A Cybersecurity Framework for Autonomous Drones: Encryption, Defenses, and Failsafe Mechanisms

David Lelis
School of Computing
University of North Florida
Jacksonville, USA
david.j.lelis@unf.edu

***Abstract*—Autonomous robotics has been implemented into modern society over the past few years for applications like environmental monitoring, product deliveries, and search-and-rescue operations. These applications often utilize multiple drones given directions to complete these objectives and communicating to users remotely through client-server programs, which are susceptible to cybersecurity attacks. This paper presents a cybersecurity framework for robotic drones that defend against cyber-threats like data interception, denial-of-service (DoS) attacks, and the lose of connection to the server. In this study, three applications to defend against these cyberattacks are implemented: data encryption, DoS detection and blockage, and fail-safe procedures. The study was simulated in Webots to safely practice these cyber-defense applications, both with a single drones and multiple drones. The results demonstrate the effectiveness of the approaches studied in using multiple drones remotely. This research contributes to the development of robust cybersecurity practices in autonomous systems, ensuring safe and reliable drone operations.**

***Index Terms*—Autonomous Robotics, Drones, Unmanned Aerial Vehicles, Cybersecurity, Framework, Encryption, Denial-of-Service, Detection, Failsafe Mechanisms**

I. Introduction

Autonomous drones, also known as Unmanned Aerial Vehicles (UAVs), are aircraft that are programmed or remotely controlled to perform tasks that are either too menial or too dangerous for regular people, often utilizing advanced technologies to improve their capabilities. These tasks could include military surveillance, such as surveying dangerous areas of interest, delivery of products, such as same-day local delivery, and entertainment, such as drone light shows. Although these tasks are fairly simple for humans, their complexity still requires the onboard computer of these UAVs to utilize advanced technologies to fully evaluate and achieve their tasks. For the cases that include objectives that are too dangerous for humans, they often involve elements and scenarios that may cause harm to the drone while also requiring the delicateness that human understandings offer, which also requires advanced technologies to complete the task. Advanced technologies such as artificial intelligence (AI) and wireless communication provide assistance in performing these tasks. However, implementing these technologies can also pose cybersecurity vulnerabilities that could inhibit the drone's ability to perform its objective. Threats like data interception, signal jamming, unauthorized remote access, and unexpected disconnections pose serious threats to users, bystanders, and the environment surrounding robots. For these cases, a standard cybersecurity framework should be implemented as it is meant to defend against these threats.

A cybersecurity framework is essential to protect robotic systems from cyber threats, especially as robotics technologies continue to integrate into various sectors [20]. As robots are programmed to solve more complex problems, new technologies are being integrated into their systems as a solution, both in their hardware and software [15] [6]. These technologies include AI, wireless network communications, and various sensor technologies. Cybersecurity frameworks address the multifaceted cybersecurity challenges that robots can face during their day-to-day operations, such as unauthorized access and data breaches [10]. Modern robotic systems are interconnected and rely on network communications, making them vulnerable to remote access and network attacks. Other vulnerabilities may involve sensors, physical obstruction, or spoofing that mimic objects that are not actually in the drone's environment. The consequences of these attacks could range from data breaches to physical access to devices. A cybersecurity framework aims to counteract these threats through advanced authentication and secure communication protocols, including rigorous encryption to protect sensitive data transmitted across networks, along with environmental situations such as obstacles or unexpected disconnect from other systems [9].

II. Related Work

A. Current state of Robotics Cybersecurity

Historically, robotics has been integrating into modern societies as early as 1961 with automobile production and manufacturing and has increased its influence in the last few decades [3] [8]. The increased need for robotics in various applications resulted in the rapid development of Internet of Things (IoT) technologies for automated robotics, which use wireless network communication [4] [15]. In addition, robots utilizes many advanced technologies like AI, sensors, and control systems to achieve their objectives. Often times, these objectives require many human-robot interactions, which means that they directly involve a person in their tasks either by performing the task with the person, moving around crowds, or communicating information to the person [11]. The combination of these technologies and their direct human-robot interactions makes robots targets for attackers, with methods by way of remote network connections and interception of a robot's physical hardware [9] [23].

