Technologies for Safe & Efficient Transportation

THE NATIONAL USDOT UNIVERSITY TRANSPORTATION CENTER FOR SAFETY

Carnegie Mellon University | UNIVERSITY of PENNSYLVANIA

9 - Analyzing and Defending Cyberattacks on Electric, Hybrid, and AV Battery Systems

Final Research Report

PI: Venkat Viswanathan

Department of Mechanical Engineering

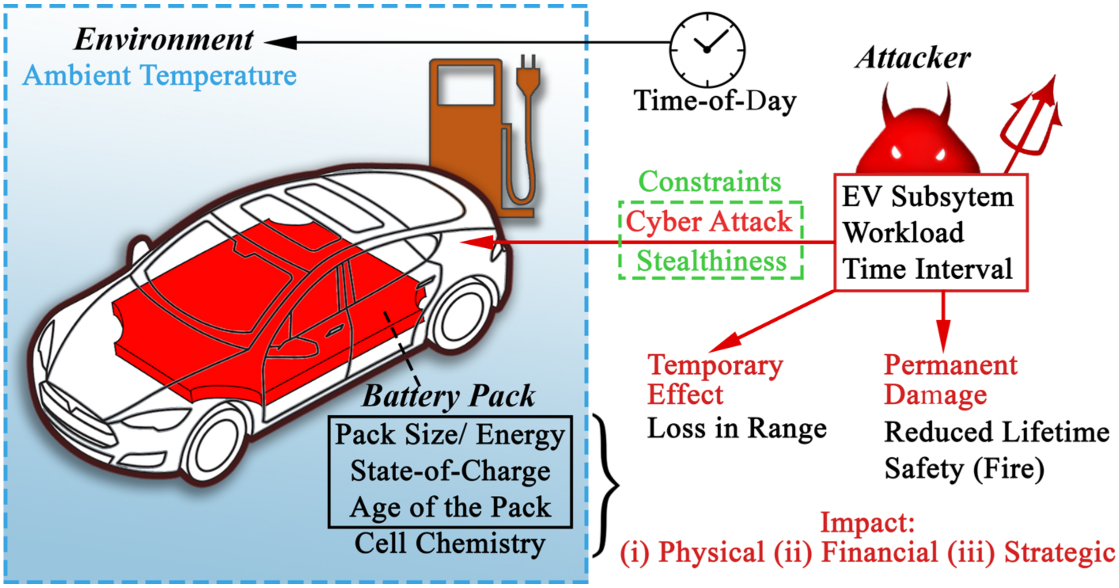
Carnegie Mellon University

DISCLAIMER

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated in the interest of information exchange. The report is funded, partially or entirely, by a grant from the U.S. Department of Transportation's University Transportation Centers Program. However, the U.S. Government assumes no liability for the contents or use thereof.

Modern vehicles consist of a myriad of devices and systems ranging from safety-critical systems that control a vehicle's brakes to auxiliary components that adjust cooling and wiper speeds. While these technologies enhance the users safety and comfort, they also render the vehicle's networks vulnerable to cyberattacks. When such vulnerabilities are exploited, attackers can gain access to safety-critical systems like the brakes and transmission of the vehicle, as demonstrated by recent work.[1,2]

Alongside, another notable development in the automotive sector is the transition to electric vehicles (EVs) motivated by efforts to downscale tailpipe emissions. Currently, widespread EV adoption is bottlenecked by limited driving range, battery pack cost, battery lifetime and safety issues associated with Li-ion batteries.[3] The battery pack forms a significant fraction of the total cost of the electric vehicle (∼20% of the vehicle cost[4]). From the standpoint of automotive cybersecurity, while the primary focus is on immediate safety concerns, EV battery packs introduce several new points of vulnerability and safety concerns which need to be explored.



