2024 NDIA MICHIGAN CHAPTER
GROUND VEHICLE SYSTEMS ENGINEERING
AND TECHNOLOGY SYMPOSIUM
MODULAR OPEN SYSTEMS APPROACH (MOSA) TECHNICAL SESSION
AUGUST 13-15, 2024 - NOVI, MICHIGAN

IMPACT ANALYSIS OF CYBERATTACKS IN ELECTRIC PROPULSION SYSTEMS FOR HYBRID TRACKED VEHICLES.

Grace Muriithi[1], Behnaz Papari[1], Ali Arsalan[1], Asif Khan[1], Elutunji Buraimoh[2], Gokhan Ozkan[2], Laxman Timilsina[2], and Christopher Edrington[2]

[1]Dept. Automotive Engineering, Clemson University, South Carolina, USA
[2]Dept. Electrical and Computer Engineering, Clemson University, South Carolina, USA

ABSTRACT

In the age of advancing digitalization and integrating complex electronics within modern vehicles, hybrid tracked vehicles (HTVs) are increasingly becoming susceptible to cybersecurity threats. Particularly vulnerable are the control units, which have become prime targets for adversarial exploitation due to their pivotal role in vehicle functionality. To address these security concerns, this study demonstrates two distinct yet equally harmful scenarios using replay and DoS attacks to uncover and evaluate vulnerabilities within the Energy Management System (EMS) of HEVs. In the replay attack scenario, the adversary surreptitiously alters the SoC control messages emanating from the Battery Management System (BMS). The attack is calibrated to strategically time and sequence the message replays across various operational states using reinforcement learning, thereby maintaining apparent legitimacy within expected SoC ranges to evade detection. The DoS attack, however, presents a more direct threat by targeting the generator's revolution speed sensors. By compromising these sensors, the attack disrupts the generator and causes subsequent engine shutdowns, compelling the battery to singularly meet the vehicle's power supply demands. Formal attack models are developed and subsequently deployed on a simulated HTV platform within MATLAB/Simulink to analyze the impacts of these cyberattacks. The simulation results illustrate the impacts of the simulated cyberattacks, further reinforcing the importance of resilient and adaptive security measures for the control layer.

Citation: G. Muriithi, B. Papari, A.Arsalan, A. Khan, E. Buraimoh, "Impact Analysis of Cyberattacks in Electric Propulsion Systems for Hybrid Tracked Vehicles," In *Proceedings of the 2024 Ground Vehicle Systems Engineering and Technology Symposium (GVSETS)*, NDIA, Novi, MI, Aug. 13-15, 2024 .

1. INTRODUCTION

Recent advancements in vehicular technology have significantly enhanced the comfort, safety, efficiency, performance, and autonomy of modern hybrid tracked vehicles (HTVs). These improvements are largely attributable to increased connectivity, facilitated by technologies such as the Internet of Things (IoT), vehicle-to-X communication, and over-the-air updates, as well as the integration of sophisticated software within a growing number of Electronic Control Units (ECUs) [1, 2]. These ECUs, interconnected through Controller Area Networks (CANs), are central to the vehicle's functionalities.

However, this connectivity and software complexity expansion inadvertently broadens the potential attack surface, escalating the risk of cybersecurity breaches. The interconnected nature of ECUs via CAN bus compounds this issue, as an attack on a single ECU can propagate to others on the network, potentially compromising the entire vehicle system [3]. Such vulnerabilities are particularly concerning in the context of vehicle energy systems, where cyberattacks may not cause immediate physical damage but can result in substantial degradation of battery capacity and energy efficiency, thereby diminishing the vehicle's monetary value [4, 5].

The CAN bus, integral to real-time ECU communication, was designed for reliability, not secure communication, leaving it exposed to a range of malicious exploits [2]. Cyber attackers with network access could compromise vehicle behavior, induce energy inefficiencies, or launch a Denial-of-Service (DoS) attack. Recent research has highlighted the feasibility of such attacks, with examples including the disabling of brakes, remote steering control, and the immobilization of vehicles on highways [6]. The fundamental issue lies in the fact that vehicle network protocols were originally developed for closed systems and lack built-in security features, such as message authentication and encryption [7].

In response to the escalating cyber threat, the automotive industry must adopt a proactive approach to identify, evaluate, and mitigate cyber-physical vulnerabilities. Penetration Testing (PT), a mainstay in cybersecurity, is one method for revealing system weaknesses [8]. However, traditional PT approaches can be time-consuming and disruptive, particularly ill-suited for mission-critical systems integral to (H)EVs, which exhibit complex cyber-physical couplings. Moreover, the variability in real-world driving conditions introduces additional challenges in detecting and characterizing cyberattack impacts in cyber-physical systems [4, 9, 10]. Guo *et al.* [4] and Ye *et al.* [11] both highlight the increasing vulnerability of powertrain systems in (H)EVs to cyber threats, with Guo *et al.* focusing on the energy management system in hybrid electric vehicles (HEVs). Ye *et al.* discussed the broader challenges in connected electric vehicles (EVs). Guo *et al.* [12] further emphasizes the need for a systematic assessment of cyber–physical security in the energy management system of connected and automated EVs, proposing a methodology for impact analysis and evaluation metrics. To address these challenges, authors in [13] also presented a physics-guided machine learning approach for cyberattack detection in EVs, which considers varying driving scenarios and leverages data features reflecting the transient physical characteristics of the vehicle. These studies underscore the critical importance of enhancing the cyber–physical security of electrified powertrain systems in modern vehicles. The study by Sripad *et al.* [14] explored the ramifications of prolonged cyberattacks on electric vehicle (EV) batteries, specifically targeting their economic and strategic implications. This research highlighted how such attacks, particularly on auxiliary components of EV subsystems, could significantly deplete the battery's charge—potentially up to 20% per hour—leading

to a gradual decline in vehicle performance over time. In a separate study by Gerdes *et al.*, [15], the focus was on cyberattacks devised to impair the efficiency of autonomous vehicles. This work revealed that such attacks could escalate the energy consumption of affected vehicles by a range of 20% to 300%. Furthermore, Khalid *et al.* [16] contributed to the discourse by presenting a comprehensive framework to scrutinize, compare, and test cybersecurity standards for EV battery systems. This framework notably identifies key elements crucial to in-vehicle cybersecurity.