As robotics have begun to assimilate further into many modern societies, cybersecurity has often become secondary to safety in development, meaning developers are more concerned about keeping the users and data safe over keeping the data secure to the network. Due to the cyber-physical nature and impact on humans robots have, it is crucial to practice risk assessment in the early stages of the robot autonomous development. Many developers and manufacturers focus on safety over security and an offensive approach during the development of autonomous robots can slow down its production [12]. While the safety of users should always come first when it comes to robotics, the data and network should be just as secure to keep the user safe digitally. Creating a cybersecurity framework that can be regularly integrated into all drones and their networks could assist in creating secure drone systems without slowing down production. In addition, practices that are used in other complex systems, like red teaming where a team is constantly simulating cyberattacks during development, can aid in identifying the vulnerabilities in a robotic system. This is known as secure by design and with cybsersecurity trainings, create the most robust defenses and preventions against cyberthreats.

In December 23, 2024, an accident at the Disney Spring outdoor shopping and entertainment complex occurred during their nightly drone light show [13]. The light show utilized drones to create images in the night sky at the pace and tone of a soundtrack. However, reportedly, an error occurred during the start-up sequence causing a nonuniform lift, which in turn caused drones to crash into other drones and fall from the sky. The incident resulted in an injury of child, which demonstrates the importance in having safety measures to prevent drones from acting out of their intended tasks. The National Transportation Safety Board and Federal Aviation Administration have expressed safety measures including on-site preparation and training [18]. The research in this study intends to extend the safety measures into a base cybersecurity framework that can be used similar types of systems to avoid these dangerous situations.

B. Types of Cybersecurity Threats and Solutions

A handful of possible cybersecurity threats have previously been studied. This includes data breaches, unauthorized access, and limited network bandwidth [7]. If these threats aren't properly assessed and defended against, the repercussions could endanger human safety and even economic damage [3]. The attacks themselves are similar threats to regular computers, and currently we have solutions through studies like data privacy, risk management, and policy development. Respectively, the solution to data breaches, unauthorized access, and limited network bandwidth have been researched through studies involving encryption, thorough authentication, and network firewalls and mitigation [20].

Other threats that robots encounter are less digital threats that involves software, and more physical threats that involve a robot's hardware [12]. As robots' full utilization involves the device to interact with the physical environment around them, robots may encounter situations that could physically harm users, bystanders, itself, or the environment around them. Scenarios like collisions, moving out of range of a server, or even a sudden gust of wind may affect the robot's performance or endanger someone. Policies that are hard-programmed into the robot to avoid these types of harm should be implemented alongside the more digital cyberthreats.

III. Proposed Approach

The study in this research is intends to provide a framework that handles cybersecurity threats that autonomous drones encounter. Specifically, the threats that are simulated include data interception via Man-in-the-Middle (MitM) attacks, signal jamming through Denial of Service (DoS), and sudden disconnections from a drone system's network. Respectively, these threats are defended by End-to-End (E2E) encryption, DoS detection and mitigation, and Failsafe mechanisms. With these three solutions, a base framework that could be implemented for large variety of autonomous drones is developed to keep the users, their data, the drones and the environment around the drones safe.

A. Environment and Tools

The project was simulated in an open-source robotics simulation software called Webots [21], which contains multiple different real-life robots including the one selected for this study, the DJI Mavic 2 Pro. The DJI Mavic 2 Pro has both a position system to locate the current position of the drone and a camera system to visually observe what the drone would see. Python was used to simulate a client-server-type network that directed the drone to move around the environment and send messages, along with the cyberattacks that would be run separately to be studied. The environment that the drone was placed in was a 10 meter by 10 meter floor containing four objects where the drone was programmed to move to above the four objects in the environment, as seen in Figure 1. While the drone moves in the environment, it will send telemetry data, including the time and drone position, to the server to act as the sensitive data a drone may send to the host server. The three different cyberattacks will run separately while the drone is active, and both the client and server will defend appropriately to the attacks.

