iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82432

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Deep Learning for LEO (Lower Earth Orbit) Satellite Attack Detection

Talha Hasan[1], Dr. Siddartha Shankar Biswas[2], Dr. Zeeshan Ali Haq[3]
School Of Engineering Science & Technology, Jamia Hamdard, New Delhi-110062

Abstract: ***Satellite-based communication infrastructure security has become a more urgent engineering issue of this decade. Networks in Low Earth Orbit Space Networks orbit the earth at altitudes between 500 and 2000 kilometres (typically) above the ground. Now they constitute active communication systems along sea routes, war zones and in those areas where ground-based broadband merely cannot penetrate. SpaceX Starlink alone was well past three million active subscribers by the end of 2023, a number that underscores the extent of adoption as well as the extent of impact in the case of such systems being targeted.***
The threat landscape of LEO constellations is not far-fetched. Attack types have been reported against operational systems as Denial-of-Service attacks on ground-to-satellite uplinks, intentional radio jamming of command channels and user terminals, as well as exploitation of predictable windows of atmospheric interference. The cyberattack on the Viasat KA-SAT network in February 2022 offered perhaps the clearest example so far of what a well-coordinated attack can accomplish - tens of thousands of modems went dead in hours, affecting communications in several countries in the middle of an ongoing military conflict.
The paper presents a critical analysis of the deep learning detection model proposed by Sitouah et al. in 2022, which compared five neural networks Multi-Layer Perceptron, Convolutional Neural Network, Recurrent Neural Network, Gated Recurrent Unit, and Long Short-Term Memory with simulated LEO attack traffic. Their GRU-MLP hybrid got a 99% detection accuracy in controlled conditions and reduced to 94 to 96 percent in multi-class settings. Even with these impressive numbers, there are four major constraints that limit the practical applicability of the framework: all the training data was synthetically created, the heavier models are out of realistic onboard compute limits, no adversarial traffic solutions were tested, and the system has no autonomous response capabilities except raising an alarm.
Based on these results, this review suggest four specific improvements - integration of operational telemetry, model compression with TinyML, Fast Gradient Sign Method adversarial hardening, and an end-to-end detection-to-response pipeline - all intended to reduce the difference between simulated performance and real orbital operation.
Keywords: Low Earth Orbit satellites, deep learning, satellite cybersecurity, intrusion detection, adversarial robustness, TinyML, GRU-MLP, neural network security

I. INTRODUCTION

Human development has been continually influenced by connectivity. Road, rail, undersea cables - with each generation of infrastructure came an increase in what people could do and who they could include. The satellite network of Low Earth Orbit satellites is the incarnation of that tale in the present generation. It is not merely an alternative to fibre optic cables; in most regions of the global world, they are the only option available of access to broadband at all. Casts of fishing in West African waters, mining in Australia, research in Antarctica - none of these are edge cases any longer. They are one of the millions of active.
network endpoints such as Starlink, OneWeb, and Project Kuiper of Amazon, which have ceased to be merely ambitious ideas and are actively being deployed into orbit in the last five years [1], [2].
The main difference between LEO constellations and previous geostationary satellite systems is largely their altitude. Located above the Earth on the range of about 550-1200 kilometres, LEO satellites are dramatically lower in signal latency namely 20-40 milliseconds as opposed to the 600-plus milliseconds in geostationary orbit [3]. That difference is not merely a technical footnote. It dictates how good a satellite connection can be to carry a live voice call, video conferencing, remote surgery control or even to process financial transactions. Its practical consequences are so great that LEO connectivity has become a real operational need of armies, emergency response departments, and operators of vulnerable infrastructure, not a backup in the case of a contingency.
The dependency, however, exposes. Whether the infrastructure is critical or not will sooner or later be targeted by adversaries that know the disruption value of targeting critical infrastructure. LEO satellite networks have a unique and in a way more difficult threat environment compared to the traditional terrestrial networks.

