Security Challenges in the Evolving Landscape of the Internet of Satellites (IoSat)

Sehajpreet Singh

104211068

Abstract—The advent of low-cost CubeSats has revolutionized the field of satellite communications, proposing the concept of an Internet of Satellites (IoSat). This network aims to enhance global connectivity and data-sharing capabilities. However, the unique operational environment of space presents significant security challenges. This report examines these challenges, focusing on the vulnerabilities introduced by long latencies, low bandwidths, limited signal power, and the harsh conditions of space.

I. Introduction

A. An Introduction to Satellite Communication Systems

Satellite communication systems utilize artificial satellites to establish communication links between different locations on Earth. This technology plays a crucial role in the global telecommunications network, with around 2,000 satellites transmitting analog and digital signals for voice, video, and data worldwide [1]. The system consists of two main components: the ground segment, which involves transmission, reception, and supporting equipment, and the space segment, which refers to the satellite itself. A typical satellite link involves transmitting a signal from an Earth station to a satellite, which then amplifies and retransmits it back to Earth for reception by Earth stations and terminals.

B. The Emergence of CubeSats

CubeSats, introduced in 1999, are a category of small, cost-effective satellites designed to democratize space science [2]. Unlike traditional satellites that are large and expensive, CubeSats adhere to a standardized size of 10 cm3 units. Their compact design has revolutionized the field by increasing accessibility to space, offering hands-on educational opportunities, and facilitating innovative and exploratory space research.

CubeSats have opened up opportunities for a wider range of users beyond government agencies and commercial industries, who have traditionally dominated satellite development and launch. These new users include universities, space agencies of smaller countries, citizen science groups, start-ups, hobbyists, and even artists [2]. CubeSats play a crucial role in expanding access to space exploration, which in turn leads to various benefits for both science and society.

C. IoSat: The Vision of a Connected Satellite Network

The field of Internet of Satellites (IoSat) is focused on developing a network model that allows satellites to communicate with each other using a peer-to-peer architecture [3]. This paradigm is a significant shift from traditional monolithic satellite systems, aiming to improve mission performance through collaborative efforts among satellites.

This new paradigm provides autonomy, flexibility, and scalability to develop FSS and other future autonomous satellite applications. The paradigm has been baptized as the Internet of Satellites (IoSat) because it is born from the concept of the Internet of Things (IoT), which promotes the interconnection of heterogeneous embedded devices using Internet technologies [4]. IoSat aims to sporadically interconnect different satellite systems, creating Inter-Satellite Networks (ISN), taking into consideration intermediate satellite states, goals, and dynamics.

D. Importance of Security in Satellite Networks

Security concerns are a critical aspect of IoSat research. With the increasing number of satellites and the complexity of networks, ensuring the security of satellite internet is paramount. Researchers analyze risks from national security, network security, and equipment security perspectives to ensure the healthy development of the satellite internet industry [5].

II. IoSat Architecture

The Internet of Satellites (IoSat) is an interconnected space paradigm that revolutionizes satellite communication through a peer-to-peer architecture. Unlike traditional approaches with a common backbone, IoSat enables autonomous satellite applications like Federated Satellite Services (FSS) by establishing temporal Inter-Satellite Networks (ISNs) based on demand [4].

ISNs are opportunistic networks created through the collaboration of intermediate nodes that forward data. They are composed of dynamic, sporadic, and opportunistic satellite networks which are temporally established depending on the required demand. These networks differ from traditional ones as they can be conceived as virtual satellite systems, representing an autonomous satellite application that deploys services through and for satellites [4].

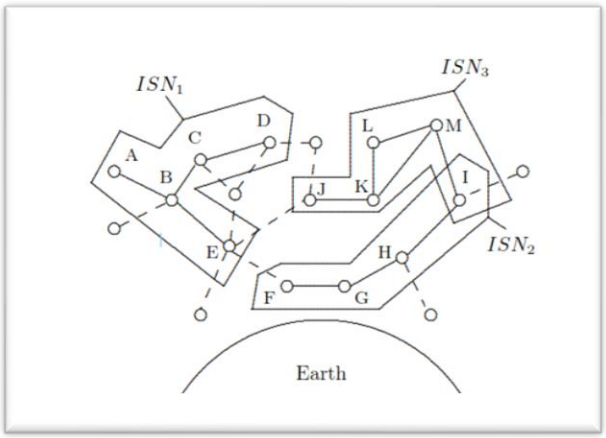

Fig.1 IoSat Space segment representation [4]

ISNs have three distinct phases:

1. Establishment Phase: During this phase, federations between intermediate nodes are negotiated. Members can decide not to accept the interaction based on their state or strategy interests. The probability that a proposed federation would be accepted or at least negotiated is analyzed. The ISN ensures that it can satisfy FSS requirements by providing the required services [4].

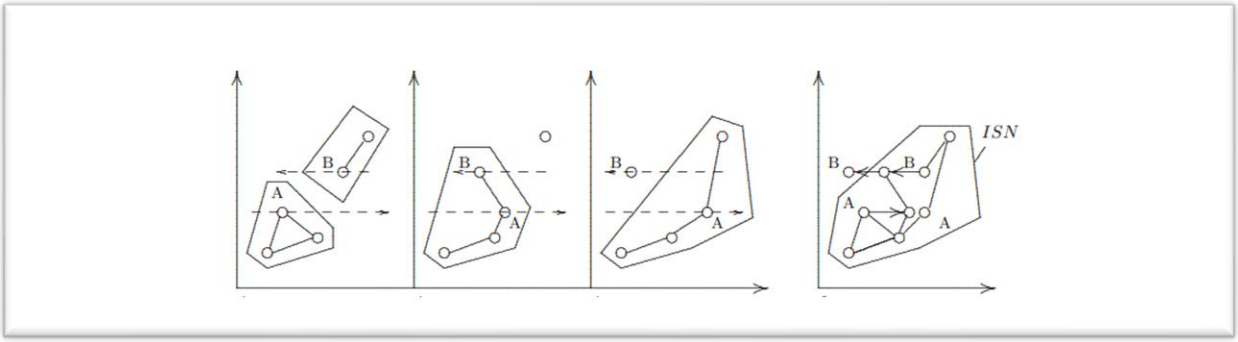

Fig. 2 Representation of the ISN Evolution [4]

2. Maintenance Phase: Once the ISN is established, this phase ensures that the network adapts to different events, such as

satellite movement and broken links. It updates network connections, replaces old intermediate nodes, and adds new ones as needed. The ISN can adhere to new satellite nodes upon request or to maintain topology stability. This phase also manages the evolution of ISN partitions over time as nodes move and establish new links [4].

3. Destruction Phase: When the ISN is no longer required, all participating nodes perform a destruction process, cleaning their internal state and recovering their usual activity. This phase is crucial for releasing resources that are no longer needed [4].

IoSat must be resource-aware and respect the severe limitations of satellites in terms of energy, computation, and data storage. Additional ISC capabilities could jeopardize the satellite's primary mission, as they are normally conceived to accomplish specific tasks. Satellites require intelligence to autonomously decide to leave the network if participation compromises their primary mission. Conventional solutions cannot implement this dynamic and constantly changing scenario [4].

To provide an overview, the physical layer represents the ensemble of all satellites in a region. A subset of these satellites agrees to participate in the network and provide the required services to deploy the FSS. They create an ISN with intermediate federations, forming a temporal network through which the end-to-end FSS is accomplished [4].

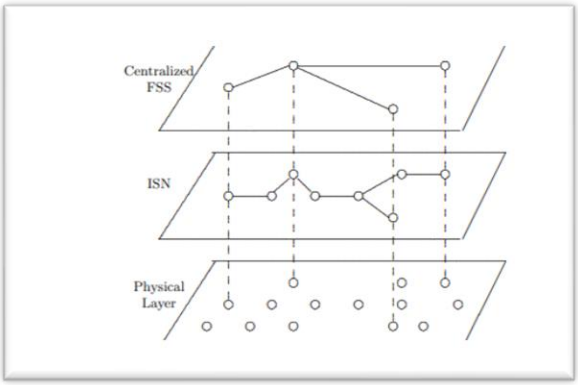

Fig. 3 Layered representation of a centralized FSS [4]

III. Operational Challenges in Space

The operational challenges in space are numerous and complex, encompassing both technical and environmental issues. Here's an overview of some of the key challenges:

A. Harsh Environmental Conditions

- Spacecraft are exposed to extreme temperatures, vacuum conditions, and radiation, all of which can degrade materials and electronics [6].

