Deep-learning-based Intrusion Detection for Software-defined Networking Space Systems

Uakomba Uhongora[1], Ronald Mulinde[1], Yee Wei Law[1] and Jill Slay[1,2]
[1]UniSA STEM, University of South Australia, Mawson Lakes, Australia
[2]SmartSat CRC, Adelaide, Australia

uakomba.uhongora@mymail.unisa.edu.au
Ronald.Mulinde@unisa.edu.au
YeeWei.Law@unisa.edu.au
Jill.Slay@unisa.edu.au

Abstract: This paper briefly reviews the application of the Software-defined Networking (SDN) architecture to satellite networks. It highlights the prominent cyber threats that SDN-based satellite networks are vulnerable to and proposes relevant defence mechanisms. SDN transforms traditional networking architectures by separating the control plane from the forwarding (data) plane. This separation enhances scalability and centralises management. In comparison, in traditional networks, the control plane and the data plane are usually combined, resulting in complex network management and reduced scalability. Satellite networks can take advantage of these benefits offered by SDN and this supports them as key enablers of critical services, including weather prediction, global broadband Internet coverage, and Internet of Things (IoT) services. Ease of configuration and flexibility are essential for satellites providing critical services to instantly adapt to network changes. These desirable attributes can be realised by applying SDN to satellite networks. Although SDN offers significant benefits to satellite networks, it is vulnerable to cyber-attacks and particularly due to its centralised architecture. A common attack on SDN is the Distributed Denial of Service (DDoS) attack which could render the entire SDN unavailable. To mitigate such threats, an efficient Intrusion Detection System (IDS) is required to monitor the network and detect any suspicious traffic. However, traditional IDSs produce too many false positives and often fail to detect advanced attacks. For their ability to learn feature hierarchies in network traffic data automatically, whether, for network traffic classification or anomaly detection, deep learning (DL) plays an increasingly important role in IDSs. In this paper, we present a brief review of recent developments in cyber security for SDN-based space systems, and we identify vulnerabilities and threats to an SDN-based satellite network. We further discuss the potential of a DL-based IDS for the detection of cyber threats. Finally, we identify further research gaps in the recent literature and propose future research directions.

Keywords: Software-defined Networking, Space Systems, Satellite Networks, Deep Learning, Intrusion Detection System.

1. Introduction

1.1 Background

A space system is a set of interrelated or interacting components that together meet one or more space-related objectives (Aguirre, 2013); examples of these components include ground control systems, launch facilities, suborbital vehicles, orbital vehicles, and space probes. Figure 1 shows the typical structure of a space system, consisting of a space segment and a ground segment, which communicate with each other via radio frequency (RF) signals (Manulis et al, 2020) and increasingly optical signals. The space segment comprises standalone or networked satellites in orbits (as well as launch vehicles designed to release satellites into orbits). Manulis et al (2020) describe the structure of the space segment which consists of a satellite containing one or more payloads. Equipment designed to perform satellite functions. A bus that houses the payload and the rest of the satellite system. Major satellite systems include telemetry, tracking and command/control (TT&C), command and data processing (C&DH), and attitude determination and control (ADCS). These subsystems are responsible for receiving and processing uplink and downlink signals, validating, decoding and transmitting commands to other subsystems, and controlling satellite stabilization or pointing.

An intelligent space system is the enhancement of space system assets by integrating sensors, actuators and intelligent technologies that can collect, analyse and communicate information to the end user. Intelligent space systems provide critical services including GPS navigation, broadband global Internet coverage, and IoT services. Remote communication between devices and systems, as well as the extension of coverage to areas without Internet and cellular network, are enhanced by intelligent space systems. Space systems are also critical to the military domain for their Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) capabilities (Pavur & Martinovic, 2020).

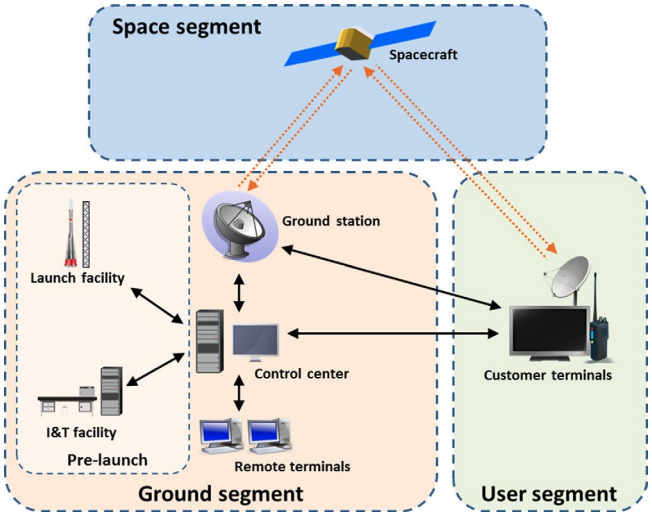

Figure 1: Space system architecture (Manulis et al, 2020)

