation, power consumption, communication patterns, etc. from the system software's typical executing path of normal behavior. Sensor attacks may be preventable with more reliable sensor fusion techniques and anti-spoofing methods [21].

4 Conclusion

To summarize, we have presented a comprehensive review and cross-layer security analysis of battery systems in the Internet of Things. Existing solutions are ad hoc and also restricted to specific attack scenarios. A comprehensive security framework for battery systems in IoT devices comprising of cross-layer security analysis capability is required to prevent rising threats. In order to develop a holistic method to thwart battery attacks and prevent battery counterfeiting, the hardware, software, and firmware should work independently and in conjunction.

References

1. Al Faruque MA, Vatanparvar K (2016) Modeling, analysis, and optimization of Electric Vehicle HVAC systems. Asia and South Pacific Design Automation Conference (ASP-DAC), pp 1–6
2. Andrea D (2010) Battery management systems for large lithium-ion battery packs. Artech House
3. Anthony S (2016) Tesla model s battery bursts into flames, car totally destroyed in 5 minutes. http://arstechnica.com/cars/2016/08/tesla-model-s-france-battery-fire/
4. Applegate SD (2013) The dawn of kinetic cyber. In: 2013 5th international conference on cyber conflict (CYCON 2013), pp 1–15
5. Badam A, Chandra R, Dutra J, Ferrese A, Hodges S, Hu P, Meinershagen J, Moscibroda T, Priyantha B, Skiani E (2015) Software defined batteries. In: Proceedings of the 25th symposium on operating systems principles, ACM. New York, NY, USA, SOSP '15, pp 215–229, doi:10.1145/2815400.2815429
6. Banerjee A, Venkatasubramanian KK, Mukherjee T, Gupta SKS (2012) Ensuring safety, security, and sustainability of mission-critical cyber physical systems. Proc IEEE 100(1):283–299. doi:10.1109/JPROC.2011.2165689
7. Barsukov Y (2005) Battery selection, safety, and monitoring in mobile applications
8. Belvedere B, Bianchi M, Borghetti A, Nucci CA, Paolone M, Peretto A (2012) A microcontroller-based power management system for standalone microgrids with hybrid power supply. IEEE Trans Sustain Energy 3(3):422–431
9. Brandl M, Gall H, Wenger M, Lorentz V, Giegerich M, Baronti F et al (2012) Batteries and battery management systems for electric vehicles. In: Design, automation & test in Europe conference and exhibition (DATE). IEEE, pp 971–976
10. Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S, Koscher K, Czeskis A, Roesner F, Kohno T et al (2011) Comprehensive experimental analyses of automotive attack surfaces. USENIX Security Symposium
11. CNET (2016) Here's why samsung note 7 phones are catching fire - CNET. https://www.cnet.com/news/why-is-samsung-galaxy-note-7-exploding-overheating/
12. Conner M (2006) Friend or foe: Battery-authentication ics separate the good guys from the bad. http://tayloredge.com/reference/Batteries/EDN-BatteryAuthentication.pdf