Despite the growing body of research on vehicular cybersecurity, there remains a notable gap in the literature concerning the specific impacts of cyber-attacks on the functionality and integrity of HTV systems. While various studies have delved into the security vulnerabilities of electric vehicles, particularly focusing on the in-vehicle ECUs, the unique interactions within HTVs between their electric components and traditional drivetrains are less understood. To bridge these gaps by gaining an understanding of the nuanced dynamics of HTVs under cyber-attack conditions, this paper presents an agent-based framework that attempts to uncover vulnerabilities in the cyber-physical domain, specifically within the vehicle's EMS. We focus on two attack scenarios: a covert replay attack that manipulates the high-voltage battery's state of charge (SoC) estimation to deceive the energy manager and a hidden DoS attack that disrupts generator revolution speed, causing engine shutdowns and forcing the battery to compensate for the entire vehicle's energy demand. Additionally, we formally analyze how these cyberattacks affect the vehicle's energy supply side. The contributions of this paper are threefold:

1. A replay attack that subtly alters SoC estimations, designed within a DRL-based PT environment modeled as a Markov Decision Process (MDP), encompassing the nuances of cyber-physical systems, attack methodologies, and their physical repercussions is presented
2. A DoS attack targeting generator revolution speed, with the attack characterized using a semi-Markov chain to capture the intricate aperiodic sampling nature caused by the DoS attack, is detailed.
3. The effects of these cyberattacks on the vehicle's energy management, highlighting their potential to compromise energy supply without directly affecting vehicle dynamics, are analyzed.

Through this work, we aim to contribute to designing, operating, and maintaining secure vehicular systems, enhancing their resilience to the ever-evolving landscape of cybersecurity threats. The rest of the paper is organized as follows. Section II presents the hybrid tracked Vehicle Modelling and System Descriptions. In section III, the mathematical model of the attack vectors is presented. The simulation results and analysis are provided in section IV. Finally, the conclusion and future research directions are presented in section V.

2. VEHICLE MODELING AND SYSTEM DESCRIPTIONS

This study centers on a high-speed series hybrid electric vehicle (HEV) equipped with tracks. The vehicle's architecture includes several key components: a battery, an engine-generator set, an electric drive system comprising motors and an inverter, an upper-level drive control system (which could be a human driver, an autonomous driving system, or adaptive cruise control), and a centralized Energy Management System (EMS). The drive control system sets the desired speed, while the EMS manages this speed target centrally. It does so by fine-tuning the torque output of the four motors to balance the energy use between the battery and the engine efficiently. Furthermore, the dynamic behavior of the tracked vehicle's steering

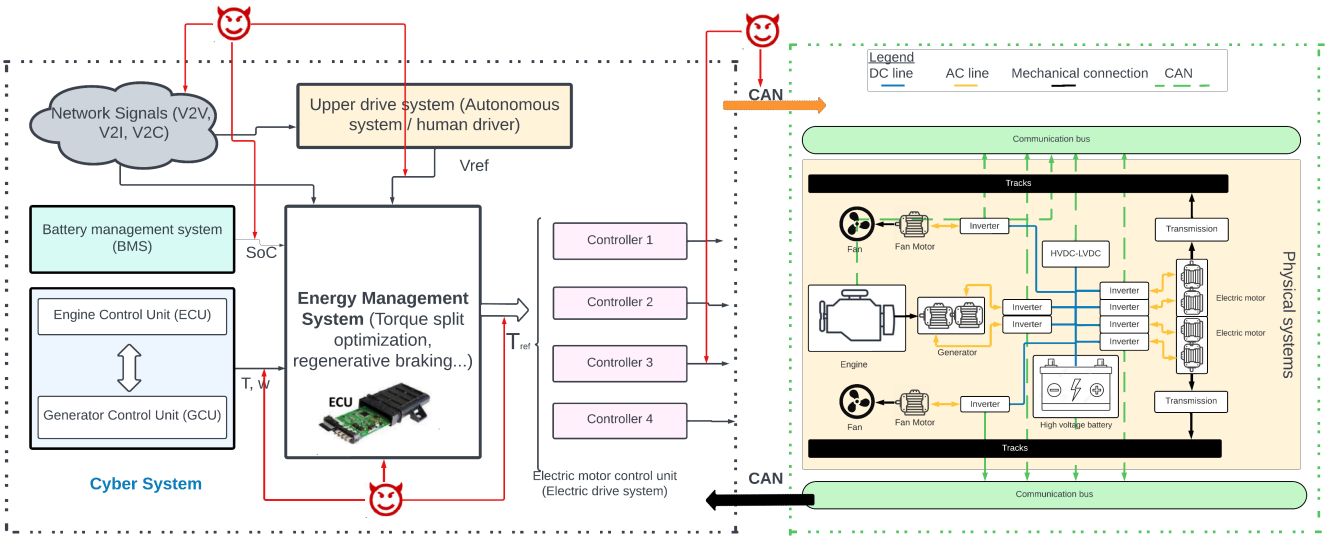

Figure 1: Cyber-physical diagram of the series HTV

is integrated into a 3-Degree of Freedom (3DOF) vehicle model. This model captures the vehicle's lateral and yaw movements, as detailed in [17]. Fig. 1 illustrates the cyber-physical vehicle diagram, highlighting potential points and signals where cyberattacks could be executed.