Unfortunately, space systems are often the target of cyber-attacks (Pavur & Martinovic, 2020). Several critical infrastructures heavily rely on space systems, and these infrastructures would be greatly affected if the space systems are breached. Remote mobile communication around the world would be negatively affected, and people in remote areas that depend on satellites for TV, radio, and the Internet could experience disrupted connectivity. GPS services required by aeroplanes, cargo vessels, and people to navigate geographical locations would be greatly affected too. Moreover, global timing synchronisation would be interrupted. Overall, the absence or disruption of space systems would greatly affect critical domains such as the military, health, critical infrastructure, business and economy, and weather forecast. Considering the dependency of critical infrastructure on space systems, space systems security is required to protect the space ecosystem from cyber threats (Plotnek & Slay, 2022). Space systems security is defined as "the assurance of the confidentiality, integrity, and availability of a space system throughout its lifecycle, including all ground, communications, and space segments as well as the data, processes, and supply chains that support it" (Plotnek & Slay, 2022). Figure 2 illustrates the different threat vectors that can be exploited by hackers on a space system.

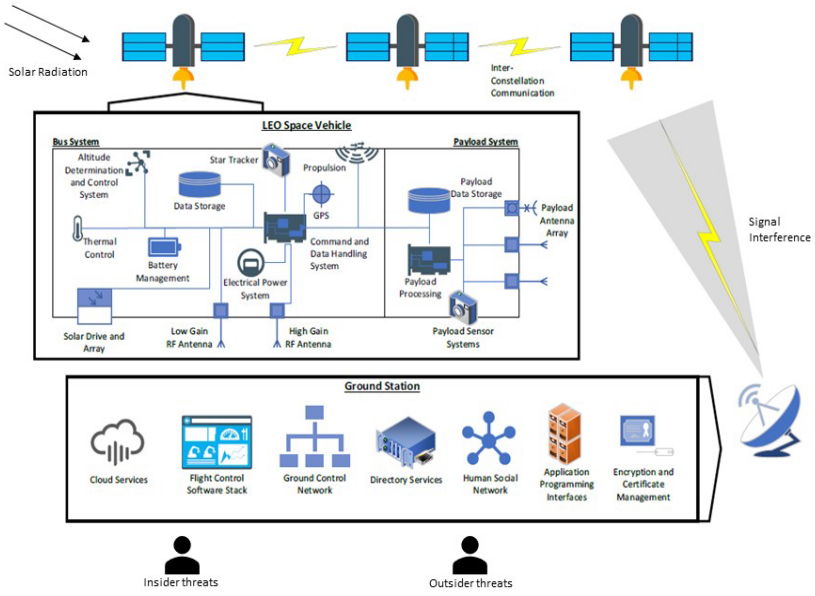

Figure 2: Space system components and threat vectors (Ormrod, Slay & Ormrod, 2021)

Due to the demand for high-performance and worldwide broadband coverage from space systems, space systems can benefit from the high bandwidth offered by SDN at a low cost and efficient packet delivery (Dey and Rahman, 2019). Space systems typically use traditional network design which limits the flexibility and configuration of the network. For space systems to enable services to the critical systems they must be easy to

configure and flexible enough to instantly adapt to network changes. These benefits can be realised by applying SDN to space systems.

SDN is a prominent network architecture that has gained popularity due to its enhancement and improvement to traditional networking. SDN is a networking paradigm that transforms the traditional networking architecture by separating the control plane from the forwarding (data) plane, thus improving the efficiency of applications on how data is transferred by optimising and routing traffic within the network (Pradhan & Mathew, 2020). SDN was developed for the improvement of the shortcomings associated with traditional networks. The controller in the SDN architecture is the "brain" of the network and it decides the paths taken by packets within the network. These networking features allow network administrators and programmers to easily monitor and control the entire network at a limited cost and optimise network resource usage. The SDN architecture enhances scalability, centralises management, and eases the programmability of a network (Bertaux et al, 2015). On the other hand, with traditional networks, the control plane and the data plane are usually combined resulting in complex network management and reduced scalability. Figure 3 illustrates the different architectural designs of SDN in contrast to traditional networks.