- Microgravity can affect fluid dynamics and mechanical systems differently than on Earth [6].

B. Radiation Damage

- Cosmic rays and solar radiation can cause single-event upsets, data corruption, and permanent damage to satellite components [6].

- Shielding and robust system design are necessary to mitigate these effects [6].

C. Orbital Debris

- Space debris poses a significant risk to operational satellites and human spaceflight [6].

- Tracking and avoiding debris requires sophisticated surveillance and manoeuvring capabilities [6].

D. Communication Latencies

- The vast distances in space result in communication delays, which can impact mission control and autonomous operations [6].

- This necessitates advanced onboard systems capable of independent decision-making [6].

E. Limited Resources

- Space missions must be planned with finite resources, including power, fuel, and onboard supplies [6].

- Efficient use and renewable sources, like solar energy, are critical for long-duration missions [6].

F. Maintenance and Repairs

- In-space maintenance and repairs are challenging due to the lack of direct human access and the need for specialized robotics [6].

- Developing self-healing materials and autonomous repair systems is an area of ongoing research [6].

G. Space Traffic Management

- The increasing number of satellites and space missions requires effective coordination to prevent collisions and interference [5].

- International regulations and agreements are essential for maintaining a safe space environment [5].

These challenges underscore the importance of continued innovation and international cooperation to ensure the sustainability and safety of space operations.

IV. Security Concerns in IoSat

A. Security Frameworks and Protocols Developed for IoSat

1) Quantum Key Distribution (QKD):

- Quantum Key Distribution (QKD) utilizes the principles of quantum mechanics, such as the Heisenberg uncertainty principle and the no-cloning theorem, to ensure the utmost security of cryptographic keys [7].

- By measuring quantum states, QKD enables the detection of any eavesdropping attempts, as any measurement disturbs the delicate quantum system [7].

- Notable implementations of QKD include the BB84 protocol, decoy-state protocol, and continuous-variable QKD [7].

2) Blockchain-based Security:

- Blockchain-based security leverages distributed ledger technology to establish an immutable and transparent record of transactions and data exchanges [8].

- In this system, each satellite functions as a node within the blockchain network,

validating and recording transactions through consensus mechanisms like Proof-of-Work (PoW) or Proof-of-Stake (PoS) [8].

- The utilization of smart contracts enables the automation of secure data sharing and access control policies, enhancing overall security [8].

3) Machine Learning for Anomaly Detection:

- Utilizes supervised, unsupervised, and semi-supervised learning algorithms to identify anomalous patterns and potential security threats [9].

- Techniques such as support vector machines (SVM), neural networks, and clustering algorithms are employed to analyze multidimensional data streams [9].

- Reinforcement learning can be used to adapt to evolving threats and optimize detection strategies [9].

4) Secure Software Development:

- Formal verification methods like model checking and theorem proving are utilized to mathematically analyze and prove the absence of vulnerabilities in satellite software.

- Secure coding guidelines and best practices are followed to write secure and resilient code for space systems.

- Techniques such as penetration testing, fuzz testing, and code reviews are employed to identify and fix security flaws in the software."

5) Byzantine Fault Tolerance (BFT):

- Enables the IoSat network to reach consensus and maintain correct operation even in the presence of malicious or faulty nodes [10].

- Algorithms like Practical Byzantine Fault Tolerance (PBFT) and Stellar Consensus Protocol (SCP) are employed to ensure agreement among honest nodes [10].

- Redundancy and diversity in satellite design and deployment contribute to the overall resilience of the IoSat network [10].

B. Problems Addressed by the Frameworks and Protocols

1) QKD addresses:

- The need for secure key distribution in the presence of eavesdropping threats [7].

- The risk of key compromise during transmission, ensuring keys remain secret [7].

2) Blockchain-based security addresses:

- The need for tamper-proof and transparent record-keeping in IoSat [8].

- Secure data sharing and access control among satellites and ground stations [8].

3) Machine learning addresses:

- The challenge of detecting novel and evolving security threats in real-time [9].

- The need to analyse vast amounts of data generated by the IoSat network [9].

4) Secure software development addresses:

- The presence of vulnerabilities and weaknesses in satellite software.

- The need for rigorous testing and verification to ensure software integrity.

5) BFT addresses:

- The risk of malicious or faulty nodes disrupting the operation of the IoSat network [10].

- The need for consensus and agreement among honest nodes to maintain correct operation [10].

C. Unresolved Issues in IoSat Security

1) Constraints in computational capabilities:

- Satellites face limitations in processing power, memory, and energy, which pose difficulties in deploying complex security algorithms [11].

- Managing security needs within the confines of limited resources remains a persistent obstacle [11].

2) Hurdles in implementing QKD:

- Accurately directing and tracking narrow QKD beams amidst satellite movements and vibrations [12].

- Addressing the impact of atmospheric turbulence on QKD signals, which may result in signal loss and inaccuracies [12].

- Expanding QKD to worldwide networks while upholding key distribution rates and security measures [12].

3) Blockchain consensus in space:

- Adapting blockchain consensus algorithms to the unique characteristics of the space environment, such as intermittent connectivity and long propagation delays [13].

- Ensuring the efficiency and scalability of consensus algorithms for large-scale IoSat networks [13].

4) Machine learning model robustness:

- Ensuring the quality, diversity, and representativeness of training data for machine learning models in the context of IoSat applications.

- Developing mechanisms to continually update and adapt machine learning models to detect and respond to evolving security threats.

- Addressing the risk of adversarial attacks on machine learning models, such as data poisoning and evasion attacks, as discussed in [9] for satellite systems.

5) Regulatory and legal challenges:

- Navigating the complex landscape of national and international laws and regulations governing satellite operations and data security [14].

- Harmonizing security standards and best practices across different jurisdictions to ensure a consistent level of security in the global IoSat network [14].

D. Approaches Being Considered for Unresolved Issues

1) Lightweight cryptography and key management:

- Developing lightweight cryptographic algorithms that provide strong security while being computationally efficient for resource-constrained satellites [11].

- Designing secure key management systems that enable efficient key generation, distribution, and revocation in the IoSat network [11].

2) QKD advancements:

- Investigating advanced pointing and tracking mechanisms, such as fine-steering mirrors and adaptive optics, to improve QKD beam alignment [12].

- Developing quantum repeaters and satellite-based quantum networks to extend the range and scalability of QKD [12].

- Exploring hybrid QKD protocols that combine different QKD schemes to enhance security and efficiency [12].

3) Efficient blockchain consensus:

- Creating consensus algorithms specifically designed for the unique challenges of the space environment, taking into account intermittent connectivity, long propagation delays, and limited resources [13].

- Investigating the use of hybrid consensus methods that combine different mechanisms to achieve the best possible performance and security [13].

4) Robust machine learning:

- Employing data augmentation, synthetic data generation, and transfer learning techniques to enhance the quality and diversity of training datasets.

- Implementing online learning and incremental learning methods to enable real-time updates and adaptations of machine learning models based on new data and threat scenarios.

- Utilizing adversarial training and defensive approaches like adversarial example detection and model ensembling to increase the resilience of machine learning models against adversarial attacks.

5) International collaboration and standardization:

- Engaging in international forums and working groups, such as the Inter-Agency Space Debris Coordination Committee (IADC) and the Consultative Committee for Space Data Systems (CCSDS), to develop common security standards and best practices [14].

- Fostering collaboration among space agencies, industry partners, and academic institutions to share knowledge, expertise, and resources in addressing IoSat security challenges [14].

- Establishing international agreements and frameworks for responsible behavior in space, including provisions for data security and privacy [14].

V. Conclusion

The primary focus of the initial approach has been on the emergence of CubeSats and the advancement of this technology. Additionally, the IoSat concept has been introduced, which represents a novel space segment paradigm. In this paradigm, diverse satellites are sporadically interconnected to establish a communication platform for independent satellite applications. This approach promotes the implementation of multi-hop Fixed Satellite Service (FSS), which overcomes the limitations of point-to-point scenarios by deploying temporal Integrated Satellite Networks (ISN).

As previously discussed, the current solutions provided by the International Space Community (ISC) are unable to achieve this type of behavior. The dynamic nature of this environment poses a significant challenge, particularly in terms of communication protocols, specifically routing protocols. These protocols are responsible for defining and maintaining a path between a source and a destination. By analyzing existing solutions and adapting them to manage this behavior, interoperability and interconnection can be achieved. Furthermore, the operational and security challenges associated with IoSat have been addressed. Effectively addressing these security concerns is crucial for the successful deployment and operation of IoSat. It necessitates a multi-layered approach that combines technological innovation with international cooperation and regulatory frameworks.

