2024 IEEE 29th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) | 979-8-3503-7764-4/24/$31.00 ©2024 IEEE | DOI: 10.1109/CAMAD62243.2024.10942990

Blockchain-Enhanced Security for LEO Satellite Firmware Updates in Beyond-5G NTN Networks

Yonatan M. Worku *, Petro M. Tshakwanda†, Henok B. Tsegaye‡, Christos Christodoulou§, Michael Devetsikiotis¶, Claudio Sacchi‖
*†§¶‖Department of Electrical and Computer Engineering, University of New Mexico, USA
‡‖Department of Information Engineering and Computer Science, University of Trento, Italy
{*yonatanmelese61, †pmushidi, §christos, ¶mdevets}@unm.edu, {‡henokberhanu.tsegaye, ‖claudio.sacchi}@unitn.it,
‖claudio.sacchi.unm@outlook.com

***Abstract*—The integration of terrestrial and Non-Terrestrial Networks (NTNs) represents a significant advancement in communication technology in the framework of the ongoing beyond-5G standardization process. This integration offers broader coverage, especially in remote and underserved areas, and improved reliability through diversified network paths. Additionally, it paves the way for new services and applications that benefit from ubiquitous connectivity. To achieve enhanced Quality of Service (QoS) and Service Level Agreements (SLAs), the end-to-end network should be open and visible to service providers and users. However, such a clear-mode approach introduces various security threats, making the network susceptible to unauthorized access and service disruption. To address these challenges, a blockchain-based satellite firmware update strategy across terrestrial 5G core and access networks is proposed. This study explores the tradeoff between throughput and QoS in the 5G NTN network when blockchain is implemented. Our experimental setup involved a network of Low Earth Orbit (LEO) satellites integrated with a 5G core, deploying a blockchain-based authentication mechanisms to secure satellite communications. The results show a tangible improvement in authentication efficiency, despite a throughput degradation of around 10% and a latency increase of 17% from the baseline values obtained without blockchain security. This tradeoff highlights the cost of enhanced security countermeasures in terms of network performance. Nonetheless, the security benefits, measured through successful authentication attempts, fully justify blockchain integration in scenarios where security is paramount. The proposed approach promises to secure communications in "5G and beyond" NTN hybrid environments by ensuring integrity and confidentiality to the traffic flows.**

***Index Terms*—Blockchain, NTN, 6G, Security, QoS, Throughput.**

I. Introduction

The proliferation of 5G technology promises to change the communication network paradigms thanks to its unparalleled speed, reliability, and connection capabilities. Integrating 5G with Non-Terrestrial Networks (NTN), particularly Low Earth Orbit (LEO) satellites, can considerably extend coverage to remote and underserved regions. LEO satellite constellations have significantly empowered global communication networks, enabling enhanced data exchange and connectivity across various actors. Companies like SpaceX and OneWeb are leading this revolution, launching thousands of satellites to create mega-constellations capable of providing high-speed Internet [1].

Integrating LEO satellites within 5G infrastructures targets ubiquitous coverage and enhanced connectivity. Nonetheless, the dynamic nature of satellite networks and the long distances involved raise significant security concerns, such as unauthorized access and data breaches [2].

Traditional centralized security mechanisms often fail to address these challenges, thus necessitating innovative solutions. Blockchain technology, with its decentralized and immutable characteristics, represents a viable approach to enhance security in 5G NTN. Utilizing blockchain in LEO satellite networks presents its own set of challenges. Issues such as latency, computational overhead, and network throughput require careful consideration. The trade-off between the blockchain security gain and the Quality of Service (QoS) should be evaluated to assess its viability [3], [4].

This work discusses the implementation of a blockchain-based authentication mechanism to enhance the security of data exchanges and remote firmware updates in LEO satellite constellations in 5G NTN networks. Firmware updates are crucial for maintaining satellite functionality and performance. Blockchain can provide a trustworthy framework for updating satellite firmware, protecting the network from potential vulnerabilities introduced during the update operations [5], [6].