Communication geometry - Signals carried hundreds of kilometres across open atmosphere over satellites and the ground stations provide numerous interception and interference points, which are unavailable for a wired network [4]. Denial-of-Service attacks on uplink channels may saturate the small amount of bandwidth used on command and control communications. Radio frequency jamming at user terminals can be used to isolate whole service areas without even having to make contact with the satellite equipment itself. Certain other forms of threat that prove quite hard to detect in real time include spoofing attacks where false signals are introduced to deceive the navigation or timing systems [5].

The vulnerabilities could not be ignored as February 2022 attack on the Viasat KA-SAT network has proven. About one hour after Russian military troops invaded Ukraine a carefully planned cyberattack took advantage of a system bug in the ground segment management OS of the satellite to broadcast harmful firmware updates to tens of thousands of customer modems in Europe [6]. The modems were not only shown permanently out of commission, but destroyed outright. Remote monitoring was lost to wind turbine operators in Germany. The communication between the Ukrainian military was interfered with during the first hours of the war. The attack showed that the consequences of the successful attack on satellites infrastructure may cause long-lasting effects that extend far beyond the target and live months longer than the attack.

It is against this backdrop that the use of deep learning in detecting intrusion of satellite networks has gained increased research interest. Deep learning models, especially those that work with sequential or time-series data, provide detection features that are unmatched by traditional threshold-based and signature-matching models on novel or dynamically generated attack traffic [7]. Notably, in a 2022 study, Sitouah, Merazka, and Hedjazi compared the five neural architectures, Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Gated Recurrent Unit (GRU), and Long Short-Term Memory (LSTM), based on their capacity to classify interruption attacks within a simulated LEO network environment implemented with the OMNeT++/INET simulation framework [8]. Their optimal architecture, a GRUbased-MLP hybrid, was 99% accurate when classification was performed under binary detect conditions, and 94-96% accurate when classification was performed under multi-class conditions where multiple simultaneous attack types exist. Figure 1 represents the overall structure of an LEO satellite network and the threat vectors which detection systems of these naturemanage to deal with.

Figure1:LowEarthOrbitSatelliteNetworkWeavingGlobalConnectivity

The findings presented by Sitouah et al. are truly promising, yet a close examination of the methodology can show that there are certain limitations, which are of great significance to anyone planning to implement them in the real world. All of their training samples were synthetically created by simulation, stating the models had never seen the noise properties, hardware artifacts, and random traffic patterns that are present in reality in operational data. The larger architectures, especially GRU and LSTM, have computational demands that are too much to sustain with existing satellite onboard processors without important redesign [9]. This paper has no comparison of model performance with adversarially designed traffic - packets with attack packets designed specifically to elicit the worst result on neural network classifiers - even though these techniques are very well documented and now accessible to advanced threat agents [10]. Most importantly, perhaps, the framework is limited to detection. Upon detection of a threat, a warning is issued and processing stops at this point, leaving the actual response all to the human operators.

This paper critically reviews and proposes four concrete enhancements to the framework presented by Sitouah et al., which includes substituting synthetic training data with genuine LEO operational telemetry, utilizing TinyML compression algorithms to reduce the complexity of the model to fit into the onboard hardware capabilities, using Fast Gradient Sign Method adversarial training to enhance resistance to evasion attacks, and developing an integrated detection-to-response pipeline that can automatically activate mitigation when threats are identified. The rest of this paper will be laid out in the following manner. Section II introduces the problem and the framework of proposed solution. Part III summarizes existing pertinent literature.

The Sitouah et al. study is analyzed in Section IV. Section V compares the results of assessed models. V will examine the strengths and weaknesses of the study. Section VII gives suggested improvements. In Section VIII the wider implications of this work are discussed and Section IX concludes.

II. PROBLEMSTATEMENTANDPROPOSEDSOLUTION

There are four interrelated security challenges facing LEO satellite networks which are yet to be addressed by current research. First, as traffic moves through these constellations, the basis of anomalies is constantly changing with the movement of the orbit, and it is hard to maintain stable bases of anomaly [9]. Second, onboard processors are chosen due to their radiation tolerance and not speed, restricting the types of detection models that can be effectively implemented. in orbit [10]. Third, adversarial agents have the ability to create traffic that was explicitly constructed to optimize around neural classifiers, something that most published works have not tested [11]. Fourth, identification that goes unresponded exposes a network even after some threat has been detected - alerting and terminating an attack are at minimum different [12].