Pictorial illustration of attack scenarios. The illustration enumerates all the variables that need to be considered for analyzing the impact of a cyberattack, which could be (i) Physical or (ii) Financial. The attack could utilize auxiliary components or the charging systems. We can also see the attacker's various control dimensions. The attacks can cause temporary effects or permanent damage with attacks that span longer timescales. The only environmental state variable of relevance is the ambient temperature. The different variables that define the state of the battery pack influence the magnitude of impact due to the cyberattack. (The automobile outline illustration is published with permission from Chris Philpot.)

One challenge in assessing systems involving batteries is to accurately analyze the complex molecular-scale processes occurring inside a closed system. A practical battery system stores a fixed amount of energy via reversible electrochemical reactions. During normal operation, several unwanted side reactions also occur, which eventually degrade the battery's ability to store energy and thus, reduce the lifetime.[5] In addition, from a safety standpoint, batteries have a specified range of temperatures for safe operation, outside of which there is a potential risk of fire.[3] Cyberattacks may compromise driving range by draining energy through a higher load, reduce lifetime by enhancing side reactions, and compromise safety by pushing the operating conditions to unsafe limits.

In this article, we develop a physics-driven approach to systematically analyze cyberattacks against EV batteries through simulations of the operation of an EV along with its subsystems. Using this framework, we identify different cyberattack scenarios that can cause either temporary or permanent damage to battery systems.

Attack Model

The threat model for an EV is centered around an attacker who aims to cause either physical or financial losses through cyberattacks. Modern vehicles, including EVs, contain several devices called Electronic Control Units (ECUs) that are responsible for the majority of vehicle's functions. These ECUs gather sensor inputs and actuate mechanical components within the vehicle.[1] Recent efforts have demonstrated numerous vulnerabilities in automotive networks, particularly those that employ the Controller Area Network (CAN) communication protocol. CAN is the prevailing standard for intra-vehicle communication due to low cost and robustness; however, there are many CAN exploits.[1] An attacker can gain access to the vehicle's internal network via direct physical access[1,6] or the remote exploitation of an ECU with existing direct access.[2]

Introduction to Attack Scenarios: If an attacker aims to cause financial impact, one attack trajectory could be reducing the lifetime of the battery pack by enhancing the rate of degradation. In terms of physical damage, cyberattacks could increase the risk of thermal runaway where the attacker can overcharge or overdischarge the battery pack through attacks on the battery management systems (BMS) used in conjunction with parasitic loads.

In order to enable an analysis of attacks that involve auxiliary components, we have systematically compiled and curated the energy consumption patterns of different auxiliary components along with their characteristic power profiles.**Add figshare link?** The attacks on charging systems are simulated through modifications incorporated within the charging protocols. A physics-based experimentally validated battery model[7] is used within a vehicle dynamics model to simulate the operation of the EV.[8,9] We also explore the concept of 'stealthiness of attacks' and the trade-offs between stealthiness of attack and extent of damage from the attack.

Results

In this project, we analyze either financial and physical losses incurred through either: (i) permanent damage, defined as a change in the state of system that is irreversible, for example, irreversible capacity loss in a battery pack and (ii) temporary damage, defined as a change in the state of system that is (mostly) reversible, for e.g., reduction in state-of-charge which can be recovered by re-charging.

Permanent Damage

As we stated previously, cyberattacks can accelerate cell degradation and shorten the lifetime of the battery pack. Experimental demonstration of degradation is typically indirect as batteries are closed systems and measuring the internal states of the batteries is extraordinarily difficult. Thus, a validated physics-based model that can track the internal states of a battery packs provides a convincing means to demonstrate permanent damage due to cyberattacks.

