A Link Planning and DDoS Attack Detection in SDN Based Integrated Space-Terrestrial Networks

Deepa Vickramasingam and Sivakumar Bangar*
SRM Institute of Science and Technology, Kattankulathur, India; Email: dv1018@srmist.edu.in (D.V.)
*Correspondence: sivakumb2@srmist.edu.in

***Abstract*—It is expected that 5G networks would require both great dependability and stability as fundamental requirements. The introduction of a satellite component into LTE (long term evolution) networks has emerged as an attractive solution for meeting these requirements. This will enable the provision of backup interoperability to essential base stations and the routing of traffic away from crowded locations. During peak hours, the demand for their terrestrial links must be increased or even adopted in the case of anticipated breakdown or repair. Integrated space-terrestrial networks have shown to be an advantageous design due to its broad coverage and high precision. Designing a network routing plan is not a straightforward process when the complex relative motion of low-earth-orbit (LEO) satellites and unmanned aircraft systems (UAS) is considered (UAS). To be more explicit, the major difficulty is discovering how to locate acceptable connections in time-varying network settings to offer reliable and effective UAS data transmission. This study begins with a motion analysis of satellites and UASs to discover which access satellites are most suited for usage with UASs. This is done in order to resolve the aforementioned problem. In order to provide an effective and reliable intersatellite link (ISL) deployment between access satellites, double exponential smoothing (DES) is afterwards proposed as an alternative to traditional routing. This is required to guarantee the timely delivery of UAS data. The simulation results demonstrate that the proposed DES approach is both feasible and effective. A time series-based method known as DES is used to compute the port information in an adjustable manner, and an algorithm known as SVM (Support Vector Machine) is utilized to determine if a Distributed Denial of Service (DDoS) attack has really occurred. Experiments that are typical demonstrate that the UAS may greatly reduce the controller's workload while maintaining dependable detection accuracy.**

***Keywords*—intersatellite link, software-defined networks, unmanned aircraft systems (UAS), DDoS attack, time varying network, integrated space-terrestrial networks**

I. Introduction

It is widely acknowledged that one of the most important requirements for 5G is pervasive broadband connectivity [1, 2] that can be extended to low-density and rural regions, as well as long-distance transportation (such as aero planes). Reconsideration is being given to role that satellite communications may play in the ecosystem that will eventually support 5G [2, 3]. In addition, 5G networks increasingly employed as the principal method for providing applications and meeting the demands of various industries, as well as for achieving network accessibility.

Incorporating sufficient redundancy into the network is one of the strategies that may be used to cut down on the network's susceptibilities. In this case, Satellite connectivity can also be deployed as a capacity to operate in challenging scenarios. The Satellite links might give additional bandwidth to backup connectivity and critical networks as well as to divert traffic from congested locations. This would allow the capacity of terrestrial links to be supplemented during peak times or even replaced in the event of total or partial failures, as well as for emergency mobile cell deployments.

In this regard, the development of satellite gateways and terminal segment systems are closed solutions towards more open architectures based on Software Defined Networking (SDN) and Network Function Virtualization (NFV) [4] technologies emerge as a crucial step, not only to bring into the satellite industry the benefits associated with the currently being implemented improvements in network softwarization technologies. In general, 5G systems are progressively integrating SDN technology to facilitate control and management of networking services. This is occurring in several distinct ways.

Therefore, satellite networks must be outfitted with controller and management/infrastructure functions and API interfaces/protocols that are compatible with the prevalent SDN architectures and technologies being utilized in 5G [5]. This is required in order to identify a full networking notion, in which the behavior of the complete space-terrestrial network may be defined in a compatible and programmable manner.

Consider the shortcomings below (Fig. 1), in this paper, we provide a time-series approach that is incorporated into the GEO (SDN controller) and DDoS [6-8] attack detection and protection strategy that is based on statistical analysis. This will allow us to handle the issue as follows:

Manuscript received December 26, 2022; revised January 13, 2023, accepted February 1, 2023.

doi:10.12720/jcm.18.4.267-273

(1) Considering the time-dependent graph [9] as a resource during the construction of integrating space-terrestrial network. It has been proposed that the UAS technique utilized to create an intersatellite link, which can also improve the link's reliability.

