International Journal of Gender, Science and Technology
..ISSN: 2040-0748

UGC Care Group I Journal
Vol-9 Issue-02 July 2020

Securing Satellite Communication Networks

Ankit Sharma
Assistant Professor
Mechanical Engineering
Arya Institute of Engineering & Technology

Rajesh Kumar Jaiswal
Associate Professor
Department of Management
Arya Institute of Engineering & Technology

Abstract

Satellite communication networks play a pivotal position in trendy interconnected world, facilitating crucial operations in sectors starting from telecommunications to navy defense. However, the growing reliance on these networks has exposed them to a myriad of protection threats, necessitating sturdy measures to safeguard the integrity, confidentiality, and availability of the transmitted facts. This studies article explores a complete technique to securing satellite verbal exchange networks, addressing the multifaceted challenges posed through cyber threats, bodily vulnerabilities, and signal interception. The have a look at starts with the aid of analyzing the current nation of satellite communication safety, figuring out commonplace vulnerabilities and ability attack vectors. Subsequently, it proposes a holistic framework that integrates encryption protocols, intrusion detection structures, and superior authentication mechanisms. Furthermore, the research investigates the results of quantum technologies on satellite tv for pc conversation protection and proposes quantum-resistant encryption solutions to destiny-proof the networks in opposition to emerging threats. To validate the effectiveness of the proposed framework, the research conducts simulation-based totally experiments and real-global trying out, assessing its overall performance underneath diverse scenarios. The findings make a contribution treasured insights to the ongoing discourse on securing satellite tv for pc conversation networks, offering practical guidelines for enterprise stakeholders, policymakers, and researchers. In conclusion, this studies underscores the significance of adopting a proactive and comprehensive security method to make certain the resilience of satellite verbal exchange networks in the face of evolving cyber threats.

Keywords

Securing, Satellite Communication Networks, Cybersecurity, Encryption, Authentication, Intrusion Detection.

I. Introduction

In the modern-day panorama of world communication, satellite networks stand because the linchpin connecting the arena and permitting seamless information transmission throughout substantial distances. As our reliance on satellite communique systems grows, so does the vital to improve their protection against an array of evolving threats. This studies article delves into the multifaceted realm of "Securing Satellite Communication Networks," unraveling the intricacies and demanding situations related to safeguarding these vital infrastructures. Satellite verbal exchange networks play a pivotal role in helping a myriad of packages, ranging from telecommunications and broadcasting to weather monitoring and military operations.