Among the different mechanisms that cause cell degradation, two main processes of interest are: (i) growth of the solid-electrolyte interphase (SEI) layer at the graphite anode and (ii) lithium plating.[10,11] The SEI layer grows as a result of solvent reduction at the anode-electrolyte interface and consumes Li^+ ions, thereby causing a decrease in the amount of active Li^+ ions available and a reduction in capacity. Plating of Lithium at the anode similarly leads to a loss in capacity as well as an increase in the risk of internal shorts which could lead to catastrophic safety issues.[3]

We propose that the permanent damage due to a cyberattack can be quantified using the rise in the internal resistance of the cell. The rise in the internal resistance is estimated using the increase in the thickness of the SEI layer.[10] The extent of Li-plating is controlled by the electrochemical potential for lithium deposition or the 'Li-plating potential'.[11] The EV battery pack end-of-life is characterized by degradation in capacity to 80% of the initial capacity. We define the usable 20% of the capacity as the 'vital capacity' of the battery pack.

Compromised Auxiliary Components: Compromised auxiliary components effectively act as parasitic loads. Quantifying the impact of such attacks requires a close examination of different operating and environmental variables. The variations in each of the state variables like temperature, state-of-charge (SOC), pack size, age of the pack, etc. and the set of variables that defines a given auxiliary component attack workload affects the degradation in vital capacity in a different manner. A parametric analysis of all the variables, exploring the effect of each variable, similar to other studies[12,13] reveals that the damage to vital capacity increases with the temperature by following the Arrehenius relationship which implies that cyberattacks conducted at higher ambient temperature would cause greater impact. Damage to vital capacity also increases with the State-of-Charge of the battery pack which suggests that attacks on fully charged battery packs would cause more damage. As the age of the pack increases, the damage caused by a fixed load in the same conditions decreases. The damage to vital capacity is seen to be a sub-linear function of the total time of attack, characteristic of a diffusion-limited process. Further, damage to vital capacity increases linearly with an increase in the cumulative energy consumption of the load.**add refs**

Following the insights from the parametric analysis, attacks which comprise of energy intensive auxiliary components engaged after a new battery pack is fully charged would cause the most damage. We design the attack scenarios accordingly. We consider two types of EV users based on charging behavior, either charging once at 'Home' or charging one at 'Home' and at 'Work'. The sample attack workload spans a duration of one hour and is based on the combination of A/C at high power along with Lights, Power-Steering and Wipers. We analyze the cases where these users are located in Oslo, San Francisco, Beijing, Delhi and Phoenix which serve as proxies for the environment state variable of temperature and are chosen to represent a wide range of temperature conditions. In order to analyze the impact of auxiliary component cyberattacks, we use ΔR, a quantity which represents the increase in internal resistance of the cell compared to a cell which has not been subjected to the attack workloads. ΔR essentially provides information on the effectiveness of the cyberattack. We calculate ΔR after 400 days for each case using the following relationship,

$$\Delta \mathrm{R} = \frac{\mathrm{R}_{\mathrm{SEI}}^{\mathrm{A}} - \mathrm{R}_{\mathrm{SEI}}^{\mathrm{B}}}{\mathrm{R}_{\mathrm{SEI}}^{\mathrm{B}}}, \tag{1}$$

where $\mathrm{R}_{\mathrm{SEI}}$ is the resistance due to the SEI layer, and 'A' and 'B' represent the attack and baseline scenario. For the quantities reported in (Fig. 1), $\Delta\mathrm{R}^*$ values are obtained by normalizing all the ΔR values with the minimum value in a given set which facilitates the comparison of values within the set.