The proposed setup will demonstrate effective traffic control across the satellite network and will ensure secure transactions between the local blockchain network and the 5G NTN. Such a setup relies on the immutable nature of blockchain, which enhances the security and the integrity of the network.

The paper is organized as follows: Section II discusses some existing literature contributions by emphasizing the motivation of the proposed methodology. Section III describes the implementation of blockchain in 5G NTN networks, considering a secure firmware update application. Section IV is concerned with the proposed network architecture and methodology. Section V discusses the experimental setup showing the implementation procedures of the end-to-end blockchain-based NTN emulated network. Section VI focuses on the discussion of emulation results. Finally, Section VII draws the paper's conclusion and highlights some future research directions that may be addressed.

979-8-3503-7764-4/24/$31.00 ©2024 IEEE

Authorized licensed use limited to: New Mexico State University. Downloaded on July 18,2025 at 00:22:03 UTC from IEEE Xplore. Restrictions apply.

II. Related Work

The integration of blockchain technology with 5G and satellite networks has raised significant attention in recent years. Several studies have explored various aspects of this integration, highlighting its potential benefits and challenges. [7] conducted a comprehensive survey on the application of blockchain in "5G and beyond" networks [8], emphasizing the enhanced security and trust given to the network operations. This work provides a foundational understanding of how blockchain can mitigate security threats in these advanced communication networks.

In the satellite communications context, the study of [9] outlines challenges and potential solutions for integrating blockchain in the space industry. The paper discusses the role of blockchain in ensuring secure and reliable communication through satellite networks by addressing issues such as data integrity and authentication. Similarly, [10] explores blockchain-empowered space-air-ground integrated networks, presenting solutions for seamless and secure data transmission across different network layers.

The work in [11] proposes a blockchain-based framework for securing over-the-air firmware updates in IoT devices, which can be extended to satellite networks, to enhance security during data transmission and software updates. Another notable paper is [12], which focuses on blockchain-based authentication for 5G networks, regarded as crucial for maintaining secure connections and preventing unauthorized access in satellite communication systems.

In addition to these studies, [7] introduces a new framework, namely: MSNET-Blockchain, for securing mobile and satellite networks using blockchain. This framework addresses the unique security requirements of satellite networks and proposes solutions for achieving robust and scalable security mechanisms. Furthermore, [13] examines the mitigation of signaling storms in 5G networks using blockchain, highlighting the technology's potential to enhance network resilience and performance.

Our work builds on these foundational studies by implementing a blockchain-based traffic authentication system for a 5G NTN network in the cloud-native emulated environment. Unlike previous studies that primarily focus on theoretical frameworks and high-level solutions, the approach considered in this work involves the practical deployment and evaluation of blockchain technology in an end-to-end 5G NTN setup. More specifically the tradeoff between security (inherent to the utilization of blockchain) and achieved QoS is analyzed by providing empirical data on throughput, latency, and authorization efficiency of the local blockchain. This insight will contribute to the existing literature by demonstrating the impact of blockchain integration in 5G NTNs, along with its viability.

III. Blockchain-based 5G NTN networks

The distributed and decentralized nature of 5G and service-based architecture involve different security and privacy challenges. The contrast to security threats is becoming a pivotal research focus in academia and industry. Thanks to its decentralized nature, blockchain is considered a promising technology that is anticipated to be part of the future "5G and beyond" networking standards. 5G NTN networks are going to be open, virtualized, and scalable, which strengthens the necessity of adopting countermeasures to achieve a high level of end-to-end security and prevent inefficient centralized processing and decision. Such a security enforcement should pave the way to other network performance enhancement techniques, such as multi-access edge computing (MEC) and federated learning (FL) [7]. Moreover, the decentralized operation mode of blockchain has the advantage of deploying the network with transparent and immutable storage.