B. MitM Attacks and E2E Encryption

MitM attacks are cyberthreats that directly attempt to intercept data from a source. This data is often sensitive and respective to the task that is being completed. For example, a drone that is tasked to deliver a product from a warehouse could contain a customer's address, credit card information, or other personal information. To intercept the data, MitM

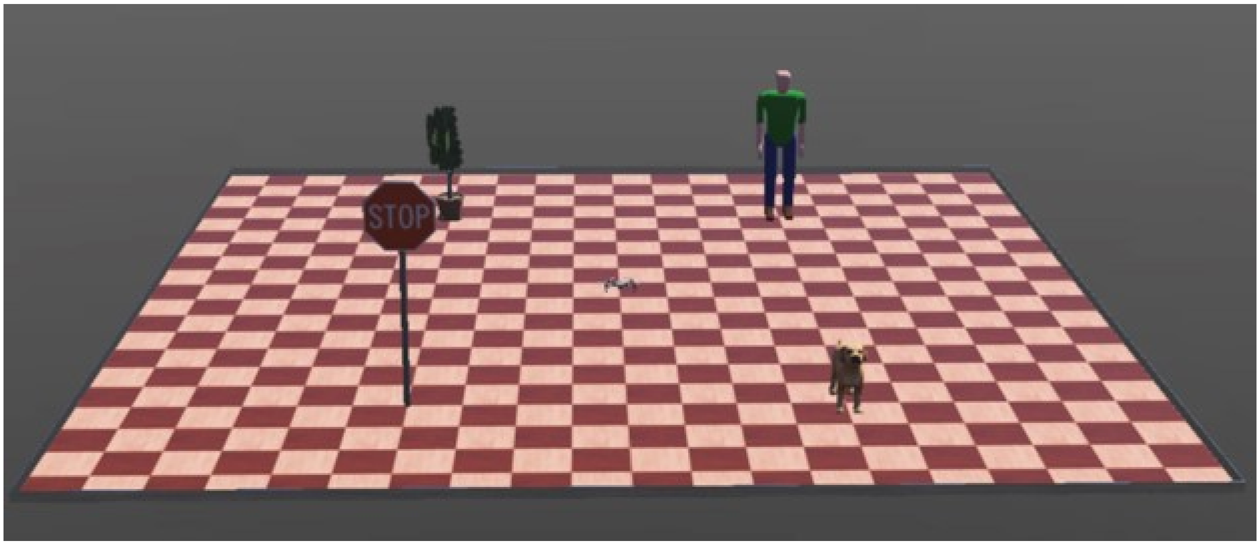


Fig. 1. Webots Simulation Environment

attacks mimic the host server that a client expects to connect to, catches the data the client sends since the client believes it is sending to the host server, and the MitM server sends the data to the host server. MitM attacks often send the data to the originally intended host server to avoid suspicion that the data was ever intercepted so that it can collect as much data as possible. It is very important that the information stays private to only the company and the customer. However, MitM attacks make it difficult to do that as the purpose is not to fully intercept the message but to also avoid suspicion that the message was intercepted.

E2E encryption is a cybersecurity defense practice where data is scrambled based on an encryption key that is only available to the client and server. The way that the data is saved and sent out is scrambled so that it is difficult for any attackers to read, as the message is seemingly just a string of random letters and numbers, until it is decrypted. Once decrypted, the client or server would be able to continue with their function and respond back to the message if necessary. This method does not necessarily defend against data interception, but still protects the data from malicious uses of attackers.

C. Signal Jamming and DoS Detection/Defense

Signal jamming is a type of cyberattack that is meant to interrupt or create interference in a device or network. For example on a robot, this could involve sensors or communication networks. This research studied a specific type of signal jamming, DoS attacks. DoS attacks use a large amount of network connections from a third party device to create blockages and heavy traffic which then creates disruptions in communication between devices. This is done to prevent the system from providing their intended services to legitimate users [14]. Robots, specifically, are often limited both computationally and through their network resources, making them easy, susceptible targets to these attacks [3] [20]. The results from this would be a waste of resources, delays in communication and services, forcing users to abandon the system; but the physical results in a system that utilizes drones to could be dangerous, like suicidal drones or sudden disconnections, as the drones uses reliable communication for instructions to move around it's environment.