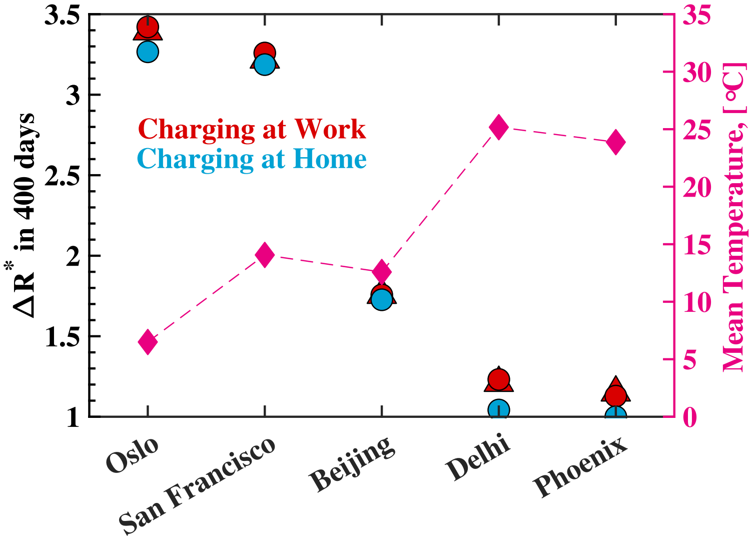


Figure 1: We can study the impact of auxiliary component cyberattacks here, based on the results for simulations equivalent to ∼400 days. $\Delta\mathrm{R}^*$ represents the increase in the resistance of the cell due to the cyberattack when compared to the baseline scenario. The triangular markers indicate situations where the vehicle is attacked twice in a day. In such cases, the average $\Delta\mathrm{R}^*$ of the two attacks is shown, while the circular markers represent the cases with one attack over the day.

In (Fig. 1), the rise in $\Delta\mathrm{R}^*$ is the most for Oslo, which has the lowest average ambient temperature. While an increase in ambient temperature causes an increase in the thickness of the SEI layer, the resistance due to the formation of SEI layer impedes further growth. This phenomenon leads to the fact that places like Phoenix, where the ambient temperature is high, already feature a substantial SEI layer thickness, thereby minimizing any additional damage to vital capacity due to the attack workload. However, it is worth highlighting that the average resistance due to the SEI film formed is higher in warmer regions compared to colder regions. The two cases of charging, at Home and at Work, do not show any substantial difference, although, if the EV is charged in both locations, then we have two separate time windows for attack.

Compromised Battery Management Systems, Overdischarge: When a BMS is compromised, an override of the lower cut-off voltage is possible.[14] An attack on an EV with a depleted battery pack and compromised BMS can lead to overdischarge through energy-intensive auxiliary components. In terms of such cyberattacks occurring on an EV with the depleted battery pack, the idea of using wake-up functions as attacks has been demonstrated recently.[15] Such attacks could be followed by auxiliary component attacks discussed in this work, to overdischarge the cells. During overdischarge, the initial stages involve the decomposition of the SEI layer which is composed of Lithium containing compounds and subsequently Copper dissolution from the current collector begins.[16] The dissolved Copper ions eventually lead to deposition of metallic Copper and potential internal shorts. The time for potential failure can be estimated using the time required for the decomposition of the SEI layer during the cyberattack, as shown in (Fig. 2). The cells shown in (Fig. 2) correspond to that of a 100 kWh battery pack based on NCA ($Ni_{0.8}Co_{0.15}Al_{0.05}O_2$) cathode and Graphite anode. The thickness of the SEI layer is a function of the age of the battery pack where 50nm is assumed to be equivalent to a battery pack aged over 2 years, however, the thickness would change with the vehicle operating conditions. We observe that attacks that involve components with an energy consumption rate of over 200W, the timescale for the complete decomposition of the SEI layer and potential failure is under 2 hours. While the consequences of overdischarge in Li-ion batteries depend on the kind of materials used in the cells, the impact could range from the loss of energy through the internal short to thermal and safety events as well.[14,16]