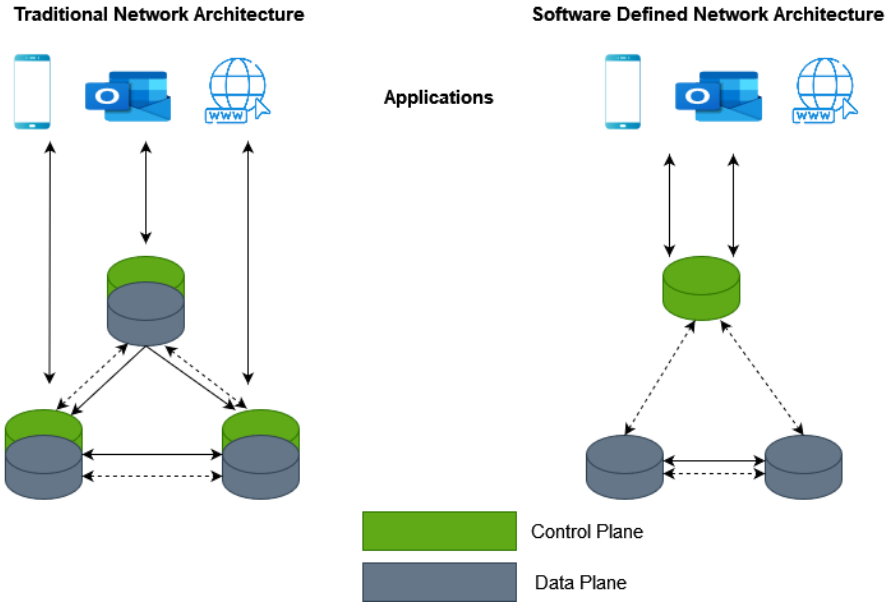

Figure 3: Traditional network architecture vs SDN architecture

Although SDN offers exceptional features for space systems, it brings new security challenges that are unique to SDN (Akhunzada, Ahmed, Gani, Khan and Imran, 2015). The decoupling of the data plane from the control plane in SDN makes it vulnerable to attacks mainly at its control plane. Since the controller makes all the decisions in the network when the controller is compromised the entire network becomes vulnerable. The Distributed Denial of Service (DDoS) attack is one of the most common attacks against the SDN controller. A DDoS attack could flood the controller with large traffic resulting in the unavailability of the network. Network programmability enabled by SDN is a double-edged sword because an attacker could hijack the controller and maliciously reprogram the entire network.

These cyber-attacks amongst others, aim to manipulate data, exhaust network resources and sometimes deny legitimate users access to required network servers. Unfortunately, the adoption of SDN in space systems inherently exposes them to cyber-attacks targeted at SDN. If the vulnerabilities are not managed, SDN-based space systems are exposed to attacks that could render them unavailable or attacks that intercept satellite communication. Thus, there is a need to address the security challenges in SDN-based space systems.

1.2 Research Context

The proposed research aims to address the security issues/cyber threats faced by SDN-based space systems by developing intelligent security controls.
There is a demand for space systems due to their use in a variety of critical systems such as the military, weather services, and global timing. Due to the reliance on critical systems on the space system, cybercriminals see space

systems as a "single point of failure in many critical services" (Pavur & Martinovic, 2020). Space systems experience the challenge of inflexible network management due to their use of traditional networks (Li et al, 2016) that fail to adapt to the demands in bandwidth, computing and storage of current applications. To resolve this problem, adopting SDN for space systems can greatly provide scalability and flexible networking architecture required by critical systems such as space systems. SDN is one of the most promising evolving network technologies (Liu *et al.*, 2020) as it transforms the traditional network architecture into an independent setup where the control plane is separated from the data plane, allowing greater control and programmability functions to the network administrator (Malik *et al.*, 2020).

