Securing Cislunar Missions: A Location-Based Authentication Approach

Nesrine Benchoubane, Baris Donmez, Olfa Ben Yahia, Gunes Karabulut Kurt
Poly-Grames Research Center, Department of Electrical Engineering, Polytechnique Montréal, Montréal, QC, Canada

Emails: {*nesrine.benchoubane, baris.donmez, olfa.ben-yahia, gunes.kurt*}*@polymtl.ca*

***Abstract*—As the evolution of next-generation communications networks proceeds, a multitude of wireless devices are gaining access to the network, and the amount of transmitted data is rapidly increasing. Yet, with more and more critical data requiring confidential transmission and protection on the network, the security risks for wireless communications networks are even more significant. Considering the fixed-trajectory nature of satellites orbiting the Earth, it is worth investigating how this invariant can be leveraged to ensure security and reliability. In this paper, we propose a location-based authentication framework for the cislunar space with distance verification for secure authentication. Expanding on this foundation, our work supports tolerance variations based on relative orbit positions and noise sources in space. In addition, we perform Monte Carlo simulations under noisy propagation conditions assumption, providing a robust evaluation of the proposed framework's performance in diverse and challenging lunar communication scenarios.**

***Index Terms*—Authentication, cislunar, satellite network, physical layer security, location estimation.**

I. Introduction

NASA, along with initiatives supported by the USA, the EU, Canada, Japan, China, and India, is looking into missions that go beyond low Earth orbit (LEO) but remain within the region between Earth and the Moon. This research is part of their preparation for sending humans further into deep space exploration, including missions to Mars [1]. Since 1968, exploring the Moon has been a significant objective for humanity, and over recent years, our understanding of the Moon has greatly improved thanks to missions involving orbiting satellites, landings, robots, human exploration, and the return of lunar samples [2]. The latest lunar mission, Chandrayaan-3, launched on August 23, 2023, successfully deployed a lander and rover in the Moon's southern highlands near the South Pole. This mission aims to conduct various scientific measurements both on the lunar surface and from orbit [3]. NASA's Artemis II mission, which is a preparatory step for a scheduled lunar landing in 2025, marks a significant milestone as the first instance since the Apollo 17 mission in 1972 where astronauts will venture beyond LEO. In the coming years, there will be a series of over a dozen lunar missions. Various missions will orbit or fly by the Moon; others will perform landings; and some will release rovers and robotic explorers to further investigate the lunar surface.

There are several unresolved challenges concerning lunar exploration, particularly in areas like communication systems and security. Establishing and designing a reliable communication network between the Moon, spacecraft, and Earth is crucial, as the vast distance can cause significant delays and interruptions. Security is another critical issue, as systems must be secure against potential threats and malfunctions in the harsh lunar environment. Additionally, the technology must be robust enough to handle the unique problems posed by lunar dust and extreme temperature variations. Addressing these issues is essential for the success of future missions to the Moon.

Future Moon missions will rely on new space networks that include relay satellites and spacecraft to improve communication between various users, like exploration vehicles, landers, and astronauts. Having a strong and safe communication system is key to the success of these missions. Although there has been progress in establishing these networks, the security and reliability of these communication systems still need more research. Since space communications can be easily interrupted or hacked due to their wireless broadcast nature, it is important to make these networks secure against any threats to keep missions safe and secure [4]. It is evident that these missions require more sophisticated capabilities like detection, tracking, and identification. However, we anticipate that the security approaches and technologies used in satellite networks can be updated and extended to these missions.

To ensure the confidentiality of wireless communications, two approaches are generally used: upper-layer encryption and physical-layer security [5]. In terms of satellite network security, it is essential to not only preserve the security and authenticity of network components but also to secure communication sessions, data, and links between network elements. Furthermore, protecting the privacy of users, which encompasses their location and account details, is crucial.

A. Related Work

In the context of deep space communication, particularly in cislunar environments, there is a limited body of knowledge regarding establishing secure communication, specifically authentication schemes. To address this gap, we turn our attention to the authentication methodologies employed in satellite networks. Despite the different operational contexts, analyzing satellite network authentication provides valuable insights that can inform our understanding of potential strategies and pitfalls in cislunar authentication.

This exploration is particularly pertinent given the critical role of satellites in maintaining communication links with various points, including users and ground stations, throughout their deployment in space. Therefore, this diverse network of communication links necessitates robust authentication measures on these systems. By definition, authentication refers to the security measures put in place to ascertain the validity of transmissions, messages, and the eligibility of the source to access information [6], [7].

Nevertheless, authentication measures face numerous threats that can potentially circumvent or compromise access control, thereby granting unauthorized individuals the ability to carry out operations or access sensitive data [8]. Various types of attacks targeting authentication mechanisms can be identified, including brute force attacks, insufficient authentication, weak recovery procedures (as described by IBM [9]), and spoofing attacks.