(2) A simple and effective approach for detection is presented, which detects assault events from the victim's perspective and localizes the attackers. Because we handle each set of flow rules broadcast and received separately by DES, it is reasonable to anticipate that our detection systems can identify assaults with great performance.

(3) This study aims to address the excessive resource consumption and inefficiency of current DDoS detection methods within the context of SDN.

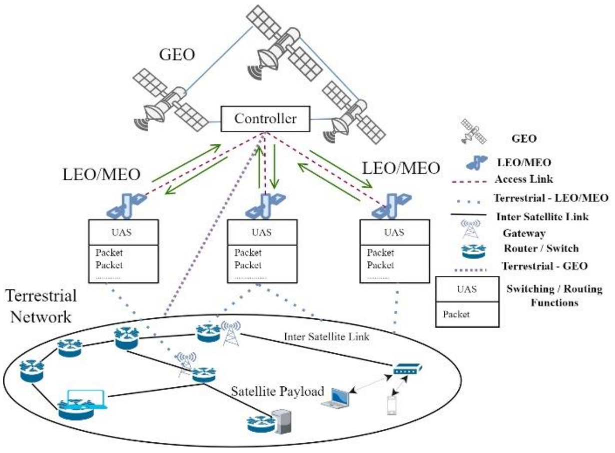

Figure 1. System design of integrated space-terrestrial networks.

A. *Motivation*

The high reliability is associated with satellite interactions and persuasive assertion that should be taken advantage to fulfil these requirements. This would improve the accessibility and dependability of transmission networks, which supplement terrestrial systems, Kato and Fadlillah, *et al.* [10] and are often more susceptible to outages due to natural or man-made disasters. Given the extent to which effective disaster mitigation depends on communication infrastructure, this is of particular relevance in public safety and disaster relief operations. In such a scenario, satellite capability may be offered as a static multihop capacity to any network node, and it may also be available in challenging post-disaster environments. This permits rapid deployment of emergency data communications based on truck or transportable network nodes, such as ground stations.

The remaining parts of the article are structured as described below. In the section II, we provide a summary of the previous research that has been published. In Section III, about the background knowledge required for the linked technologies. In Section IV, an explanation of our DDoS attack detection and system in more detail. In the next Section V, discuss the results of the performance assessment of our system and Section VI concludes the paper.

II. Related works

The SDN architecture is considered for inclusion in the route planning of satellite networks in order to enable the exercise of global control over satellite networks. In Shi and Cao *et al*. [11], the authors created a cross-domain SDN architecture for space-terrestrial integrated networks with several layers. In this design, the writers identified several impediments and unsolved issues that needed to be addressed. The intersatellite connection distribution, which includes satellites and UAV, has been the subject of several extensive studies. Broadband LEO satellite communications are described in Su and Liu *et al*. [12], which provides an overview of several important designs and technologies. Fakoor and Amozegary *et al.* [13] presented a complete analytical solution to the problem of satellite relative motion, which guided the development of the ISL (Inter Satellite Link). The authors of [14] provided an MPWLC based on service likelihood and a successful deployment of the connection. However, the factors that have the potential to affect the link quality were not explored in detail. In [15], a technique for determining the shortest path from a source satellite to a destination satellite was presented, and when routing priority-based traffic in LEO satellite networks, both the shortest path and link congestion were taken into account. The authors of [16] proposed an SDN-based end-to-end fragment-aware routing solution in a LEO satellite-terrestrial network to reduce wavelength fragmentation and bandwidth consumption.

Li and Zhou *et al.* [17] established a software-defined framework for satellite communication using the global control structure of software-defined networks (SDN) to realize the routing algorithm design.