Defenses against DoS attacks are difficult for numerous reasons, but they are still important to create defenses for. As these attacks occur in networks, they require real-time attention to be able to dynamically respond to the attack to avoid interruptions [11] [22]. However, solutions for these can be integrated on a network governance level by creating private networks with redundant communications, anomaly detection, and traffic filters [5] [10] [19] [23]. This is done by creating smaller isolated channels of communication for devices to communicate through and control traffic flow, while also actively detecting if an unexpected amount of communications are made from a specific device and mitigating traffic from that one device. This research will primarily focus on anomaly detection.

D. Sudden Disconnection and Failsafe Mechanisms

Sudden, unexpected disconnection from one robot to the rest of the system it works with should always be expected during the development of the system itself. As cyberattacks and the environment drones work in are always changing and evolving, the possibility for a robot to be overridden or simply disconnected by being out of range or blocked by materials will always be present. If a robot is disconnected from the system it works within, it is important to still be able to control or provide instructions to the drone to avoid causing any harm to users, the environment around them, and itself, if possible. Being able to predict what the robot is going to do and where it is going to be will allow developers to safely protect other users and the environment.

Failsafe mechanisms and procedures are the backup plans in the event that a robot goes rogue and cannot communicate to the users. Sometimes, these are unexpected, like when a third-party tries to override a robot to take control of it. Other times, they're necessary to avoid cyberattacks, like when a strong DoS attack is being used and the robot disconnects to avoid harming its surroundings. Ensuring that there are instructions for the drone to follow to navigate its surroundings safely is important to further avoid any harm [2] [23]. This research will practice a failsafe mechanism to instruct the drone to return to its original landing cite when the drone is suddenly unable to communicate to its host server.

IV. Evaluation Results

In the simulation, the drone is instructed to move to four points in the environment while being connected to a server to send telemetry data: time, altitude, roll, and pitch. This is done to simulate network communication where a drone may be calculating data while in operation and need to return the data back to users to study or respond to. For example, this could include a surveillance system that utilizes drones to respond to different emergencies in a search-and-rescue operation. While the simulation is running, on a separate terminal, the three cyberattacks are being executed to simulate a third-party attacking the system so that the client or server can react. Each individual defense is important, so the results were evaluated based on the drone's ability to complete its task of moving around the environment, communicating with the server, and keeping the users and the environment safe. The cyberdefenses were successful in protecting both the data, the users, the environment, and the drone from any harm. All demonstrations can be found online [1] and the full study can be found on GitHub [2].

A. E2E Encryption Results

The first simulation tested the system to defend against data interception via MitM attacks by way of E2E Encryption. During the startup, both the client and the server call a function that looks for an encryption key respectively on the drone's local directory and the server's local directory, and if not found creates an encryption key and saves the same encryption key on both directories. At the same time, a separate sever that mimics the host server starts up for the drone to connect to believing it is the host server. The drone then begins to move around the environment creating the message to send to the server. The drone then encrypts the message using the encryption key and sends the message out to the server. However, because the client is actually connected to the MitM server, the message is sent to the MitM server, and the MitM server sends out the message to the host server to avoid suspicion. However, the message is encrypted, so the message becomes unreadable to the MitM server as seen in Figure 2. As the encryption is made by a program that is called by the drone and real host server, the data is safe from unwanted viewers that intercepted the message. These results showcase that basic E2E encryption practices can provide a secure method of communication across a network, which important especially if the network constantly passes personal information for it's objective.

B. Anomaly Detection Results

The next cyberattack simulated was a DoS attack, where the client or the server should detect when an anomalous amount of connections are being made. In this simulation, the drone is hard-programmed to move around an environment with no other purpose but to send messages to the server, while the server is meant to read and store messages in a file, so for this research the DoS attack was placed on the server. The server successfully detected a surge of traffic and can promptly implement countermeasures by blocking IP addresses of the attacking system. Other methods that were not demonstrated in this research would be to mitigate traffic to only allow a set amount of connections at a time or utilizing firewalls to mitigate all network traffic. Overall, the results demonstrate that integrating basic traffic analysis and filtering mechanisms into the server can provide a viable first-line of defense against common DoS cyberattacks.