2.1. Vehicle Dynamics

Newton's second law of motion predominantly governs the longitudinal behavior of the vehicle. For the purposes of this design, the prediction horizon is segmented into N_p discrete intervals along an axis with a constant time step Δt. Within this framework, the dynamics of the vehicle along the longitudinal axis for the duration t within the range from $t \in [1, N_p]$ are modeled as [12]

$$s(t+1) = s(t) + v(t)\Delta t, \tag{1}$$

$$v(t+1) = v(t) + \frac{\Delta t[T_{total}(t)/r_w - G(t)]}{m} \tag{2}$$

$$G(t) = F_w(t) + F_g(t) + F_r(t), \tag{3}$$

$$T_{total}(t) = \sum_{i=1}^{4} T_{ref,i}(t) \tag{4}$$

where t represents the t-th time step, s and v indicate the cumulative distance traveled. The speed of the vehicle, respectively, and $s(1) = s_0$, $v(1) = v_0$; T_{total} refers to the aggregate torque requirement; r_w signifies the radius of the tire under dynamic conditions. The forces acting on the vehicle, namely F_w for aerodynamic drag, F_g for the resistance due to gradients and F_r for the resistance caused by tire rolling, are essential components of the vehicle's dynamics. These forces are calculated as shown below, where α denotes the road grade.

$$F_w(t) = \frac{1}{2}\rho_a A_f C_D v^2(t), \tag{5}$$

$$F_g(t) = mg\sin(\alpha(t)), \tag{6}$$

$$F_r(t) = mgf\cos(\alpha(t)). \tag{7}$$

2.2. Engine, Battery and Motor Model

The rate at which fuel flows through the engine is determined by a static mapping that correlates with the engine's torque, T_{ice} and its rotational speed ω_{ice}. This relationship is mathematically represented as $\dot{m}_f = f(\omega_{ice}, T_{ice})$, which effectively characterizes the engine's fuel consumption rate.

$$P_{fuel} = LHV \cdot \dot{m}_f \tag{8}$$

here LHV is the lower heating value of the fuel. Generally, the dynamics of the battery in the majority EMSs of (H)EVs are simplified to an equivalent resistance model [18]. At the t-th time instance, these dynamics are expressed as:

$$I_{bat}(t) = \frac{V_{oc}(t) - \sqrt{V_{oc}^2(t) - 4P_{bat}(t)R_b(t)}}{2R_b(t)} \tag{9}$$

Here, P_{bat} signifies the power either discharged or charged by the battery; I_{bat} denotes the electric current flowing through the battery; V_{oc} represents the open-circuit voltage of the battery, and R_b stands for the battery's internal resistance. Each of these variables is subject to change based on the battery's SoC, computed as follows:

$$SoC(t+1) = SoC(t) - \frac{\Delta t \cdot I_{bat}(t)}{C_{bat}} \tag{10}$$

where C_{bat} denotes the battery's nominal capacity. The power contributions of the battery and engine are typically derived from the mechanical power and efficiency of the motors, calculated as:

$$P_{bat}(t) + P_{eng}(t) = \sum_{i=1}^{4} \omega_i(t) T_i(k) \eta_i(\omega_i(t), T_i(t)) \tag{11}$$

where ω_i and T_i correspond to the angular velocity and the force exerted by the rotation of the motor number i-th motor, respectively. The efficiency with which these motors convert power, η_i, is typically quantified based on a mapping that relies on practical, experimental data. The state of the electric drive system's operation is indicated by ν with $\nu = -1$ indicating motor operation and $\nu = 1$ designating generator mode. Notably, the rotational speed ω_i (expressed in revolutions per minute) is directly related to the vehicle's velocity (measured in meters per second) under the assumption that tire slip is minimal [12]. In this vehicle configuration, the engine is connected to an electric generator. This generator and the battery are linked to a high-voltage DC conduit through inverters. This setup ensures an adequate electrical power supply to the electric motors downstream.

2.3. Energy Management System

The EMS adopts a rule-based approach to simplify the powertrain's design process. This strategy's fundamental goal is to provide the necessary electrical power to the high-voltage DC link. Simultaneously, it efficiently manages the power distribution between the battery pack and the generator. This distribution strategy is meticulously optimized to reduce fuel consumption while ensuring the operation consistently sustains the battery's charge. To adapt to real-time conditions, the EMS leverages feedback on the powertrain's state, including data on battery temperature, state of charge, and overall battery health. These metrics are crucial for dynamically adjusting power distribution to guarantee the vehicle's safe functioning. The vehicle's model has been crafted within the MATLAB/Simulink framework, which facilitates evaluating the series hybrid tracked vehicle's performance across diverse driving conditions and accurately reflects the control architecture employed in the actual vehicle prototype. Further elaboration on this vehicle model can be found in the referenced work [17].