Notably, Braga and E. Mota *et al.* [18] provided a lightweight approach that periodically requests flow rules statistics and turns them into 6-significant characteristics. The sample is then classified utilizing the Self-Organizing Map (SOM) technique. Using the SDN controller and sFlow agents, Hu, and P. Hong *et al*. [19] acquire information about network traffic. Then, an entropy-based approach is used to quantify the network's characteristics, and an SVM classifier is applied to identify any anomalies inside the network. The machine learning-based systems also seek to identify packet-in messages that utilizes flow rules. Authors of [20, 21], made a different approach to identify the victim and offender. Their method employs spatial adaptation to regulate diverse fluxes. In particular, coarse-grained rules for tracking expected flows and fine-grained rules for tracking traffic with a high likelihood of being the target of a DDoS attack. The strategy of Yan encourages the detection algorithm to merely monitor traffic destined for the questionable application.

III. Background

In this section, the theoretical underpinnings of the many notions that will be applied in the article. First, we will go through the link installations of UAS and provide the significant challenges for the routing analysis. After providing a quick introduction pertaining to the protocol, discussing the double exponential smoothing (DES) model and mathematical paradigm that underlies in it. These ideas are key to the identification of DDoS assaults within the context of this research.

A. Accessing Satellite Link Selection

The selection of a control satellite should be done with the end purpose of achieving steady real-time control of the UAS. In addition to this, it ought to make the data transfer between satellites easier. It's possible that data transmission and signal attenuation will be the most important aspects to consider when choosing a control satellite. This is how the particular analysis breaks down.

During the data transmission, the interaction between the control satellite *A* and the UAS data is continual, and the satellites continue to control the UAS constantly. If the data transmission connection between A and UAS is created, the maximum transmission rate will be restricted to maximum Mbps. We will assume, without limiting our scope, that the transmission rate is at its maximum value during the data exchange and that it does not vary. Then, the amount of time it takes for the control satellites and the UAS to link should be taken into consideration. The stability of the data transmission is positively correlated with the length of time that a connection is active. Therefore, visibility conditions will determine the maximum connection time *T* that may be maintained between satellite *A* and UAS. C_T represents the maximum number of nodes connected with transmission time capacity to satellite. For the UAS, U_s specifies the maximum quantity of data that can be delivered to the satellite. A higher C_T number suggests that the satellite can gradually gather more conflict data before the next accessing, which may aid control satellites better with data processing. This is because the satellite has greater capacity and standardize the value of C_T as $C_{T\text{-}A\text{-}n}$, so that the computation may be done more easily. The value of *n* is from 0 to 1.

$$C_{T-A-n} = \frac{C_{T}-A}{C_{T-A-max}} \tag{1}$$

When modelling a time-variable satellite network, an investigation of the physical visibility of the satellites may help simplify the topology in each time slot. It is dependent on the positions of the Earth and the satellites in relation to one another. According to what is depicted in Fig. 2, we determine *R* to be the radius of the Earth, *S* to be the satellite that orbits the Earth, and *D* to be the distance between satellites. The following is a list of the satellites' locations in relation to one another:

- *D1* is the distance that can be travelled from satellite *S1* to satellite *S2*, and *P1* is the distance that can be travelled from *A* to *S1*, *S2*. If the following equation is true, then the two satellites are able to communicate with one another through an inter-satellite link connection since they are noticeable.

$$P1 \geq R \tag{2}$$

- *D2* represents the distance that separates satellites *S2* and *S3*, whereas *P2* indicates the distance that separates *A* and *S2*, *S3*. If the following equation is true, then the satellites are not physically observable, and it is not possible to create linkages between the satellites.

$$(P2 < R) \cap 90° \tag{3}$$

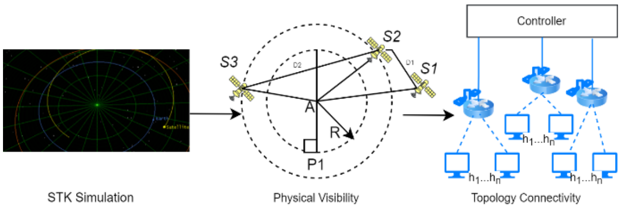

Figure 2. Deploy of Time-variable Satellite Network.