Sitouah et al. discuss the issue of detection in a very comprehensive manner, but the other three challenges are not discussed much. Four specific improvements are suggested in this paper. Synthetic training data should give way to real operational telemetry of LEO operators to enhance generalisability. The compression methods of TinyML have the potential to simplify a model to an extent that can be supported by a satellite hardware without an equivalent decrease in accuracy [13]. Adversarial training using Fast Gradient Sign Method can defend against evasion [11]. Lastly, a detection-to-response pipeline, which would be able to start traffic rerouting or frequency switching in case of an actual threat detection, would turn a passive monitoring system into a proactive defence mechanism.

III. LITERATURE REVIEW

The study of satellite network security has had a series of limited phases, each bringing forth new limitations that inspired the following generation of strategies. The initial efforts were based on the conventional machine learning classifiers. One of the most widely used were Support Vector Machines, and research indicated that the detection rate was 85 to 90 percent on satellite traffic data [14]. SVM-based systems can overcome the attack signatures that are known, well-defined, but when the traffic of attackers changes or when there are multiple types of attacks that appear one after another, they fail significantly [15]. Alternatively, the use of random forest classifiers was addressed that has slightly better multi-class performance but with the same limitations on dynamic network settings [16]. The transition to deep learning was accompanied by tangible gains. Hybrid CNN-LSTM networks, that is, implementing convolutional layers to extract spatial information of traffic snapshots and then feeding the result to recurrent layers to model the time series, demonstrated accuracy rates of approximately 95 percent in benchmarks (intrusion detection) [17]. Computational cost was a trade-off - the models need inference hardware that is many times more expensive than is available today in satellite onboard processors [10]. Single LSTM models were also as good as multi-task networks on time-series classification tasks and were slightly smaller in size, but again, currently infeasible to run in the car without compression [18]. Lightweight model research is a different line of the literature, in which deployability is more important than raw accuracy. Experiments on pruning and quantisation of neural networks to embedded systems showed that it is possible to compress a large model down to just two to five percentage points of accuracy loss [13], [19]. This body of work has however been developed in large part without considering satellite security research work and direct application to LEO intrusion detection has not been studied. A more recent trend is federated learning which has been proposed as a system that can enable distributed ground stations to cooperatively learn detection models without raw traffic access, simultaneously mitigating privacy and bandwidth limitations [20]. Findings are tentative, but they indicate a good prospect of future research. Sitouah et al. take a beneficial space in the landscape, and their multi-model analysis gives a better vision of relative deep learning performance on LEO-specific traffic than any single-model work, though their use of simulation and lack of adversarial analysis give directives to the future research [8].

IV. PAPEROVERVIEWANDMETHODOLOGY

Sitouah et al. created their experimental setup in OMNeT++/INET which is a discrete event modeling tool that is frequently applied in modelling behaviour of communication networks [8]. Their simulated LEO topology had several orbital nodes that swapped traffic in normal operating conditions as well as three attack scenarios of Denial-of-Service flooding, signal jamming, and atmospheric disruption events. MLP, CNN, RNN, GRU, and LSTM are five deep learning architectures that were trained and tested in this setting. All models were fed with the same preprocessed traffic features such as the packet rate, signal strength change, delay measures and link utilisation metrics.

The training was done under a supervised classification scheme whereby labelled samples were used to determine the presence and the category of attack traffic. There were two conditions of performance. The former addressed detection as a binary recognition problem - attack vs. no attack. The second one was multi-class classification, where models can only differentiate between particular types of attacks at the same time. GRU-MLP hybrid provided the best performance in either case, with the highest accuracy of 99 percent in binary classification, and 94 to 96 percent in the multi-class environment. Figure 2 shows the detection pipeline that was used in their study.

