Enhancing UAV Swarm Security through an RSSI-based Protocol for GNSS-Compromised Environments

Mauro Conti
University of Padua, Italy
mauro.conti@unipd.it

Federico Corò
University of Padua, Italy
federico.coro@unipd.it

Giulio Rigoni
Sapienza University of Rome, Italy
giulio.rigoni@uniroma1.it

***Abstract*—The UAV market has experienced significant growth, with an expanding range of applications. However, the reliance of UAV missions on GNSS makes them vulnerable to attacks, particularly GNSS spoofing and jamming, which can cause mission failure or even physical damage. To mitigate this risk, we propose a lightweight fleet protocol designed to ensure that drones can complete their missions securely, even when under attack. Our system utilizes intra-fleet communication and Received Signal Strength Indicator (RSSI) measurements for positioning, enabling the fleet to maintain formation and reach its destination even under GNSS attacks, or in a GNSS compromised scenario, thus avoiding its vulnerabilities. The proposed protocol was evaluated through extensive simulations using NS-3. The results reveal that the proposed protocol achieves a high mission success rate, reaching 100% in most single-attack scenarios, and demonstrates robust attack identification even when multiple drones are attacked or compromised. The average attack detection delay was measured at 300 milliseconds for single-attacker scenarios, while the RSSI table was updated every 50 to 55 milliseconds, ensuring data freshness. These findings highlight the potential of our solution to improve the resilience of UAV swarms in GNSS-compromised environments.**

***Index Terms*—UAV, Drone, GNSS Attack Countermeasure, Cyber-security**

I. Introduction

The proliferation of Unmanned Aerial Vehicles (UAVs) in sectors such as agriculture, surveying, and military operations [1] has simultaneously highlighted critical security vulnerabilities [2]. A primary concern is the reliance on unencrypted civilian Global Navigation Satellite System (GNSS) signals for navigation. The inherent weakness of these signals makes UAVs highly susceptible to jamming and, more critically, spoofing attacks [3]. By broadcasting counterfeit GNSS signals, an attacker can hijack a drone's navigation system, leading to mission failure, collisions, or unauthorized landings by faking flight into restricted airspace [4].

To counteract this threat, researchers have proposed various detection mechanisms. One line of work uses onboard inertial sensors, combining data from gyroscopes, accelerometers, and IMUs to spot inconsistencies with the reported positions of the GNSS [5]–[8]. Others apply machine learning models like SVM or XGBoost to learn patterns indicative of an attack from sensor data [9], [10]. Another approach utilizes external data sources, such as comparing real-time aerial imagery with satellite maps [11], [12], using crowdsourced data [13], or employing ground control stations to verify fleet positions [14]. However, many of these solutions are computationally intensive or require additional hardware (e.g., specialized antennas, LIDAR) [15]–[17], making them ill-suited for small UAVs with limited resources. Furthermore, most of the existing literature focuses on single-drone defense rather than cooperative fleet resilience.

To address these gaps, this paper introduces a novel lightweight protocol for UAV swarms that ensures mission success even when the GNSS is compromised. Our system is designed to be computationally efficient and does not require additional hardware. The key contributions of this work are the introduction of a decentralized intra-fleet communication protocol that uses Received Signal Strength Indicator (RSSI) measurements for relative positioning, enabling the fleet to collectively detect, counter, and mitigate GNSS attacks. This approach allows the swarm to maintain formation integrity and navigate to its destination without relying on vulnerable GNSS signals post-attack. Our protocol assumes initial GNSS trustworthiness at the mission's start; addressing pre-flight compromise is a direction for future work.

II. Problem Overview

We consider a fleet of UAVs that autonomously navigate toward a designated destination while maintaining a predefined formation. Initially, each drone relies on its GNSS system for navigation, plotting a path towards the mission destination.

However, the fleet is vulnerable to GNSS spoofing attacks, which can target any one of the drones, compromising its ability to safely use GNSS for the remainder of the mission. After the successful attack, the GNSS becomes unreliable for the compromised drone, thus forcing it to rely on an alternative method (our proposed RSSI-based system) to track its position and follow the initial route to reach the destination.