Following, the satellite link model may be characterized by the *G (S, T, E)* time-dependent graph [22], in where *S* is the satellite node, *E* is the edge of node, and *T* is the time interval. Because of the visibility in the real world, *G* is able to assist simplify the sets of Satellite node *(S)* and *(E)*. After that, the routing method may be used to locate an appropriate route of whole link. If the connection time between two satellites that are near to one another is T_n, then the connection time *T* for the whole link is calculated as follows:

$$T = \min\,(1{,}2, \ldots \ldots T_i\,) \tag{4}$$

The vast majority of research on ISL routing, however, are not applicable to construction of integrating space-terrestrial network situations since the control satellites are fixed nodes in G. This makes the majority of the studies unsuitable. In a time-dependent integrating space-terrestrial network, we discover that the ISL LEO satellites in each orbital is more consistent, but the ISL linking nearby orbits is shifting. This is because of the time-dependent nature of the integrating space-terrestrial network. There are crucial steps that must be taken during the connection planning phase of integrating space-terrestrial network [23] in order to guarantee the reliability of data transfer. The first is choosing which control satellites to use, and the second is choosing which relay nodes through the UAS information. Because the satellites in the same orbit keep a reasonably constant distance from one another, consistent data transmission rates are possible.

B. Double Exponential Smoothing (DES)

The DES algorithm is a method for predicting trends with a time series approach. The goal is to determine the link between the most recent data and previous values in order to arrive at an accurate forecast of the future state. The time constant and choosing initial smoothened value are two conditions that must be satisfied before the DES model may be used.

When there is a discernible pattern in the data, exponential smoothing fails spectacularly. In these circumstances, a number of techniques were developed and given names like "double exponential smoothing" or "f''(x) (second-order) exponential smoothing." The recursive application of an exponential filter twice, which is why the technique is called "double exponential smoothing." The purpose of include a factor in double exponential smoothing is to take into consideration the chance that a series may demonstrate a trend of inclination feature up to date. Let $x_t$be a data sequence at time T=0, and a typical $f'(\text{x})$ DES model is represented as,

$$f'(\text{x}) = s_t + m.f_t \tag{5}$$
$$s_t = \alpha x_t + (1-\alpha)(s_{t-1} + f_{t-1}), \tag{6}$$
$$f_t = \beta(s_{t-1}) + (1-\beta)(f_{t-1}), \tag{7}$$

where,
s_t – first data smoothed value for time T, $s_0 = x_0$,
f_t – finest estimate inclination value at time T,
$m > 0$ – based on data availability at time T,
$\alpha(0 < \alpha < 1) -$ data smoothed factor,
$\beta(0 < \alpha < 1) -$ inclination smoothed factor.

$$f''(\text{x}) = e_t + m.f_t \tag{8}$$
$$e_t = 2s'_t - s''_t, \tag{9}$$
$$f_t = \frac{\beta}{1-\beta}(s'_t - s''_t), \tag{10}$$

where,
e_t – estimated data smoothed value for time T

The weight coefficients are denoted by the α (link delay) and β (connection time) respectively. The value of the weight coefficient may be altered to respond for particular requirements. The satellite with the highest e_t value is chosen to serve as the node for satellite. This choice is made from among all of the potential alternative satellites. Since received each set of flow rules or flow status *(the speed of source IP(SSIP), the speed of source port (SSP), the speed of flow entries (SFE), the standard deviation of flow packets (SDFP), the deviation of flow bytes (DFB), the ratio of pair-flow (RPF))* [24][25][26] individually in the GEO controller are stored and used eventually in next stage.

C. Support Vector Machine (SVM)

SVM is able to find the hyperplane in the high-dimensional space that best represents the data so it can categorize the associated class label. Because, SVM is easy to use, reliable, and resilient, it has found widespread algorithm in DDoS detection within the framework of SDN. Our solution will include the categorization and testing of the characteristics present on both the normal data and the attacker using a variety of different classifiers.

As our datasets are non-linear separable and a result of the presence of non-linear correlation in some features, a "non-linear SVM" kernel function was selected as the solution.

