A Time-Stamp Attack on Digital Twin-Based Lithium-ion Battery Monitoring for Electric Vehicles*

Mitra Pooyandeh
Division of Electronics & Electrical Engineering
Dongguk University
Seoul, Republic of Korea
mitra.p@dgu.ac.kr

Insoo Sohn
Division of Electronics & Electrical Engineering
Dongguk University
Seoul, Republic of Korea
isohn@dongguk.edu

***Abstract*—Digital twin technology plays a crucial role in accurately estimating the State of Charge (SoC) for Lithium-ion Batteries (LIBs) in the field of electric vehicles. These digital replicas provide real-time insights into LIB behavior, enabling predictive maintenance and ensuring vehicle performance and safety. However, the security of digital twin-based LIB monitoring systems has become a critical concern, despite their numerous benefits.This study delves into the security aspect of digital twin technology, focusing on the vulnerability of SoC estimation to timestamp attacks. These covert attacks disrupt the chronological order of data packets, casting a shadow on the integrity and accuracy of LIB state predictions. This research aims to shed light on the disruptive capability of timestamp attacks, emphasizing the need for robust defense mechanisms to safeguard the integrity of EV battery data and the reliability of prediction models.**

***Index Terms*—Digital Twin, Security, Lithium-ion Batteries(LIBs), Time-Stamp Attack**

I. Introduction

In an era defined by the ever-expanding universe of electric vehicles (EVs), the precise monitoring and predictive maintenance of Lithium-ion Batteries (LIBs) are paramount for ensuring vehicle performance, safety, and longevity. To achieve these goals, digital twin technology has emerged as a transformative force, enabling real-time insights into LIB behavior. Yet, with the introduction of digital twins into LIB monitoring systems comes a new set of challenges. It is important to ensure the security of the digital twins as they can be vulnerable to cyberattacks, which can result in data theft or complete system takeover [1]. A security breach can have severe consequences, including compromising the accuracy and reliability of the physical systems that the digital twins represent. Among these challenges the vulnerability to timestamp attacks stands out. These covert attacks strategically manipulate the chronological order of timestamps within data packets while leaving data contents intact, casting a shadow on the integrity and accuracy of LIB state predictions.

In the world of Cyber-Physical Systems (CPS), wireless networks enable smooth connectivity [2], and the transfer of time-critical information is crucial for remote state estimation and control to function effectively. However, the reliance on wireless channels has unearthed a significant security concern. Consequently, researchers have extensively explored attacks from an adversary's perspective, mapping out a three-dimensional attack space that encompasses the adversary's prior knowledge, disclosure, and disruption resources.

These investigations have categorized attacks into two distinct yet interconnected domains: deception attacks and disruption attacks. Deception attacks involve the injection of additional data to sow doubt and reduce the accuracy of remote estimators [3]. Researchers have meticulously crafted optimal deception attacks and explored multi-sensor scenarios where malicious actors compromise target sensors. In parallel, disruption attacks focus on the interruption of data reception, epitomized by denial of service (DoS) attacks. These attacks have undergone thorough examination, with researchers optimizing control signals and probing the energy consumption–bit error rate relationship. Yan et. al [4] focused on the synchronization control problem in a two-link master-slave manipulator system. The system faced deception attacks on the communication channel, resulting in inaccurate sensor data and disrupted control. To address this issue, a deception attack parameter was introduced into the manipulator's dynamics. An adaptive law was developed for model estimation and compensation, improving system stability. A new analytics framework has been developed by Choi et. al [5] to analyze cyber attacks on Industrial Control Systems (ICS) by specifically examining the communication channels between HMIs and PLCs. This framework enables security researchers to assess ICS attacks without the need for specialized tools or knowledge of ICS protocols, PLCs, or network penetration testing. By using digital twin scenarios, the framework has successfully demonstrated deceptive attacks that are difficult to detect, introduced heuristic inference attacks, validated experiments using a water utilities scenario, and suggested countermeasures based on time complexity theory. Li et. al [6] examines the use of deception attacks in remote state estimation, where multiple sensors, both reliable and unreliable, are used to trick anomaly detectors and hinder the accuracy of the estimation. A strategy for linear attacks is introduced, which

involves using disclosure and disruption resources. The study establishes criteria for avoiding detection by existing detectors, analyzes how the estimation error covariance changes during attacks, and derives a mathematical expression for the optimal linear deception attack. In this nuanced landscape, a significant security challenge has emerged, standing between the realms of deception and disruption attacks. Here, a distinctive capability takes shape: attackers with limited resources can manipulate the timestamps of data packets without altering the data's core content. This scenario, with practical implications especially in real-time applications, introduces the concept of the "time-stamp attack." As part of this article, we analyze the workings and ramifications of time-stamp attacks in the context of both LIB monitoring systems and CPS based on digital twins. By analyzing the disruptive potential of time-stamp attacks, we aim to raise awareness of the security challenges faced by these systems. Our work contributes to the understanding of potential vulnerabilities and emphasizes the need for robust defense mechanisms to preserve the integrity of EV battery data and the reliability of prediction models. As the landscape of electric vehicles continues to evolve, addressing these security challenges becomes not only pivotal but a linchpin in the broader mission of fostering the widespread adoption of electric vehicles and a sustainable automotive future.

The remainder of the paper is organized as follows: Section II introduces the overall system model and attack structure. The simulation results are presented in Section III, and Section IV concludes the paper.

II. Problem Formulation

A. System Structure

The proposed system contains two parts: On the physical side, it employs a cloud-based IoT network that connects and monitors EVs equipped with a Battery Management System (BMS) for tracking essential battery parameters and an offline model [7] driven by machine learning to make accurate State of Charge (SOC) predictions.The SOC indicates how much energy is being stored in a battery or energy storage system. It measures the remaining capacity of the battery, indicating the amount of energy that can still be utilized, usually represented as a percentage of the total capacity. The digital side introduces a Digital Twin, enabling real-time monitoring and forecasting of battery activities, supplemented by the creation of synthetic data to enhance SOC prediction precision. Through the integration of these components, the system advances LIB monitoring, fostering ideal performance and safety in EVs.

Dataset [8]: The dataset used in this study comprises Multivariate time series data obtained from Li-ion batteries, containing 45122 samples and eight features. These features include ID-cycle, Voltage-measured, Current-measured, Temperature-measured, Capacity, Current-charge, Voltage-charge, and Time. This comprehensive dataset is instrumental for analyzing battery behavior and capturing temporal relationships. It serves various purposes, including anomaly detection, pattern recognition, and the prediction of LIB performance and longevity in the context of Electric Vehicles (EVs).

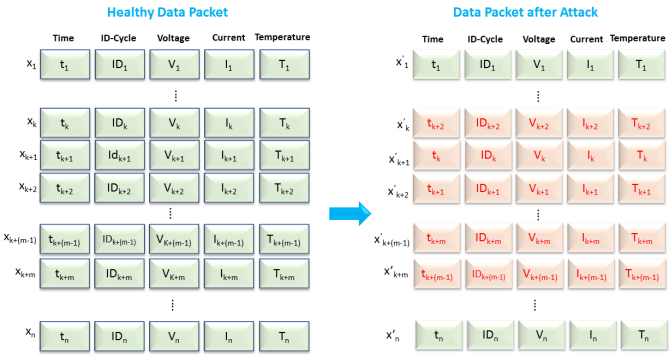

Fig. 1. Transmission of data with a Time-stamp attack.

B. Attack model

This study focuses on a scenario where an attacker with limited capabilities aims to disrupt the order of data packets, thereby compromising the estimation performance of the LSTM estimator in the digital twin. Five crucial features, selected for State of Charge (SoC) estimation by LSTM, include Voltage-measured, Current-measured, ID-cycle, Temperature-measured, and Time. The assumptions about the attacker's abilities are as follows:

- The adversary has restricted attack capabilities and cannot modify the data itself.
- The adversary can manipulate the timestamps of data packets stored in the buffer, typically through EVs charge stations.

C. Time-Stamp Attack Structure

A timestamp attack involves altering the order of data packets to disrupt their chronological sequence [9]. Our data sequence consists of five features: time (t), ID cycle (ID), voltage (V), current (I), and temperature (T).

The original data sequence is represented as: $[x_1, x_k, x_{k+1}, \ldots, x_{k+m}, \ldots, x_n]$, with $n = 45122$, and $1 < k < m < n$.

Each data point (x_i) within this sequence includes values for the five features: $[t_i, ID_i, V_i, I_i, T_i]$.

In a timestamp attack, the adversary's goal is to reorder the timestamps to introduce disruption. Mathematically, the manipulated sequence can be depicted as: Manipulated Data Sequence: $[x'_1, x'_k, x'_{k+1}, \ldots, x'_{k+m}, \ldots, x'_n]$ In this scenario, we assume the adversary is attacking data packets $x_k, \ldots, x_{k+m}$.

Within this manipulated sequence, timestamps have been reordered with the aim of negatively impacting the LSTM estimator's performance. For example:

$x'_1 = [t_1, ID_1, V_1, I_1, T_1]$
$x'_k = [t_{k+2}, ID_{k+2}, V_{k+2}, I_{k+2}, T_{k+2}]$
$x'_{k+m} = [t_{k+(m-1)}, ID_{k+(m-1)}, V_{k+(m-1)}, I_{k+(m-1)}, T_{k+(m-1)}]$
$x'_n = [t_n, ID_n, V_n, I_n, T_n]$

Here, the timestamps have been reordered to disrupt the chronological order. we can see the attack structure in Fig. 1.

D. Evaluating Estimation Performance Metrics

In the realm of digital twin-based systems, the error covariance is of utmost importance when it comes to evaluating the precision and dependability of state estimation. The error covariance measures the connections between various state variables and their uncertainties. The covariance can reflect the extent to which the attack disrupts the accuracy and reliability of state predictions. By analyzing the error covariance before and after the attack, we quantify how the attack affects the system's ability to estimate states accurately.

Using Error Vector and Covariance Matrix, we can calculate error covariance:

The error vector represents the differences between the estimated states and the true states. Let's denote this error vector as E where E can be expressed as:

$$E = X - X' \tag{1}$$

where E is the error vector, X is the true state vector, and X' is the estimated state vector. Now we calculate the covariance matrix for the error vector E. The covariance matrix, denoted as Σ, captures the variances and covariances between different elements of the error vector. The covariance matrix Calculated as follows:

$$\sum = \frac{1}{N} \sum_{i=1}^{N} E_i E_i^T \tag{2}$$

where, N is the number of data points, E_i is the error vector for the i_{th} data point,and E_i^T is the transpose of the error vector for the i_{th} data point.

III. Simulation and Experimental Results

We provide in Fig. 2 a comparative analysis of State of Charge (SOC) estimations. The plot (a), represents the SOC values provided by the battery manufacturer. Plot (b),illustrates the SOC predictions made by the digital twin system prior to a simulated attack. Finally, plot (c),shows the stark contrast between the digital twin's predictions before and after a timestamp attack. SOC estimation accuracy is clearly illustrated by this visual representation, highlighting the importance of securing battery monitoring systems in electric vehicles. Fig. 3 shows the relationship between State of Charge (SOC) Covariance and timestamp over time. SOC Covariance measures how the SOC values vary with each other. The plot reveals fluctuations in SOC Covariance over time, indicating variations in the accuracy and precision of SOC predictions. A timestamp attack that alter the chronological order of data packets can cause these fluctuations. In order to ensure reliability and security, this plot helps assess the impact of timestamp attacks on SOC estimation and develop defense mechanisms for ensuring reliability and security.

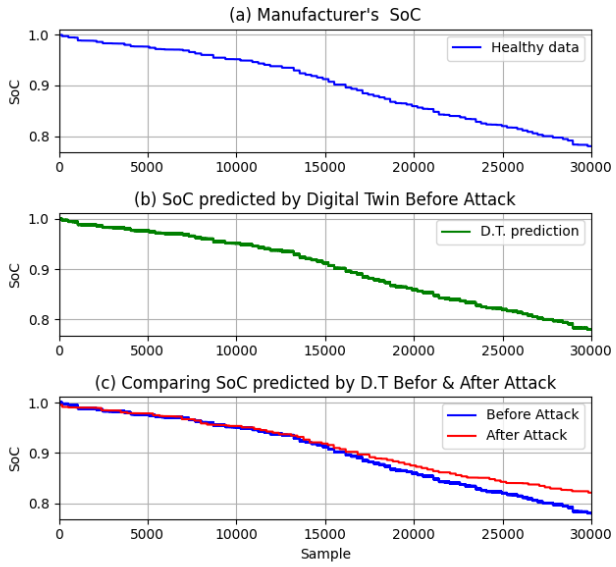

Fig. 2. Impact of Time-stamp Attack on SOC Estimation by Digital Twin.

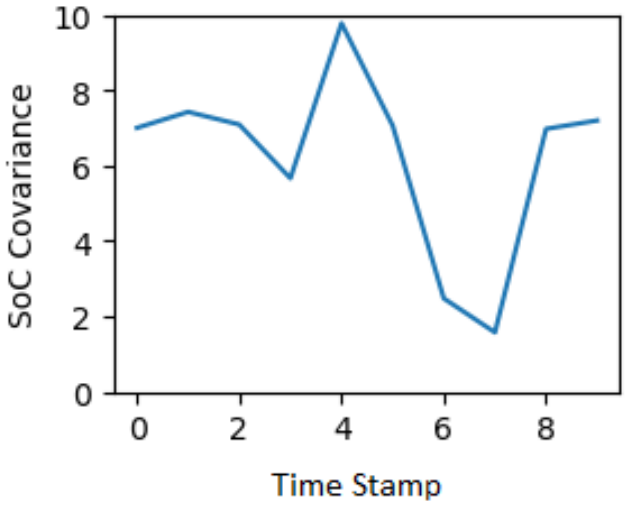

Fig. 3. Error Covariance of SoC with Time-stamp Attack.

IV. Conclusion

In this paper we explored a timestamp attack on a digital twin. The security of Lithium-ion Battery (LIB) monitoring is of utmost importance in the age of electric vehicles. Although digital twin technology improves the accuracy of state-of-charge (SoC) estimation, our investigation highlights the susceptibility of these systems to timestamp attacks. As electric vehicles advance, securing LIB monitoring systems is vital for their growth. Our proposed attack model forms a basis for further research in this area. By addressing these security challenges, we contribute to a safer and more efficient automotive future. The focus of future efforts will be to

develop a solution to prevent the timestamp attack.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. RS-2023-00252328).

REFERENCES

[1] E. Karaarslan and M. Babiker, "Digital Twin Security Threats and Countermeasures: An Introduction," 2021 International Conference on Information Security and Cryptology (ISCTURKEY), Ankara, Turkey, 2021, pp. 7-11.

[2] Pooyandeh, M. and Sohn, I., "Edge network optimization based on ai techniques: A survey," Electronics , 10 (22), 2830,2021.

[3] Shamshiri, S., Han, K.J., Sohn, I. "DB-COVIDNet: A Defense Method against Backdoor Attacks," Mathematics 11, 4236, November 2023.

[4] C. Yan,and J. Ge, "Synchronous control of master-slave manipulator system under deception attacks," Chinese Control And Decision Conference (CCDC), pp. 1778–1782, August 2020.

[5] T. Choi, G. Bai, R. K. L. Ko, N. Dong, W. Zhang and S. Wang, "An Analytics Framework for Heuristic Inference Attacks Against Industrial Control Systems," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp. 827-835.

[6] Y. Li, Y. Yang, Z. Zhao, J. Zhou and D. E. Quevedo, "Deception Attacks on Remote Estimation With Disclosure and Disruption Resources," in IEEE Transactions on Automatic Control, vol. 68, no. 7, pp. 4096-4112, July 2023.

[7] Y. Qin, A. Arunan and C. Yuen, "Digital Twin for Real-time Li-Ion Battery State of Health Estimation With Partially Discharged Cycling Data," in IEEE Transactions on Industrial Informatics, vol. 19, no. 5, pp. 7247-7257, May 2023, doi: 10.1109/TII.2022.3230698.

[8] Chen Fei, October 13, 2022, "Lithium-ion battery data set", IEEE Dataport, doi: https://dx.doi.org/10.21227/fh1g-8k11.

[9] F. Qu, N. Yang, H. Liu, Y. Li and D. E. Quevedo, "Time-Stamp Attacks on Remote State Estimation in Cyber-Physical Systems," in IEEE Transactions on Control of Network Systems, doi: 10.1109/TCNS.2023.3285866.