A closer examination of recent incidents highlights the significant impact of brute-force attacks. While many of these occurrences go unreported [10], their nature involves stealthily seeking entry into systems, often remaining undetected until it's too late. The Viasat satellite company encountered such an attack, accusing Russia of employing brute force tactics against modems and routers [11]. Similarly, the Thales team conducted an ethical hack, showcasing the exploitation of standard privileges to assert control over the application layer [12]. Past incidents underscore the vulnerability of satellite systems, as seen in the 2007 and 2008 hacking of two US government Earth satellites, where the attackers gained access but refrained from issuing commands [13].

Similarly, spoofing attacks represent another significant threat, aiming to deceive systems into granting unauthorized access. These attacks take various forms, from directing false signals towards the victim receiver [14] to more sophisticated strategies that replicate physical signal characteristics [15]. Recognizing the severity of these threats, numerous defense mechanisms against spoofing attacks have been proposed. One such proposal involves the development of a comprehensive spoofing framework deployed at both the transmitting and receiving ends [16]. Additionally, a detailed exploration of anti-spoofing techniques is presented in [17]. This not only enhances the security posture against spoofing attacks but also enables individuals to accurately ascertain their location in the presence of potential attackers.

Moreover, insufficient authentication poses a critical risk, inherently tied to the methods in use. Contemporary strategies incorporate digital signatures into authentication processes [18], [19], seamlessly integrating them into challenge-response and zero-knowledge authentication protocols to ensure robust security. However, the implementation of digital signatures brings accompanying risks, especially regarding key management [20] and the potential exposure of private keys. This vulnerability ultimately leads to unauthorized access.

To address these challenges, novel approaches propose elevating satellite security through location-based authentication. One method, detailed in [19], introduces a framework tying authentication to the satellite's location, addressing challenges related to link disconnection by enabling location key updates. Another approach, as presented in [21], explores the fusion of satellite orbit details with observable Time Difference of Arrival (TDOA)-based signatures for authentication.

B. Motivations and Contributions

Inspired by the research gap in the security authentication mechanism for satellite networks in deep space, in this paper, we introduce a location-based authentication scheme tailored for a cislunar system. The main contributions of this work are summarized as follows:

- We present a hypothetical attack scenario envisioning an attacker with the capability to assume any location within a confined sphere between the Earth and the Moon.
- We propose the integration of distance verification as a pivotal component within our authentication framework by leveraging time variant error thresholds to ensure the accuracy and security of communication links.
- We conduct comprehensive Monte Carlo simulations under noisy assumptions to assess the robustness and performance of the proposed authentication scheme in varying lunar communication scenarios.

C. Paper Organization

The subsequent sections of the paper are structured as follows. In Section II, we introduce our proposed system model along with the parameters considered. Section III outlines the proposed approach. Section IV depicts the scenario under consideration. In Section V numerical results are presented and discussed. Finally, we conclude and highlight open issues in Section VI.

II. System Model

In our dynamic Cislunar space model, the Moon around which the two different satellites orbit in elliptical southern near rectilinear orbit (NRO) and low lunar orbit (LLO) [1] revolves around the Earth, on which three deep space network stations (DSNSs) in California, Madrid, and Canberra [22] rotate as a function of time, as presented in Fig. 1. Three DSNS locations [23] on the Earth-centered Earth-fixed (ECEF) reference frame [24] rotate along with the Earth as a function of time and enable continuous communication between the Earth and satellites over the lunar orbits. Meanwhile, the attacker is positioned randomly in the vicinity of the midpoint between the Earth centroid and the moving or changing lunar centroid as a function of time as well.

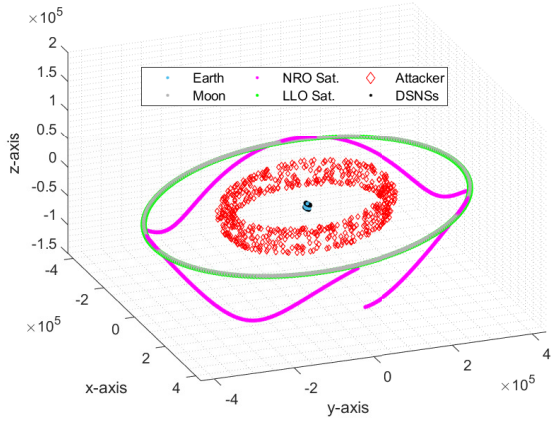

Fig. 1. Cislunar space communication model at different time intervals.

TABLE I
TEMPORAL EARTH-MOON SYSTEM MODEL PARAMETERS

Temporal Parameters	Values
Earth's rotation	1 day [25]
Moon's rotation	27 days [26]
Moon's revolution	27 days [26]
Near Rectilinear Orbit (NRO) period	8 days [1]
Low Lunar Orbit (LLO) period	2 hours [1]
Total simulation time	648 hours
Sampling time	1 hour
Angular velocity of Earth	15°/hour [25]
Angular velocity of Moon	0.56°/hour [26]

A single revolution of the Moon around the Earth, as well as a rotation, takes approximately 27 Earth days since it is tidally locked to the Earth [26], as presented in Table I[1].