1.2.1 Software-defined Networking

The existing architectures of space systems are inflexible due to their dependence on hardware (Bertaux et al, 2015). SDN brings flexibility, automation, and customization to space systems (Ferrús et al, 2016; Bertaux et al, 2015). Recent literature has introduced the concept of applying SDN to space systems to benefit from the features of SDN. SDN enables arbitration of resources, e.g., a ground station operator to dynamically switch mission operators to their allocated antenna system at the scheduled time (Liu et al, 2020). SDN provides effective traffic scheduling for space systems (Li et al, 2016). In addition, the SDN-based space system "architecture integrates functions such as data routing, resource allocation, network failure and security monitoring in the satellite network into the controller under the concept of SDN" (Liu et al, 2018). However, these great benefits of SDN come with security vulnerabilities. For instance, the SDN control plane poses a great vulnerability because it is the point of configuration and administration of the entire network and can be a single point of failure during an attack. Unfortunately, SDN vulnerabilities are inevitably transferred to space systems. These vulnerabilities expose space systems to the disruption of network services or accessibility and eavesdropping of signals transmitted between space systems and ground stations (Shadbolt, 2021). There is a need to secure SDN-based space systems, for they enable the connection and efficiency of critical systems. Consequently, we propose intelligent security control that will protect space systems from known and unknown malicious activities.

1.2.2 Cyber threat landscape

Cybercriminals have improved their attack strategies, and this has produced novel attacks that traditional security controls are unable to withstand (Kaloudi & Li, 2020). Cybercriminals have started to integrate Artificial Intelligence (AI) techniques to enhance the impact and ease of performing more powerful and extensive cyber-attacks (Kaloudi & Li, 2020). The use of AI to perform cyber-attacks has bred intelligent attacks that require intelligent security controls. Additionally, the cyber threats faced by space systems originate from electronic and digital sources and kinetic and physical sources and from inside or outside the space system. Thus, the cyber threat landscape for space systems has broadened, leaving the space system exposed to cyber-attacks.

1.3 Research objective and Research questions

The main objective of this research is to develop intelligent security controls for integrated SDN-based space systems. This research aims to answer one major question, which is:

1. *How can intelligent security controls for integrated SDN-based space systems be developed and implemented?*

This research question is supported by a series of ancillary sub-questions:

1. *How is space system security defined and mapped?*
2. *What are intelligent space systems?*
3. *What are SDN vulnerabilities and how are they mitigated?*
4. *How is SDN used for the flexible integration of space and terrestrial systems?*
5. *What kind of attacks is SDN subject to?*

2. Literature review

In this section, we present a review of previous work in our multi-disciplinary domain. Firstly, we analyse work that has examined space systems in context and the cyber threats they face. Secondly, we discuss literature that has focused on SDN, its benefits in contrast to traditional networks, and its vulnerabilities. Thirdly, we present a review of previous work on the cyber threat landscape. It is by reviewing this literature that we identified the

research gap to be addressed by this research. We also explore the potential use of deep-learning-based intrusion detection solutions for our research context and research objective.

2.1 Space systems

2.1.1 Space systems context

Space systems play a major role in the digital communication era. There is an increased demand for space systems to enhance "ubiquitous broadband service and remote sensing capacity" (Pavur & Martinovic, 2020). Fortunately, the procurement and launching of space systems have become so inexpensive that even new organizations in the space industry can afford them.

2.1.2 Space systems security domain

Any component of a space system is a potential attack vector (Falco, 2018). Space systems are vulnerable to cyber-attacks such as hijacking, DDoS, and ransomware.

2.2 Software-defined Networking

2.2.1 Software-defined Networking context

Software-defined Networking (SDN) has made a dramatic impact in the computer networking area. This can be attributed to its scalability, cost-effectiveness, and centralised intelligence (Javeed, Gao & Khan, 2021). SDN has demonstrated major benefits and it has been adopted by tech giant companies such as Google and Microsoft. The scalability of SDN enables organizations to easily adapt to changes within their network infrastructure in response to network needs. Since SDN is vendor-independent, an organization can configure or change the device software without having to replace the hardware (Javeed, Gao & Khan, 2021).

2.2.2 Software-defined Networking architecture

The SDN architecture consists of three planes namely, the application, control, and data plane. According to (Liu 2016), the SDN architecture "solves the bottleneck problem of large delay in response to end-to-end transmission in the big data environment by the caching function of the network node". The decoupling of the data plane from the control plane has "simplified network control and improves service deployment flexibility" (Liu 2016).

2.2.3 Software-defined Networking Security

Akhunzada et al (2015) state that "the integrity and security of SDNs remain unproven when it comes to the placement of management functionality in a single centralised virtual server." Akhunzada et al (2015) provide a way to "classify the state-of-the-art security solutions by devising a thematic taxonomy considering SDN layers/interfaces, security mechanisms, simulation environments, and security objectives."

2.3 Cyber Threat Landscape

The word cyber-security encompasses several very different considerations; thus the cyber threat landscape will also depend on a range of factors for a given country. The priorities and potentials for addressing cyber threats will vary among countries and actors within a country, as they have different national, social, economic, and organizational priorities. The cyber threat landscape is composed of eight foundational elements, some of which are technical and others non-technical, and these elements are represented as vectors of attack and response as depicted in Figure 4. This begins to answer questions concerning the nature of the cyber threat landscape faced by companies or countries as they design, develop, launch, fly and sustain intelligent space systems.

Factors affecting the cyber threat landscape of intelligent space systems include the need to secure people, processes, and tools and, as is often encountered, space systems security is not a simple issue of telecommunications security. In an era of borderless networks, one is faced with the weaponization of networking and the Internet, targeted attack on all kinds of IoT devices and commercial and Defence platforms

and the use of offensive cyber warfare or cyber effects in the Grey Zone between a declared war and intelligence operations.

At an organisational, and management level, there is often a lack of understanding of cyber threats and a lack of a security culture. Many smaller companies have little or no cyber threat understanding or protection. It has been found that many Critical Infrastructure companies lack good communication between the engineering, ICT and OT section and have poor security policies or regulations (Slay & Miller, 2007).

Figure 4: Eight vectors of attack and response (Slay & Austin, 2018)

One useful method to produce a mapping of the cyber threat landscape of a given technical context is to map the threat landscape across a range of technical and socio-technical components. This can be considered, for example, by using an old mapping of the domains of cyber security as developed by ISC^2, which are; "Access Control Systems and Methodology; Telecommunications and Network Security; Business Continuity Planning and Disaster Recovery Planning; Security Management Practices; Security Architecture and Models; Law, Investigation, and Ethics; Application and Systems Development Security; Cryptography; Computer Operations Security; and Physical Security" (ISC^2).

Thus, when considering the cyber threat landscape for an intelligent space system the obvious features of network security and telecommunications security need to be considered as do features such as the security of the applications and systems used by or drawn on by the space system and the appropriate use of cryptography. Less obvious security threats emanate from business continuity issues (how will a company respond if its satellite is hacked?) and those of cyber law and ethics.

2.4 Intelligent Security Controls for Software-defined Networking Space Systems

The Internet of Things (IoT) allows the connection of physical and virtual objects integrated with sensors and technologies that accommodate the exchange of data between devices worldwide over the Internet (Krishna et al, 2021). Smart satellite networks connect IoT devices by providing remote communication between devices and systems, as well as the extension of coverage to areas without Internet and cellular network. Smart satellite networks provide these features to IoT devices by amplifying signals that are transmitted from the sensors on the ground and transmitting them back to earth (Al-Hawawreh et al, 2021). It is estimated that IoT devices will be 25.44 billion by 2030 globally (Krishna et al, 2021). This increase in IoT devices has become a challenge for security due to unencrypted traffic, the difference in device firmware and integrated security features. These loopholes in IoT devices essentially affect technologies such as space systems which incorporate the smart or autonomous feature, leaving them vulnerable to the disruption of network services or accessibility and eavesdropping of signals transmitted between the smart satellite and the ground station to name a few issues (Shadbolt et al, 2021).

Smart satellite networks experience the challenge of inflexible network management due to their use of traditional network features and architectures (Li et al, 2016) that fail to adapt to the demands of bandwidth, computing and storage of current applications. To resolve this problem, the adoption of SDN in smart satellite networks can greatly provide scalability and flexible networking architecture that is required by critical applications such as smart satellites. SDN is one of the most promising evolving network technologies Khairi et

al, 2018) as it transforms the traditional network architecture into an independent setup where the control plane is separated from the data plane, allowing greater control and programmability functions to the network administrator (Dey & Rahman, 2019). However, these great benefits of SDN come with major security vulnerabilities. The SDN control plane poses a great vulnerability because it is the point of configuration and administration of the entire network and can be a single point of failure during an attack. There is a need to secure smart satellite networks with intelligent security controls, as they are a critical technology that supports the efficiency of IoT device connectivity.

3. Potential Solution

Based on our analysis above, intelligent security controls are thus needed for the assurance of SDN-based space systems and services. The security control proposed here is an Intrusion Detection System (IDS) with the intelligence to adapt to evolving threats. Development of the IDS is a three-stage process.

Stage 1 – Development of an SDN testbed: An SDN testbed is necessary because existing datasets such as UNSW-NB15 (Moustafa & Slay, 2015) and CSE-CIC-IDS2018 (Leevy & Khoshgoftaar, 2020) are useful for the data plane, but do not cover the control plane.

Despite the benefits of SDN mentioned in Sec. 1, SDN in its centralised form introduces a single point of failure/vulnerability. Distributed SDN can address this issue, in addition to the issues of scalability and reliability (Dixit et al, 2013). In distributed SDN, the control plane is physically distributed, but the control plane can either be logically centralised or logically distributed (Bannour et al, 2018). Over the last decade, a plethora of distributed SDN platforms have been designed and developed. For example, the Open Network Operating System (ONOS) by the Open Networking Foundation (ONF) is an open-source, extensible, modular, distributed SDN platform that implements a logically centralised control plane (Berde et al, 2014).

An SDN testbed based on ONOS will be developed, in integration with a satellite network simulator, to simulate networking scenarios. Candidate satellite network simulators include EXata, Systems Tool Kit (STK) (Li et al, 2016), Satellite Network Simulator 3 (SNS3) and OPNET (Liu et al, 2020). The attack surface of this testbed will be analysed and based on this analysis, novel attacks will be discovered.

Stage 2 – Design of an IDS for the testbed: The proposed IDS adopts the contemporary, hybrid design of combining signature-based detection and behaviour-based detection.

Against known attacks (Khairi et al, 2018; Haider et al., 2020; Malik et al, 2020; Javeed et al, 2021), features of these known attacks will be determined through feature selection and used to develop correlation rules and train supervised learning algorithms.

Against the novel attacks discovered in Stage 1, an anomaly detection scheme will be developed. The No Free Lunch Theorem (Wolpert & Macready, 1997) implies no machine learning algorithm is universally better than any other, and thus simply adopting a state-of-the-art algorithm in the anomaly detection literature is inadequate.

To support the development of the proposed algorithms, network traffic will be generated using the SDN testbed developed in Stage 1, cleaned and split into training, validation and test datasets. Deep neural network architectures will be standard as deep features are efficient to extract and as effective as handcrafted features. Furthermore, continual learning of evolving threats will be achieved through adaptive model updates (Stocco & Tonella, 2020). To cope with the large data volume and processing power requirements, National Computational Infrastructure's Gadi supercomputer will be used.

Stage 3 – Testing of the IDS: k-fold cross-validation (Goodfellow et al, 2016) will be used to characterise the performance of the algorithms developed in Stage 2 in terms of the confusion matrix (for classification of attack types), detection accuracy, detection precision (capturing the false positive rate), detection recall (capturing the false negative rate), area under the receiver operating characteristic curve, computational complexity as well as memory consumption. Table 1 defines the metrics that will be used for testing the IDS.

Table 1: Evaluation metrics used to assess the performance of the proposed DL-based IDS

Metrics	Description
Confusion matrix	This measures the performance of a model based on TP, FP, TN and FN values.
Accuracy (A)	Returns the probability that an instance is correctly classified by the IDS.

Precision (PR)	The ratio of correctly classified attack instances (TP), in front of all classified flows (TP+FP).
Recall (RC)	The ratio of correctly classified attack instances (TP), in front of all generated flows (TP+FN).
Loss	This is an indication of the model's prediction ability. If the model has an excellent prediction, the loss value is zero or closer to zero; else, the loss value is far greater than zero.
True Positive Rate (TPR)	Measures how often the model correctly predicts positive instances.
False Positive Rate (FPR)	Measures how often the model incorrectly predicts positive instances.
ROC AUC curve	Measures the false alarm rates against the actual predicted rates, showing how well a model can make a distinction among classes.
Central Processing Unit (CPU) usage (%)	Measures the capacity of the CPU used in training the model.
Train and Test Time	This is the time taken for training and testing the model.

4. Conclusion

Space systems are important to critical systems such as the military, weather services, and global timing. Remote communication between devices and systems, as well as the extension of coverage to areas without Internet and cellular network, are enhanced by intelligent space systems. Due to space systems using terrestrial networks, there are limitations such as inflexibility and complex network management. Thus, we propose the integration of SDN and space systems to take advantage of the advancements provided by SDN. SDN is a communication network approach that enhances a network's flexibility, scalability, and programmability. However, SDN and space systems, individually and when combined, are at risk of cyber-attacks that intend to maliciously compromise the confidentiality, integrity, and availability of SDN and space systems. Thus, we propose intelligent security controls that will protect SDN-based space systems from the rising novel cyber-attacks.