Although prior research has extensively explored the vulnerabilities of standalone GNSS receivers to spoofing (e.g., [18]), our work focuses on the fleet-level response to such attacks.

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

979-8-3503-9281-4/25/$31.00 ©2025 IEEE

Specifically, our primary objective is to ensure the safe recovery of all drones within the fleet and that the entire fleet reaches the designated destination.

To achieve this, we focus on two critical aspects: Developing methods for the earliest detection of spoofing attacks during the mission; and designing and implementing effective countermeasures to support a compromised drone, enabling it to rejoin the fleet formation and complete the mission.

In this scenario, there are two distinct perspectives to consider: the attacker's point of view and that of the fleet of drones. Each perspective operates based on its own set of assumptions, which are outlined below.

Attacker Assumptions: (i) We assume that the targeted UAV is within the attacker's range and thus susceptible to receiving these fake GNSS spoofing signals. (ii) Furthermore, we assume that the attacker has successfully compromised at least one UAV, achieving control over the positional information received by the drone. (iii) While the primary focus of our threat model considers an attacker capable of compromising one drone at a time due to the significantly increased difficulty of simultaneously spoofing multiple UAVs as highlighted in [19], our evaluation also explores the protocol's resilience against scenarios where multiple drones are concurrently attacked to assess its broader robustness (see Section IV-E).

UAV Fleet Assumptions: (i) The UAV fleet starts with and maintains a predefined formation throughout the mission. Deviation from this formation is only permitted for collision avoidance or to accommodate a compromised drone that rejoins the formation. (ii) There is a secure and reliable communication protocol between drones, enabling them to share positional data (relative or absolute), status updates, and coordinate maneuvers. This channel is assumed to be immune to the attacker's influence. (iii) A robust collision avoidance protocol is implemented to prevent collisions between drones within the fleet and with any external obstacles. (iv) Initial trustworthiness of the GNSS at the beginning of the mission.

While UAV swarms can be susceptible to a variety of cyber-physical attacks, this paper specifically focuses on mitigating GNSS spoofing attacks. Other potential attack vectors exist (such as communication jamming or data spoofing) but those types of attacks are considered outside the primary focus of this work for several reasons. Our proposed solution relies on the integrity of the intra-fleet communication channel for its defense mechanism. Addressing attacks that directly compromise this communication channel would require different defense strategies, such as cryptographic protection of messages or advanced channel hopping techniques, which are beyond the scope of the current research.

A. Communication Protocol

The core of this work is the development of an intra-fleet protocol for GNSS-attack resilience, thus a communication protocol between drones is essential. The literature proposes two main techniques for communication for fleet control [20]: Centralized and Decentralized Structure. We chose to develop a fully Decentralized System to avoid the single point of failure which is a major safety issue regarding the Centralized method. Additionally, a decentralized system offers greater robustness and scalability, as each drone communicates directly with others using radio signals, like in a typical WiFi network, through an ad-hoc or Wireless Ad Hoc Network. In our implementation, the drones establish UDP sockets for communication throughout the simulation. The broadcast rate ranges between 1 and 100 ms and is chosen randomly each time to minimize packet collisions between drones. This approach helps maintain good RSSI freshness while preventing excessive packet transmission and reducing the likelihood of collisions.

B. Fleet Formation

To identify a practical and effective static fleet formation, this study focuses on balancing safety with communication efficiency. This involves considering the minimum number of drones needed for redundancy against attacks, the maximum number to maintain scalability and manageable overhead, and how the geometric arrangement impacts communication and resilience. The ideal formation must ensure reliable communication, stability, and mission effectiveness, while being flexible enough to adapt to different fleet sizes and requirements. We evaluated various geometric configurations against key criteria, including scalability, simplicity, and compatibility with a decentralized communication protocol. Based on this analysis, we selected the Line, Grid, Circle, and Star formations.