IV. Simulation and Results

A. Simulation Setup

With the help of the Satellite Tool Kit (STK) [27] simulator and Mininet emulation environment [28], the simulation is carried out on a deterministic integrated satellite-terrestrial platform. In order to ensure the theoretical concept, LEO satellite (60) model was developed with reference to the Iridium constellation. During this time, we sent a UAS in the STK direction from SRM University to Delhi and collecting dataset size of 1GB. After that, we link STK with Mininet to collect the satellite and UAS data as it is being connected. This is also where we do the calculations and comparisons of the suggested DES scheme and other approaches. By acquiring the datasets from connection and generate DDoS attacks through hping3 tool, is defined in respect of SYN Flood, DNS Amplification, SSDP Amplification, ACK Flood, UDP Flood, and ICMP Flood DDoS.

B. Connectivity and Feature Extraction

Physical Observation: In the simulation, we will evaluate the suggested DES which is relation to the other primary approaches, such as the longest connection time Dijkstra algorithm (LCT), and the route-finding using travelling salesman algorithm (RFT). The control satellite fleet of UAS is used across all three algorithms. In DES, the value 0.333 is assigned to each of the coefficients for α (link delay) and β (connection time). To begin, the amount of time it takes for transmission and the number of resources that controller satellites used are compared so that the total performance may be determined.

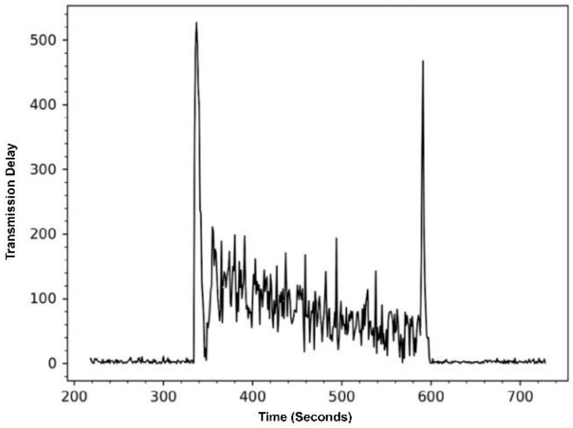

Figure 3. Transmission Delay Vs Time (Seconds).

As shown in Fig. 3, we determine the maximum transmission delay of the connection to be the amount of time it takes for data to be sent from the UAS to the final control satellites. By calculating, each technique several times and averaging the results, we may get an understandable depiction of the connection pattern. It can be observed that transmission delays are decreasing for all techniques over time. Since the LCT technique focuses on locating appropriate relay nodes to reduce the total of control satellite connection distance, both the DES and RFT methods have an excellent real-time data transmission capacity. This is in contrast to the DES method, which finds optimal relay nodes to minimize the link delay and connection time.

Feature extraction: Based on DES first-order exponential smoothing the extraction of a predetermined characteristics based on first-order intervals that represent samples of the flow from LEO are collected. These features are derived from the flow itself and the subsequent stage, which is the aggregation of the characteristics that were extracted are stored. More than one sample of the preset characteristics may be taken and logged within the one-second period, and the majority of the aggregated features can be computed throughout the course of the flow's lifespan. When the flow comes to an end, calculate the amount of time needed to make a choice.

Using OF (OpenFlow) switches as a gateway, the GEO controller will collect statistical data from the network edge points. The DES flow rules that are implemented to guarantee that data flows (LEO) are directed to the right area within the private network are given the greatest priority, while the general flow rules are put on the second-layer switches. Because we are utilizing a supervised classification model, we are able to train the model on a range of regular and abnormal traffic types and then utilize the learnt model to classify actual network flows.

C. Trace a DDoS Attack

In this step, we will go into more detail on the phase that consists of training (15,796 samples) and testing (10,681 samples). The controller is able to identify the switches and request the statistics from all of the OF gateway switches independently. After that, the controller can link the collected statistics to each flow by referring to the information contained in the packet header. The controller is responsible for organizing the network traffic that is carried by the switches. Once the stage has been reached, the module responsible for feature extraction begin to gather data from flow tables for each switch on a coefficient basis and will then extract their features.

After that, the feature is processed by the anomaly identification algorithm, which applies a time-series technique based on DES to provide an anomaly score to the sample. This score indicates how likely it is that the sample is affected by an abnormality. In the end, SVM detection system determines whether the instance being sampled is an instance of regular traffic or an instance of an attack.