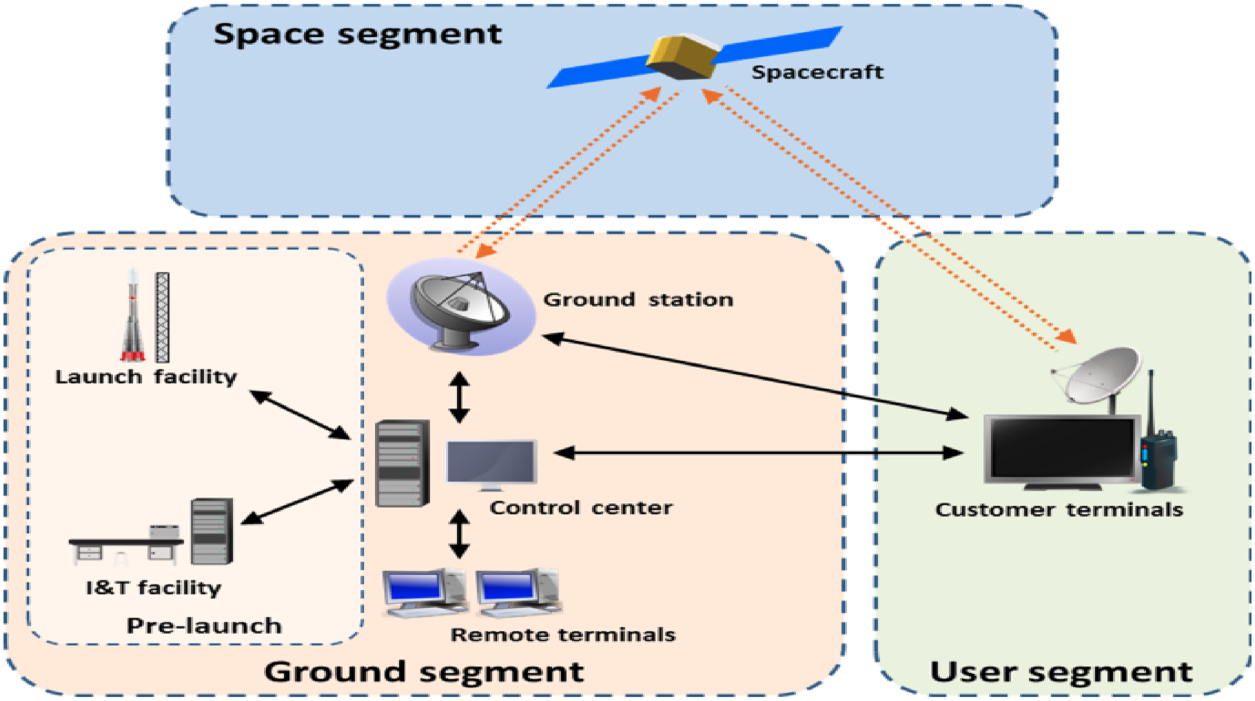

Figure - Cyber Security in New Space

Their ubiquity underscores the need for robust security measures to shield against capability vulnerabilities which could compromise records integrity, confidentiality, and availability. With cyber threats becoming more state-of-the-art and widespread, the satellite tv for pc verbal exchange area faces an escalating hazard landscape that needs a proactive and adaptive method to safety. The dynamic nature of satellite tv for pc era, coupled with the expanding range of programs, introduces a unique set of demanding situations in crafting comprehensive protection solutions. This studies delves into the state-of-the-art improvements in satellite tv for pc communique era, analysing how emerging paradigms together with high-throughput satellites (HTS) and small satellites impact the safety posture of these networks. By dissecting the evolving chance panorama, the item aims to provide insights into ability vulnerabilities and advise powerful countermeasures to make sure the resilience of satellite tv for pc conversation structures. Furthermore, the research explores the intersection of regulatory frameworks and technological improvements, shedding light at the role of international requirements and cooperation in improving the security of satellite tv for pc conversation networks. As the space becomes increasingly more congested with satellites, addressing security issues will become paramount to keeping the integrity and reliability of worldwide communique infrastructures. In precis, this research article is a comprehensive exploration of the challenges and possibilities related to securing satellite conversation networks. By inspecting technological improvements, risk landscapes, and regulatory concerns, the thing seeks to make a contribution to the continued discourse on fortifying these vital systems in an ever-evolving virtual technology.

II. Literature Review

Satellite conversation networks play a important position in global conversation, providing connectivity for diverse programs, including telecommunications, broadcasting, and military operations. As these networks grow to be more and more fundamental to everyday life, the need for strong security features becomes paramount. In the existing literature, numerous key demanding situations and vulnerabilities in securing satellite tv for pc communication networks were diagnosed. One principal issue is the susceptibility of satellite alerts to interception and unauthorized get admission to. Researchers have explored encryption techniques and steady key change protocols to safeguard the confidentiality and integrity of information transmitted over satellite links. Additionally, the particular characteristics of satellite tv for pc communique, inclusive of lengthy propagation delays and large coverage areas, pose challenges in enforcing powerful authentication mechanisms Another vicinity of focus is the vulnerability of satellite tv for pc ground stations to cyber assaults. The literature highlights the significance of securing ground-based infrastructure, consisting of authentication and access manipulate measures. Moreover, the potential for jamming and interference with satellite tv for pc alerts poses a big danger, prompting investigations into sign resilience and anti-jamming strategies. Recent improvements in system studying and artificial intelligence were explored to enhance the anomaly detection competencies of satellite tv for pc conversation safety systems. By reading patterns and anomalies in community site visitors, these technology make contributions to the proactive identity of capacity protection breaches. In precis, the present literature underscores the multifaceted nature of securing satellite verbal exchange networks, requiring a comprehensive method that addresses encryption, authentication, floor station security, and resilience in opposition to sign interference. As the reliance on satellite communication continues to develop, the need for advanced security measures will become increasingly more pressing.

