Demo: Recovering Autonomous Robotic Vehicles from Physical Attacks

Pritam Dash and Karthik Pattabiraman
University of British Columbia

***Abstract*—Robotic Vehicles (RV) rely extensively on sensor inputs to operate autonomously. Physical attacks such as sensor tampering and spoofing feed erroneous sensor measurements to deviate RVs from their course and result in mission failures. We present *PID-Piper* , a novel framework for automatically recovering RVs from physical attacks. We use machine learning (ML) to design an attack resilient FeedForward Controller (FFC), which runs in tandem with the RV's primary controller and monitors it. Under attacks, the FFC takes over from the RV's primary controller to recover the RV, and allows the RV to complete its mission successfully. Our evaluation on 6 RV systems including 3 real RVs shows that *PID-Piper* allows RVs to complete their missions successfully despite attacks in 83% of the cases.**

I. Motivation

Autonomous Robotic Vehicles (RV) such as drones and rovers rely extensively on sensors to perceive their physical states e.g., a GPS provides geographic position information, a gyroscope and accelerometer sensors measure angular and orientation. Unfortunately, RVs have been shown vulnerable to physical attacks such as sensor tampering and spoofing that feeds erroneous sensor measurements through external means to deviate RVs from their course resulting in mission failures.

Prior work in RV security mainly focuses on attack detection. Upon detecting the attack, most techniques raise an alarm and trigger the fail-safe modes of the RV (e.g., forced landing for drones or return to home) as a response to the detected attack. Unfortunately, this is not a complete solution. Because erroneous sensor signals lead to erroneous actuator signals, in most cases, the RV crashes as a result [1]. Furthermore, activation of fail-safe amidst the mission often leads to failure of the RV's mission (i.e., the RV does not reach its destination). As RVs are projected to be deployed in mission-critical tasks such as drug delivery, disaster relief, and are expected to operate in urban environments, they must be resilient to attacks and operate despite the malicious intervention, and complete their missions. Therefore, the focus has to be on developing attack resilient counter-measures and not just detection.

We present *PID-Piper* [2], a framework for automated attack recovery in RVs by using a secondary controller in tandem with the RV's primary controller (i.e., PID control). RV's controller consists of position controller and attitude controller both of which use PID control for error correction. We design *PID-Piper* based on the following observation. PID control is designed to handle faults such as sensor noise and environmental disturbances by compensating for the resulting errors in RV's physical states (increase thrust to minimize drift due to wind). However, unlike environmental noise, attacks are not transient in nature. We find that the persistent nature of attack induced error in RV's physical state causes PID control to overcompensate which results in erroneous actuator signals. Therefore, PID compensation, which is effective in handling transient errors, becomes undesirable under attacks.

To address the above weakness, *PID-Piper* uses a Feedforward controller (FFC) in tandem with the PID controller. The FFC takes the current sensor measurements (i.e., GPS, IMU sensor measurements), velocity, position variance, and the given waypoint as inputs to predict actuator signals.

Under attacks, unlike PID which is a feedback control technique, the FFC does not measure and compensate for the error in RV's physical states. Instead, the FFC proactively prevents sensor perturbations from influencing the actuator signals. This means the FFC predicts robust actuator signals even under attacks. The FFC is built using machine learning (ML) models, and trained to reject attack induced sensor perturbations by correlating past and present sensor inputs in predicting actuator signals. Both the FFC and PID operate in tandem. When an attack is detected, the RV's switches to FFC's predictions to recover from the attack, and once the attack subsides, it switches back to the PID controller.

II. Results

Success Metric We consider a mission to be successful, if after the mission is complete and the total deviation from the original destination is *less than* $10m$ with no crashes or stalls.

We evaluate *PID-Piper* [1] on 3 real RVs and 3 simulated RVs. We find that (1) *PID-Piper* recovers the RVs from attacks and achieves mission success in 83% of the cases. (2) For the remaining 13% of the missions, *PID-Piper* could not navigate the RV close to the target but it prevented crashes. (3) *PID-Piper* achieves 0% false positives in the absence of attacks, and (4) incurs $\approx$ 7% CPU overhead and $\approx$ 1% energy overhead.

References

[1] P. Dash, M. Karimibiuki, and K. Pattabiraman, "Out of control: Stealthy attacks against robotic vehicles protected by control-based techniques," in *Proceedings of the 35th Annual Computer Security Applications Conference*, ser. ACSAC '19, 2019, p. 660–672.

[2] P. Dash, G. Li, Z. Chen, M. Karimibiuki, and K. Pattabiraman, "Pid-piper: Recovering robotic vehicles from physical attacks," in *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2021, pp. 26–38.

[1] *PID-Piper* attack recovery videos: https://bit.ly/3oswuTc

Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022
24 April 2022, San Diego, CA, USA
ISBN 1-891562-75-4
https://dx.doi.org/10.14722/autosec.2022.23009
www.ndss-symposium.org