V. Performance Metrics

We simulate a typical DDoS assault by using a variety of attack rates, and the constant idle-timeout value used for flow rule. The results and detection of the DDoS attacks with performance of our detection algorithm could be evaluated using Table I and accuracy, F1 score, and false-alarm rate-based metrics in Eqs. (11-13), respectively.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{11}$$

$$F1\ Score = 2 * \frac{Precision*Recall}{Precision+Recall} \tag{12}$$

$$False\ Alarm\ Rate = \frac{FP}{FP+TN} \tag{13}$$

TP: number of attack logs classified as attacks,

FP: number of valid logs that were categorized as attacks,

TN: number of legitimate logs classified as legitimate,

FN: number of valid attack logs that have been compiled.

TABLE I. Simulation Results

Algorithm	$TP\%$	$TN\%$	$FP\%$	$FN\%$
LCT	78.01	81.12	8.76	7.67
RFT	84.32	87.43	6.79	5.54
SVM	89.94	88.42	2.15	0.72

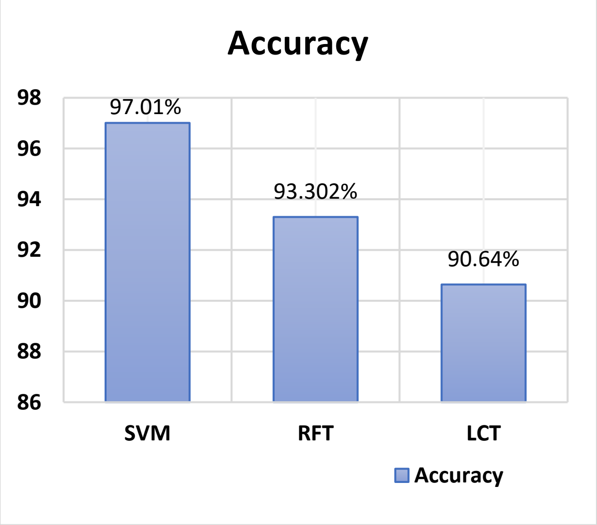

Figure 4. Comparative Accuracy of SVM, RFT, and LCT.

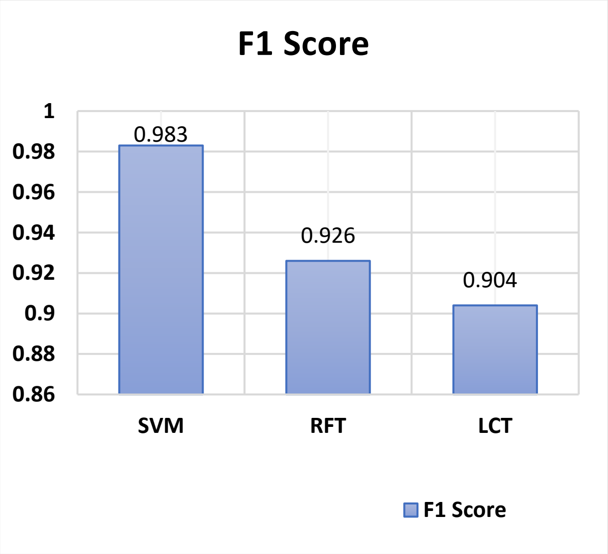

Figure 5. Comparative F1 Score of SVM, RFT, and LCT.

TABLE II: Evaluation Results of F1 Score

Algorithm	Precision $\left(\frac{TP}{TP+FP}\right)$	Recall $\left(\frac{TP}{TP+FN}\right)$	$F1\ Score$
LCT	0.899	0.910	0.904
RFT	0.92	0.938	0.926
SVM	0.976	0.9920	0.983

In Figs. 4-6 the comparative analysis of accuracy, F1 Score, False Alarm Rate for SVM, RFT, LCT are shown. We set the idle-timeout to various levels and conduct a series of tests. First, common DDoS attack types are picked to test the precision (shown in Table II.) of our system. SVM is also used as their classifier for different characteristics. Following their methodology, we replicated their findings and evaluated with DES. Since attacks with greater rates often result in more apparent abnormalities on both the attacker side and the victim side.