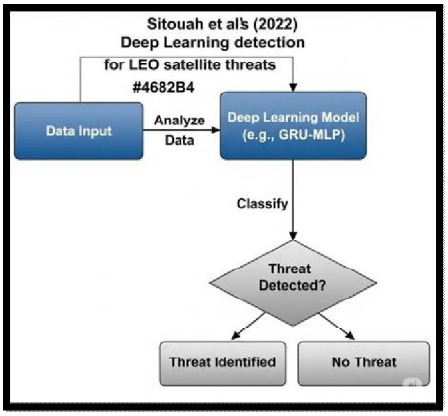


Figure2:DeepLearningDetectionProcessinSitouahetal.'sStudy

V. MODELCOMPARISONANDANALYSIS

Table 1 summarises the five architectures evaluated by Sitouah et al. alongside SVM, which serves as a conventional baseline for comparison purposes.

MODEL	ACCURACY	COMPUTE COST	SUITABILITY
MLP	90%	Low	Simple detection
CNN	92%	Medium	Pattern analysis
RNN	93%	High	Sequential data
GRU	94-99%	High	Time-series
LSTM	95%	High	Time-series
SVM	85%	Low	Resource-limited

Table1:ComparisonofModelsforAttackDetection

MLP is the model with the lowest computational costs across all the deep learning models, implying that it is the model that can be deployed to the onboard, although, with an 90 percent accuracy, it is limited to recognizing intricate patterns [22]. This was enhanced by CNN that made spatial features out of the snapshots of traffic, with 92 percent hit [17]. All three models, RNN, GRU, and LSTM, showed higher performance on sequential traffic data, as this is anticipated due to the architecture of these models that receives time-series inputs [18]. GRU was the most consistent performer with 94-99 percent accuracy, the standalone LSTM having its fair share with a slight but steady advantage over the other. This resource efficiency benefit is what makes GRU a more viable option than LSTM in resources sensitive scenarios, but neither architecture is currently capable of achieving onboard hardware limits without compression. All five deep learning models showed an evident improvement compared to the SVM baseline of 85-90 percent reported in previous satellite security research [14], especially in multi-class scenarios where the SVM performance suffers the most [15].

VI. STRENGTHSANDWEAKNESSES

A. *Strengths*

The closest strength of the study by Sitouah et al. is that it is comparative. Conclusions on relative performance are more reliable when five architectures are tested on the same conditions than when a single model is studied, which constitute the bulk of the current literature on satellite security [25]. The OMNeT++/INET usage offers a reproducible simulation platform and the presence of binary and multi-class evaluation situations offers a clearer insight into realistic detection capability than accuracy scores of a single task only [21]. The 99 percentage binary classification accuracy of the GRU-MLP hybrid is a real improvement over the previous SVM-based methods, and is comparable with CNN-LSTM hybrids which need significantly more computation resources [17].

B. *Weaknesses*

There are four limitations that should be taken seriously. Training on simulated data can make the models identify simulator artefacts as opposed to real attack properties, an issue that has been well known in research on intrusion detection [13]. GRU and LSTM designs surpass the real-world capabilities of onboard processors and cannot be deployed autonomously in orbit [10]. Adversarial evaluation of traffic was not done, and the model resilience to evasion attacks was not tested at all [11]. Lastly, there is also no automated response mechanism in place, and only by way of detection, the disruption of the service can be prevented after the attack was established [26].

VII. PROPOSED ENHANCEMENTS

There are four specific improvements which are suggested to overcome the limitations found in Section VI. Figure 3 demonstrates the entire detection-to-response pipeline which accommodates all four enhancements.

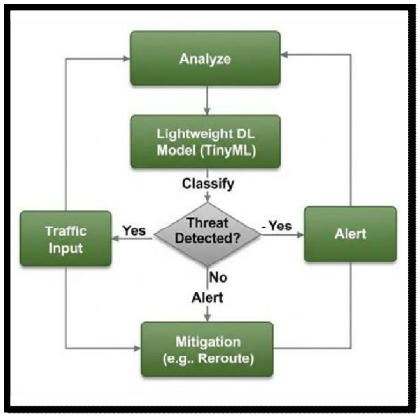


Figure3:ProposedDetection-to-ResponsePipelineforLEOSecurity

A. *RealOperationalTelemetry*

Substituting synthetic training data with realistic LEO traffic logs would introduce models to noise attributes, hardware anomalies, and topology changes found in live networks. Experiments using real traffic measurements to test intrusion detection on the ground are as well documented to achieve higher generalisation than those that are trained on simulations [13]. The most direct route to this objective is to enter into data sharing agreements with LEO operators.