13. Davidson D, Wu H, Jellinek R, Ristenpart T, Singh V (2016) Controlling uavs with sensor input spoofing attacks. In: Proceedings of the 10th USENIX conference on offensive technologies, USENIX association. Berkeley, CA, USA, WOOT'16, pp 221–231. http://dl.acm.org/citation.cfm?id=3027019.3027039
14. Department of Energy (2014) Overview of the doe advanced battery research and development program. http://energy.gov/sites/prod/files/2014/09/f18/battery_rd_amr_plenary_june_2014_final.pdf
15. Engels S (2010) Counterfeiting and piracy: the industry perspective. J Intell Prop Law Prac 5(5):327. doi:10.1093/jiplp/jpq023
16. Fiore U, Palmieri F, Castiglione A, Loia V, De Santis A (2014) Multimedia-based battery drain attacks for android devices. In: Proceedings of the 2014 IEEE 11th consumer communications and networking conference (CCNC). IEEE, pp 145–150
17. Florence L (2013) Safety issues for lithium-ion batteries. http://www.ul.com/wp-content/uploads/2016/02/Safety_Issues_for_Lithium_Ion_Batteries1.pdf
18. Georgi S (2004) Counterfeit cell phone and laptop batteries: Caution, credibility, causes and cures. http://www.tayloredge.com/reference/Batteries/CounterfeitBatteries.pdf
19. Guin U, DiMase D, Tehranipoor M (2014) Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead. J Electron Test 30(1):9–23
20. Harshan J, Chang S, Hu Y (2017) Insider-attacks on physical-layer group secret-key generation in wireless networks. CoRR arXiv:1701.03568
21. Hartmann K, Steup C (2013) The vulnerability of uavs to cyber attacks - an approach to the risk assessment. In: 2013 5th international conference on cyber conflict (CYCON 2013), pp 1–23
22. Hu C, Youn BD, Chung J (2012) A multiscale framework with extended kalman filter for lithium-ion battery {SOC} and capacity estimation. Appl Energy 92:694–704. doi:10.1016/j.apenergy.2011.08.002. http://www.sciencedirect.com/science/article/pii/S0306261911004971
23. Ishtiaq Roufa RM, Mustafaa H, Travis Taylora SO, Xua W, Gruteserb M, Trappeb W, Seskarb I (2010) Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In: 19th USENIX security symposium. Washington DC, 11–13
24. Jacoby GA, Marchany R, Davis N (2006) Using battery constraints within mobile hosts to improve network security. IEEE Secur Privacy 4(5):40–49
25. Jindal A, Pathak A, Hu YC, Midkiff S (2013) On death, taxes, and sleep disorder bugs in smartphones. In: Proceedings of the workshop on power-aware computing and systems. ACM, p 1
26. Kane M (2013) Panasonic to supply tesla with 2 billion lithium-ion battery cells from 2014 to 2017. http://insideevs.com/panasonic-to-supply-tesla-with-2-billion-lithium-ion-battery-cells-from-2014-to-2017/
27. Karimi G, Li X (2013) Thermal management of lithium-ion batteries for electric vehicles. J Energy Res 13–24
28. KomoNews (2011) Girl's iphone bursts into flames mid-flight. i thought we were going down. http://komonews.com/news/local/girls-iphone-bursts-into-flames-mid-flight-i-thought-we-were-going-down
29. Lawson B (2017) Buying batteries in china. http://www.mpoweruk.com/china_batteries.pdf
30. Lu L, Han X, Li J, Hua J, Ouyang M (2013) A review on the key issues for lithium-ion battery management in electric vehicles. J Power Sources 226:272–288
31. Martin T, Hsiao M, Ha D, Krishnaswami J (2004) Denial-of-service attacks on battery-powered mobile computers. In: Proceedings of the 2nd IEEE annual conference on pervasive computing and communications 2004, PerCom 2004. IEEE, pp 309–318
32. Miller C (2011) Battery firmware hacking: Inside the innards of a smart battery. Black Hat USA https://media.blackhat.com/bh-us-11/Miller/BH_US_11_Miller_Battery_Firmware_Public_WP.pdf
33. Millner A (2010) Modeling lithium ion battery degradation in electric vehicles. In: IEEE conference on innovative technologies for an efficient and reliable electricity supply, pp 349–356
34. Moyers BR, Dunning JP, Marchany RC, Tront JG (2010) Effects of wi-fi and bluetooth battery exhaustion attacks on mobile devices
35. Moynihan T (2015) Why hoverboards keep exploding. http://www.wired.com/2015/12/why-hoverboards-keep-exploding/
36. Nash DC, Martin TL, Ha DS, Hsiao MS (2005) Towards an intrusion detection system for battery exhaustion attacks on mobile computing devices. In: Third IEEE international conference on pervasive computing and communications workshops 2005, PerCom 2005 Workshops. IEEE, pp 141–145
37. National Transportation Safety Board (2013) Auxiliary power unit battery fire japan airlines boeing 787-8, ja829j. http://www.ntsb.gov/investigations/accidentreports/pages/AIR1401.aspx
38. O'donnell CW, Suh GE, Devadas S (2004) Puf-based random number generation. In: MIT CSAIL CSG technical memo
39. Olejnik Ł, Acar G, Castelluccia C, Diaz C (2015) The leaking battery. In: International workshop on data privacy management. Springer, pp 254–263
40. Racic R, Ma D, Chen H (2006) Exploiting mms vulnerabilities to stealthily exhaust mobile phone's battery. In: Securecomm and Workshops, 2006. IEEE, pp 1–10
41. Sagstetter F, Lukasiewycz M, Steinhorst S, Wolf M, Bouard A, Harris WR, Jha S, Peyrin T, Poschmann A, Chakraborty S (2013) Security challenges in automotive hardware/software architecture design. In: Proceedings of the conference on design, automation and test in Europe, EDA Consortium, pp 458–463
42. Sagstetter F, Lukasiewycz M, Steinhorst S, Wolf M, Bouard A, Harris WR, Jha S, Peyrin T, Poschmann A, Chakraborty S (2013) Security challenges in automotive hardware/software architecture design. In: 2013 design, automation test in Europe conference exhibition (DATE), pp 458–463. doi:10.7873/DATE.2013.102
43. Saxena A, Celaya J, Roychoudhury I, Saha S, Saha B, Goebel K (2010) Designing data-driven battery prognostic approaches for variable loading profiles: Some lessons learned. Int J Energy Res 34(2):152–163. doi:10.1002/er.1655
44. Shiau JK, Ma DM, Yang PY, Wang GF, Gong JH (2009) Design of a solar power management system for an experimental uav. IEEE Trans Aerosp Electron Syst 45(4)
45. Shin D, Poncino M, Macii E (2014) Thermal management of batteries using a hybrid supercapacitor architecture. In: Proceedings of the conference on design, automation & test in Europe (DATE'14)
46. Shin D, Poncino M, Macii E, Chang N (2015) A statistical model-based cell-to-cell variability management of li-ion battery pack. IEEE Trans Comput Aided Des Integr Circuits Syst 34(2):252–265. doi:10.1109/TCAD.2014.2384506
47. Solpad (2017) SolPad - the smart home solar solution is here. http://solpad.com/solpad_mobile
48. Solpad (2017) SolPad - the smart home solar solution is here. http://solpad.com/solcontrol
49. Stajano F, Anderson RJ (2000) The resurrecting duckling: Security issues for ad-hoc wireless networks. In: Proceedings of the 7th international workshop on security protocols. Springer-Verlag, London, UK, pp 172–194. http://dl.acm.org/citation.cfm?id=647217.760118
50. Suzuki KAO, Kemper Filho P, Morrison JR (2012) Automatic battery replacement system for uavs: Analysis and design. J Intell Rob Syst 65(1):563–586. doi:10.1007/s10846-011-9616-y
51. Tehranipoor M, Koushanfar F (2010) A survey of hardware trojan taxonomy and detection. IEEE Des Test Comput 27(1):10–25. doi:10.1109/MDT.2010.7