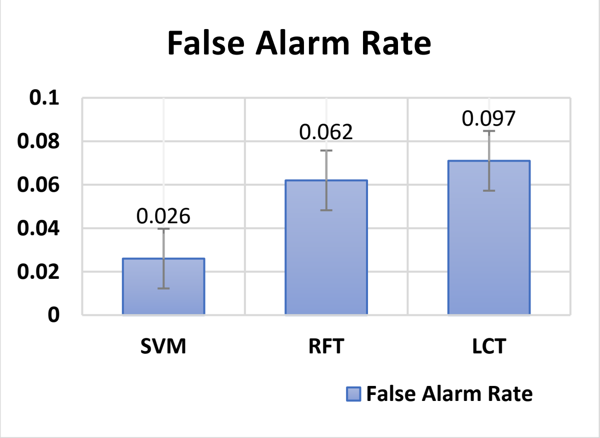

Figure 6. Comparative False Alarm Rate of SVM, RFT, and LCT.

Figs. 4-5 findings support our hypothesis that detection accuracy tends to rise as attack rate increases. The false-alarm rate (FAR) is a critical assessment factor for DDoS detection since a high FAR may start a mistake mitigation procedure, which affects how servers and clients normally communicate. Hence, the valid samples are collected and another portion of the legal dataset is replayed in order to get the FAR. The idle-timeout =6 seconds in order to save SDN resources.

VI. Conclusions and Future Work

In this paper, we investigated how to create an integrated satellite-terrestrial network utilizing SDN to detect DDoS assaults. A procedure of detecting congested flows and route-finding involving the selection of control satellites and the deployment of the ISL. When picking control satellites, it is necessary to take into account many crucial factors. Using a time-varying SVM model, we describe the DES approach for directing ISL deployment. This technique optimizes the network's data transmission efficiency. The simulation findings indicate that employing the DES protocol for UAS data transfer may improve its overall performance. In addition, DES's aptitude for dynamic modification enhances its dependability and dependability. Our suggested method may identify attacks from both the attacker's and the victim's perspectives. Using simulation testing, we were able to demonstrate that not only is the DES available in SDN environments, but that our detection approaches are also extremely reliable. Compared to previous models, we have obtained more accuracy, a higher F1 score, and a reduced false alarm rate here. The future plans include differentiating between other attack traffic and valid traffic in order to safeguard legitimate communication while also fighting against DDoS attacks.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Deepa Vickramasingam - Article Preparation, Design, Implementation. Sivakumar Bangar - Conceptual Analysis, Design, Review and approval, Language Editing.

Acknowledgment

The authors wish to thank School of Computing. This work was supported in part by a grant from SRM Institute of Science and Technology, Kattankulathur, India.

References

[1] A. Osseiran, F. Boccardi, B. Volker *et al.*, "Scenarios for 5G mobile and wireless communications: The vision of the METIS PROJECT," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 26-35, May 2014.

[2] F. Minucci, D. Verbryggen *et al.*, "Measuring 5G electric fields strength with software defined radios," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 2258-2271, 2022.

[3] C.-C. Teng, M.-C. Chen, M.-H. Hung, and H. -J. Chen, "End-to-end service assurance in 5G Crosshaul networks," in *Proc. 2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Daegu, Korea (South), 2020, pp. 306-309.

[4] L. Bertaux, *et al.*, "Software defined networking and virtualization for broadband satellite networks," *IEEE Communications Magazine*, vol. 53, no. 3, pp. 54-60, March 2015.

[5] F. Mendoza, R. Ferrús, and O. Sallent, "A traffic distribution scheme for 5G resilient backhauling using integrated satellite networks," in *Proc. 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Valencia, Spain, 2017, pp. 1671-1676.

[6] T. Ubale and A. K. Jain, "Survey on DDoS attack techniques and solutions in software-defined network," *Handbook of computer Networks and Cyber Security*, Springer, 2020, pp. 389–419.

[7] N. Meti, D. G. Narayan, and V. P. Baligar, "Detection of distributed denial of service attacks using machine learning algorithms in software defined networks," in *Proc. 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Udupi, India, 2017, pp. 1366-1371.