C. Log-Distance Path Loss Model for Distance Estimation

To estimate inter-drone distance from RSSI, we employ the standard Log-Distance Path Loss Model, $PL(d) = PL(d_0) + 10 \cdot n \cdot log_{10}(d/d_0) + x$, where, d is the distance between the transmitter and the receiver, and d_0 is the reference distance, usually 1 meter. $PL(d)$ is the total path loss in decibels (dB) at distance d. $PL(d_0)$ is the path loss in dB at a known reference distance d_0. This value is usually measured in the field or calculated based on free space path loss if the environment is similar. For our simulations, the reference path loss $PL(d_0)$ at 1m is 46.6777 dB, and the path loss exponent n is set to 3. Finally, x represents a noise factor from a random variable that models the shadow effect, typically caused by obstacles and other environmental factors, often modeled as a Gaussian random variable with zero mean and standard deviation. In our code, this random variable is multiplied by the estimated distance to add noise to the calculation.

III. Proposed Solution

The proposed solution is an intra-fleet communication protocol, with different tasks:

A. Fleet control

Our approach involves employing a fixed fleet formation for UAVs, using both communication mechanisms and position tracking methods to ensure coordinated operations. During the initial phase of the mission, the drones rely on the GNSS system for navigation and positioning. However, once a potential

attack is detected and one of the drones is compromised, the GNSS signals are deemed ”untrusted” for that specific drone, necessitating a transition to an alternative positioning strategy.

At this critical point, the compromised drone must adopt a different method to maintain its relative positions within the fleet and navigate effectively. Additionally, the velocity of the fleet becomes a key parameter that must be continuously monitored and controlled to ensure mission success conditions.

To address these challenges, we have selected an RSSI table (Received Signal Strength Indicator) as the foundation of our alternative positioning system. This approach allows drones to estimate relative distances and maintain formation integrity without relying on vulnerable GNSS signals, thereby improving the fleet's resilience against attacks.

B. RSSI Table

To estimate inter-drone distances, we use the Log-Distance Path Loss Model [21], which is suitable for environments where obstacles influence signal propagation. This allows the creation of a shared table of estimated distances via RSSI measurements to defend against GNSS spoofing attacks. In our decentralized approach, each drone helps maintain this table. Drones perform local updates by measuring RSSI from neighbors, periodically broadcast their data for dissemination, and fuse received information to maintain a consistent network view. A synchronized timer, with a randomized broadcast rate between 1 and 100 ms, coordinates these updates to ensure data freshness while minimizing packet collisions.

Given the drones' motion, this frequent communication is necessary to keep the distance table up-to-date with minimal latency. Each drone uses the RSSI table for relative positioning, supplementing its GNSS. By constantly comparing these RSSI-derived positions against the predefined fleet formation, significant deviations can be quickly detected as inconsistencies, which may be attributed to a GNSS spoofing attack.

a) RSSI challenges: Although RSSI is a valuable tool for relative positioning, its accuracy can be impacted by environmental factors, such as obstacles and interference, that affect signal strength. To address these challenges, our solution incorporates two strategies. First, frequent communication between drones maintains an up-to-date RSSI table, which minimizes the impact of temporary fluctuations in signal strength. Second, the use of a fixed fleet formation allows quick detection of inconsistencies in RSSI measurements that may indicate an attack or environmental interference.

C. Attack Detection

The most common GNSS spoofing attack follows a two-phase pattern. First, the attacker initiates a jamming phase by transmitting noise or interference on the same frequency as genuine GNSS signals. This degrades signal quality, making it harder for drones to determine their position accurately. Once the authentic signals are sufficiently weakened, the attacker introduces spoofed GNSS signals, which appear stronger and reliable, containing false coordinates. As the drones latch onto these fake signals, they fall under the attacker's control, potentially forcing them to change route. To detect this change in the compromised drone's trajectory, each drone maintains an RSSI table that stores the estimated distances between all drones in the fleet. At the start of the mission, each drone establishes an average distance from all other drones based on the initial GNSS positions and the predefined fleet formation. Throughout the mission, drones continuously monitor these distances, comparing them to the established averages.