C. Failsafe Mechanism Results

The last cyberattack that was simulated in the research was to design a failsafe mechanism in response to situations where a drone may be disconnected to the system's network. This is critical as when a drone goes rogue from the system, it may be intercepted by attackers or harm bystanders in it's environment. It is important that the drone is able to safely return back to its users. While the drone simulation was running and the drone moves along the four predefined points in the environment, the connection between the client and server was disconnected by shutting down the server. In response, the drone reattempts to connect to the server for the next ten seconds in the event that the disconnection is only temporary or network-related. After the attempts, the drone began to initial it's failsafe procedure and perform an emergency landing to return back to the center of the environment, that is acting as the drone's home base. Once it arrives at the center of the environment, the drone begins to slowly descends and lands. The process was completed without harming any bystanders, the environment, or the drone's structural integrity. The simulation confirms and demonstrates the reliability of a robust and predictable failsafe mechanism in a cyber-physical system.

V. Future Work

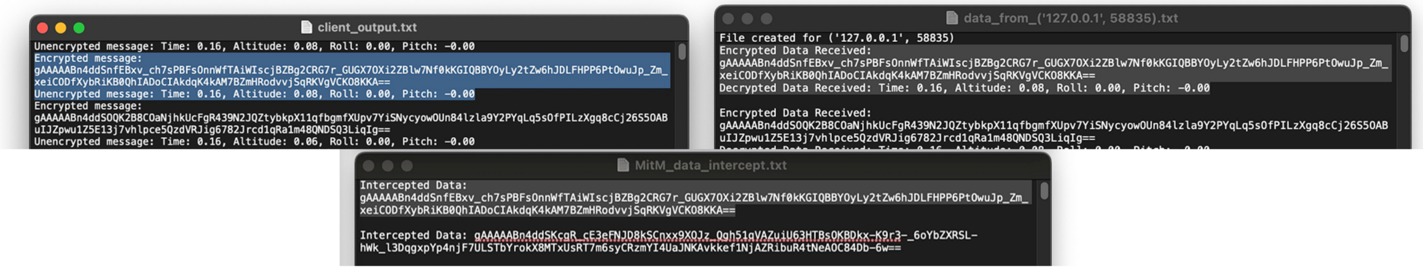
Though this framework protects from a significant variety of threats, there are areas in the framework that would need improvements and more research to be made in order be properly implemented in drone systems. These areas include improvements and research on the defenses used existing framework and additions to the framework that would make the framework more robust.

A. Improvements on Existing Defenses

The current state of the framework is fairly basic and requires more research to fine-tune details of the defenses. As network protection is important for both the security of data and the drone, research into authentication, secure key

[1] Demonstration video available: https://youtu.be/0JJQ03N_g8U

[2] GitHub Repository: https://github.com/davidjlelis/drone_cybersecurity_framework



```
Unencrypted message: Time: 0.16, Altitude: 0.08, Roll: 0.00, Pitch: -0.00
Encrypted message:
gAAAAABn4ddSnfEBxv_ch7sPBFsOnnWfTAiWIscjBZBg2CRG7r_GUGX7OXi2ZBlw7Nf0kKGIQBBYOyLy2tZw6hJDLFHPP6PtOwuJp_Zm_
xeiCODfXybRiKB0QhIADoCIAkdqK4kAM7BZmHRodvvjSqRKVgVCKO8KKA==
Unencrypted message: Time: 0.16, Altitude: 0.08, Roll: 0.00, Pitch: -0.00
Encrypted message:
gAAAAABn4ddSOQK2B8COaNjhkUcFgR439N2JQZtybkpX11qfbgmfXUpv7YiSNycyowOUn84lzla9Y2PYqLq5sOfPILzXgq8cCj26S5OAB
uIJZpwu1Z5E13j7vhlpce5QzdVRJig6782Jrcd1qRa1m48QNDSQ3LiqIg==
Unencrypted message: Time: 0.16, Altitude: 0.06, Roll: 0.00, Pitch: -0.00
```

