Report 4 - Project Development 1

David Lelis N00957151

Project Topic Discussion & Proposed Approach

This project will showcase the type of cybersecurity issues that drones may experience, and the current state of the simulation is in development. The simulation is planned to showcase three types of scenarios that may be encountered: taking control of drones, intercepting drone communications, and interrupting/jamming drone signals. Encryption should help in preventing hackers from attacking drones via these scenarios. Having encryption keys would allow for authentication so that drones are taking in signals from their original/expected source, secure communication so that anyone who may have intercepted the data will have difficulty decrypting it, and provide safeguards so that if drones experience a lack of communication they can fall back on default instructions.

The current progress of the project has been going fairly well. The simulation software being used is Webots, an open-source robotics simulation software. The environment being used has been created and the drone nodes have been placed. However, actual communication between the drones has been difficult to implement since it's a new software for me. For the time being, demonstrating the encrypted communication between client and server has been completed separately in non-drone python file, which will be implemented into working with drones. Some attacker programs have also been created to demonstrate data interception and jamming.

Next Phase Plan

The next phase will be implementing different attacks and solutions to the attacks into the actual drones. These attacks are expected to include signal jamming, overriding drone control, and data interception. A solution for this is to make authentication, encryption, and failsafe mechanisms. Authentication would entrust that any signals that drones are taking in are trustworthy and should be completed. Encryption would provide a layer of protection from data interception. And if all else fails, failsafe mechanisms that provide a default command to complete would protect the environment, any bystanders, and the drone.

Reference Papers

Matellán, Vicente, Francisco-J. Rodríguez-Lera, Ángel-M. Guerrero-Higueras, Francisco-Martín Rico, and Jonatan Ginés. "The role of cybersecurity and HPC in the explainability of autonomous robots behavior." In 2021 IEEE International Conference on Advanced Robotics and Its Social Impacts (ARSO), pp. 1-5. IEEE, 2021.

Yaacoub, Jean-Paul A., Hassan N. Noura, Ola Salman, and Ali Chehab. "Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations." International Journal of Information Security 21, no. 1 (2022): 115-158.

Mayoral-Vilches, Víctor. "Robot cybersecurity, a review." International Journal of Cyber Forensics and Advanced Threat Investigations (2022).

Ranganathan, Sathishkumar, Muralindran Mariappan, and Karthigayan Muthukaruppan PG. "Design Methodology For Using Blockchain In Swarm Robotics." In 2021 IEEE 19th Student Conference on Research and Development (SCOReD), pp. 76-81. IEEE, 2021.

Clark, George W., Michael V. Doran, and Todd R. Andel. "Cybersecurity issues in robotics." In 2017 IEEE conference on cognitive and computational aspects of situation management (CogSIMA), pp. 1-5. IEEE, 2017.

Hristov, Grozdan, Ivan Stankov, and Dayana Mladenova. "CyberAttacks and robotics." In 2023 31st National Conference with International Participation (TELECOM), pp. 1-4. IEEE, 2023.

Botta, Alessio, Sayna Rotbei, Stefania Zinno, and Giorgio Ventre. "Cyber security of robots: A comprehensive survey." Intelligent Systems with Applications 18 (2023): 200237.

Rahman, SM Mizanoor. "An IoT-based common platform integrating robots and virtual characters for high performance and cybersecurity." In 2019 SoutheastCon, pp. 1-6. IEEE, 2019.

Tanimu, Jibrilla Abubakar, and Wafia Abada. "Addressing cybersecurity challenges in robotics: A comprehensive overview." Cyber Security and Applications (2024): 100074.

Jawhar, Imad, Nader Mohamed, and Jameela Al-Jaroodi. "Secure communication in multi-robot systems." In *2020 IEEE Systems Security Symposium (SSS)*, pp. 1-8. IEEE, 2020.

McCord, Cassandra, Jorge Pena Queralta, Tuan Nguyen Gia, and Tomi Westerlund. "Distributed progressive formation control for multi-agent systems: 2d and 3d deployment of uavs in ros/gazebo with rotors." In *2019 European Conference on Mobile Robots (ECMR)*, pp. 1-6. IEEE, 2019.

Mañas-Álvarez, Francisco-José, María Guinaldo, Raquel Dormido, and Sebastian Dormido. "Robotic park: Multi-agent platform for teaching control and robotics." *IEEE Access* 11 (2023): 34899-34911.

Qin, Mingxing, Zhong Wang, and Xin Liu. "ROS-based Collaborative Algorithm Verification Framework for Multi-agent Systems." In *2022 34th Chinese Control and Decision Conference (CCDC)*, pp. 2006-2010. IEEE, 2022.