References

Aguirre, M.A. (2013) 'Introduction to Space Systems: Design and Synthesis', *Springer*, 5(3), pp. 248–253. Available at: https://doi.org/10.1007/978-1-4614-3758-1.

Akhunzada, A. *et al.* (2015) 'Securing software defined networks: Taxonomy, requirements, and open issues', *IEEE Communications Magazine*, 53(4), pp. 36–44. Available at: https://doi.org/10.1109/MCOM.2015.7081073.

Al-Hawawreh, M., Moustafa, N. and Slay, J. (2021) 'A threat intelligence framework for protecting smart satellite-based healthcare networks', *Neural Computing and Applications*, 5. Available at: https://doi.org/10.1007/s00521-021-06441-5.

Bannour, F., Souihi, S. and Mellouk, A. (2018) 'Distributed SDN Control: Survey, Taxonomy, and Challenges', *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 333–354. DOI: 10.1109/COMST.2017.2782482.

Berde, P. et al. (2014) 'ONOS: Towards an Open, Distributed SDN OS', *Proceedings of the Third Workshop on Hot Topics in Software Defined Networking, HotSDN* '14, New York, NY, USA, Association for Computing Machinery, pp. 1–6. DOI: 10.1145/2620728.2620744.

Bertaux, L. *et al*. (2015) 'Software defined networking and virtualization for broadband satellite networks', *IEEE Communications Magazine*, 53(3), pp. 54–60. Available at: https://doi.org/10.1109/MCOM.2015.7060482.

Bradbury, M. *et al.* (2020) 'Identifying Attack Surfaces in the Evolving Space Industry Using Reference Architectures', *2020 IEEE Aerospace Conference*, pp. 1–20. Available at: https://doi.org/10.1109/AERO47225.2020.9172785.

Dey, S.K. and Rahman, M.M. (2019) 'Flow Based Anomaly Detection in Software Defined Networking: A Deep Learning Approach With Feature Selection Method', *4th International Conference on Electrical Engineering and Information and Communication Technology, ICEEICT*, pp. 630–635. Available at: https://doi.org/10.1109/CEEICT.2018.8628069.

Dixit, A. *et al.* (2013) 'Towards an Elastic Distributed SDN Controller', in *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, 43(4), pp. 7–12. Available at: https://doi.org/10.1145/2491185.2491193.

Falco, G. (2018) 'Cybersecurity Principles for Space Systems', *Journal of Aerospace Information Systems*, (December 2018). Available at: https://doi.org/10.2514/1.I010693.

Ferrús, R. *et al.* (2016) 'SDN/NFV-enabled satellite communications networks: Opportunities, scenarios and challenges', *Physical Communication*, 18, pp. 95–112. Available at: https://doi.org/10.1016/j.phycom.2015.10.007.

Goodfellow, I., Bengio, Y., and Courville, A. (2016) 'Deep Learning', *MIT Press.* Available at: http://www.deeplearningbook.org.

Khairi, M. et al. (2018) 'A Review of Anomaly Detection Techniques and Distributed Denial of Service (DDoS) on Software Defined Network (SDN)', *Engineering, Technology & Applied Science Research*, 8. Available at: https://doi.org/10.48084/etasr.1840.

Haider, S. *et al.* (2020) 'A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks', *IEEE Access*, 8, pp. 53972–53983. Available at: https://doi.org/10.1109/ACCESS.2020.2976908.

Javeed, D., Gao, T. and Khan, M.T. (2021) 'SDN-Enabled Hybrid DL-Driven Framework for the Detection of Emerging Cyber Threats in IoT', *Electronics*, 10(8), pp. 1–16. Available at: https://doi.org/10.3390/electronics10080918.

Kaloudi, N. and Li, J. (2020) 'The AI-Based Cyber Threat Landscape : A Survey', *ACM Computing Surveys*, 53(1), pp. 1-34. Available at: https://doi.org/10.1145/3372823.

Krishna, R.R. *et al.* (2021) 'State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions', *Sustainability*, 13(16), pp. 1–45. Available at: https://doi.org/10.3390/su13169463.