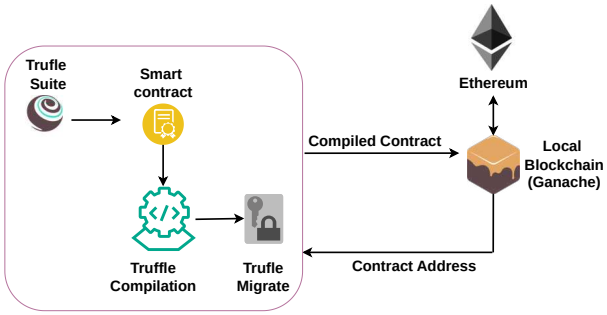

Fig. 1: Ethereum-based local blockchain

Blockchain technology offers several key properties that significantly strengthen its application in enhancing the security and reliability of satellite and 5G networks. The decentralized nature of blockchain eliminates the need for a central authority, thereby reducing single points of failure and enhancing resilience against attacks. The immutability of blockchain ensures that once data is recorded, it cannot be altered or tampered with, which is critical for maintaining data integrity and trust in communication networks. Additionally, blockchain's transparency and traceability enable real-time monitoring and auditing of network activities, ensuring that all transactions are verifiable and accountable. Finally, the use of smart contracts automates the enforcement of security policies and protocols, reducing human error and enhancing operational efficiency.

A. Ethereum-based local blockchain deployment

In this work, a private blockchain using Ethereum (Ganache) is implemented, which offers controlled access and higher transaction throughput as compared to public blockchains. This choice is particularly suited for the 5G NTN emulation, where the speed and security of transactions are paramount. The inherent properties of blockchain, such as decentralization, immutability, transparency, and automation through smart contracts, provide a robust foundation for securing the communication and authorization processes in our 5G NTN setup.

Fig. 1 shows the general working principle of the Ethereum local blockchain during the compilation of smart contracts.

The smart contract is written using solidity language and compiled using Truffle Suite IDE. After the smart contract is compiled, an Application Binary Interface (ABI) file and

Authorized licensed use limited to: New Mexico State University. Downloaded on July 18,2025 at 00:22:03 UTC from IEEE Xplore. Restrictions apply.

the bytecode are generated. After that, the smart contract will be deployed to the Ethereum Virtual Machine (EVM) and a contract address will be provided to the interacting applications. The ABI file is then used as an interface between the applications that interact with the blockchain.

B. Satellite firmware update strategy

Efficient strategies for LEO satellite firmware updates are vital for ensuring satellite constellations' operational efficiency and security. Different strategies are employed for LEO satellite firmware updates, such as the utilization of over-the-air (OTA) updates for IoT devices, which leverage the high-speed and low-latency capabilities of 5G networks to transmit firmware updates directly to satellites [11]. This method allows for rapid and efficient deployment of updates. However, it exhibits some significant security vulnerabilities, when the traffic flows from the 5G core network to the satellite requesting update by redirecting data to the wrong (malicious) network server as shown in Fig. 2.

IV. Network Architecture and Methodology

The emulated network setup for the secure end-to-end 5G NTN leverages blockchain technology to enhance security across satellite networks. As shown in Figs. 2 and 3 the network is comprised of a 5G core network, radio access network, satellite network, local blockchain node, and middleware. The core network is emulated using Free5GC [14] which is an open-source decentralized core network set compliant with 3GPP release 15. The radio access network is simulated using UERANSIM [15] which encompasses the gNB and the user equipment.

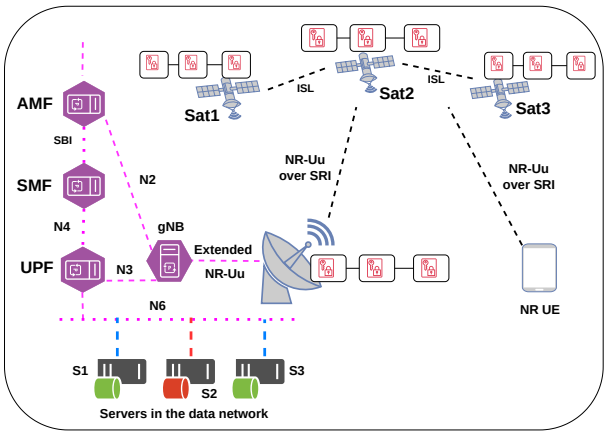

Fig. 2: Proposed Blockchain based 5G NTN

The access network (gNB) is considered to be located in the terrestrial segment. This last is connected to the satellite gateway to extend 5G services via the LEO satellite constellation to a remote UE. This means that the satellite is considered to work as a transparent node connecting the terrestrial gNB with the destination UE.

The satellite network is emulated using Opensand [16] emulator and it consists of three separate components: gateway, satellite, and terminal. The gateway is connected to the terrestrial gNB to extend the 5G network services over the satellite radio interface (SRI) [17].

Ethereum's local blockchain environment (Ganache) [18], is used as a local blockchain network to host the smart contact and interact with the 5G NTN network for securing transactions between the 5G data plane network and the satellite network. The interaction between the 5G NTN network and the Ethereum node is realized using the Flask Web micro-framework, which is employed as a middleware.

V. Experimental Setup

The principle behind the integration of the Ganache blockchain into the 5G NTN revolves around leveraging the blockchain's decentralized and immutable nature to enhance satellite network security. Ganache is a local Ethereum blockchain environment which used to test and deploy smart contracts that manage and authorize servers from the 5G data network (see Fig. 3). The strategy involves to use smart contracts to control the access to the satellite network by verifying data plane servers, and ensuring that only authorized servers can be accessed to generate traffic through the satellite network components. This approach prevents unauthorized access and secures data integrity across the NTN.

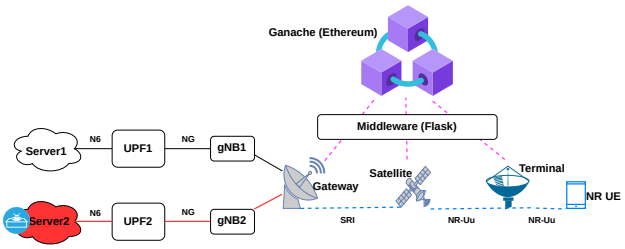

Fig. 3: Data plane authorization

All the network components are implemented in a docker-compose environment, properly configured, and sequentially triggered to achieve the proposed objective. The first setup step is to run the Ganache CLI environment as a docker container that listens at port 8545. Next, we develop and compile a smart contract defining the server authorization rules. This smart contract is then deployed to the Ganache by using the Truffle suite compiler. Every time a smart contract is compiled and deployed, an Application Binary Interface (ABI) file is generated. The ABI file allows external applications to interact with a deployed smart contract on the local blockchain across the middleware. The Ganache and middleware containers are properly networked to enable seamless communication between the deployed smart contract and the NTN components.

After the smart contract is deployed, the ABI file, contract address, and private key of the Ganache account address will be provided to the middleware. The middleware, implemented using Flask and Web3, is configured to interact with the smart contract as shown in Algorithm 1. The middleware will be initialized as a docker container and exposed to listen at port 5000 so that the satellite components will interact

Authorized licensed use limited to: New Mexico State University. Downloaded on July 18,2025 at 00:22:03 UTC from IEEE Xplore. Restrictions apply.

Algorithm 1 Deploy and Interact with Smart Contract

1: **Initialize** Ganache CLI `listens at port 8545`
2: **Compile** Smart contract `Authorization.sol`
3: **Deploy** `smart contract`
4: **Load** `contract ABI` into the middleware
5: **Configure** the contract address and private key to the middleware
6: **Start** middleware container `listens at port 5000`

with it at this port to access the smart contract. It allows for querying the authorization status of data network servers and updating the blockchain with the authorization changes.