[1]Rotations, lunar revolution, period of lunar orbits, simulation times, and angular velocities of the celestial bodies are defined in Table I.

TABLE II
GEOMETRIC EARTH-MOON SYSTEM MODEL PARAMETERS

Geometric Parameters	Values
Earth radius	6,371 km [28]
Moon radius	1,737.4 km [28]
Lunar orbit radius (Average distance between the centers of the Earth and Moon)	385,000 km [26]
Elliptic Near Rectilinear Orbit (NRO) with perilune	2,000 km [1]
Elliptic Near Rectilinear Orbit (NRO) with apolune	75,000 km [1]
Circular Low Lunar Orbit (LLO) with perilune/apolune	100 km [1]
Earth obliquity (to Ecliptic plane)	23.44° [27]
Lunar obliquity (to Lunar plane)	6.68° [27]
Lunar obliquity to Ecliptic plane	1.54° [27]
Lunar orbital plane inclination to Ecliptic plane	5.14° [27]

The obliquity and inclination angles of the elements in our system model are considered as per the cislunar space model geometry presented in Fig. 2. The obliquity, or axial tilt, is the angle between a celestial body's rotational axis and an orbital axis perpendicular to the corresponding orbital plane. Therefore, Earth's obliquity is an angle between its rotational axis and the perpendicular axis of its orbital plane, which is the ecliptic plane. In contrast, lunar obliquity is the angle between the Moon's rotational axis and the perpendicular axis of the lunar plane, which is inclined to 5.14° from the ecliptic plane. However, the angle between the Moon's rotational axis and the axis perpendicular to the ecliptic plane is 1.54° therefore, the lunar obliquity can be computed as 6.68° [27] as shown in Fig. 2.

The geometric cislunar space model parameters and corresponding values are summarized in Table II. It can be inferred that the z-axes of the Earth-centered and Moon-

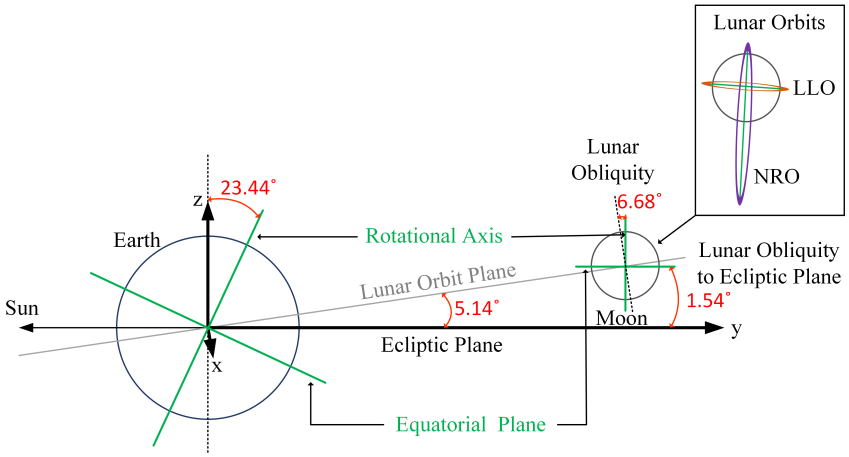

Fig. 2. Geometry of the Cislunar space model.