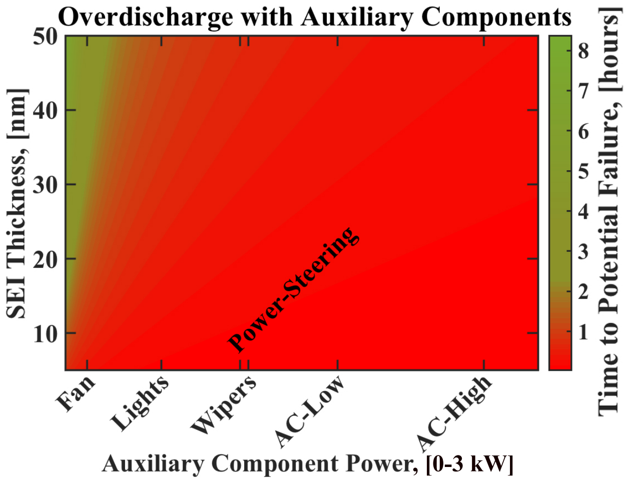


Figure 2: A compromised battery management system, is vulnerable to attacks that override the lower voltage cutoff which can overdischarge the pack. During overdischarge, one of the initial steps is the decomposition of the Li-ion containing SEI layer which is followed by the dissolution of copper ions from the current collectors, with the possibility of internal shorts and other safety events. The estimated time to the onset of copper dissolution occurs during overdischarge is shown above for the cells based on NCA ($Ni_0.8Co_0.15Al_0.05O_2$) cathode and Graphite anode. For components with the power consumption equivalent to lights (~200 W), the time to onset of copper dissolution is under 2 hours while components with a high power consumption like air-conditioning have a timescale of less than an hour.

Compromised Battery Management Systems, Overcharge: A compromised BMS can modify the upper cut-off voltage.[17] The pack can then be charged at a voltage higher than the

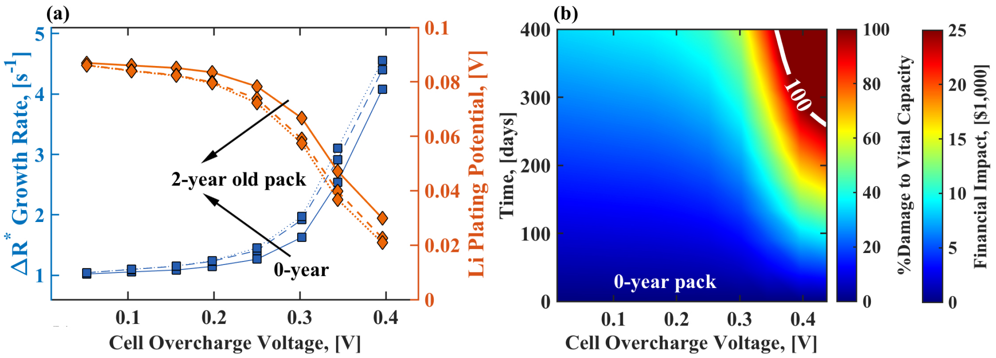


Figure 3: The impact of cyberattacks on charging systems specifically aimed at overcharging the battery pack is summarized here.(a) The attacks studied here span one hour after charging. We can study the increase in the SEI growth rate and ΔR*.(b) This increase along with Li-plating translates to capacity fade and could shoten the lifetime to about 200 days at an overcharge voltage of about 0.4V. The reduction in the Li-plating potential due to overcharge in (Fig. 3a), which provides a metric to quantify the risk of internal shorts and safety events like fire. As the same attacks are performed on older packs, we can observe that the ΔR* growth rate increases while the Li-plating potential decreases, both of which are detrimental to the state-of-health of the battery pack.

normal charging voltage leading to overcharging. Within a constant current-constant voltage protocol, an increase in the charging current would lead to an increased rate of degradation which is an extension of the previously mentioned parametric analysis on the discharge rate of the battery pack. However, overcharging the battery pack leads to various other issues as shown in (Fig. 3).