Leevy, J.L. and Khoshgoftaar, T.M. (2020) 'A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 Big Data', *Journal of Big Data*, 7(1), p. 104. Available at: https://doi.org/10.1186/s40537-020-00382-x.

Li, T. *et al.* (2016) 'Using SDN and NFV to Implement Satellite Communication Networks', *Proceedings - 2016 International Conference on Networking and Network Applications, NaNA 2016*, pp. 131–134. Available at: https://doi.org/10.1109/NaNA.2016.22.

Liu, M. *et al.* (2020a) 'Large-Scale Small Satellite Network Simulator: Design and Evaluation', *2020 3rd International Conference on Hot Information-Centric Networking, HotICN 2020*, pp. 194–199. Available at: https://doi.org/10.1109/HotICN50779.2020.9350838.

Liu, Y. *et al.* (2020b) 'A Shared Satellite Ground Station Using User-Oriented Virtualization Technology', *IEEE Access*, 8, pp. 63923–63934. Available at: https://doi.org/10.1109/ACCESS.2020.2984485.

Liu, Z. *et al.* (2018) 'Satellite Network Architecture Design Based on SDN and ICN Technology', *2018 8th Proceedings of 2018 IEEE 8th International Conference on Electronics Information and Emergency Communication, ICEIEC*, pp. 124–131. Available at: https://doi.org/10.1109/ICEIEC.2018.8473548.

Malik, J. *et al.* (2020) 'Hybrid Deep Learning: An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN', *IEEE Access*, 8, pp. 134695–134706. Available at: https://doi.org/10.1109/access.2020.3009849.

Manulis, M. et al. (2020) 'Cyber security in New Space: Analysis of threats, key enabling technologies and challenges', International Journal of Information Security, 20(3), pp. 287–311. Available at: https://doi.org/10.1007/s10207-020-00503-w.

Moustafa, N. and Slay, J. (2015) 'UNSW-NB15: A Comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)', *2015 Military Communications and Information Systems Conference, MilCIS*, pp. 1–6. Available at: https://doi.org/10.1109/MilCIS.2015.7348942.

Ormrod, D., Slay, J. and Ormrod, A. (2021) 'Cyber-Worthiness and Cyber-Resilience to Secure Low Earth Orbit Satellites', *International Conference on Cyber Warfare and Security*, pp. 257-266. Available at: https://www.proquest.com/docview/2505729841?pq-origsite=primo.

Pavur, J. and Martinovic, I. (2020) 'SOK : Building a Launchpad for Impactful Satellite Cyber-Security Research', pp. 1–32. Available at: https://doi.org/10.48550/arxiv.2010.10872.

Plotnek, J. and Slay, J. (2022) 'Space Systems Security: A Definition and Knowledge Domain for the Contemporary Context', *Journal of Information Warfare*, 21(3), pp. 103–119. Available at: https://www.jinfowar.com/journal-issue/volume-21-issue-3.

Pradhan, A. and Mathew, R. (2020) 'Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN)', *Procedia Computer Science*, 171, pp. 2581–2589. Available at: https://doi.org/10.1016/j.procs.2020.04.280.

Shadbolt, L. (2021) *Technical Study Satellite Cyberattacks and Security*, *HDI Global Specialty SE*. Available at: https://www.hdi.global/infocenter/insights/specialty/technical-study/.

Slay, J. and Austin, G. (2018) 'Development in Training and Education for Australian Cyber Security : Filling the Gaps', *Journal of The Colloquium for Information System Security Education (CISSE)*, 5(2), pp. 1–27. Available at: https://cisse.info/journal/index.php/cisse/article/view/80.

Slay, J. and Miller, M. (2007) 'Lessons Learned from the Maroochy Water Breach', *Critical Infrastructure Protection*, 253, pp. 73–82. Available at: https://doi.org/10.1007/978-0-387-75462-8_6.

Stocco, A. and Tonella, P. (2020) 'Towards Anomaly Detectors that Learn Continuously', *ISSREW 2020*, pp. 201-208. Available at: https://doi.org/10.1109/ISSREW51248.2020.00073.

The International Information Systems Security Certification Consortium, Inc., (ISC)², Certification Programs, CISSP Domains. Available at: https://www.isc2.org/cissp-domains/default.aspx.

Wolpert, D. H. and Macready, W. G. (1997) 'No free lunch theorems for optimization', *IEEE Transactions on Evolutionary Computation*, vol. 1, no. 1, pp. 67–82. DOI: 10.1109/4235.585893.