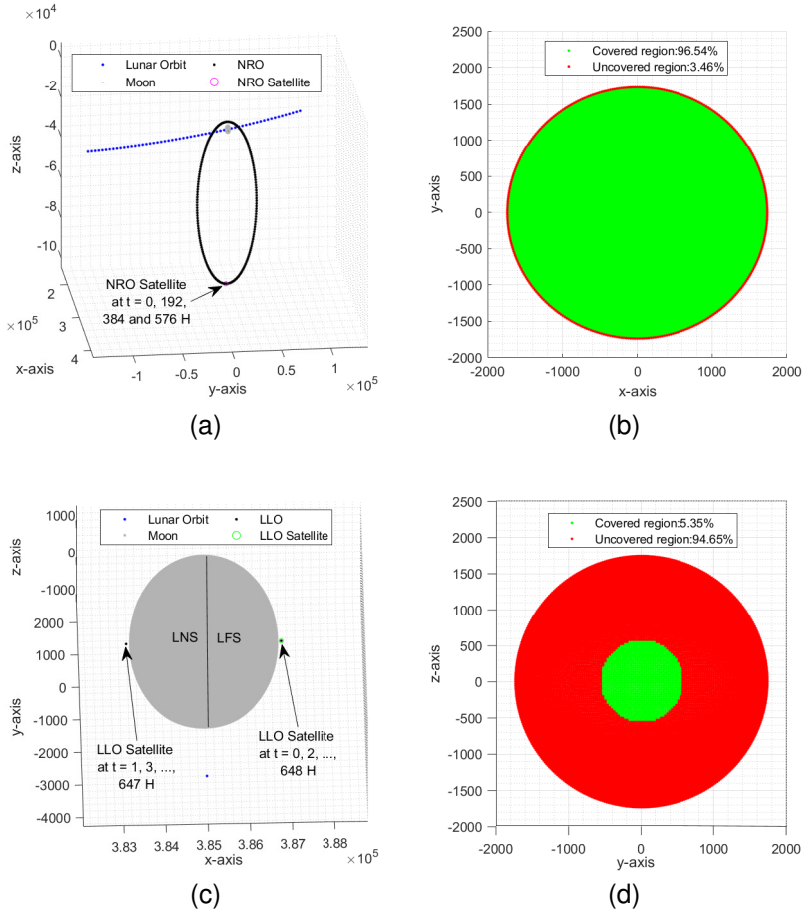

Fig. 3. Satellite locations and SCP values at $t = 0$ hour (a) NRO satellite location, (b) LSH SCP, (c) LLO satellite location, (d) LFS SCP, which is the same for lunar near side (LNS) SCP at odd hours such as $t = 1$ hour

centered rotating reference frames (i.e., fixed frames [24]) coincide before the intrinsic rotations [29] about the x-axis (i.e., $23.44°$ and $1.54°$ to the ecliptic plane) and the z-axis (i.e., $15°$/hour and $0.56°$/hour) are applied by using rotation matrices.

Since these two reference frames are rotating about their z-axes, as in ECEF [24], and their rotations take 24 hours and 648 hours, as shown in Table I, we can assume that our simulations start when the rotating x and y axes of these frames are aligned as well. In other words, when simulation time $t = 0$, only the translation transformation (i.e., movement) between the origin of these frames at each simulation time interval would be sufficient without the need for additional rotations for the alignment of all axes since rotation transformations for tilts and spins must be applied after the translation [30].

In our methodology, the affine transformations that are composed of rotation, translation, scaling, and shear are used. Note that affine transformations are not commutative; therefore, the correct order of the operations is crucial [30].

The direction cosine matrix (DCM), or rotation matrix $\mathbf{R}_{ab}$, enables coordinate transformations from reference frame b to reference frame a. A reference frame is defined as the three orthogonal unit vectors that follow the right-hand rule, and its origin $(0, 0, 0)$ is the point where these unit vectors, or coordinate axes, are crossed. The rotation transformation is linear and provides a rotation of the set of points around the origin of a given reference frame [30]. The rotation matrix $\mathbf{R}_{ab}$ is parameterized with a unit-axis vector $\mathbf{a}$ and an arbitrary angle ϕ by using the Rodrigues' formula [31].

The translation transformation that is used to move the origin of a reference frame, is a non-linear transform unlike the rotation thus, the homogeneous coordinates are used to overcome this problem [30].

Therefore, to rotate any surface point on the Moon, or any possible satellite location over a lunar orbit, about the Moon instead of the Earth, the translation transformation and intrinsic rotations (i.e., x-z') are used to determine the affine transformation matrix [29].

The surface coverage percentage (SCP) of the lunar far side (LFS) and lunar southern hemisphere (LSH) for LLO and NRO satellites, respectively, at $t = 0$ are determined [32]–[34], and presented in Fig. 3. It is assumed that there is no constraint on the orientational movement of the laser transmitter and hence the zero elevation angle, or maximum possible coverage, can be attained and the largest nadir angle and the central angle can be determined accordingly [32].

III. Proposed Approach

In this section, we present our dynamic approach to location-based authentication.

A. Distance Estimator System

Optical laser ranging offers a more precise and independent approach compared to traditional methods for positioning spacecraft in cislunar space. Advancements in laser ranging technology are closely tied to the development of fully autonomous orbit determination and synchronization systems, especially at key locations like the Lunar Gateway [35]. Expanding on these advancements, our distance estimator system can leverage laser ranging technology to accurately measure the distance between the Lunar Gateway and the relay satellite.

B. Distance Verification System

The verification of distances within our system is a critical component. We model the actual distance $d(t)$ between the Moon gateway and the relay as the sum of the estimated distance $d_{estimated}(t)$ and an estimation noise term $d_{noise}(t)$. This noise term represents the inherent uncertainties and disturbances present in the lunar communication environment, including thermal fluctuations, electromagnetic interference, and signal degradation over long distances.

1) Planned and estimated distances: Both planned and estimated distances are integral to verifying legitimacy. The planned distance $d_{planned}$ is defined as the intended secure communication distance between the Moon gateway and the relay. This mission-planned distance serves as a reference point for authentication. Concurrently, the estimated distance $d_{estimated}$ is obtained through the localization system, providing an estimate of the actual distance between the Moon gateway and the relay.

2) Time-dependent error threshold: To verify the legitimacy of the communication link, we assess the difference between the planned and estimated distances against a time-dependent error threshold $\eta(t)$. This is essential due to the dynamic nature of lunar orbits and evolving conditions during a mission.

