Demo: Impact of Stealthy Attacks on Autonomous Robotic Vehicle Missions

Pritam Dash, Mehdi Karimibiuki, and Karthik Pattabiraman
University of British Columbia

I. Motivation and Key Insights

Robotic Vehicles (RV) use sensors to measure their physical states and derive the appropriate actuator signals for autonomous navigation and other control operations. Unfortunately, attackers can manipulate sensor and actuator signals through malicious code injection [2], sensor spoofing [7], and acoustic noise injection [6].

Model-based techniques have been recently proposed to detect attacks against RVs. Control Invariants (CI) [3] and Extended Kalman Filter (EKF) [1] are techniques that use control-based estimations to derive invariants and monitor the RV's runtime behaviour to detect attacks. In this paper, we demonstrate three stealthy attacks, namely false data injection (FDI), artificial delay (AD), and switch mode (SM) attacks, based on the findings of our previous work [4], [5]. The stealthy attacks evade the CI and EKF detection techniques and result in significant adverse impact on the RV's mission (e.g., significant deviations from the target or result in a crash).

Our main insight is that by design, CI and EKF techniques have to tolerate some degree of deviation from the planned trajectory due to environmental factors such as wind or sensor noise, and hence set a threshold for flagging errors between model estimations and observed behaviour as attacks. Further, we found that the control based estimation techniques fail to accurately model RV's runtime behavior. Because of the model inaccuracies, CI and EKF techniques set a high threshold, and perform stateless analysis in order to avoid false alarms. This opens up new vulnerabilities, and allows attackers to launch stealthy sensor and actuator attacks against RVs.

The FDI attack injects bias values to sensor and actuator measurements, such that the deviations in the control output (e.g., Euler angles, motor rotation rates) are always maintained under the detection threshold. The AD attack injects intermittent delays in the reception of the RV's gyroscopic sensor measurements, which will, in turn influence the estimation of RV's angular orientation while eluding detection. The SM attack injects strong bias values into actuators when the RV switches it's modes of operation (e.g., when a drone switches from steady flight to landing). By launching stealthy attacks over a prolonged duration the attacker will be able to cause mission failure or adversely influence RV's performance.

Autonomous RVs are deployed in variety of industrial sectors such as agriculture, package delivery etc. Further, RVs are projected to be deployed in mission-critical tasks such as drug delivery and disaster relief. Therefore, it is critical to protect RVs from attacks in order to maximize their performance and prevent adverse consequences. Our findings show that using inaccurate models for invariant analysis in non-linear RV systems, opens the door to new vulnerabilities.

Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021
25 February 2021, Virtual
ISBN 1-891562-68-1
https://dx.doi.org/10.14722/autosec.2021.23014
www.ndss-symposium.org

II. Attack Impact

We demonstrate the three stealthy attacks on 6 RVs including 3 real RVs (2 drones and a rover) in presence of both CI and EKF techniques. We found that the stealthy attacks can cause severe disruptions in RV missions while remaining undetected [1]. For example, we found that the FDI attack can deviate RVs by 8 to 15 meters from its target for short RV missions (50 meters), and by more than 160 meters for long RV missions (5 kilometers). Similarly, the AD attack increases the mission duration of a rover and drone by more than 65% and 30% respectively. Finally, the SM attack, when launched at vulnerable states during a drone mission, can result in a crash (in more than 50% of the cases in our experiments).

References

[1] P.-J. Bristeau, E. Dorveaux, D. Vissière, and N. Petit, "Hardware and software architecture for state estimation on an experimental low-cost small-scaled helicopter," *Control Engineering Practice*, vol. 18, no. 7, pp. 733 – 746, 2010, special Issue on Aerial Robotics.

[2] N. Carlini, A. Barresi, M. Payer, D. Wagner, and T. R. Gross, "Control-flow bending: On the effectiveness of control-flow integrity," in *24th USENIX Security Symposium (USENIX Security 15)*. Washington, D.C.: USENIX Association, Aug. 2015, pp. 161–176.

[3] H. Choi, W.-C. Lee, Y. Aafer, F. Fei, Z. Tu, X. Zhang, D. Xu, and X. Deng, "Detecting attacks against robotic vehicles: A control invariant approach," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: ACM, 2018, pp. 801–816.

[4] 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. New York, NY, USA: ACM, 2019.

[5] P. Dash, M. Karimibiuki, K. Pattabiraman, "Stealthy attacks against robotic vehicles protected by control-based intrusion detection techniques," *Digital Threats: Research and Practice*, vol. 2, no. 1, Jan. 2021.

[6] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, "Rocking drones with intentional sound noise on gyroscopic sensors," in *24th USENIX Security Symposium (USENIX Security 15)*. Washington, D.C.: USENIX Association, 2015, pp. 881–896.

[7] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful gps spoofing attacks," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, ser. CCS '11. New York, NY, USA: ACM, 2011, pp. 75–86.

[1] Videos showing the attacks. The stealthy attacks code can be found at https://github.com/DependableSystemsLab/stealthy-attacks