Algorithm 2 Authorize Servers

1: **procedure** AUTHORIZE_SERVER(server_address)
2: **Connect** to Ganache via Middleware
3: **Build** transaction for `authorizeServer` function
4: **Sign** transaction with private key
5: **Send** transaction to Ganache
6: **Update** blockchain state
7: **end procedure**

Once the Ganache and the middleware start their communication, the NTN will be deployed and the satellite components (Gateway, Satellite, and Terminal) will start interacting with the blockchain to check whether the server from which the network is trying to access should be authorized or not as can be seen from Algorithms 2 and 3.

Algorithm 3 Deauthorize Server

1: **procedure** DEAUTHORIZE_SERVER(server_address)
2: **Connect** to Ganache via Middleware
3: **Build** transaction for `deauthorizeServer` function
4: **Sign** transaction with private key
5: **Send** transaction to Ganache
6: **Update** blockchain state
7: **end procedure**

The configuration files of the gateway, satellite, and terminal will be updated in a way that enables communication with the middleware to check for authorization. These satellite components will sign transactions using the Ganache network's private key for integrity.

Algorithm 4 Check Authorization Status

1: **procedure** IS_AUTHORIZED(server_address)
2: **Query** blockchain for authorization status
3: **Return** authorization status
4: **end procedure**

As seen from Algorithm 4, an authorization status will be provided to the satellite network in boolean format, and the satellite network will accept or reject the incoming traffic depending on the provided authorization status. The complete code for this experiment can be found at https://github.com/HenokBerhanu/ntn-5g-bl.

VI. Result and Discussion

The emulated network setup showcases the integration of blockchain technology into 5G NTN to enhance the security of satellite network communication. The use of smart contracts for device authorization provides a robust mechanism to ensure that only legitimate traffic traverses the satellite network. This approach not only secures the communication channels but also demonstrates the potential of blockchain in managing complex 5G NTN architectures.

Fig. 4 shows the latency between terrestrial gNB and user equipment located in different geographical locations and connected using a LEO satellite network. VoIP traffic is generated from the 5G data network considering a maximum delay of 50 ms with 5% packet loss to simulate the distance of the LEO constellation. Initially, traffic is collected without utilizing the blockchain authentication setup for comparison. Then, a blockchain middleware service is triggered so the satellite components have to make transactions to the blockchain to check for authorization of incoming VoIP traffic. Considering the situation when the traffic is authorized to pass through the satellite network, a maximum delay of 18 ms is recorded between the terrestrial gNB and UE with a 5 ms deviation from the normal NTN traffic delay. This is due to the time required by the transaction of the satellite network to the blockchain to generate the authenticated traffic flow.

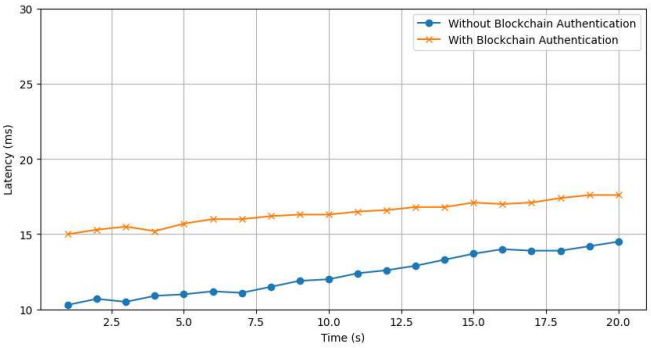

Fig. 4: Latency with and without blockchain authentication

Fig. 5 shows the throughput computed with and without utilization of blockchain authentication. The result shows that the throughput achieved during the traffic authentication process exhibits lower readings than those without blockchain authentication. This is because the traffic forwarding capacity of the NTN network will degrade when the satellite components interact with the local blockchain via the middleware. However, the primary goal of the blockchain approach is to ensure the security of the NTN network for critical tasks, like e.g. the satellite firmware update, rather than improving throughput performance.

Plots of Fig. 6 show the tradeoff related to the authorization attempts of multiple traffic flows coming from different servers versus network performance. As the number of traffic flows authorized to traverse across the satellite

Authorized licensed use limited to: New Mexico State University. Downloaded on July 18,2025 at 00:22:03 UTC from IEEE Xplore. Restrictions apply.

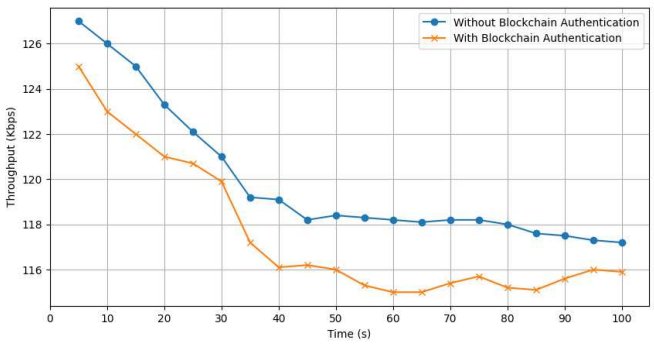

Fig. 5: Throughput with and without blockchain authentication

network increases the performance of the network tends to decrease, such as the throughput degrades and the latency between terrestrial gNB and the UE increases. This is due to the overhead imposed by the authentication process of the blockchain node. This suggests that while the network becomes more secure, it also becomes less efficient in terms of data handling capacity and speed. The authorization attempts can be expressed by the ratio of successful authorizations to the total number of authorization attempts $A_{Attempts}(\%)$ (both authorized and unauthorized traffic) as shown in eq. 1.

$$A_{Attempts}(\%) = \left(\frac{\text{Successful Authorizations}}{\text{Total Attempts}}\right) \times 100 \quad (1)$$

As can be seen from Fig. 6, a maximum throughput degradation $T_{Degradation}(\%)$ (see eq. 2) of 9.38% is exhibited with a maximum latency increase $L_{Increase}(\%)$ (see eq. 3) of 16.5% through the course of increasing the number of authorized traffic flows. For sake of clarity, T_{baseline} is the baseline VoIP throughput equal to 128 kbps and T_{current} is the current throughput (measured from the network). Similarly, L_{baseline} is the baseline latency (20 ms), and L_{current} is the current latency measured from the network.

$$T_{Degradation}(\%) = \left(\frac{T_{\text{baseline}} - T_{\text{current}}}{T_{\text{baseline}}}\right) \times 100 \quad (2)$$

$$L_{Increase}(\%) = \left(\frac{L_{\text{current}} - L_{\text{baseline}}}{L_{\text{baseline}}}\right) \times 100 \quad (3)$$

Fig. 7 shows the packet loss measured by launching the *iper3* command between the terrestrial user equipment and the gNB across the satellite network. The higher packet loss is recorded using Linux *tc* and *iptables* commands which impose a high probability of packet drop to mimic the distance of the LEO satellite from the earth's surface and the loss imposed by the satellite component interaction with the Ganache for traffic authorization. The simulation of 5G NTN with blockchain authentication exhibited more than 10% of packet loss as compared to the normal simulation without blockchain.

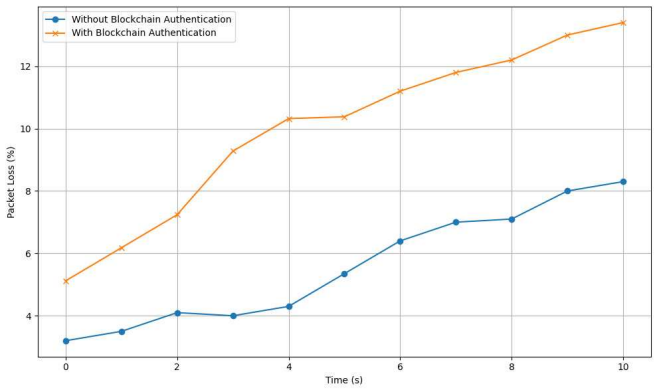

Fig. 7: Packet loss with and without blockchain authentication

VII. Conclusion and Future Works

In this work, a secure end-to-end 5G Non-Terrestrial Network (NTN) is developed and implemented using blockchain technology to enhance the security of the satellite network segment. By leveraging the capabilities of the Ethereum-based local blockchain (Ganache) and smart contracts, a robust and secure 5G NTN is developed, which ensures that only authorized traffic sources can transmit data across the satellite network, thus significantly enhancing the security and integrity of the satellite communication.

The experimental setup considered a network of Low Earth Orbit (LEO) satellites integrated with a 5G core and access network, where blockchain-based authorization mechanisms are deployed to secure inter-satellite communications. The results demonstrated a tangible improvement in the security of the NTN, albeit with a tradeoff in terms of slightly decreased network performance. Indeed, a throughput degradation ranging between 2.34% and 9.38% has been observed, while the measured latency increase ranged from 3% to 16.5%. These results highlight the price to be paid when we decide to implement enhanced security countermeasures. Despite these tradeoffs, the security gain, measured through successful authorization attempts, fully justifies blockchain integration in scenarios (like satellite firmware updating) where security is paramount. The study effectively demonstrates the feasibility of blockchain in enhancing security in 5G NTN environments, setting a foundational basis for future improvement and optimization.

Despite the promising results, there are areas for future research. Enhancements might focus on reducing the latency introduced by the blockchain verification process and improving the system's scalability to handle several network components using the multi-agent concept [19], [20]. Further research could also explore the integration of advanced security features and investigate the use of alternative platforms to optimize network performance.

VIII. Acknowledgements

The research activities presented in this paper fall within the field of interest of the IEEE AESS technical panel on Glue Technologies for Space Systems and IoT Lab of The

Authorized licensed use limited to: New Mexico State University. Downloaded on July 18,2025 at 00:22:03 UTC from IEEE Xplore. Restrictions apply.

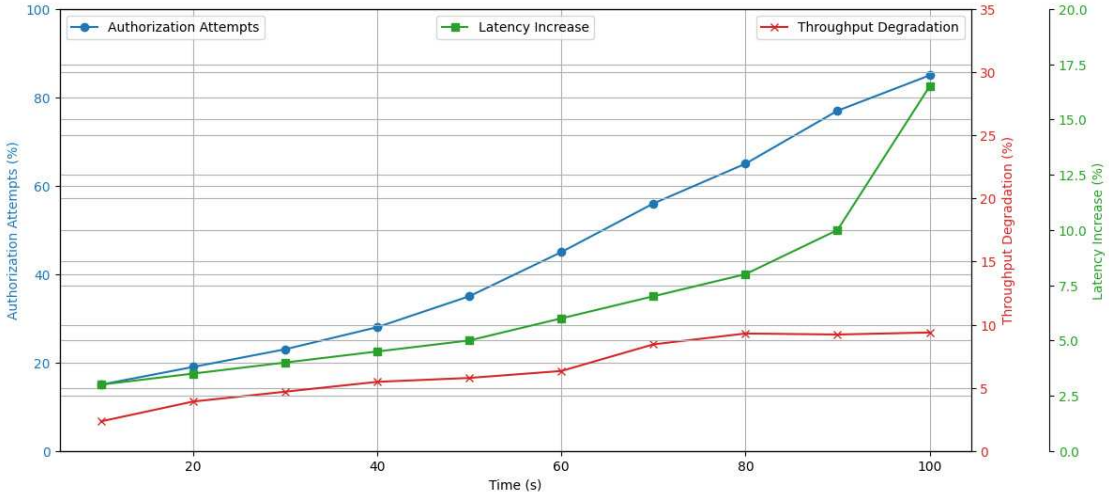

Fig. 6: Tradeoff between authorization attempts, throughput, and latency

University of New Mexico, Department of Electrical and Computer Engineering. This work was also supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU partnership on "Telecommunications of the Future" (PE00000001 – program "RESTART").

REFERENCES

[1] B. Al Homssi, A. Al-Hourani, K. Wang, P. Conder, S. Kandeepan, J. Choi, B. Allen, and B. Moores, "Next Generation Mega Satellite Networks for Access Equality: Opportunities, Challenges, and Performance," *IEEE Communications Magazine*, vol. 60, no. 4, pp. 18–24, 2022.

[2] P. Yue, J. An, J. Zhang, J. Ye, G. Pan, S. Wang, P. Xiao, and L. Hanzo, "Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1604–1652, 2023.

[3] Y. Wang, Z. Su, J. Ni, N. Zhang, and X. Shen, "Blockchain-Empowered Space-Air-Ground Integrated Networks: Opportunities, Challenges, and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 160–209, 2022.

[4] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, J. Querol, L. Lei, T. X. Vu, and G. Goussetis, "Satellite Communications in the New Space Era: A Survey and Future Challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 70–109, 2021.

[5] S. Fu, J. Gao, and L. Zhao, "Integrated Resource Management for Terrestrial-Satellite Systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 3256–3266, 2020.

[6] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[7] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *Journal of Network and Computer Applications*, vol. 166, p. 102693, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804520301673

[8] P. M. Tshakwanda, S. T. Arzo, and M. Devetsikiotis, "Advancing 6G Network Performance: AI/ML Framework for Proactive Management and Dynamic Optimal Routing," *IEEE Open Journal of the Computer Society*, vol. 5, pp. 303–314, 2024.

[9] M. Torky, T. Gaber, E. Goda, V. Snasel, and A. E. Hassanien, "A blockchain protocol for authenticating space communications between satellites constellations," *Aerospace*, vol. 9, no. 9, 2022. [Online]. Available: https://www.mdpi.com/2226-4310/9/9/495

[10] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38 437–38 450, 2018.

[11] X. He, S. Alqahtani, R. Gamble, and M. Papa, "Securing Over-The-Air IoT Firmware Updates using Blockchain," in *Proceedings of the International Conference on Omni-Layer Intelligent Systems*, ser. COINS '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 164–171. [Online]. Available: https://doi.org/10.1145/3312614.3312649

[12] Z. Haddad, M. M. Fouda, M. Mahmoud, and M. Abdallah, "Blockchain-based Authentication for 5G Networks," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 2020, pp. 189–194.

[13] B. Zhang, P. Zeinaty, N. Limam, and R. Boutaba, "Mitigating Signaling Storms in 5G with Blockchain-assisted 5GAKA," in *2023 19th International Conference on Network and Service Management (CNSM)*, 2023, pp. 1–9.

[14] Free5GC. (2024) Open source 5g core network base on 3gpp r15. Accessed on June 10, 2024. [Online]. Available: https://free5gc.org/

[15] A. Güngör. (2024) Open collective. Accessed on June 10, 2024. [Online]. Available: https://opencollective.com/UERANSIM

[16] T. A. space. (2024) Opensand satellite emulator. Accessed on June 10, 2024. [Online]. Available: https://www.opensand.org/

[17] H. B. Tsegaye and C. Sacchi, "MEC-based Experimental Framework for Service Availability in 3D Non-Terrestrial Networks," in *2024 IEEE Aerospace Conference*, 2024, pp. 1–10.

[18] T. suite. (2024) Ganache one-click blockchain. Accessed on June 18, 2024. [Online]. Available: https://archive.trufflesuite.com/ganache/

[19] S. T. Arzo, P. M. Tshakwanda, Y. M. Worku, H. Kumar, and M. Devetsikiotis, "Intelligent QoS Agent Design for QoS Monitoring and Provisioning in 6G Network," in *ICC 2023 - IEEE International Conference on Communications*, 2023, pp. 2364–2369.

[20] P. M. Tshakwanda, S. T. Arzo, and M. Devetsikiotis, "Multi-agent-based simulation of intelligent network system," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, 2023, pp. 0813–0819.

Authorized licensed use limited to: New Mexico State University. Downloaded on July 18,2025 at 00:22:03 UTC from IEEE Xplore. Restrictions apply.