3) Authentication decision criteria: Our final component outlines the decision criteria that determine the security of the communication link. Specifically:

- **Secure Connection Identification:** When the absolute difference is under the threshold, the authentication request falls within the designated authentication window, and the spacecraft's actual location aligns with the planned location, the connection is identified as potentially secure.

$$|d_{planned}(t) - d_{estimated}(t)| \leq \eta(t) \tag{1}$$

  - The authentication window is only open under this condition and when it aligns with mission requirements and orbital dynamics.
  - Location alignment ensures that the spacecraft is positioned within an acceptable deviation from the planned location during the authentication window.
- **Connection Refusal:** When the absolute difference exceeds the threshold, the authentication request occurs outside the designated authentication window, or the spacecraft's actual location deviates significantly from the planned location, the connection is refused due to potential security risks.

$$|d_{planned}(t) - d_{estimated}(t)| > \eta(t) \tag{2}$$

  - If the authentication request occurs outside the designated window, it suggests a deviation from the planned temporal synchronization. Connection refusal under this criterion helps mitigate potential threats during non-designated time periods.
  - If the spacecraft's actual location deviates significantly from the planned location, it indicates a potential security risk.

IV. Proposed Scenario

We investigate a scenario that specifically addresses the authentication process, aiming to differentiate between legitimate entities and potential malicious actors seeking entry into the communication network. In this context, we introduce a potential threat posed by an on-orbit attacker strategically positioned near the midpoint between the Earth centroid and the dynamically changing lunar centroid. This threat exhibits two distinctive modes of operation:

A. Continuous Orbit Following

In this mode, the attacker skillfully imitates a perpetual orbit around the moon, constantly tracking the communications gateway. This continuous orbit emulation reflects long-term attacks with subtle techniques.

B. Dynamic Positioning Within Orbit

Contrastingly, an attacker can possess the capability to dynamically position itself anywhere within the centroid. The dynamic nature of this mode introduces an element of unpredictability.

In both cases, the scenario illustrates the range of attacks that pose significant risks to the authentication process. These attacks can be exemplified by man-in-the-middle attacks, where the attacker intercepts and manipulates authentication messages; replay attacks involving the reuse of captured authentication data; and credential spoofing, where the attacker attempts to forge or mimic valid credentials.

Importantly, these threats are versatile and can be adapted to either mode of attack. For instance, in continuous orbit following, the attacker might employ persistent man-in-the-middle tactics, gradually increasing the intensity of interference over time. Similarly, replay attacks can be prolonged and carefully timed to align with the continuous tracking of communication. On the other hand, in dynamic positioning within the orbit, the agility of the attacker allows for quick, short-term execution

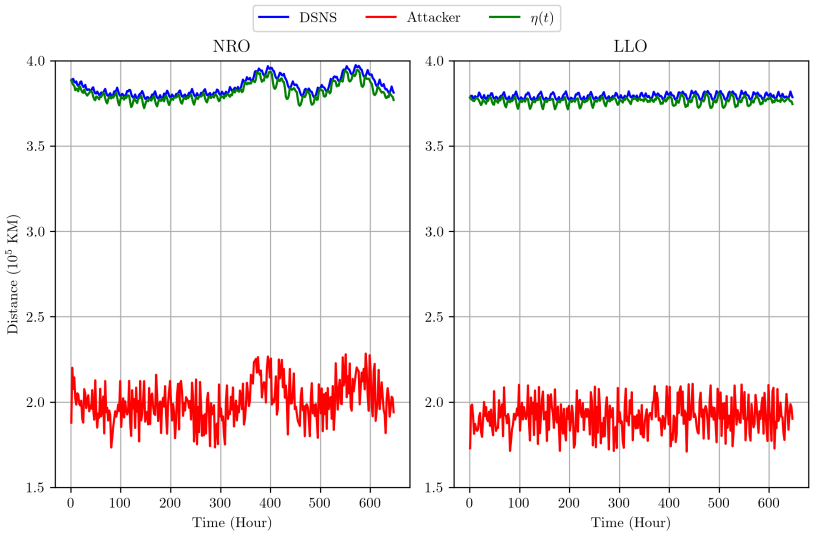

Fig. 4. Time-varying distance to LLO and NRO satellite at LNS comparison between DSNS and attacker with time-varying threshold

of man-in-the-middle attacks or opportunistic replay attacks, taking advantage of specific positions within the lunar orbit.

V. Results and Discussion

In this section, we present our numerical results, shedding light on various aspects of our proposed authentication framework. Initially, we explore the time-varying distances between the satellites to NRO and LLO (Fig. 4), drawing comparisons between the DSNS and attacker.

The signals from the attacker exhibit an intriguing ability to closely mimic the shape of DSNS signals, with notable instances at $t = 300\ h$ and $t = 600\ h$. We also make the observation of the significance of amplitude as a discriminative feature, as evidenced by the consistent pattern of lower amplitude and increased noise in the attacker's signal.