52. Torralba C (2012) Busting the myth: Yes, cell phones can explode. http://www.androidauthority.com/busting-the-myth-yes-cell-phones-can-explode-42582/
53. (2015) Former simi valley ceo convicted of selling navy knock-off batteries used on subs and aircraft carriers. https://www.ice.gov/news/releases/former-simi-valley-ceo-convicted-selling-navy-knock-batteries-used-subs-and-aircraft
54. Vanyo T, Qian J (2004) Battery authentication architecture and implementation for portable devices
55. Vatanparvar K, Al Faruque MA (2015) Battery lifetime-aware automotive climate control for electric vehicles. In: Proceedings of the design automation conference (DAC'15). pp 1–6
56. Vatanparvar K, Al Faruque MA (2016) Eco-friendly automotive climate control and navigation system for electric vehicles. In: International conference on cyber-physical systems (ICCPS), pp 1–10
57. Vatanparvar K, Al Faruque MA (2016) OTEM: optimized thermal and energy management for hybrid electrical energy storage in electric vehicles. In: Design automation and test in Europe (DATE), pp 1–6
58. Vatanparvar K, Wan J, Al Faruque MA (2015) Battery-aware energy-optimal electric vehicle driving management. In: International symposium on low power electronics and design (ISLPED), pp 353–358
59. Weintraub S (2016) Gogoro scooter and battery swap distribution model get smarter and spread to new cities. https://electrek.co/2016/01/06/gogoro-scooter-battery-swap/
60. Woithe H, Brozas W, Wills C, Pichai B, Kremer U, Eichhorn M, Riepen MNoulard E, Vernhes S (eds) (2012) Enabling computation intensive applications in battery-operated cyber-physical systems. The French Aerospace Lab, Toulouse, France. https://hal.archives-ouvertes.fr/hal-00719031
61. Yang K, Hicks M, Dong Q, Austin T, Sylvester D (2016) A2: Analog Malicious hardware. In: 2016 IEEE symposium on security and privacy (SP). IEEE, pp 18–37