3. ATTACK MODELLING

In Figure 1, the EMS system illustrates the primary signals susceptible to cyberattacks within common data channels, including sensory and actuation signals. It's essential to formulate mathematical models that encapsulate the nature of these attacks to analyze the effects of such cyberattacks on these critical feedback signals. The literature predominantly categorizes cyberattacks into DoS,

replay, and deception attacks. This study explores the influence of two specific types of cyberattacks - a hidden stochastic DoS attack and an automated replay attack - and how they impact the vehicle's energy management system.

3.1. DoS Attack Problem Formulation

The intervals of DoS attacks initiated by attackers to disrupt the communication between ECUs i and j are identified as the k-th period during which the communication link is obstructed. These intervals are mathematically expressed as $k \in N^+$, and specifically as $I(i,j)_k$ for each interval,where $I(i,j)_k = [a_{ij}^k, a_{ij}^k + l_{ij}^k)$ delineates the duration of blockage. In this notation, a_{ij}^k marks the commencement of the k-th DoS attack, while l_{ij}^k indicates its duration. Consequently, the set $\Pi_D^{(i,j)}(t_1,t_2)$ is defined to represent the time frame during which communication between ECUs i and j is interrupted by attackers between moments (t_1,t_2). This set is established as follows:

$$\Pi_D(t_1,t_2) = \bigcup_{(i,j)\in E} \Pi_D^{(i,j)}(t_1,t_2), \tag{12}$$

$$\Pi_N(t_1,t_2) = (t_1,t_2) \setminus \Pi_D(t_1,t_2), \tag{13}$$

In this context, $\Pi_D(t_1,t_2)$ defines the set of all time periods within (t_1,t_2) during which communication is disrupted, at least once, between any ECUs and the CAN. Conversely, $\Pi_N(t_1,t_2)$ designates the time intervals where communication operates without any interruptions within the same timeframe. The potential for DoS attacks exists across any communication channel linking the ECUs and the CAN. The limitations and conditions governing these DoS attacks are encapsulated in the following key assumption:

Assumption 1: [19] (DoS Duration): There are specific positive scalar values $\zeta_1 > 0$, $\zeta_2 > 1$, ν_1 and ν_2 which ascertain that:

i) The total duration of blocked communication, $|\Pi_D(t_1,t_2)| \leq \frac{t_2-t_1}{\zeta_2} + \zeta_1, \forall t_2 > t_1 \geq 0$

ii) The frequency of DoS attacks $n(t_1,t_2) \leq \nu_1 + \frac{t_2-t_1}{\nu_2}, \forall t_2 > t_1 \geq 0$

here $|(\cdot)|$ and $n(t_1,t_2)$ respectively denote the total length of the time period $(\cdot)$ and the count of DoS attacks within the interval $[t_1,t_2)$, as explained in [20]. It's important to note that the frequency and duration of DoS attacks are governed by the criteria specified in Assumption 1. Additionally, there is a distinct difference between packet losses and DoS attacks in terms of their characteristics and duration, which is crucial to understanding their impacts on the system. Firstly, packet losses are typically quantified as an integer count and are limited to relatively short, finite sequences, in contrast to DoS attacks, which can extend over significantly longer periods. Secondly, while packet losses are generally random and incidental, DoS attacks are strategically executed by skilled adversaries who may, for instance, exploit fixed sampling periods in the system. Additionally, it's important to note that the semi-Markov model developed in this study addresses DoS attacks and can complement existing methods for handling packet losses within the CAN, provided that Assumption 1 is met.

3.2. Formulation of Replay Attacks as MDP

The replay attack is executed in three sub-actions: packet recording, packet replay, and a do-nothing action. The recording action captures the battery's State of Charge (SoC) estimates into the attacker's buffer, and the replay action subsequently broadcasts the last captured SoC data from this buffer. The 'do-nothing' action represents periods where the penetration tester, functioning as a Reinforcement Learning (RL) agent, chooses not to interfere with the system's operations. This could be a strategic choice to avoid detection or when the conditions are unfavorable for impactful interference, which is system instability.

The attacking methodology we have developed for the replay attack is structured as a Markov

Decision Process (MDP). An MDP is a mathematical framework characterized by a quintuple $\langle S, A, P(s_{t+1} \mid s_t, a_t), R(s_{t+1} \mid s_t, a_t)\rangle$ [21]. This framework includes S, a set representing the various states of the system, and $s_t \in S$, which specifies the state at a particular time t. The set A encompasses possible actions, with $a_t \in A$ indicating an action the agent executes at time t. The function $P(s_{t+1} \mid s_t, a_t)$ denotes the probability of transitioning between states, providing insights into how the state of the environment evolves as the agent implements action a_t in state s_t. The function $R(s_{t+1} \mid s_t, a_t)$ is a reward function that calculates the immediate benefit the agent gains from the environment post-action. Additionally, the constant $\gamma \in [0, 1)$ serves as a discount factor for rewards over time, underscoring the diminishing value of future rewards compared to immediate ones.

Action Definition: At each time step t, the agent selects an action a_t from a predefined set of actions $a = \{a^1, a^2, a^3\}$. Here, a^1 denotes the 'Record Action,' a^2 is the 'Replay Action,' and a^3 signifies the 'Stop Action.' These actions persist for a fixed duration of δ seconds.