To distinguish between the signals of the attacker and DSNS, a time-varying threshold is applied in Fig. 4. The selection of the threshold involves a dynamic approach, considering a local window of data points around each specific moment in time. This adaptive strategy ensures that the threshold aligns finely with the characteristics of the signal at the planned distance, with our current implementation maintaining a fixed window.

Now, focusing deliberately on the estimation noise, we introduce a uniform distribution across the system (Fig. 5), maintaining different noise levels in NRO and LLO orbits. To

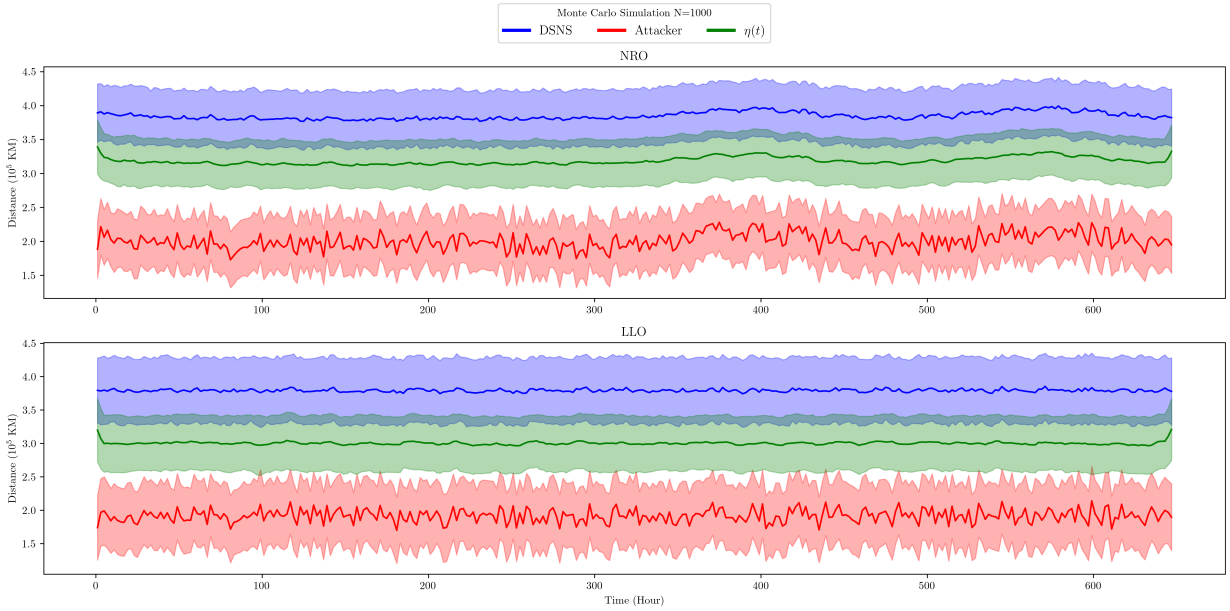

Fig. 5. Monte Carlo simulation results: varying distance of NRO and LLO

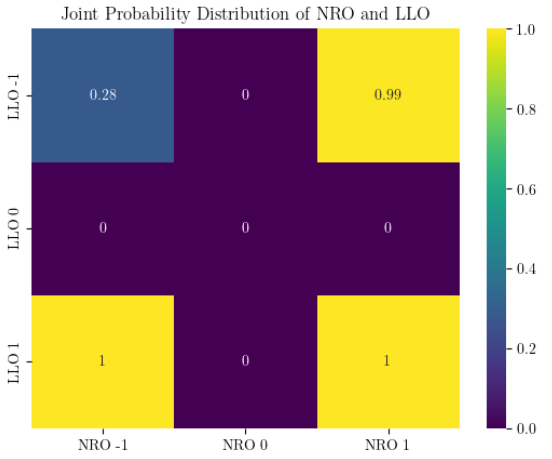

Fig. 6. Joint probability distribution of NRO and LLO

assess the robustness under total noise, we conducted Monte Carlo simulations over 1000 frames. We include plots of the standard variation and mean of the signal over the simulation, applying these features to the threshold variation and both estimates of the distances.

Subsequently, we perform probability calculations to evaluate threshold performance. A successful threshold (1) isolates the attacker from DSNS while remaining closer to the DSNS signal. A failure (0) occurs if requests from the attacker are allowed, and (-1) indicates either a miss on both or allowing both.

Our results, presented in Fig. 6, indicate over 90% success for both NRO and LLO, underscoring the effectiveness of our proposed framework in distinguishing between DSNS and an attacker. In detail, for NRO, a 97% success rate indicates that our system accurately identifies and authorizes only DSNS signals (1), with no instances of permitting the attacker (0). The system demonstrates a high level of effectiveness 2.01% in scenarios where neither signals nor both signals are permitted (-1). Similarly, in the LLO scenario, a success rate of 95.17% showcases the precision in recognizing and permitting only DSNS signals, while attacker signals are consistently refused (0). A minimal occurrence of 4.83% of permitting neither signals nor both signals (-1) emphasizes the framework's selectivity and accuracy.