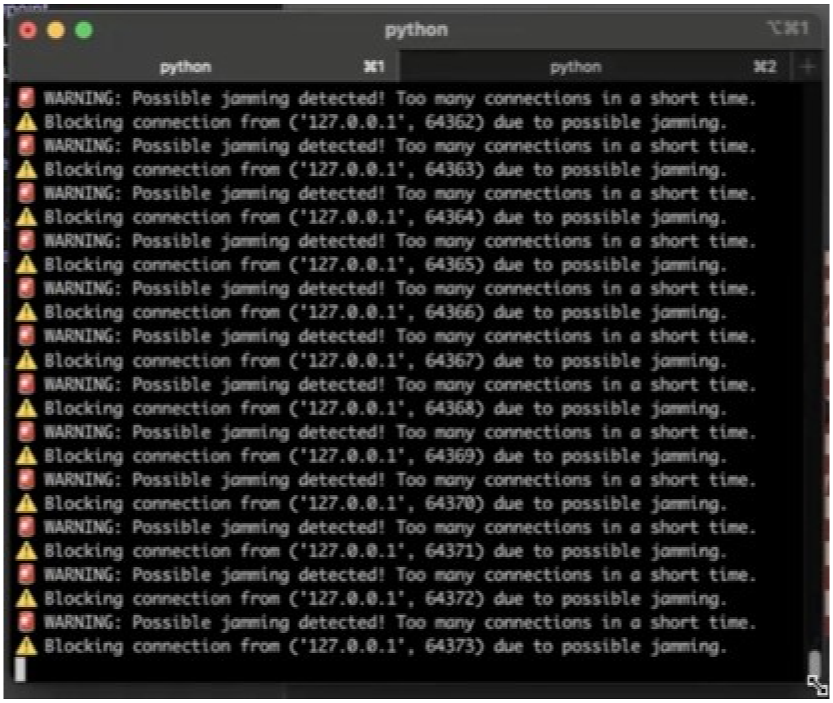
```
File created for ('127.0.0.1', 58835)
Encrypted Data Received:
gAAAAABn4ddSnfEBxv_ch7sPBFsOnnWfTAiWIscjBZBg2CRG7r_GUGX7OXi2ZBlw7Nf0kKGIQBBYOyLy2tZw6hJDLFHPP6PtOwuJp_Zm_
xeiCODfXybRiKB0QhIADoCIAkdqK4kAM7BZmHRodvvjSqRKVgVCKO8KKA==
Decrypted Data Received: Time: 0.16, Altitude: 0.08, Roll: 0.00, Pitch: -0.00

Encrypted Data Received:
gAAAAABn4ddSOQK2B8COaNjhkUcFgR439N2JQZtybkpX11qfbgmfXUpv7YiSNycyowOUn84lzla9Y2PYqLq5sOfPILzXgq8cCj26S5OAB
uIJZpwu1Z5E13j7vhlpce5QzdVRJig6782Jrcd1qRa1m48QNDSQ3LiqIg==
Decrypted Data Received: Time: 0.16, Altitude: 0.08, Roll: 0.00, Pitch: -0.00
```

```
Intercepted Data:
gAAAAABn4ddSnfEBxv_ch7sPBFsOnnWfTAiWIscjBZBg2CRG7r_GUGX7OXi2ZBlw7Nf0kKGIQBBYOyLy2tZw6hJDLFHPP6PtOwuJp_Zm_
xeiCODfXybRiKB0QhIADoCIAkdqK4kAM7BZmHRodvvjSqRKVgVCKO8KKA==

Intercepted Data: gAAAAABn4ddSKcgR_cE3eFNJD8kSCnxx9XOJz_Qgh51qVAZuiU63HTBsOKBDkx-K9r3-_6oYbZXRSL-
hWk_l3DqgxpYp4njF7ULSTbYrokX8MTxUsRT7m6syCRzmYI4UaJNKAvkkef1NjAZRibuR4tNeAOC84Db-6w==
```