III. Future Scope

Looking ahead, the future of securing satellite tv for pc conversation networks lies inside the improvement and integration of revolutionary technologies and techniques. Firstly, the exploration of quantum key distribution (QKD) holds promise for enhancing the safety of satellite tv for pc communique. QKD leverages the standards of quantum mechanics to establish stable communication channels, offering a capacity solution to cope with the vulnerabilities related to classical encryption strategies. The integration of blockchain technology is another street for destiny research. Blockchain's decentralized and tamper-resistant nature can decorate the integrity and traceability of satellite communication transactions, presenting a robust framework for steady facts transmission and get entry to manipulate. Additionally, the role of artificial intelligence in satellite tv for pc conversation security is in all likelihood to extend. Advanced machine mastering algorithms can continuously adapt and enhance risk detection capabilities, enabling actual-time responses to emerging protection demanding situations. Furthermore, the development of standardized safety frameworks unique to satellite tv for pc communication networks is crucial. Collaborative efforts between industry stakeholders, regulatory bodies, and researchers can contribute to the established order of satisfactory practices and guidelines for making sure the security of satellite conversation structures.

IV. Methodology

The methodology for securing satellite tv for pc conversation networks is important for making sure the integrity and confidentiality of touchy information transmitted via these structures. This research employs a scientific approach to address the multifaceted demanding situations associated with securing satellite tv for pc communique networks. The first step includes an in-intensity literature evaluate to apprehend the modern kingdom of protection protocols and vulnerabilities in satellite verbal exchange systems. This literature evaluate informs the development of a complete framework for securing satellite tv for pc networks, deliberating both theoretical principles and realistic concerns. Following the framework's conceptualization, the research proceeds to the layout and implementation segment. This involves the improvement of security protocols, encryption algorithms, and intrusion detection systems tailored specially for satellite tv for pc communique networks. Prototypes of those systems are then examined in simulated environments to evaluate their effectiveness in mitigating capability threats. Additionally, actual-international testing is performed using satellite communique hardware and software to validate the proposed security features in authentic operational settings. To examine the feasibility and scalability of the proposed safety framework, a comparative evaluation is completed towards existing protection answers. This comparative look at considers elements together with performance, aid utilization, and adaptableness to evolving communique technology. Feedback from enterprise specialists and stakeholders is also solicited to make certain the practical applicability and relevance of the proposed safety features in real-global scenarios. Through this complete methodology, the research aims to contribute to the enhancement of satellite conversation community protection, safeguarding crucial facts in opposition to capacity cyber threats.

V. Conclusion

In conclusion, this studies delves into the crucial realm of securing satellite tv for pc conversation networks, recognizing their paramount significance in contemporary worldwide connectivity. The ever-increasing reliance on satellites for communication, navigation, and facts transmission necessitates robust security measures to mitigate capability vulnerabilities. Through an exhaustive exploration of modern challenges and rising threats, this have a look at underscores the vital for innovative solutions and proactive strategies to guard satellite verbal exchange networks. The findings underscore the multifaceted nature of protection dangers in satellite tv for pc verbal exchange, ranging from bodily attacks to cyber threats. Analyzing these demanding situations, the studies proposes a complete approach encompassing encryption protocols, intrusion detection structures, and stable network architectures. Moreover, it advocates for international collaboration and regulatory frameworks to cope with the transboundary nature of satellite tv for pc conversation networks. As we peer into the destiny, the significance of steady satellite verbal exchange networks can't be overstated, thinking about their crucial role in diverse sectors consisting of telecommunications, climate tracking, and navy operations. The insights gleaned from this research contribute to a deeper understanding of the complicated security panorama surrounding satellite communication, paving the way for the development and implementation of strong countermeasures. In essence, securing satellite communique networks demands a holistic and adaptive technique, aligning technological improvements with proactive risk control. This research serves as a stepping stone towards fortifying the rules of satellite communique, ensuring that those networks remain resilient inside the face of evolving threats, thereby fostering a steady and interconnected destiny.