B. *TinyMLModelCompression*

GRU and LSTM models can be reduced by at least 60 to 80 percent in size and accuracy by quantisation and structured pruning methods that usually lose less than five percent of accuracy [13], [19]. This introduces inference requirements into the capability of existing satellite onboard processors, and allows autonomous detection without ground station participation.

C. *AdversarialTraining*

Fast Gradient Sign Method training uses perturbed traffic samples when training the model, which exposes the model to evasion attempts prior to deployment [11].

This strategy has proven to be stable in terms of strengthening network security applications and has no extra inference-time computational costs [27].

D. Detection-to-ResponsePipeline

Figure 3 illustrates the proposed pipeline that takes the output of classification directly to automated mitigation. When hitting a certain confidence threshold, pre-set responses are triggered by the system. -- rerouting or frequency switching or escalation by an operator-- without automatic intervention [26], [28].

VIII. DISCUSSION AND CONCLUSION

A. Discussion

This review indicates that deep learning appears to have real potential in LEO satellite intrusion detection, though the difference between the simulation performance and operational readiness is even further than the published figures would suggest. What the Sitouah et al. study indicates to show is possible given controlled conditions; the four limitations found herein, all work together to justify why the conditions are not yet indicative of deployment reality.

The synthetic data problem is, perhaps, the most significant of these restrictions. The accuracy numbers of the models as based on simulated traffic cannot be assumed to be true predictors of pattern in comparison to actual live network data unless it has been tested directly. Even anonymised or aggregated to ensure the issue of commercial sensitivities, the research community would gain quite a lot of benchmark datasets based on operational LEO infrastructure [13], [25].

Hardware limitations are an equally viable obstacle. The computing power in the current state of technology would not support the current state of technology in computers in space is not a trivial matter - the difference between the computing needs of the current high-accuracy models and the processing power in orbit is large enough that onboard autonomous detection is currently not viable without compression. The approaches provided by TinyML can help bridge this gap effectively, and their implementation in satellite security models should be the focus of special research [13], [19].

The adversarial robustness and automated response may not matter as much as limiting but become more important when LEO networks become more valuable objects. A motivated and technically capable attacker will ultimately test the detection systems to see avenues of evasion and a network can be capable of detecting threats but not autonomously act on them is operationally exposed [11], [26].