Fig. 2. E2E Encryption Results: Drone/Client (Top Left) and Host Server (Top Right) Encryption with Man-in-the-Middle (Bottom Center) Intercepted Message



```
🛑 WARNING: Possible jamming detected! Too many connections in a short time.
⚠ Blocking connection from ('127.0.0.1', 64362) due to possible jamming.
🛑 WARNING: Possible jamming detected! Too many connections in a short time.
⚠ Blocking connection from ('127.0.0.1', 64363) due to possible jamming.
🛑 WARNING: Possible jamming detected! Too many connections in a short time.
⚠ Blocking connection from ('127.0.0.1', 64364) due to possible jamming.
🛑 WARNING: Possible jamming detected! Too many connections in a short time.
⚠ Blocking connection from ('127.0.0.1', 64365) due to possible jamming.
🛑 WARNING: Possible jamming detected! Too many connections in a short time.
⚠ Blocking connection from ('127.0.0.1', 64366) due to possible jamming.
🛑 WARNING: Possible jamming detected! Too many connections in a short time.
⚠ Blocking connection from ('127.0.0.1', 64367) due to possible jamming.
🛑 WARNING: Possible jamming detected! Too many connections in a short time.
⚠ Blocking connection from ('127.0.0.1', 64368) due to possible jamming.
🛑 WARNING: Possible jamming detected! Too many connections in a short time.
⚠ Blocking connection from ('127.0.0.1', 64369) due to possible jamming.
🛑 WARNING: Possible jamming detected! Too many connections in a short time.
⚠ Blocking connection from ('127.0.0.1', 64370) due to possible jamming.
🛑 WARNING: Possible jamming detected! Too many connections in a short time.
⚠ Blocking connection from ('127.0.0.1', 64371) due to possible jamming.
🛑 WARNING: Possible jamming detected! Too many connections in a short time.
⚠ Blocking connection from ('127.0.0.1', 64372) due to possible jamming.
🛑 WARNING: Possible jamming detected! Too many connections in a short time.
⚠ Blocking connection from ('127.0.0.1', 64373) due to possible jamming.
```

Fig. 3. Anomaly Detection Results

exchange protocols, the utilization of advance technologies like AI and the blockchain, and incorporating adaptive thresholds on the network would be beneficial [1] [5] [16] [17]. As for failsafe procedures, research and studies on scenarios regarding the drones hardware like battery life, common drone sensors like LiDAR, and drone location would improve the current failsafe mechanism procedures. Respectively, future research should involve securing the drone before the battery of the drone dies, defenses against spoofing camera vision systems, and the utilization the drone location via GPS. These upgrades and enhancements would ensure that the framework is more reliable, secure, and trusted by users.

B. Additions to the Framework

With the framework its current state, only a subset of the type of cyberattacks that drones may experience are covered. As drones are often utilized in multi-agent systems, where the task may involve a large amount of drones like light shows or search-and-rescue operations, it is important to secure the system's network, sensor, and protect access control across drones. This is vital to not only to complete the drone system's objective, but also to keep users and the environment safe. The consequences for the lack of security in these cybersecurity areas could include network infiltration, tampering, misinformation, and system malfunction [20]. Another side of security for research is the implementation and social aspect, like how a drone system may assimilate into an environment and how the inhabitants of the environment may respond. For example, a patrol drone system may have difficulty when being integrated into law enforcement operations, both by the environment itself via buildings that are difficult to move around and the inhabitants who may attempt to apprehend the drone. The last area of interest for including into the framework would be avoiding direct harm to users in scenarios where drones may be directly interacting with humans and animals. As the sole purpose of robotic systems is to help society, any scenario that can cause harm, injury, and death should be avoided as much as possible.

VI. Conclusion

A cybersecurity framework for new technologies is important to keep users' data and personal information safe, and in the case of robots where their influence directly impacts bystanders and the environment, it is very important to secure these technologies to keep the users and environment physically safe. The research carried out in this paper proposes a framework that focuses on autonomous drones by securing data communications, mitigating networks, and providing a failsafe in the event that the drones disconnect from its system network. It is important for developers to implement a drone cybersecurity framework during the development of the drone system to be proactive, resilient, and provide a standard level of security [22]. In all, a technology-specific standard of cybersecurity would aid drones in their ability to perform their tasks in a trusting and reliable way so that the person's data and safety are secured in the drone's purpose.

References

[1] Ilya Afanasyev, Alexander Kolotov, Ruslan Rezin, Konstantin Danilov, Manuel Mazzara, Subham Chakraborty, Alexey Kashevnik, Andrey Chechulin, Aleksandr Kapitonov, Vladimir Jotsov, et al. Towards blockchain-based multi-agent robotic systems: Analysis, classification and applications, 2019.

[2] Alessio Botta, Sayna Rotbei, Stefania Zinno, and Giorgio Ventre. Cyber security of robots: A comprehensive survey. *Intelligent Systems with Applications*, 18:200237, 2023.

[3] George W Clark, Michael V Doran, and Todd R Andel. Cybersecurity issues in robotics. In *2017 IEEE conference on cognitive and computational aspects of situation management (CogSIMA)*, pages 1–5. IEEE, 2017.

[4] Vibekananda Dutta and Teresa Zielińska. Cybersecurity of robotic systems: Leading challenges and robotic system design methodology. *Electronics*, 10(22):2850, 2021.

[5] Salvo Finistrella, Stefano Mariani, Franco Zambonelli, et al. Multi-agent reinforcement learning for cybersecurity: Approaches and challenges. In *CEUR WORKSHOP PROCEEDINGS*, volume 3735, pages 103–118. CEUR-WS, 2024.

[6] Pranav Guruprasad, Harshvardhan Sikka, Jaewoo Song, Yangyue Wang, and Paul Pu Liang. Benchmarking vision, language, & action models on robotic learning tasks. *arXiv preprint arXiv:2411.05821*, 2024.

[7] Don Harriss, Raymond Sheh, and Karen Geappen. Autonomous aerial drones connecting public safety: Opportunities and challenges for the future. 2024.

[8] N. Hockstein, C. Gourin, Russell Faust, and D. Terris. A history of robots: From science fiction to surgical robotics. *Journal of Robotic Surgery*, 1:113–118, 07 2007.

[9] Grozdan Hristov, Ivan Stankov, and Dayana Mladenova. Cyberattacks and robotics. In *2023 31st National Conference with International Participation (TELECOM)*, pages 1–4. IEEE, 2023.

[10] Lee Kasowaki and Adem Burak. Cybersecurity essentials for robotics process automation deployments. 2023.

[11] Vicente Matellán, 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)*, pages 1–5. IEEE, 2021.

[12] Víctor Mayoral-Vilches. Robot cybersecurity, a review. *International Journal of Cyber Forensics and Advanced Threat Investigations*, 2022.

[13] Cheryl McCloud. Falling drone during florida holiday show seriously injures 7-year-old boy. what we know. *Florida Today*, December 2024. Accessed: 2025-04-18.

[14] Richard Owoputi and Sandip Ray. Security of multi-agent cyber-physical systems: A survey. *IEEE Access*, 10:121465–121479, 2022.

[15] SM Mizanoor Rahman. An iot-based common platform integrating robots and virtual characters for high performance and cybersecurity. In *2019 SoutheastCon*, pages 1–6. IEEE, 2019.

[16] Sathishkumar Ranganathan, 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)*, pages 76–81. IEEE, 2021.

[17] Fendy Santoso and Anthony Finn. An in-depth examination of artificial intelligence-enhanced cybersecurity in robotics, autonomous systems, and critical infrastructures. *IEEE Transactions on Services Computing*, 17(3):1293–1310, 2023.

[18] Spectrum News Staff. Ntsb's preliminary report on orlando drone show mishap notes what went wrong. *Spectrum News 13*, January 2025. Accessed: 2025-04-18.

[19] Wojciech Szynkiewicz, Ewa Niewiadomska-Szynkiewicz, and Kamila Lis. Deep learning of sensor data in cybersecurity of robotic systems: Overview and case study results. *Electronics*, 12(19):4146, 2023.

[20] Jibrilla Abubakar Tanimu and Wafia Abada. Addressing cybersecurity challenges in robotics: A comprehensive overview. *Cyber Security and Applications*, page 100074, 2024.

[21] Webots. http://www.cyberbotics.com. Open-source Mobile Robot Simulation Software.

[22] Jean-Paul A Yaacoub, Hassan N Noura, Ola Salman, and Ali Chehab. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, 21(1):115–158, 2022.

[23] Quanyan Zhu, Stefan Rass, Bernhard Dieber, and Vıctor Mayoral Vilches. An introduction to robot system cybersecurity. *arXiv preprint arXiv:2103.05789*, 2021.