Lastly, we investigate the impact of the fixed window on the determination of the threshold algorithm, as can be seen in Fig. 7. Running Monte Carlo simulations with varying window sizes, we evaluate system performance.

For a window size of 1, the system achieves a perfect success rate, indicating optimal adaptability to dynamic authentication scenarios. In contrast, as the window size increases, such as with a window size of 5, we witness a slight degradation in performance. The success rate drops marginally, and a minimal occurrence of -1 indicates instances where neither signal nor both signals are permitted.

Further increasing the window size over 8 and beyond exacerbates this degradation (especially for LLO), as evi-

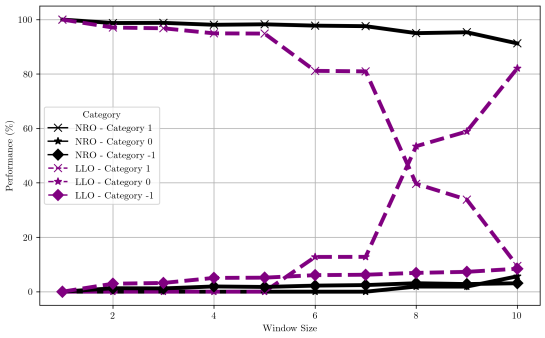

Fig. 7. Performance scores with varying window size (NRO and LLO)

denced by the decline in success rates. The threshold, persisting over larger windows, results in reduced adaptability to changing conditions and a potential increase in false positives or negatives. The degradation in performance highlights the importance of dynamically adjusting the authentication window, ensuring it aligns closely with mission requirements and orbital dynamics. Future optimizations may involve developing adaptive windowing strategies to enhance the system's resilience and adaptability in varying lunar communication conditions.

Building upon the assessment of the authentication system's performance under varying window sizes, it is crucial to relate these findings to the system's robustness against the attack scenarios we set.

Despite the window size's impact on system performance, our results indicate that the authentication framework maintains robustness in distinguishing between the DSNS signal and an attacker, achieving success rates exceeding 90% at a window size $\leq$ 10. In the continuous orbit following the scenario, the high success rates underscore the system's adaptability to long-term, subtle attack techniques. The continuous nature of the attack does not significantly impede the authentication process.

Similarly, in the dynamic positioning within orbit scenario, where the attacker dynamically moves within the centroid, the success rates remain consistently high. This emphasizes the framework's effectiveness in handling dynamic and unpredictable attacker movements.

VI. Conclusion

In conclusion, our location-based authentication framework addresses lunar communication security comprehensively. Integrating distance verification and adaptive decision criteria, we establish an authentication framework system for cislunar missions. Monte Carlo simulation validates its effectiveness under diverse lunar conditions. As lunar missions rise, ensuring data confidentiality is crucial. Future work involves the formal integration of monitoring and alert systems, enhancing adaptability. This evolution promises early threat detection, reinforcing reliability amid evolving security concerns in space missions.

A significant concern arises with the potential presence of highly intelligent space robots that could mimic legitimate devices. If such an advanced robotic attacker exists, capable of changing its location and even positioning itself above authentic equipment, it could pose a serious security challenge. It would be difficult to distinguish between legitimate signals and those from the attacker, making it a critical issue that needs to be addressed to ensure the integrity and reliability of these missions.

REFERENCES

[1] R. Whitley and R. Martinez, "Options for staging orbits in cislunar space," in *IEEE Aerospace Conference*, 2016, pp. 1–9.

[2] L. R. Gaddis, K. H. Joy, B. J. Bussey, J. D. Carpenter, I. A. Crawford, R. C. Elphic, J. S. Halekas, S. J. Lawrence, and L. Xiao, "Recent exploration of the Moon: Science from lunar missions since 2006," *Reviews in Mineralogy and Geochemistry*, vol. 89, no. 1, pp. 1–51, 2023.

[3] "Chandrayaan 3 - NSSDCA/COSPAR ID: 2023-098A," https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=2023-098A, 2023, accessed: 2024-02-06.

[4] S. G. Cetin, G. Karabulut Kurt, and A. Vazquez-Castro, "Secure and robust communications for cislunar space networks," *International Communications Satellite Systems Conference (ICSSC)*, 2023. [Online]. Available: https://arxiv.org/abs/2310.09835

[5] W. U. Khan, A. Mahmood, C. K. Sheemar, E. Lagunas, S. Chatzinotas, and B. Ottersten, "Reconfigurable intelligent surfaces for 6G non-terrestrial networks: Assisting connectivity from the sky," *IEEE Internet of Things Magazine*, vol. 7, no. 1, pp. 34–39, 2024.

[6] Committee on National Security Systems, "CNSSI 4009-2015 from CNSSI 4005," National Security Agency/Central Security Service, Tech. Rep., 2015.

[7] National Security Agency/Central Security Service, "NSA/CSS Manual Number 3-16 (COMSEC)," National Security Agency/Central Security Service, Tech. Rep., 2016.