[8] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in cloud computing environments: a survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602-622, 2016.

[9] Y. Li *et al.*, "GraphDDoS: Effective DDoS attack detection using graph neural networks," in *Proc. 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, Hangzhou, China, 2022, pp. 1275-1280.

[10] N. Kato, Z. Md. Fadlillah *et al.*, "Optimizing space-air-ground integrated networks by artificial intelligence," *IEEE Wireless Communications*, vol. 26, no. 4, pp. 140-147, August 2019.

[11] Y. Shi, Y. Cao, J. Liu and N. Kato, "A cross-domain SDN architecture for multi-layered space-terrestrial integrated networks," *IEEE Network*, vol. 33, no. 1, pp. 29-35, January/February 2019.

[12] Y. Su, Y. Liu, Y. Zhou, J. Yuan, H. Cao, and J. Shi, "Broadband LEO satellite communications: Architectures and key technologies," *IEEE Wireless Communications*, vol. 26, no. 2, pp. 55-61, April 2019.

[13] M. Fakoor, F. Amozegary, M. Bakhtiari *et al.* "Relative tracking control of constellation satellites considering inter-satellite link," *Advances in Space Research*, vol. 60, no. 9, pp. 2021-2046, 2017.

[14] Z. Huang, Q. Zhang *et al.*, "DTN routing algorithm based on service probability and limited copy for satellite networks," in *Proc. 2017 16th International Conference on Optical Communications and Networks (ICOCN)*, Wuzhen, China, 2017, pp. 1-3.

[15] Y. Yang, G. Hu, F. Jin *et al.*, "Routing in LEO satellite networks over packets trapped by inter satellite-link switch," in *Proc. CST'17*, 2017, pp. 406- 415.

[16] Q. Guo *et al.*, "SDN-based end-to-end fragment-aware routing for elastic data flows in LEO satellite-terrestrial network," *IEEE Access*, vol. 7, pp. 396-410, 2019.

[17] T. Li, H. Zhou, H. Luo and S. Yu, "Service: A software defined framework for integrated space-terrestrial satellite communication," *IEEE Transactions on Mobile Computing*, vol. 17, no. 3, pp. 703-716, 1 March 2018.

[18] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in *Proc. IEEE Local Computer Network Conference*, Denver, CO, USA, 2010, pp. 408-415.

[19] D. Hu, P. Hong, and Y. Chen, "FADM: DDoS flooding attack detection and mitigation system in software-defined networking," in *Proc. GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Singapore, 2017, pp. 1-7.

[20] S. Sezer *et al.*, "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE Commun. Mag.*, vol. 51, no. 7, pp. 36-43, Jul. 2013.

[21] Y. Cao, H. Jiang, Y. Deng, J. Wu, P. Zhou, and W. Luo, "Detecting and mitigating DDoS attacks in SDN using spatial-temporal graph convolutional network," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 6, pp. 3855-3872, 1 Nov.-Dec. 2022.

[22] J. Weiwei, "Graph-based deep learning for communication networks: A survey," *Computer Communications*, vol. 185, pp. 40-54, 2022.

[23] A. Ivanov, K. Tonchev, V. Poulkov, A. Manolova, and N. N. Neshov, "Graph-Based resource allocation for integrated space and terrestrial communications," *Sensors*, vol. 22, no.15, p. 5778, 2022.

[24] V. V. Thieu, N. The Anh, and T. Hoang Hai, "A variational information bottleneck method for network intrusion detection," *Journal of Communications*, vol. 17, no. 11, pp. 933-940, November 2022.

[25] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using artificial neural networks," *Neurocomputing*, vol. 172, pp. 385–393, 2016.

[26] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS attack detection method based on SVM in software defined network," *Security and Communication Networks*, Article ID: 9804061, p. 8, 2018.

[27] Systems Tool Kit. (November 2020). Analytical and Visualizing tools of complex system. [Online]. Available: https://www.agi.com/products/stk

[28] Mininet. (June 2015). Rapid Virtual Network. [Online]. Available: http://mininet.org