The attack detection algorithm works in five main steps: (i) Each drone continuously measures the RSSI values of signals received from its neighbors and updates its local RSSI table. (ii) The drone compares the current estimated distances in its RSSI table with the established average distances. (iii) If the deviation between the current distance and the average distance for a particular neighbor exceeds a predefined threshold, the drone marks that neighbor as ”dangerous”. The threshold is determined based on the expected accuracy of the RSSI measurements and the desired sensitivity of the detection algorithm. (iv) A drone under attack will observe a majority of its neighbors as ”dangerous” due to the inconsistencies in its perceived distances. On the other hand, safe drones will only see a minority of their neighbors as ”dangerous”. (v) If a drone observes that a majority of its neighbors are marked as ”dangerous,” It triggers the countermeasure protocol, recognizing that it is likely under attack. This distinction between the perspectives of the compromised drone and the safe drones allows for a targeted response to the attack. While this describes the fundamental detection mechanism, often from the perspective of a single compromised drone or its immediate non-compromised neighbors, Section IV-E details how these principles extend to scenarios involving multiple compromised drones and how overall fleet-level attack identification is assessed.

In real-world environments, factors such as obstacles, interference, and environmental noise can affect the accuracy of RSSI measurements and lead to false positives. To mitigate this, the proposed protocol incorporates two strategies: Drones communicate frequently to maintain an up-to-date RSSI table, minimizing the impact of temporary fluctuations in signal strength; and the use of a fixed fleet formation allows for quick detection of inconsistencies in RSSI measurements that may indicate an attack or environmental interference.

One critical challenge in detecting compromised drones within a fleet arises when their behavior mimics that of non-compromised drones. If a compromised drone follows the same trajectory as the unaffected drones, distinguishing it becomes increasingly difficult, thus we decided to move the drone in a direction different from that of the fleet to avoid overlapping routes. In a real-world scenario, the attacker's primary objective is to steal the drone, making it highly unlikely that the injected path would match the original trajectory.

D. Attack Mitigation

Upon detection of an attack, the mitigation strategy assumes that each drone has an independent compass, which most drones has, to determine direction. This compass provides

a reliable source of heading information that is not affected by GNSS spoofing. The mitigation strategy works as follows. Safe drones continuously broadcast their direction information, relative to their compass readings, to the compromised drone. The compromised drone, unable to rely on its GNSS for accurate positioning, uses the direction information received from the safe drones to adjust its trajectory and follow the rest of the fleet. The compromised drone estimates its relative position to its neighbors using the RSSI table and adjusts its trajectory to rejoin the fleet formation. This approach relies on continuous communication between the drones and the presence of a reliable compass on each one. As long as the compromised drone receives directional information and remains within a suitable distance to perform the necessary maneuver, it can effectively stay with the fleet and continue the mission. It is important to acknowledge that this strategy is not without limitations and may result in the loss of the compromised drone under certain circumstances. For example, if the attacked drone begins to follow instructions later in the mission, it may fail to reach the destination if all other drones have already arrived and ceased movement. In such cases, the delayed drone might remain significantly distant from the fleet, and it is considered lost. This outcome occurs when the compromised drone exceeds the predefined time threshold for a successful arrival at the destination, causing it to receive a stop command while still far from its target. If the time threshold had been extended, the drone might still have been able to reach the destination. Nevertheless, our experiments demonstrate that the proposed protocol generally achieves a high mission success rate. In most scenarios, the fleet achieves a 100% success rate, highlighting the robustness of the strategy despite its occasional limitations.

IV. Evaluation

To evaluate the effectiveness of our proposed solution, we conducted simulations using NS-3[1], a discrete-event network simulator. NS-3 was chosen due to its widespread adoption in networking research, particularly for studies involving UAV communications, mobility, and wireless protocols. Furthermore, the modules required for our simulations, such as those for Wi-Fi networking, mobility models, and energy consumption, are well-established and extensively tested within the NS-3 framework, providing a reliable basis for our evaluations. This allowed us to simulate different attack scenarios and analyze the performance of our system with confidence in the underlying models. In our simulations, we considered a variety of factors including the number of drones in the fleet (4 and 9), the number of simultaneously attacked drones, different fleet formations (line, circle, grid, star), drone speed (5, 10, 15, 20 m/s), and communication readiness to assess the impact of these factors on the system's resilience to GNSS spoofing attacks. In addition, all evaluations in this study were performed using the average results of five independent runs for each scenario. This approach ensured that the findings were robust and accounted for the variability of the results due to random factors in the simulations, thus minimizing the impact of outliers and obtaining more reliable results.

We focused on several key metrics to comprehensively assess the performance and effectiveness of the proposed strategies. These metrics were carefully chosen to capture different aspects of the system's behavior and its ability to achieve mission objectives under varying conditions. These metrics are as follows. (i) Communication Overhead: We measured the average number of packets sent and received per drone to assess the efficiency of the communication protocol. (ii) RSSI Table Freshness: We evaluated how quickly the RSSI table is updated by measuring the time elapsed between updates. (iii) Successful Attack Detection Lag: We measured the time it took the system to detect a successful GNSS spoof attack (i.e., a compromised drone). (iv) Mission Success Rate: We evaluated the percentage of drones that successfully reached the destination in different attack scenarios.

A. Communication Performance and Reliability

We evaluated the communication performance of the system by measuring network traffic volume and packet loss rates. The experiments varied the size of the fleet (4 and 9 drones), the formation, and the operational speed. Our analysis of communication overhead confirmed that traffic volume scaled predictably with the number of drones, while it was largely unaffected by changes in fleet formation or speed.

The more critical metric for our evaluation was the reliability of communication under attack, assessed by the packet loss rate. In scenarios without attacks, the packet loss rate was minimal, remaining below 0.4% for the 4-drone fleet and at 2.5% for the 9-drone fleet. The introduction of an attack had a varied impact depending on the size of the fleet. For the 4-drone fleet, the packet loss rate remained low (¡0.4%). However, for the 9-drone fleet, the packet loss rate increased to approximately 3%.

These results indicate that, while the base communication overhead is predictable, the reliability of the network under attack is more sensitive to the scale of the fleet.

B. RSSI Table Freshness

We evaluated the freshness of the RSSI table by measuring how many milliseconds elapse between updates to the table.

To measure the freshness of the RSSI table, we recorded the timestamps of consecutive updates to the table. The difference between these timestamps gives us the time elapsed between updates. We conducted this measurement across different formations and speeds to assess if these factors influence the update frequency. The results are presented in Figures 1.

From the results, we can observe that the median time between updates to the RSSI table hovers between 50 and 55 milliseconds. This update frequency remains consistent across the spectrum of formations and speeds tested. While minor variations do exist, they do not appear significant enough to suggest any dependence on specific formations or speeds.

[1]http://www.nsnam.org/

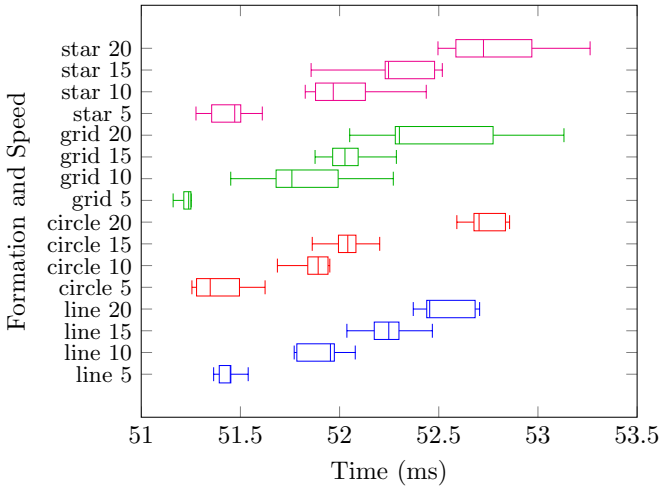

Fig. 1. Distribution of RSSI table update intervals (ms) for 9 drones.

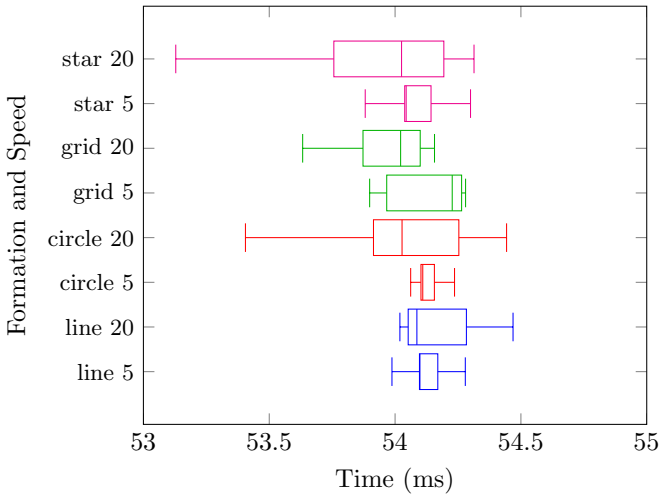

Fig. 2. Distribution of RSSI table update intervals (ms) for 9 drones in the absence of attack.

Then we also tested the RSSI table freshness in the absence of attacks, our analysis in this case revealed that while the updates are more stable without attacks, they are slightly slower than under attack, see Fig. 2. This observation can be explained by considering the drones' behavior in each scenario. When not under attack, the drones fly in a predictable, controlled formation, leading to slightly slower but more consistent updates.

Conversely, during a GNSS spoofing attack, the drones' navigation is disrupted, and the system needs to react to maintain the formation. This results in a slightly faster, but less stable, update frequency.

C. Attack Detection Lag

We evaluated the attack detection lag by measuring the average time it takes for the formation to detect that the fleet is under attack. The attack detection lag was a consistent 300 ms across nearly all scenarios. The only minor deviation was a 340 ms lag observed in the 9-drone line formation at a low speed of 5 m/s, likely attributable to the greater inter-drone distances in that specific configuration

D. Mission Success Rate

Finally, we analyzed the mission success rate, which we define as the percentage of drones that successfully reached the designated destination. This metric was evaluated in various attack scenarios to assess the effectiveness of the proposed mitigation strategies. These strategies considered key parameters such as the number of drones deployed, their flight speed, and the formation they maintained during the mission. By varying these parameters, we aim to identify configurations that best mitigate the impact of attacks and maximize mission success.

A drone was considered to have successfully reached the destination if it came to a complete stop within a 2.5-meter radius of the destination point, ensuring it was sufficiently close for practical purposes. Alternatively, a drone was also considered successful if it stopped within 1 meter of another drone that had already satisfied the first condition. This secondary condition was included to account for the inherent physical limitations of the drone's size and configuration.

The inclusion of the second condition reflects the physical realities of the drones' 40 cm diameter, which can impose constraints in densely packed formations. For example, in scenarios where drones were arranged in a tight 9-drone line formation, it would not always be feasible for all drones to simultaneously stop within the 2.5-meter radius of the target. The second condition accommodates this by acknowledging that a drone's proximity to another successful drone effectively brings it into the target area, particularly in cases where physical space near the destination is limited.

The effectiveness of the protocol was ultimately measured by the mission success rate, defined as the percentage of drones reaching the destination. The system was proved highly robust, achieving a success rate 100% in the vast majority of scenarios, including all tests involving 9-drone fleets. The few exceptions occurred in smaller 4-drone fleets at high speeds (15 m/s and 20 m/s), where the success rate was 90-95% for the Line and Grid formations. These instances highlight the inherent difficulty of post-attack formation recovery with a minimal number of drones at high velocity.

A significant advantage is the algorithm's excellent mission success rate even with small fleet formations. This ability to maintain high performance with fewer drones makes the system practical and scalable for various operational scenarios, underscoring the robustness of our approach.

E. Multi-Drone Attack Scenarios

To further assess the robustness of our protocol, we conducted experiments in which multiple drones within the fleet were simultaneously compromised by GNSS spoofing attacks. The methodology involved fixing the size of the fleet, the formation, and the speed of the drones. We then incrementally increased the number of simultaneously attacked drones.

In this scenario we computed the attack identification rate, defined as the percentage of simulation runs in which the fleet correctly identified that it was under a multi-drone attack. Fig. 3 presents the attack identification rates for the star formation with 4 and 9 drones, respectively, at a speed of 5 m/s and 20 m/s. Each value in the plot is the average over 5 different run.

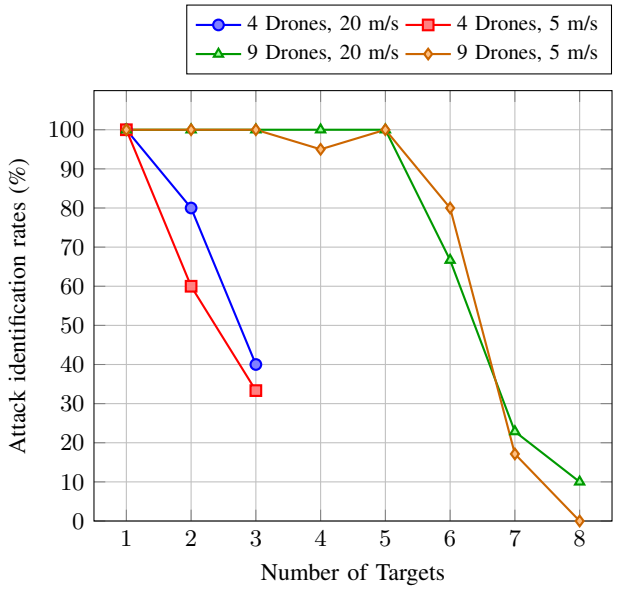

Fig. 3. Attack identification rates for different number of drones and speeds using the star formation.

As anticipated, the attack identification rate decreases as more drones are simultaneously compromised. This occurs because numerous compromised drones create widespread and conflicting RSSI inconsistencies, which complicates detection for the remaining drones. However, the identification rate remains remarkably high even when a significant portion of the fleet is under attack, demonstrating the strong resilience of the proposed RSSI-based detection mechanism. While overall mission success also depends on the mitigation strategy, this high identification rate is a promising indicator of the system's ability to recognize widespread threats.

V. Conclusion and Future works

This paper introduced an efficient and robust RSSI-based protocol for the navigation of the UAV fleet in environments characterized by GNSS. Extensive simulations validated its effectiveness, demonstrating consistently high mission success rates, particularly in single-attacker scenarios, and robust attack identification even when multiple drones were compromised. A key strength is the system's excellent performance even with small fleet sizes, highlighting its practicality and scalability without requiring a large number of drones.

Future work will focus on several enhancements. We plan to introduce a leader drone mechanism for improved situational awareness, expand the positioning framework by integrating time-of-arrival and angle-of-arrival data to develop a more precise multilateration algorithm, and explore dynamic fleet formations that adapt to mission needs, potentially using machine learning for real-time optimization.

References

[1] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (uavs): Practical aspects, applications, open challenges, security issues, and future trends," *Intelligent Service Robotics*, vol. 16, no. 1, pp. 109–137, 2023.

[2] G. Butler and R. Montasari, "Unmanned aerial vehicles (uavs): Forensic, privacy, and security challenges in the era of drone proliferation," in *Space Governance: Challenges, Threats and Countermeasures*. Springer, 2024, pp. 229–239.

[3] B. Van den Bergh and S. Pollin, "Keeping uavs under control during gps jamming," *IEEE Systems Journal*, vol. 13, no. 2, pp. 2010–2021, 2018.

[4] S. Z. Khan, M. Mohsin, and W. Iqbal, "On gps spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions," *PeerJ Computer Science*, vol. 7, p. e507, 2021.

[5] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi, "An efficient uav hijacking detection method using onboard inertial measurement unit," *ACM Transactions on Embedded Computing Systems*, vol. 17, no. 6, pp. 1–19, 2018.

[6] M. Kok, J. D. Hol, and T. B. Schön, "Using inertial sensors for position and orientation estimation," *arXiv preprint arXiv:1704.06053*, 2017.

[7] Z. Tu, F. Fei, M. Eagon, D. Xu, and X. Deng, "Flight recovery of mavs with compromised imu," in *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 2019, pp. 3638–3644.

[8] J. Xiao, Y. Li, C. Zhang, and Z. Zhang, "Ins/gps integrated navigation for unmanned ships based on eemd noise reduction and ssa-elm," *Journal of Marine Science and Engineering*, vol. 10, no. 11, p. 1733, 2022.

[9] G. Panice, S. Luongo, G. Gigante, D. Pascarella, C. Di Benedetto, A. Vozella, and A. Pescapè, "A svm-based detection approach for gps spoofing attacks to uav," in *International Conference on Automation and Computing (ICAC)*. IEEE, 2017, pp. 1–11.

[10] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi, "Efficient drone hijacking detection using two-step ga-xgboost," *Journal of Systems Architecture*, vol. 103, p. 101694, 2020.

[11] N. Xue, L. Niu, X. Hong, Z. Li, L. Hoffaeller, and C. Pöpper, "Deepsim: Gps spoofing detection on uavs using satellite imagery matching," in *Annual Computer Security Applications Conference*, 2020, pp. 304–319.

[12] B. Davidovich, B. Nassi, and Y. Elovici, "Towards the detection of gps spoofing attacks against drones by analyzing camera's video stream," *Sensors*, vol. 22, no. 7, p. 2608, 2022.

[13] K. Jansen, M. Schäfer, D. Moser, V. Lenders, C. Pöpper, and J. Schmitt, "Crowd-gps-sec: Leveraging crowdsourcing to detect and localize gps spoofing attacks," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 1018–1031.

[14] C. Liang, M. Miao, J. Ma, H. Yan, Q. Zhang, X. Li, and T. Li, "Detection of gps spoofing attack on unmanned aerial vehicle system," in *Machine Learning for Cyber Security: Second International Conference (ML4CS)*. Springer, 2019, pp. 123–139.

[15] J. Ho, S. Phang, and H. Mun, "2-d uav navigation solution with lidar sensor under gps-denied environment," in *Journal of Physics: Conference Series*, vol. 2120, no. 1. IOP Publishing, 2021, p. 012026.

[16] K. Jansen, N. O. Tippenhauer, and C. Pöpper, "Multi-receiver gps spoofing detection: Error models and realization," in *Annual Conference on Computer Security Applications*, 2016, pp. 237–250.

[17] H. Sathaye, G. LaMountain, P. Closas, and A. Ranganathan, "Semperfi: Anti-spoofing gps receiver for uavs," in *Network and Distributed Systems Security (NDSS) Symposium*, 2022.

[18] A. Altaweel, H. Mukkath, and I. Kamel, "Gps spoofing attacks in fanets: A systematic literature review," *IEEE Access*, vol. 11, pp. 55 233–55 280, 2023.

[19] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful gps spoofing attacks," in *ACM Conference on Computer and Communications Security*. ACM, 2011, p. 75–86.

[20] G. Pantelimon, K. Tepe, R. Carriveau, and S. Ahmed, "Survey of multi-agent communication strategies for information exchange and mission control of drone deployments," *Journal of Intelligent & Robotic Systems*, vol. 95, pp. 779–788, 2019.

[21] J. Seybold, "Introduction to rf propagation," *John Wiley & Sons google schola*, vol. 2, pp. 517–526, 2005.