[8] M. A. Amanullah *et al.*, "Deep learning and big data technologies for IoT security," *Computer Communications*, vol. 151, pp. 495–517, 2020.

[9] IBM Corporation, "Authentication Attacks - IBM Security Network Intrusion Prevention System - Version 4.6.2," https://www.ibm.com/docs/en/snips/4.6.2?topic=categories-authentication-attacks, 2021, accessed: 2024-04-19.

[10] D. Livingstone and P. Lewis, *Space, the Final Frontier for Cybersecurity?*. Chatham House. The Royal Institute of International Affairs, 2016.

[11] CyberPeace Institute, "Case Study: Viasat," https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat, 2022, accessed: 2024-04-19.

[12] Thales Group. (2022) Thales seizes control of esa demonstration satellite in first cybersecurity exercise of its kind. Accessed: 2024-04-19. [Online]. Available: https://www.thalesgroup.com/en/worldwide/security/press_release/thales-seizes-control-esa-demonstration-satellite-first

[13] US-China Economic and Security Review Commission, "2011 Report to Congress of the U.S.-China Economic and Security Review Commission," http://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf, Washington, DC, 2011, accessed: 2024-04-19.

[14] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, P. M. Kintner *et al.*, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, 2008, pp. 2314–2325.

[15] D. Wesson, D. Shepard, and T. Humphreys, "Straight talk on anti-spoofing," *GPS World*, vol. 23, no. 1, pp. 32–39, 2012.

[16] L. Crosara, F. Ardizzon, S. Tomasin, and N. Laurenti, "On the optimal spoofing attack and countermeasure in satellite navigation systems," 2023.

[17] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, pp. 1–16, 2012.

[18] M. Yuan, X. Tang, and G. Ou, "Authenticating GNSS civilian signals: A survey," *Satellite Navigation*, vol. 4, no. 1, p. 6, 2023.

[19] Y. Yang, J. Cao, X. Ren, B. Niu, Y. Zhang, and H. Li, "LK-AKA: A lightweight location key-based authentication and key agreement protocol for S2S communication," *Computer Communications*, vol. 197, pp. 214–229, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366422004169

[20] R. Singh, I. Ahmad, and J. Huusko, "The role of physical layer security in satellite-based networks," in *Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2023, pp. 36–41.

[21] E. Jedermann, M. Strohmeier, M. Schäfer, J. Schmitt, and V. Lenders, "Orbit-based authentication using TDOA signatures in satellite networks," in *ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2021, pp. 175–180.

[22] "What is the Deep Space Network? - NASA," Mar. 2020. [Online]. Available: https://www.nasa.gov/directorates/somd/space-communications-navigation-program/what-is-the-deep-space-network/

[23] S. D. Slobin, "Coverage and Geometry," *DSN No. 810*, vol. 5, pp. 810–005, 2014.

[24] J. Farrell, *Aided navigation: GPS with high rate sensors*. McGraw-Hill, Inc., 2008.

[25] "Chapter 2: Reference Systems - NASA Science." [Online]. Available: https://science.nasa.gov/learn/basics-of-space-flight/chapter2-1/

[26] "Moon Facts - NASA Science." [Online]. Available: https://science.nasa.gov/moon/facts/

[27] C. Olthoff, D. Kaschubek, and M. Killian, "Dynamic thermal interactions between spacesuits and lunar regolith in permanently shaded regions on the moon," *Acta Astronautica*, vol. 203, pp. 351–369, 2023.

[28] "Moon Fact Sheet." [Online]. Available: https://nssdc.gsfc.nasa.gov/planetary/factsheet/moonfact.html

[29] R. P. Paul, *Robot manipulators: Mathematics, programming, and control: The computer control of robot manipulators*. Richard Paul, 1981.

[30] D. House and J. C. Keyser, *Foundations of physically based modeling and animation*. CRC Press, 2016.

[31] O. Rodrigues, "Des lois géométriques qui régissent les déplacements d'un système solide dans l'espace, et de la variation des coordonnées provenant de ces déplacements considérés indépendamment des causes qui peuvent les produire," *Journal de Mathématiques Pures et Appliquées*, vol. 5, pp. 380–440, 1840.

[32] S. Cakaj, *LEO Coverage*, 2023, pp. 103–119.

[33] Z. Song, G. Dai, M. Wang, and X. Chen, "A novel grid point approach for efficiently solving the constellation-to-ground regional coverage problem," *IEEE Access*, vol. 6, pp. 44 445–44 458, 2018.

[34] Z.-Y. Gao and X.-Y. Hou, "Coverage analysis of lunar communication/navigation constellations based on halo orbits and distant retrograde orbits," *The Journal of Navigation*, vol. 73, no. 4, pp. 932–952, 2020.

[35] G. Sirbu and M. Leonardi, "Fully autonomous orbit determination and synchronization for satellite navigation and communication systems in halo orbits," *Remote Sensing*, vol. 15, no. 5, 2023.