Observation Mechanics: Assume the attacker has access to manipulate various readings within the vehicle's battery management system. Let N represent the total count of sensor readings that can be subject to replay attacks by the sophisticated attacker. Over the duration of each action, the attacker compiles data from these readings into a feature vector $f_t = [SoC^-, SoC, SoC_-]$. In this vector, SoC^- captures the highest battery SoC estimation across N readings, SoC_- denotes the lowest value, and SoC is the mean value computed over the δ seconds of action duration. An observation vector is then constructed as $o_t = [f_t^c, f_t^m]$, where f_t^c encompasses features extracted from the current readings, and f_t^m includes features derived from the most recent 'Record Action.' The inclusion of f_t^m in the observation vector is crucial, as different packets might be replayed from the buffer under identical system states, potentially leading to uncertain system states. Consequently, the current state integrates information from the preceding 'Replay Action,' enhancing the agent's observability throughout its training phase [8].

Reward Function: A comprehensive reward function $r(s_t, a_t)$ is designed to reflect the battery limits violation extent by assessing four aspects of the attack scheme. The formulation of the various sub-rewards. For the effectiveness subreward $R_{E(t)}$, the agent is rewarded for recording and replaying the data at times that would have maximum impact, i.e., the deviation of the replayed data is larger than the actual sensor measurement. This is modeled as normalized;

$$R_{E(t)} = |S_{actual}(t) - S_{replay}(t)|, \tag{14}$$

The stealthiness score $R_{S(t)}$ captures the ability of the attack to mimic the normal behavior of the system so that it's not easily detectable. The agent is rewarded for making the replayed data as consistent with what the temperature sensor would expect under normal conditions. This reward indicates the agent's ability to minimize the difference between the replayed and actual system condition at time t,

$$R_{S(t)} = \frac{1}{1 + E(t)} \tag{15}$$

The detection score $R_{D(t)}$ is calculated using the sigmoid function, making it useful for things like probability estimation. The reward enables the agent to remain more covert. This is modeled as

$$R_{D(t)} = \frac{1}{1 + e^{-E(t)}} \tag{16}$$

Finally, the conservation score $R_{C(t)}$ measures the benefits of the agent choosing to do nothing in order to reduce the chance of detection or wait for a better time to record or replay data. This sub-reward is designed such that it is dependent on the current state of the system. For example, if the vehicle's acceleration is above a certain threshold, the agent

might get a higher reward for doing nothing, as this could be a time when recording or replaying data is riskier or less beneficial.

$$R_{C(t)} = \{\, 1\ if a \leq threshold 0 otherwise \quad (17)$$

The total reward $r(t)$ is enumerated as follows:

$$r(t) = \alpha R_{E(t)} + \beta R_{S(t)} + \gamma R_{D(t)} + \xi R_{C(t)} \quad (18)$$

Where $\{\alpha, \beta, \gamma, \xi\}$ are weights reflecting the importance of each sub-reward. The PT agent's primary objective is the maximization of the accumulated discounted rewards over the duration of the PT. This is mathematically represented as

$$G = \sum_{t=1}^{|T|} \gamma^{t-1} R_t \quad (19)$$

In this context, $|T|$ signifies the cumulative count of actions undertaken throughout the training process. The term γ represents the discount factor, while R_t refers to the reward obtained at each specific time step t. The primary objective is to identify an optimal PT strategy, denoted as π^*, which aims to maximize the anticipated value of G. This goal effectively reshapes the task into a problem of optimization, ideally suited for resolution through the application of proximal policy optimization (PPO), a prominent algorithm in the domain of DRL. For those interested in gaining a more comprehensive insight into the utilization of PPO for solving such optimization challenges, it is advisable to consult [22]. The detailed methodologies are directly applicable to the scenarios presented in this research, offering a clear and in-depth perspective on applying PPO in similar contexts.

3.3. Simulation Setup

For this study, a comprehensive simulation testbed has been established, leveraging the strengths of a co-simulation platform that synergistically combines the capabilities of Matlab/Simulink with Python. The detailed modeling of the HTV, encompassing its complex control mechanisms and dynamic responses, is built within the Matlab Simulink environment. Concurrently, the Python environment is utilized to develop and implement the simulated cyberattacks, providing a realistic and controlled setting to assess their impacts. The simulation incorporates a highway driving cycle, which tests the behavior of the vehicle under normal driving conditions. In the subsequent sections, we delve into the simulation results, offering an in-depth analysis of how different types of cyberattacks influence the HTV's energy supply dynamics.

4. SIMULATION RESULTS

4.1. Impact of DoS Attacks

Fig. 2 contrasts the generator's speed in rpm under normal operating conditions and during the DoS attacks. The generator speed is typically synchronized with the engine speed to ensure cohesive power delivery. However, we observe drastic and repeated drops to zero rpm during the DoS attack. These drops signify periods of inactivity from the generator speed sensor, indicating disruption or data flooding, rendering the sensor unable to report accurate speeds. Such disruption in the sensor's data stream can lead to the engine's shutdown as it fails to receive necessary speed signals, causing an interruption in the power supply from the generator. The second graph in fig. 2 shows the generator's power output, revealing a stark contrast between a smooth power delivery under normal conditions and erratic fluctuations during the DoS attacks. These fluctuations illustrate the instability induced. When the generator speed sensor relays incorrect or no data, the EMS struggles to appropriately manage the energy distribution between the generator and the battery. Misinterpreting the generator as non-operational, the EMS underutilizes the generator, consequently increasing dependency on the battery.

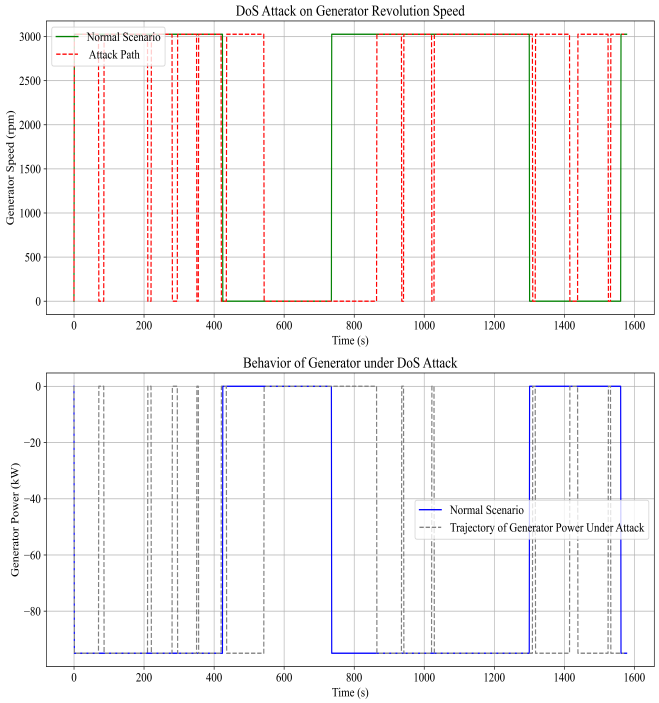

Figure 2: DoS Attacks Sequence on Generator Revolution Speed

Fig. 3 illustrates the battery's SoC, where the attack scenario shows more volatile fluctuations than observed under normal conditions. These fluctuations are a direct response to the generator's unreliable output, as the battery is compelled to adjust for the energy supply's irregularities. Erratic disruptions of the generator's output due to the DoS attacks result in improper battery discharging and other SoC anomalies. The fuel consumption graph indicates reduced usage during the DoS attack, attributed to the generator's inconsistent behavior. This inconsistency reduces engine efficiency and further affects fuel consumption as the system attempts to offset the erratic power supply. The DoS attack's impact on the generator revolution speed sensors directly compromises the EMS's capacity to manage and distribute energy efficiently on the supply side. This inefficiency leads to underutilization of the generator and unnecessarily strains the battery by requiring it to cover the generator's deficits. The increased reliance on the battery due to generator inconsistencies may further lead to a shortened battery lifespan and increased wear due to more frequent charging and discharging cycles.

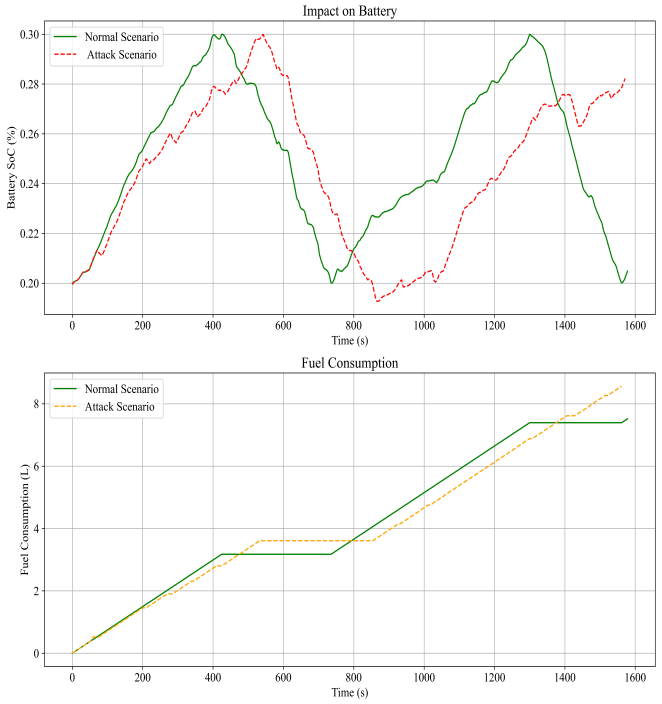

Figure 3: Impact of DoS attacks on Battery and Engine

4.2. *Impact of Replay Attacks*

As observed in fig. 4, the attack path generated by the DRL agent exhibits only minor deviations from the normal SoC trajectory, demonstrating the agent's capacity for discreet influence over the battery's SoC readings. This subtlety is a deliberate outcome shaped by the DRL framework's reward function. The reward function encourages

the agent to maximize the attack's impact on the vehicle's systems and closely mimic expected sensor measurements to avoid detection. The attack's gradual influence on SoC estimation is critical to its stealthiness, avoiding immediate alarms that could trigger swift remedial actions. This slow progression, in line with the reward function's design, makes detection and response more challenging as the replayed data remains within acceptable SoC ranges.

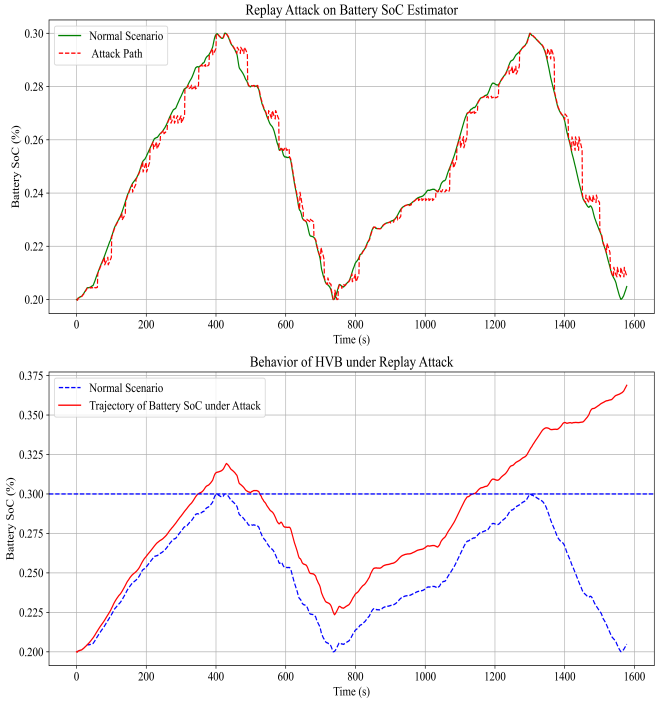

Figure 4: Attack path on SoC and Impact on the Physical Battery

Fig. 5 reveals that, as a direct result of the replay attack, the generator fails to shut off around the 1300-second mark, preventing the battery from entering its discharging phase. This denial of discharge coerces the battery into a continuous charging state, as depicted in fig.4, contrary to its expected behavior during a normal driving cycle. This forced charging results in overcharging, as indicated by the SoC trajectory surpassing the safety threshold of 0.3 at certain points—a scenario absent in normal conditions. The continuous operation of the generator and the resultant overcharging of the battery poses several risks: diminished battery life due to the stress of constant charging, potential damage to battery cells from prolonged overcharging, and the increased likelihood of thermal runaway—a hazardous condition where the battery could dangerously overheat and potentially catch fire.

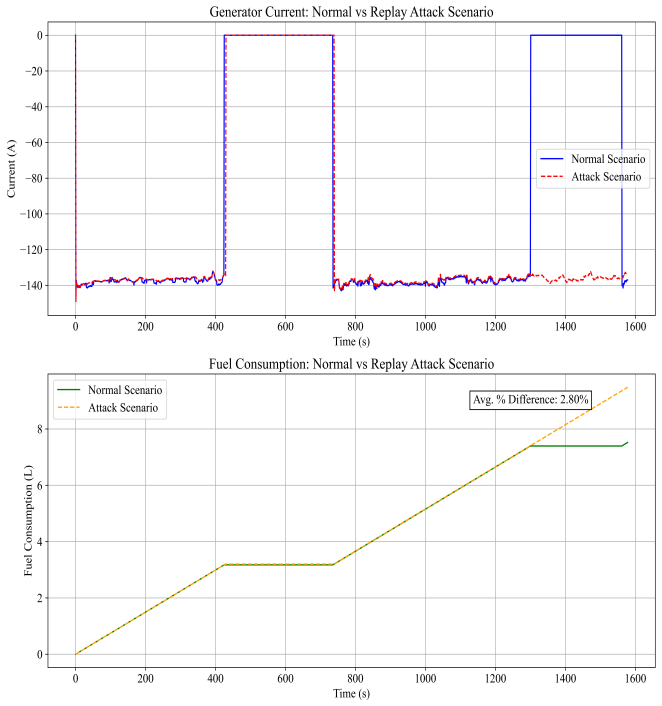

Figure 5: Impact on Generator and Engine system

Fig. 5 also indicates that, under normal circumstances, the generator is programmed to shut down at 1300 seconds, likely to prevent battery overcharging or to optimize fuel consumption. Contrarily, the attack scenario shows that the generator continues to produce power past its intended shutdown time. Despite the anticipated halt, the generator's non-stop operation correlates

with the battery's SoC breaching the designated limit. This observation suggests that the replay attack successfully misled the energy manager, causing the generator to disregard its control protocols and resulting in the battery's overcharging. It is important to note that while the vehicle's dynamics remain unchanged, the attack significantly compromises the electrical and charging systems. The second plot illustrates that the generator's unwarranted activity increases operational costs, as demonstrated by a 2.8% increase in fuel consumption for the evaluated drive cycle.

5. CONCLUSION

This paper delves into the intricate security challenges faced by the EMS of a high-speed, tracked, off-road HEV, particularly under the duress of replay and DoS attacks. An automated replay attack conceptualized as a triad of actions within a Markov Decision Process is presented. Through this framework, a DRL agent is trained to adeptly master the sequencing and timing of the replay attack, targeting to violate the battery's SoC limit. Simultaneously, the complexity of DoS attacks was meticulously captured using a semi-Markov chain model. The impacts of these attack models are tested on a co-simulation environment, integrating MATLAB/Simulink with a Python environment. The experiments revealed the replay attack's stealth and efficacy in manipulating the BMS's SoC estimations. Such breaches led to battery limit violations and exposed vehicle energy control vulnerabilities. Similarly, the DoS attack, by targeting generator speed sensors, emerged as a threat to the EMS, disrupting the vehicle's energy supply chain. This disruption manifested as excessive strain on the battery system, underscoring the need for sophisticated anomaly detection systems to discern between normal operational variances and malicious activities. Future research directions will be dedicated to developing an advanced intrusion detection system.

ACKNOWLEDGMENTS

This work was supported by Clemson University's Virtual Prototyping of Autonomy Enabled Ground Systems (VIPR-GS) under Cooperative Agreement W56HZV-21-2-0001 with the US Army DEVCOM Ground Vehicle Systems Center (GVSC). The authors would like to express their gratitude for the valuable resources and facilities provided by the Secure Energy and Automation Laboratory (SEAL) and Real Time Controls and Optimization Laboratory (RTCOOL).

The authors would like to acknowledge the Warren H. Owen Distinguished Professorship Endowment for supporting this research effort.