References

[1] "Satellite Communication," Encyclopædia Britannica. [Online]. Available: https://www.britannica.com/technology/satellite-communication

[2] B. Lal, E. Sylak-Glassman, and M. Mineiro, "The Rise of CubeSats: Opportunities and Challenges," Wilson

Center, 06-Aug-2018. [Online]. Available: https://www.wilsoncenter.org/blog-post/rise-cubesats-opportunities-and-challenges

[3] J. A. Ruiz-de-Azua, A. Calveras, and A. Camps, "Internet of Satellites (IoSat): Analysis of Network Models and Routing Protocol Requirements," IEEE Access, vol. 6, pp. 20390-20411, 2018

https://upcommons.upc.edu/bitstream/handle/2117/117744/FINAL%20VERSION.pdf;jsessionid=65680DBAB01BEC4462937CA65A0CD6FB?sequence=1

[4] J. A. Ruiz-de-Azua, A. Camps, A. Calveras, and J. Alarcón, "IoSat, an interconnected space segment paradigm," UPCommons. [Online]. Available: https://upcommons.upc.edu/bitstream/handle/2117/115452/IoSat_an_interconnected_space_segment_paradigm.pdf?sequence=1

[5] W. Shi, J. Li, W. Xu, H. Zhou, N. Zhang, and X. Shen, "Internet of Satellites: An Interconnected Space Paradigm," IEEE Wireless Communications, vol. 26, no. 4, pp. 16-23, 2019,

[6] "Challenges and Solutions for Operating in Extreme Space Environments," Frontiers. [Online]. Available: https://www.frontiersin.org/research-topics/31693/challenges-and-solutions-for-operating-in-extreme-space-environments

[7] H. Kaushal and G. Kaddoum, "Optical Communication in Space: Challenges and Mitigation Techniques," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 57-96, 2017

[8] M. Torky, T. Gaber, and A. E. Hassanien, "Blockchain in Space Industry: Challenges and Solutions," Feb. 2020, Accessed: Jun. 06, 2023. [Online]. Available: https://www.researchgate.net/publication/339616244_Blockchain_in_Space_Industry_Challenges_and_Solutions

[9] P. Bernal-Mencia, K. Doerksen, and C. Yap, "Machine Learning for Early Satellite Anomaly Detection," Proceedings of the 35th Annual Small Satellite Conference, Logan, UT, USA, 2021, Paper SSC21-I-03.

https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=5002&context=smallsat#:~:text=A%20part%20of%20these%20tools,satellite%20behaviour%20on%20active%20satellites.

[10] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382-401, 1982

https://dl.acm.org/doi/10.1145/357172.357176

[11] R. Soosahabi and M. Naraghi-Pour, "Scalable PHY-Layer Security for Networks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 4, pp. 1118-1126, 2012

https://scholar.google.com/citations?view_op=view_citation&hl=en&user=SNFxK60AAAAJ&citation_for_view=SNFxK60AAAAJ:u-x6o8ySG0sC

[12] J. S. Sidhu, J. G. Ren, and T. Jennewein, "Quantum Key Distribution with Satellites: A Comprehensive Review," IEEE Access, vol. 9, pp. 67429-67450, 2021

https://strathprints.strath.ac.uk/79072/1/Sidhu_etal_QTDCES_2021_Key_generation_analysis_for_satellite_quantum_key_distribution.pdf

[13] W. Sun, L. Wang, P. Wang, and Y. Zhang, "Collaborative Blockchain for Space-Air-Ground Integrated Networks," IEEE Wireless Communications, vol. 27, no. 6, pp. 82-89, December 2020

https://sci-hub.se/downloads/2021-05-17/b4/sun2020.pdf

[14] M. P. Schrogl, Ed., Handbook of Space Security: Policies, Applications and Programs, 2nd ed. Cham: Springer International Publishing, 2020. [Online].

https://dokumen.pub/handbook-of-space-security-policies-applications-and-programs-2nd-edition-3030232093-9783030232092-9783030232108.html