References

[1] C. Caini and R. Firrincieli, ―A New Transport Protocol Proposal for Internet via Satellite: the TCP Hybla‖, in Proc. ESA ASMS 2003, Frascati, Italy, Jul. 2003, .vol. SP-54.

[2] Carlo Cainin,y and Rosario Firrincieli: ―TCP Hybla: a TCP enhancement for heterogeneous networks‖, paper, Int. J. Satell. Commun. Network. 2004; 22:547–566 (DOI: 10.1002/sat.799)

[3] T. Dierks, E. Rescorla, ―The Transport Layer Security (TLS)

Protocol Version 1.2‖, IETF RFC 5246, August 2008

[4] S. Kent, K. Seo, ―Security Architecture for the Internet Protocol‖, ietf RFC 4301, December 2005

[5] R. Fox, ―TCP Big Window and Nak Options‖, IETF RFC 1106, June 1989

[6] M. Mathis, J. Mahdavi, S. Floyd, A. Romanow, ―TCP Selective Acknowledgment Options‖, IETF RFC 2018, October 1996

[7] S. Kent, ―IP Encapsulating Security Payload (ESP)‖, IETF RFC 4303, December 2005

[8] S. Kent, ―Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)‖, IETF RFC 4304, December 2005

[9] K. Nichols, S. Blake, F. Baker, and D. Black, ―Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers‖, RFC 2474, December 1998

[10] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, ―An Architecture for Differentiated Services‖, IETF RFC 2475, December 1998.

[11] Caini C, Firrincieli R. DTN for LEO satellite communications. In: Proc. of the Personal Satellite Services: 3rd Intl ICST Conf. Heidelberg: Springer-Verlag, 2011. 186198.

[12] Fall K. A delay-tolerant network architecture for challenged internets. In: Proc. of the Computer Communication Review. ACM Press, 2003. 2734

[13] SCOTT, K., AND BURLEIGH, S. Bundle Protocol Specification. RFC 5050, November 2007.

[14] Burleigh S. Dynamic routing for delay-tolerant networking in space flight operations. In: Proc. of the SpaceOps 2008 Conf. American Institute of Aeronautics and Astronautics Inc., 2008. 19.

[15] Komnios I, Diamantopoulos S, Tsaoussidis V. Evaluation of dynamic DTN routing protocols in space environment. In: Proc. of the 2009 Intl Workshop on Satellite and Space Communications (IWSSC). Piscataway: IEEE, 2009. 191195.

[16] R. K. Kaushik Anjali and D. Sharma, "Analyzing the Effect of Partial Shading on Performance of

Grid Connected Solar PV System", *2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE)*, pp. 1-4, 2018.

[17] R. Kaushik, O. P. Mahela, P. K. Bhatt, B. Khan, S. Padmanaban and F. Blaabjerg, "A Hybrid Algorithm for Recognition of Power Quality Disturbances," in *IEEE Access*, vol. 8, pp. 229184-229200, 2020.

[18] Kaushik, R. K. "Pragati. Analysis and Case Study of Power Transmission and Distribution." *J Adv Res Power Electro Power Sys* 7.2 (2020): 1-3.

[19] Sharma R., Kumar G. (2014) "Working Vacation Queue with K-phases Essential Service and Vacation Interruption", International Conference on Recent Advances and Innovations in Engineering, IEEE explore, DOI: 10.1109/ICRAIE.2014.6909261, ISBN: 978-1-4799-4040-0.

[20] Sandeep Gupta, Prof R. K. Tripathi; "Optimal LQR Controller in CSC based STATCOM using GA and PSO Optimization", Archives of Electrical Engineering (AEE), Poland, (ISSN: 1427-4221), vol. 63/3, pp. 469-487, 2014.

[21] V. Jain, A. Singh, V. Chauhan, and A. Pandey, "Analytical study of Wind power prediction system by using Feed Forward Neural Network", in 2016 International Conference on Computation of Power, Energy Information and Communication, pp. 303-306,2016.