References

[1] S. Adly, A. Moro, S. Hammad, and S. A. Maged, "Prevention of controller area network (can) attacks on electric autonomous vehicles," *Applied Sciences*, vol. 13, no. 16, p. 9374, 2023.

[2] M. Kneib, O. Schell, and C. Huth, "Easi: Edge-based sender identification on resource-constrained platforms for automotive networks." in *NDSS*, 2020, pp. 1–16.

[3] W. He, W. Xu, X. Ge, Q.-L. Han, W. Du, and F. Qian, "Secure control of multiagent systems against malicious attacks: A brief survey," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 3595–3608, 2021.

[4] L. Guo, J. Ye, and L. Du, "Cyber-physical security of energy-efficient powertrain system in hybrid electric vehicles against sophisticated cyberattacks," *IEEE transactions on transportation electrification*, vol. 7, no. 2, pp. 636–648, 2020.

[5] L. Timilsina, P. R. Badr, P. H. Hoang, G. Ozkan, B. Papari, and C. S. Edrington, "Battery degradation in electric and hybrid electric vehicles: A survey study," *IEEE Access*, 2023.

[6] X. Ying, S. U. Sagong, A. Clark, L. Bushnell, and R. Poovendran, "Shape of the cloak: Formal analysis of clock skew-based intrusion detection system in controller area networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 9, pp. 2300–2314, 2019.

[7] A. Arsalan, L. Timilsina, B. Papari, G. Muriithi, G. Ozkan, P. Kumar, and C. S. Edrington, "Cyber attack detection and classification for integrated on-board electric vehicle chargers subject to stochastic charging coordination," *Transportation Research Procedia*, vol. 70, pp. 44–51, 2023.

[8] Y. Li, J. Yan, and M. Naili, "Deep reinforcement learning for penetration testing of cyber-physical attacks in the smart grid," in *2022 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2022, pp. 01–09.

[9] G. Muriithi, B. Papari, A. Moghassemi, A. Arsalan, G. Ozkan, and C. S. Edrington, "Security enhancement of cyber-physical dc ship power system using scalable deep learning method," in *2023 IEEE Electric Ship Technologies Symposium (ESTS)*, 2023, pp. 520–527.

[10] E. Gumrukcu, A. Arsalan, G. Muriithi, C. Joglekar, A. Aboulebdeh, M. A. Zehir, B. Papari, and A. Monti, "Impact of cyber-attacks on ev charging coordination: The case of single point of failure," in *2022 4th Global Power, Energy and Communication Conference (GPECOM)*. IEEE, 2022, pp. 506–511.

[11] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, pp. 4639–4657, 2020.

[12] L. Guo, B. Yang, J. Ye, H. Chen, F. Li, W. Song, L. Du, and L. Guan, "Systematic assessment of cyber-physical security of energy management system for connected and automated electric vehicles," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3335–3347, 2020.

[13] L. Guo, J. Ye, and B. Yang, "Cyberattack detection for electric vehicles using physics-guided machine learning," *IEEE transactions on transportation electrification*, vol. 7, no. 3, pp. 2010–2022, 2020.

[14] S. Sripad, S. Kulandaivel, V. Pande, V. Sekar, and V. Viswanathan, "Vulnerabilities of electric vehicle battery packs to cyberattacks," *arXiv preprint arXiv:1711.04822*, 2017.

[15] R. M. Gerdes, C. Winstead, and K. Heaslip, "Cps: an efficiency-motivated attack against autonomous vehicular transportation," in *Proceedings of the 29th Annual Computer Security Applications Conference*, 2013, pp. 99–108.

[16] A. Khalid, A. Sundararajan, A. Hernandez, and A. I. Sarwat, "Facts approach to address cybersecurity issues in electric vehicle battery systems," in *2019 IEEE Technology & Engineering Management Conference (TEMSCON)*. IEEE, 2019, pp. 1–6.

[17] Q. Zhu, A. Kumar, A. Sundar, D. Egan, H. Mirzaei, D. Chang, M. Schmid, R. Prucka, B. Lawler, and C. Paredis, "Development of a series hybrid electrified powertrain for a high-speed tracked vehicle based on driving cycle simulation," *SAE International Journal of Advances and Current Practices in Mobility*, vol. 4, no. 2022-01-0367, pp. 1403–1412, 2022.

[18] L. Tang, G. Rizzoni, and S. Onori, "Energy management strategy for hevs including battery life optimization," *IEEE Transactions on Transportation Electrification*, vol. 1, no. 3, pp. 211–222, 2015.

[19] Z. Lian, F. Guo, C. Wen, C. Deng, and P. Lin, "Distributed resilient optimal current sharing control for an islanded dc microgrid under dos attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4494–4505, 2021.

[20] C. Deng, F. Guo, C. Wen, D. Yue, and Y. Wang, "Distributed resilient secondary control for dc microgrids against heterogeneous communication delays and dos attacks," *IEEE Transactions on Industrial Electronics*, vol. 69, no. 11, pp. 11 560–11 568, 2021.

[21] G. Muriithi and S. Chowdhury, "Deep q-network application for optimal energy management in a grid-tied solar pv-battery microgrid," *The Journal of Engineering*, vol. 2022, no. 4, pp. 422–441, 2022.

[22] A. Raffin, A. Hill, A. Gleave, A. Kanervisto, M. Ernestus, and N. Dormann, "Stable-baselines3: Reliable reinforcement learning implementations," *Journal of Machine Learning Research*, vol. 22, no. 268, pp. 1–8, 2021. [Online]. Available: http://jmlr.org/papers/v22/20-1364.html