B. Conclusion

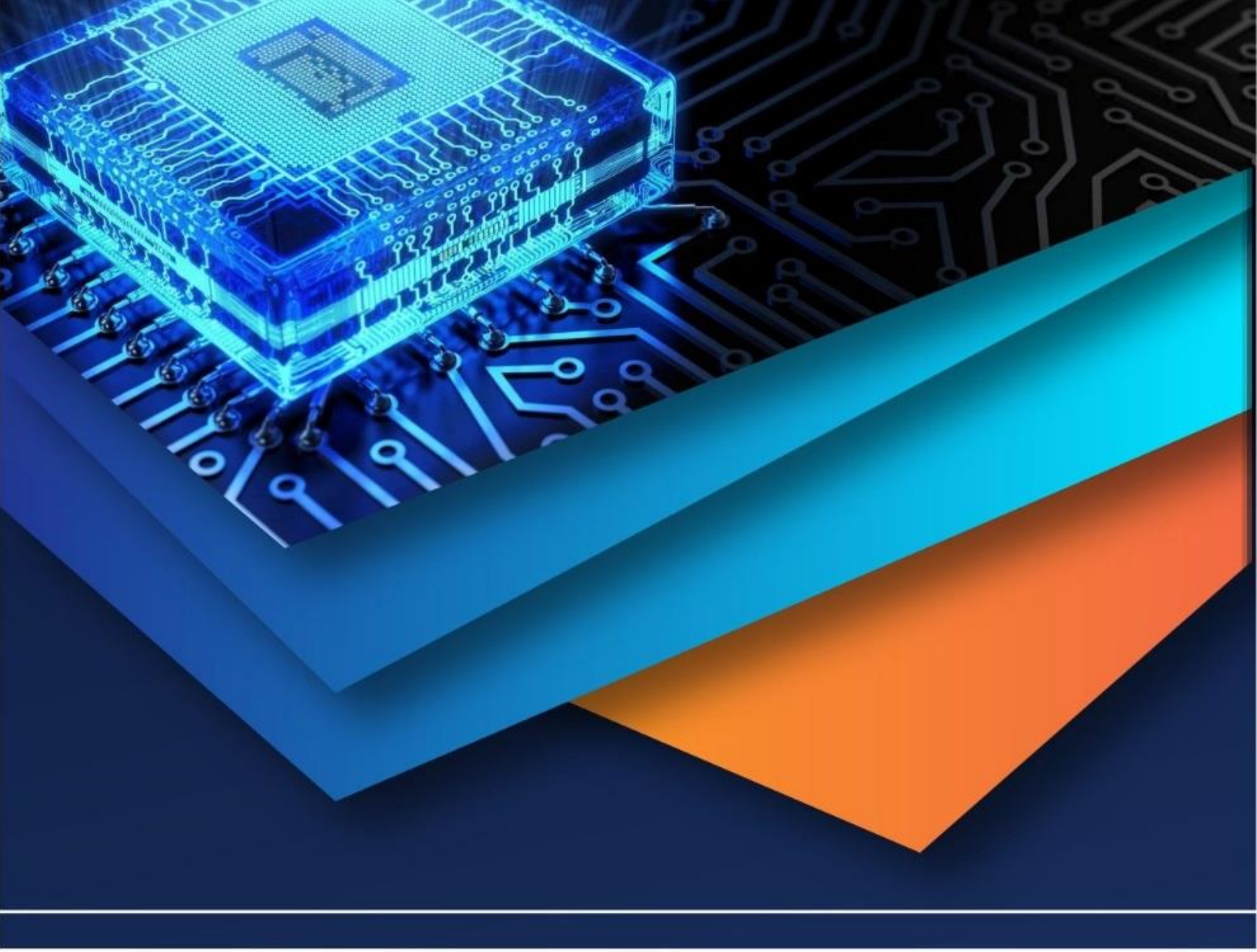
In the current paper, the deep learning framework by Sitouah et al. to identify interruption attacks in LEO satellite networks has been reviewed, four major limitations limiting its potential to operate in the real world have been identified and four specific enhancements to the framework have been suggested to overcome them. Combined with real telemetry integration, TinyML compression, adversarial hardening, and automated response pipelines, they provide a consistent direction on the way to lab accuracy to true orbital resilience.

The Viasat incident of 2022 revealed that failures in satellite network security eradication have much more far-reaching implications than just the loss of services. The gap between what research shows it can achieve and what the implementation of LEO constellations is ready to achieve will only become more urgent as LEO constellations become increasingly involved in critical communication infrastructure around the world. The suggested improvements below are supposed to be implemented as a next step.moves that way instead of hypothetical ideals and each is based on methods with proven outcomes in related areas of research [27].

REFERENCES

[1] I. del Portillo, B. G. Cameron, and E. F. Crawley, "A technical comparison of three LEO satellite constellation systems to provide global broadband," Acta Astronautica, vol. 159, pp. 123–135, Jun. 2019.
[2] M. Handley, "Delay is Not an Option: Low Latency Routing in Space," in Proc. ACM HotNets, Redmond, WA, USA, 2018, pp. 85–91.
[3] O. Kodheli et al., "Satellite communications in the new space era: A survey and future challenges," IEEE Commun. Surveys Tuts., vol. 23, no. 1, pp. 70–109, First Quarter 2021.
[4] J. Pavur, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "A tale of sea and sky: On the security of maritime VSAT communications," in Proc. IEEE Symp. Security and Privacy, San Francisco, CA, USA, 2020, pp. 1384–1400.
[5] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in Proc. ION GNSS, Savannah, GA, USA, 2008, pp. 2314–2325.
[6] M. Burgess, "The Viasat hack was a cyber act of war — it just wasn't obvious," WIRED Magazine, May 2022.