In (Fig. 3a), we observe a superlinear rise in the growth rate of ΔR* as the overvoltage per cell increases in a fresh cell. The charging system cyberattack simulated spans a duration of one hour after charging similar to the auxiliary component cyberattacks. However, the consequent damage caused to the battery pack in terms of capacity fade, as shown in (Fig. 3b), is enormous. At a cell overvoltage of 0.4V, we observe that the pack reaches its end-of-life or 100% damage to vital capacity in about 200 days. This could result in significant financial impact as shown in (Fig. 3b) where we estimate the monetary value of the loss of capacity for a 100kWh battery pack assuming the cost of battery packs of about $200/kWh.[18] (Fig. 3a) also shows the decrease in the Li-plating potential which implies that lithium would plate more readily at higher overvoltage. Over time, such attacks could lead to an increased amount of Li-plating which could have safety implications resulting in physical impact including thermal events and fire.[19]

Temporary Damage

With compromised auxiliary components, attack workloads can cause a depletion of energy contained in the battery pack, thereby a reduction in available driving range. This damage can be reversed by charging the battery pack. However, such attacks can play into the well-known issue of 'range anxiety'. For some vehicles, with battery packs <40kWh battery packs, up to 20% of the available range could be depleted in under one hour with energy intensive attack workloads which include combinations of auxiliary components as discussed previously. Such attacks which engage several components at the same time will be more energy intensive compared to single components, however, such attacks might be easier to detect for the user which is discussed in the subsequent sections.

Stealthiness of Attack

An important constraint on a cyberattack is the likelihood of it getting detected. In the case of auxiliary components, the detection is by the user and hence it is difficult to develop a quantitative metric for the same. However, in order to provide a basic overview of the issue, we develop a qualitative understanding using three scenarios, namely, ‘parked’, ‘stationary’ (at rest within driving operation) and ‘driving’. A summary of the stealth of an attack involving a given auxiliary component is given in (Tab. 1). Such a metric is heuristic but it provides a calibration for the components that are more likely to be targeted based on the attacker’s perspective. An auxiliary component that involves a high stealthiness of attack and is also energy intensive would naturally be targeted often.

Table 1: Stealthiness of attack, a qualitative metric used by attackers to reduce the chance of detection.

Auxiliary Component	Stealthiness of Attack		
	Parked	Stationary	Driving
A/C-High	High	Low	Medium
A/C-Low	High	High	High
Power Steering	N/A	High	High
Lights	High	Low	Medium
Fan	High	Low	Medium
Wipers	Medium	Very Low	Very Low
Combinations	High	Low	Low

Rowhammer Attack

Rowhammer style attacks[20] have been demonstrated previously where targeted workloads on memory systems were generated to cause corruptions which can be used to launch further attacks. We observe an analogous case here with battery systems since battery pack is made up of several cells arranged in a matrix involving a series-parallel configuration. This architecture is vulnerable to ‘rowhammer’ attacks since individual strings or cells within battery packs could be targeted through a compromised battery management system and the damage to individual strings or cells is magnified. Each of the cyberattack scenarios we have considered, like attacks on auxiliary components, overcharge, and overdischarge could be orchestrated as rowhammer attacks. We previously discussed the various factors due to which the damage to the battery pack increases with a reduction in pack size for the same workload which is especially relevant to rowhammer attacks. Such attacks could not only shorten the lifetime of the targeted subset of the battery pack but could also lead to issues related to instabilities due to the isolation of strings within the battery pack.

Conclusions

We have discussed the potential physical and financial impact due to cyberattacks on EVs and EV subsystems. We identify simple but effective cyberattacks on auxiliary components that can temporarily drain the battery pack up to 20% per hour. Furthermore, we analyze attacks could lead to a deterioration in the power capability due to an increase in the cell resistance. We use a metric which is equivalent to the 'normalized resistance increase', which can be used to quantify the extent of performance reduction. We find that normalized resistance increase is generally higher for colder regions. We find that cyberattacks on auxiliary components launched after the pack is completely charged (i.e. high state-of-charge) leads to more damage. The cell resistance increase, largely due to the formation of a solid-electrolyte-interphase (SEI) layer, follows a sublinear relationship with time. This results in a new pack being more vulnerable than an aged pack to cyberattacks on auxiliary components. Compromised battery management systems expose the pack to two kinds of attacks, (i) Overdischarge and (ii) Overcharge. Overdischarge attacks which override the lower cutoff voltage of the pack could lead to the complete decomposition of the SEI layer in under two hour thorough auxiliary components with a power rating of over 200W. The decomposition of the SEI is followed by the dissolution of Copper ions which could eventually lead to internal shorts and potential safety events. Cyberattacks launched during charging through the compromise of the voltage regulator could lead to an overcharge of the cells, which in some cases could even lead to physical safety issues (e.g. fire). Further, this could lead to a new pack being depleted to 80% of its initial capacity (end-of-life for an EV battery) in less than a year. Finally, a compromise of the battery management system could lead to novel "rowhammer"-style attacks (attacking a string of cells), which could damage a subset of cells in a short time span. We believe that the results presented here will inform the development of robust detection and prevention systems and provide a rational design approach for electric vehicle automotive security.

References

(1) Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S. Experimental security analysis of a modern automobile. 2010 IEEE Symposium on Security and Privacy. 2010; pp 447–462.

(2) Miller, C.; Valasek, C. Remote exploitation of an unaltered passenger vehicle. 2015.

(3) Crabtree, G.; Kócs, E.; Trahey, L. *MRS Bulletin* **2015**, *40*, 1067–1078.

(4) Safari, M. *Energy Policy* **2018**, *115*, 54–65.

(5) Santhanagopalan, S.; Guo, Q.; Ramadass, P.; White, R. E. *J. Power Sources* **2006**, *156*, 620–628.

(6) others,, et al. Comprehensive Experimental Analyses of Automotive Attack Surfaces. USENIX Security Symposium. 2011.

(7) Kalupson, J.; Luo, G.; Shaffer, C. E. *AutoLion^{TM}: A thermally coupled simulation tool for automotive Li-ion batteries*; 2013.

(8) Sripad, S.; Viswanathan, V. *J. Electrochem. Soc.* **2017**, *164*, E3635–E3646.

(9) Sripad, S.; Viswanathan, V. *ACS Energy Lett.* **2017**, *2*, 1669–1673.

(10) Safari, M.; Morcrette, M.; Teyssot, A.; Delacourt, C. *J. Electrochem. Soc.* **2009**, *156*, A145–A153.

(11) Yang, X.-G.; Leng, Y.; Zhang, G.; Ge, S.; Wang, C.-Y. *J. Power Sources* **2017**, *360*, 28–40.

(12) Safari, M.; Morcrette, M.; Teyssot, A.; Delacourt, C. *J. Electrochem. Soc.* **2010**, *157*, A713–A720.

(13) Safari, M.; Morcrette, M.; Teyssot, A.; Delacourt, C. *J. Electrochem. Soc.* **2010**, *157*, A892–A898.

(14) Lee, Y.-S.; Cheng, M.-W. *IEEE Transactions on Industrial electronics* **2005**, *52*, 1297–1307.

(15) Cho, K.-T.; Kim, Y.; Shin, K. G. *arXiv preprint arXiv:1801.07741* **2018**,

(16) Guo, R.; Lu, L.; Ouyang, M.; Feng, X. *Scientific reports* **2016**, *6*, 30248.

(17) Lelie, M.; Braun, T.; Knips, M.; Nordmann, H.; Ringbeck, F.; Zappen, H.; Sauer, D. U. *Applied Sciences* **2018**, *8*, 534.

(18) Kittner, N.; Lill, F.; Kammen, D. M. *Nat. Energy* **2017**, *2*, 17125.

(19) Abada, S.; Marlair, G.; Lecocq, A.; Petit, M.; Sauvant-Moynot, V.; Huet, F. *J. Power Sources* **2016**, *306*, 178–192.

(20) Kim, Y.; Daly, R.; Kim, J.; Fallin, C.; Lee, J. H.; Lee, D.; Wilkerson, C.; Lai, K.; Mutlu, O. Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors. ACM SIGARCH Computer Architecture News. 2014; pp 361–372.