[7] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, May 2015.
[8] N. Sitouah, F. Merazka, and A. Hedjazi, "Deep learning approach for interruption attacks detectionin LEO satellite networks," J. Netw. Comput. Appl., vol. 208, p. 103112, Dec. 2022.
[9] D. Bhattacherjee, W. Singla, V. Vithalkar, and A. Singla, "Network topology design at 27,000 km/hour," in Proc. ACM CoNEXT, Orlando, FL, USA, 2019, pp. 341–354.
[10] F.Leppinen,"Current useofLinuxinspacecraftflightsoftware,"IEEEAerosp.Electron.Syst.Mag., vol. 32, no. 10, pp. 4–15, Oct. 2017.
[11] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," in Proc. ICLR, San Diego, CA, USA, 2015.
[12] R. Heartfield and G. Loukas, "A taxonomy of cyber-physical threats and impact in the smart home," Computers & Security, vol. 78, pp. 398–428, Sep. 2018.
[13] P. Warden and D. Situnayake, TinyML: Machine Learning with TensorFlow Lite on Arduino and Ultra-Low-Power Microcontrollers. Sebastopol, CA: O'Reilly Media, 2019.
[14] A. K. Sharma and R. K. Singh, "SVM-based intrusion detection for satellite networks," arXiv preprint arXiv:2103.04567, Mar. 2021.
[15] M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, and H. Janicke, "RDTIDS: Rules and decision tree-based intrusion detection system for internet-of-things networks," Future Internet, vol. 12, no. 3, p. 44, 2020.
[16] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi,and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in Proc. IEEE WINCOM, Fez, Morocco, 2016, pp. 258–263.
[17] L. M. Gonzalez and T. H. Kim, "Hybrid CNN-LSTM models for network intrusion detection," Applied Sciences, vol. 12, no. 3, pp. 1456–1470, Jan. 2022.
[18] S.A.Althubiti,E.M.Jones,andK.Roy,"LSTMforanomalybasednetworkintrusiondetection,"in Proc. WATTS, Macon, GA, USA, 2018, pp. 1–6.
[19] A.G.Howardetal.,"MobileNets:Efficientconvolutionalneuralnetworksformobilevision applications," arXiv preprint arXiv:1704.04861, Apr. 2017.
[20] Y.Zhao,M.Li,L.Lai,N.Suda,D.Civin,andV.Chandra,"Federatedlearningwithnon-iiddata," arXiv preprint arXiv:1806.00582, Jun. 2018.
[21] A.Varga,"OMNeT++,"inModelingandToolsforNetworkSimulation,K.Wehrle,M.Güneş,andJ. Gross, Eds. Berlin, Germany: Springer, 2010, pp. 35–59.
[22] Y.Bengio,A.Courville,andP.Vincent,"Representationlearning:Areviewandnewperspectives," IEEE Trans. Pattern Anal. Mach. Intell., vol. 35, no. 8, pp. 1798–1828, Aug. 2013.
[23] K.Choetal.,"LearningphraserepresentationsusingRNNencoder-decoderforstatisticalmachine translation," in Proc. EMNLP, Doha, Qatar, 2014, pp. 1724–1734.
[24] S.HochreiterandJ.Schmidhuber,"Longshort-termmemory,"NeuralComputation,vol.9,no.8,pp. 1735–1780, Nov. 1997.
[25] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusiondetection, "inProc.IEEESymp. SecurityandPrivacy,Oakland,CA,USA,2010,pp.305–316.
[26] K.ScarfoneandP.Mell,"Guidetointrusiondetectionandpreventionsystems(IDPS),"NIST Special Publication 800-94, Feb. 2007.
[27] A.Madry,A.Makelov,L.Schmidt,D.Tsipras,andA.Vladu,"Towardsdeeplearningmodels resistant to adversarial attacks," in Proc. ICLR, Vancouver, BC, Canada, 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY