A DDoS Attack Detection Method Based on an Ensemble of Small Models for Multi-Layer Satellite Networks*

Xiaojing Fan, Wangjian Zhou, and Huachun Zhou†

Beijing Jiaotong University, Beijing, China
{23111043, 23125093, hchzhou}@bjtu.edu.cn

Abstract

With the increasing importance of satellite communications in B5G/6G networks, satellite network security has become a critical issue. In this paper, distinct from existing literature that primarily focuses on Distributed Denial of Service (DDoS) attack detection schemes for the uplink between ground nodes and satellite nodes, we propose a detection method specifically targeting low-rate DDoS attacks between satellite nodes in multilayer satellite networks. By combining the AlexNet convolutional neural network and the Random Forest (RF) model to construct an ensemble of small models, the proposed method effectively identifies and classifies low-rate DDoS attack traffic originating from satellite nodes. To adapt to the special characteristics of satellite networks, we designed tunnels based on the Delay-Tolerant Networking (DTN) architecture to enable the conversion between the IP stack and the Bundle Protocol (BP) stack. Experimental results demonstrate that the proposed method outperforms existing models regarding precision and F1 score for attack detection. It provides effective security protection for key nodes of multilayer satellite networks and has good potential for practical application.

Keywords: Satellite network; Attack detection; Ensemble of small models; Low-rate DDoS attacks

1 Introduction

Satellite communication has become an integral component of B5G/6G networks. To facilitate the integration of satellite networks with terrestrial systems, the 3GPP initiated the study and definition of Non-Terrestrial Networks (NTN) beginning with Release 15. Currently, NTN supports bent-pipe payload and onboard processing architectures, laying the foundation for building a service-driven space core network. Meanwhile, commercial satellites are booming. New and proposed constellations have increased the number of nodes in orbit to thousands. Constellations are expanding from single-layer to multi-layer. Satellite networks in the B5G/6G era will support rich network functions. More and more traffic flows from the ground into satellite networks. Satellite networks will also generate more and more traffic.

Compared to terrestrial networks, satellite networks exhibit periodicity and regularity. While these characteristics facilitate the study of satellite networks, they also render them highly vulnerable to various types of attacks and threats [1]. Attack traffic can originate from either terrestrial user nodes or space-based satellite nodes. Attackers exploit the global coverage of satellite networks, turning their inherent strengths into vulnerabilities. Ground users can be manipulated into forming botnets that launch Denial of Service (DoS) or Distributed

*Proceedings of the 8th International Conference on Mobile Internet Security (MobiSec'24), Article No. 12, December 17-19, 2024, Sapporo, Japan.

†Corresponding author: Huachun Zhou, Beijing Jiaotong University, No.3 Shangyuancun, Haidian District, Beijing 100044, China,Tel: +86-137-1816-8186

DoS attacks from multiple locations. This type of attack, commonly exploited in terrestrial networks, has the potential to cause significant damage and is likely to be used against satellite networks in the future [2]. The satellite network attack scenarios are illustrated in Figure 1. The forwarding nodes in the Low Earth Orbit (LEO) layer launch attacks on the key nodes in the Medium Earth Orbit (MEO) layer. Key satellite nodes are network nodes that serve special functions, such as functional nodes and control nodes in multi-layer satellite networks. When these critical nodes are compromised by network attacks, they can be rendered non-operational without physically damaging network infrastructure, leading to network congestion or even collapse. DDoS attacks have thus become a significant security concern for satellite networks [3]. However, existing solutions primarily focus on mitigating DDoS attacks on terrestrial satellite infrastructure, such as terrestrial satellite access gateways and terrestrial network management centers. While these solutions are effective for addressing satellite-terrestrial link attacks, they fail to protect against Inter-Satellite Link (ISL) attacks and Inter-Orbit Link (IOL) attacks. Consequently, they cannot provide comprehensive protection for satellite network.

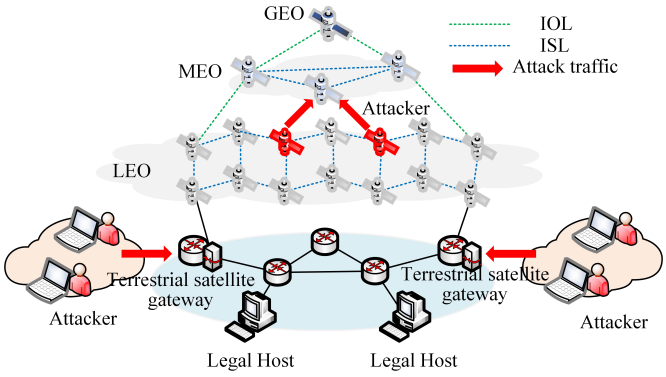

Figure 1: Satellite network attack scenarios

This paper addresses DDoS attack and defense scenarios for key nodes in multilayer satellite networks. Considering the characteristics of space network protocols and the constraints of limited resources, we propose a DDoS attack detection method based on an ensemble of small models. We design tunnels within a DTN [4] environment to facilitate the transformation between the IP stack and the BP stack. Using low-rate DDoS attack traffic as a case study, We employ an ensemble of an AlexNet convolutional neural network and a random forest model to detect abnormal traffic originating from satellite nodes. This ensures that MEO nodes can process normal traffic while intercepting attack traffic from LEO nodes, and simultaneously enables the activation of backup LEO satellites within the same orbit. The scheme proposed in this paper aims to provide valuable insights for enhancing the security of key nodes in 6G satellite-terrestrial integrated networks.

The rest of the paper proceeds as follows. Section 2 provides a brief overview of the current research status on DDoS detection in satellite-terrestrial integrated networks. Section 3 describes the design and implementation of DDoS detection based on an ensemble of small models in a satellite environment. Section 4 presents the experimental evaluation of our proposed solution. Section 5 concludes the paper and outlines potential directions for future research. Section 6 describes the program support for our work.

2 Related Work

Many threats exist in today's Internet, including viruses, malware, vulnerabilities, and DDoS attacks. For satellite networks, the potential threat of DDoS attacks is particularly serious [5]. Manulis et al. explicitly stated that from a space protocol security perspective, the CCSDS extended the data link protocol to address space security issues. However, this protocol could not protect against DDoS attacks through traffic analysis and other means [6]. Onen et al. proposed a DoS prevention mechanism based on an identification protocol. In this mechanism, request messages sent by satellite terminals were rapidly verified during each time interval using a random number broadcast by the network control center and a pre-shared key, effectively preventing DoS attacks [7]. Tu et al. proposed a satellite DDoS mitigation mechanism to address the issue of significant energy consumption caused by abnormal traffic in satellite networks. They optimized the mitigation strategy using a DRL algorithm to distinguish between normal and abnormal DDoS traffic, discarding the identified abnormal traffic to reduce the additional energy consumption incurred by satellite nodes processing such traffic [8]. Li et al. deployed a distributed intrusion detection system at the satellite gateway and terrestrial edge router of a satellite-terrestrial integrated network. They leveraged federated learning, which did not require data centralization, to enable distributed training and detection [9].

The above studies have done good work for DDoS detection in satellite networks or terrestrial networks. However, they primarily focused on deploying enhanced protocols or detection models at ground management centers or terrestrial satellite access gateways. Their research primarily addresses uplink traffic from ground nodes to satellite nodes, which still falls within the domain of terrestrial network traffic. The impact of anomalous traffic generated by satellite nodes on backhaul links or inter-satellite links has not been adequately considered. To address this gap, we propose a small-model ensemble DDoS attack detection method to mitigate the impact of abnormal traffic generated by satellite nodes on critical satellite nodes. The advantage of our method lies in using an ensemble of the AlexNet and RF, which enables effective learning of attack features from a small amount of data and exhibits excellent handling performance for imbalanced data distributions. Applying this algorithm to low-rate DDoS attack detection in satellite networks can effectively reduce model training time and enhance detection capabilities. Compared to deep and single models, it reduces the computational burden throughout the process. Furthermore, we select a version of AlexNet with fewer parameters, and combined it with Random Forest to reduce overall computational complexity by minimizing AlexNet's subsequent classification tasks.

3 Research Design and Realization

In this section, we first present the overall scheme for DDoS attack detection using ensemble miniaturized models in multilayer satellite networks. We then detail the satellite network packet transmission method. Subsequently, the process of traffic acquisition and processing is described. Finally, we highlight the AlexNet-RF ensemble model algorithm.

3.1 Overall Framework

In this paper, the proposed DDoS attack detection scheme for multi-layer satellite networks based on ensemble small models is shown in Figure 2. The scheme sequentially involves the establishment of the satellite environment, dataset generation, feature analysis and selection, offline training, and online prediction. The functions of each part are as follows:

We establish the satellite environment using ION-DTN software and model the multilayer satellite network with STK [10] to generate ephemeris information. MATLAB processes this data to create a series of ordered snapshot collections, each representing a unit-time static topology. Using the snapshot information, we configure the satellite node's neighbor mechanism, transmission protocol engine parameters, forwarding scheme, LTP parameters, and contact plan. This process generates the satellite node management file, enabling the configuration of the satellite nodes.

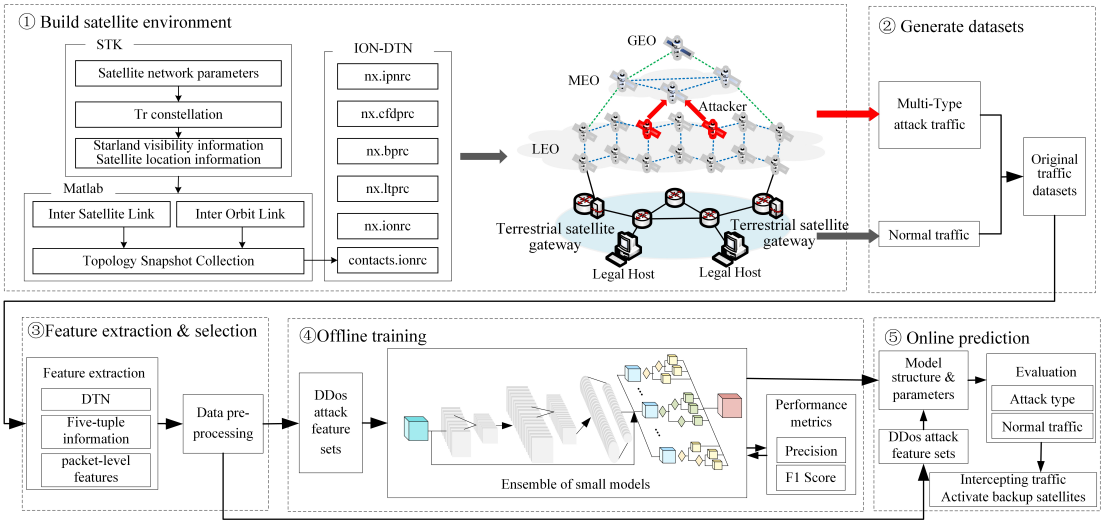

Figure 2: DDoS attack detection scheme

The generated dataset includes normal traffic from ground nodes and multiple types of low-rate DDoS attack traffic originating from satellite nodes. The normal ground traffic reaches the MEO critical nodes via the satellite access gateway, while the multi-type attack traffic is simulated by LEO satellites. The raw dataset for the satellite network, encompassing various types of traffic, is created by capturing traffic at both the ground satellite gateway and the LEO satellite nodes.

Characterization and selection involve flow feature extraction and data preprocessing. Different features of the original flow dataset are extracted using CICFlowMeter [11], and the low-rate DDoS dataset is formed by labeling the data according to flow type. The labeled data undergoes preprocessing, including cleaning and normalization. Comprehensive feature engineering and statistical thresholding are applied to analyze the characteristic performance of different attacks and to construct the DDoS attack feature set.

Feature selection is conducted based on the most effective features in the dataset. We use an ensemble of small models for training and testing. Multiple rounds of hyperparameter tuning are performed to optimize the ensemble learning model, guided by comparisons of model performance metrics. Finally, we save the structure and parameters of the optimized model.

We deploy the model at key satellite nodes in mid-orbit to perform online detection of normal traffic from the ground and attack traffic originating from space. Based on the detection results, the system intercepts the attack traffic and forwards the normal traffic. Additionally, a satellite in low orbit, positioned in the same orbit as the attacking node, is activated to mitigate the

impact.

3.2 Satellite Network Data Packet

Satellite network traffic is transmitted using DTN protocol packets. The conversion between the TCP/IP protocol and the DTN protocol for ground-based normal traffic occurs at the satellite access gateway. DTN protocol packets are based on the Bundle Protocol [12], which facilitates high-latency and intermittent transmission in satellite networks using bundled packets. We transmit space packets by designing tunnels. The format of the DTN Bundle Protocol packets exchanged between satellite nodes is illustrated in Figure 3. In this format, the Bundle header includes the source Endpoint Identifier (EID) and the destination Endpoint Identifier.

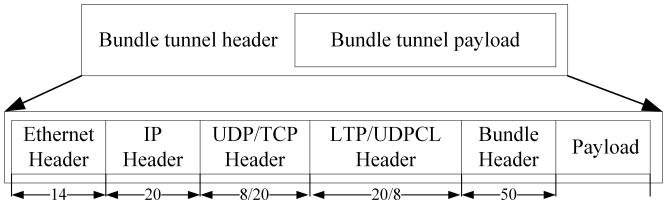

Figure 3: Satellite network packet format

3.3 Traffic Acquisition and Processing

In 5G application scenarios, legitimate traffic is simulated across four different application contexts: smart home, user PC internet access, public services, and MTC communication [13]. Four types of low-rate attacks—Slow Header, Slow Body, Slow Read, and Shrew attacks—are simulated using attack tools or scripts. A multi-threaded approach with multiple concatenations is employed to facilitate legitimate communication requests. The SlowHTTPTest tool is used to simulate low-rate DDoS attacks at the application layer under the Hypertext Transfer Protocol (HTTP). We adjust the attack parameters and set the attack duration according to the attack plan to simulate various low-rate DDoS attacks.

Fwd IAT Min	Packet Length Std	Fwd Header Length	Fwd IAT Max
Bwd Packets/s	Packet Size Avg	Total Length of Fwd Packets	Fwd IAT Mean
Active Max	FIN Flag Count	Fwd Packet Length Std	Fwd IAT Total
RST Flag Count	Fwd Act Data Pkts	Fwd Packet Length Min	Bwd Header Length
Fwd Packets/s	Packet Length Min	SYN Flag Count	Flow Packets/s
Active Mean	Bwd Bytes/b Avg	Subflow Bwd Packets	Active Std
Flow Bytes/s	Fwd Seg Size Min	Flow Duration	Bwd Bulk Rate Avg
Flow IAT Mean	Fwd Init Win Bytes	Flow IAT Std	Bwd Init Win Bytes
Total Fwd Packets	ACK Flag Count	Packet Length Mean	Packet Length Max
Subflow Fwd Packets	Fwd Seg Size Avg	Flow IAT Min	Subflow Fwd Bytes

Table 1: 40 effective features for multi-type low-rate DDoS attacks

We use the TCPdump tool [14] at the terrestrial satellite access gateway to capture legitimate communication traffic. For attack traffic, we employ TCPdump at the four low-orbit attack satellites to capture the attack traffic, enabling the collection of the satellite network

Algorithm 1 AlexNet-RF

Input: *Dataset.csv*
Output: *Classification*
function LoadAndPreprocessData(*Dataset.csv*)
    df ← read and clean data from *Dataset.csv*
    df ← convert IP addresses to integers
    return *df*
end function
function PrepareFeaturesAndLabels(*df*)
    X ← Extract features from *df*
    Y ← Encode labels from *df*
    return X, Y
end function
function DefineAndTrainAlexNetModel(X, Y)
    model ← Define AlexNet model
    model ← Train model on X, Y
    return *model*
end function
function ExtractAndStandardizeFeatures(*model*, X)
    features ← Extract *features* with model
    standardized_features ← Standardize *features*
    return *standardized_features*
end function
function TrainRandomForest(*standardized_features*, Y)
    rf_model ← Train RandomForest on *standardized_features*, Y
    return *rf_model*
end function
function EvaluateModel(*rf_model*, *X_train*, *Y_train*, *X_test*, *Y_test*)
    Classification ← Evaluate *rf_model* on *X_train*, *Y_train*, *X_test*, *Y_test*
    return *Classification*
end function
df ← LoadAndPreprocessData(*Dataset.csv*)
X, Y ← PrepareFeaturesAndLabels(*df*)
alexnet_model ← DefineAndTrainAlexNetModel(X, Y)
standardized_features ← ExtractAndStandardizeFeatures(*alexnet_model*, X)
rf_model ← TrainRandomForest(*standardized_features*, Y)
Classification ← EvaluateModel(*rf_model*, *X_train*, *Y_train*, *X_test*, *Y_test*)
return *Classification*

attack detection dataset. Based on the extracted raw traffic, a combination of statistical thresholding and feature engineering is applied to rank the feature importance for each of the four attacks. The effective features that characterize the properties of the Slow Read, Slow Headers, Slow Body, and Shrew attacks are 30, 30, 30, and 31, respectively. After aggregation, 40 valid features for multiple types of DDoS attacks are identified, as shown in Table 1, which includes both packet-level and flow-level features. For example, the effective features selected for the Slow Read attack include Flow Bytes/s and ACK Flag Count. Flow Bytes/s indicates the characteristic of the attacker sending packets at a low rate per second during the attack. ACK

Flag Count represents the need for the attacker to establish a large number of HTTP connections with the targeted server. During the establishment and disconnection of these HTTP connections, the ACK flag in the packet must be set to 1, which increments the count value by 1.

3.4 Ensemble Learning Model

We propose using an AlexNet-RF hybrid learning ensemble model for the online detection of multiple types of low-rate DDoS attacks. AlexNet, a convolutional neural network with relatively few model parameters, is employed to learn the hidden features of the low-rate DDoS attack dataset. Concurrently, a Random Forest, consisting of multiple decision trees trained in parallel, is utilized to classify the attack types. This approach leverages the powerful feature extraction capabilities of CNNs and the efficient classification performance of RFs. Figure 4 shows the block diagram of the AlexNet-RF model, which consists of three convolutional layers, three max-pooling layers, two zero-padding layers, one Alpha-Dropout layer, and two fully connected layers. The output from the final fully connected layer serves as the input to the RF classifier. The classifier's output is then used as the detection result.

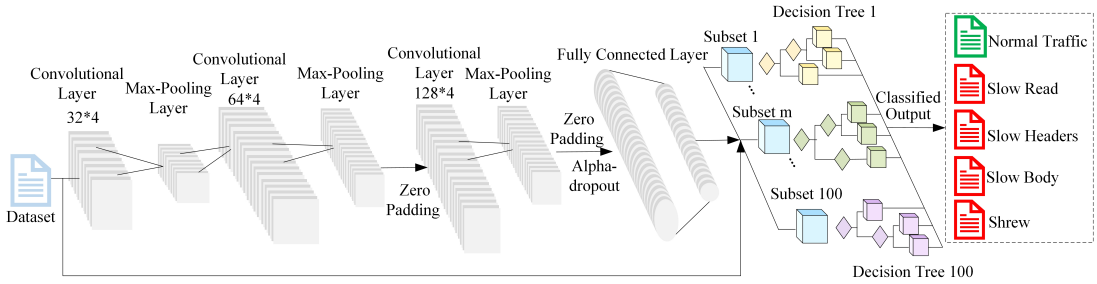

Figure 4: Block diagram of the AlexNet-RF model

Algorithm 1 illustrates the model training process. The input data to the classifier has 45 dimensions, consisting of 40 effective features from low-rate DDoS attacks and 5 features extracted from the AlexNet network. Model training is conducted by replaying different types of low-rate DDoS attack traffic in the satellite network, as well as normal traffic from various 5G scenarios.

4 Experiments and Results

The experiments simulate 5G multi-scenario legitimate traffic and various types of low-rate attacks within a satellite network environment. We analyze the performance of different ensemble models and conduct online testing of the model proposed in this paper.

4.1 Experiment Configuration

A virtual platform based on Vmware vSphere is used to build the Tr [15] constellation, which contains 3 Geostationary Earth Orbit (GEO) satellites, 10 MEO satellites, and 66 LEO satellites. All satellite nodes support the DTN protocol stack. Among them, the MEO satellites

serve as the key nodes of the Tr constellation, and the LEO satellites serve as the forwarding nodes. The experimental topology is shown in Figure 5. The IP addresses of the LEO puppet hosts are set to 36.6.0.2, 36.6.0.10, 36.6.0.11, and 36.6.0.12. The target MEO nodes of the attack have IP addresses 36.6.1.2 and 36.6.1.7. The legitimate hosts sending normal traffic use virtual IP addresses in the range of 36.6.0.20 to 36.6.0.29. We set the traffic collection time to 3 hours. Using the described traffic collection tool, 1 million flows can be captured in 10 minutes. Due to the limited processing capacity of the satellite nodes, systematic sampling is performed to obtain a subset of traffic at a ratio of 1:100. After filtering, a total of 114,352 normal flows and 89,734 attack flows are obtained. The detection model is trained using the TensorFlow framework, and the trained model and parameters are deployed on the key MEO node. The tunneling program is deployed at the satellite gateway, the four LEO satellites and the three MEO satellites in the Tr constellation, as shown in Figure 5.

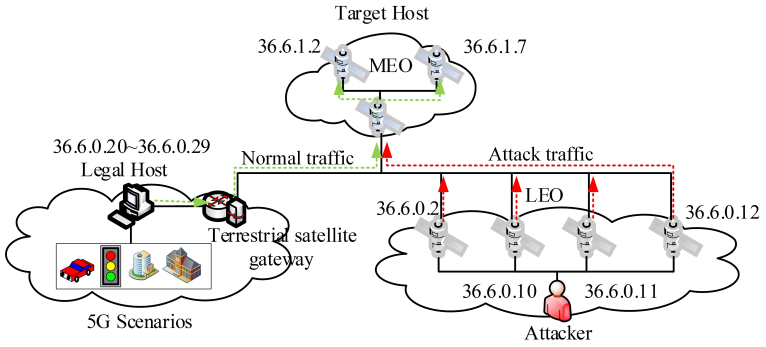

Figure 5: Network topology

4.2 Performance Metrics

In this paper, Confusion Matrix, Precision, and F1 score are used as performance metrics.

The Confusion Matrix is a tool used to measure the accuracy of a classifier's performance, particularly in multi-classification problems. Table 2 presents the confusion matrix for a binary classification model. In this context, True Positive (TP) represents instances where the true label is positive, and the model correctly classifies them as positive. True Negative (TN) denotes instances where the true label is negative, and the model correctly classifies them as negative. False Positive (FP) indicates instances where the true label is negative, but the model incorrectly classifies them as positive. False Negative (FN) represents instances where the true label is positive, but the model incorrectly classifies them as negative.

Actual values \ Predicted values	Positive	Negative
Positive	TP	FN
Negative	FP	TN

Table 2: Confusion matrix for binary classification models

Precision is defined as the proportion of samples correctly identified as attack traffic out of the total number of samples predicted as attack traffic by the model. A higher precision

indicates more precise identification of attack traffic.

$$Precision = \frac{TP}{TP + FP}$$

F1 score represents the combined metric of precision and recall, which better reflects the overall performance of the model.

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

where $Recall = \frac{TP}{TP+FN}$ is the recall rate. The recall rate is the ratio of the number of samples that accurately identify the attack traffic as attack traffic to the total number of attack traffic samples.

4.3 Evaluation Result

To verify the detection performance of the AlexNet-RF model proposed in this paper for low-rate DDoS attack traffic, we compare it with the LSTM-LightGBM model presented in [16] and the LSTM-RF model described in [17]. The models' attack detection performance is evaluated using metrics such as precision and F1 score. The best-performing model is then selected for the online detection of attack traffic.

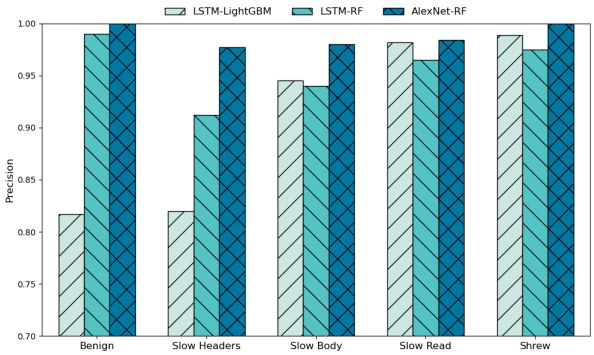

Figure 6: Precision of the three models LSTM-LightGBM, LSTM-RF and AlexNet-RF

Figures 6 and 7 show the precision and F1 scores of the three detection models. For benign legitimate traffic and Slow Headers attacks, the AlexNet-RF model achieves the highest detection rate, exceeding 95%. In contrast, the LSTM-LightGBM model performs poorly, with precision below 85%. The F1 Score distribution for the LSTM-RF and AlexNet-RF models is similar, while the LSTM-LightGBM model exhibits the worst detection performance. For Slow Body and Slow Read attacks, the AlexNet-RF model outperforms the other two models in both precision and F1 score, with the other models showing varying degrees of inferiority. In the case of Shrew attacks, all three models demonstrate excellent performance in terms of both precision and F1 Score. Based on these evaluation metrics, the AlexNet-RF model proposed in this paper outperforms the LSTM-LightGBM and LSTM-RF models in detecting and categorizing all four types of attacks, accurately identifying different types of low-rate DDoS attacks.

Figure 8 presents the confusion matrix of the AlexNet-RF algorithm for the online classification of low-rate DDoS attack traffic at the MEO node. The model achieves up to 91%

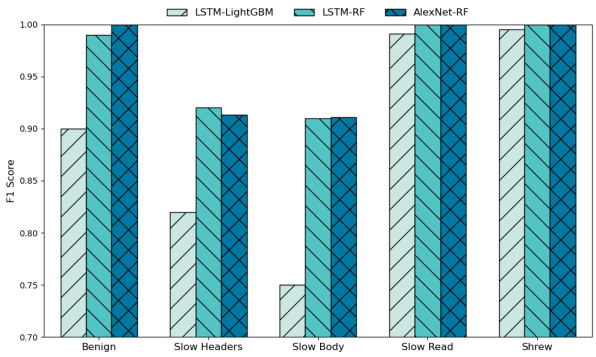

Figure 7: F1 Score for the three models LSTM-LightGBM, LSTM-RF and AlexNet-RF

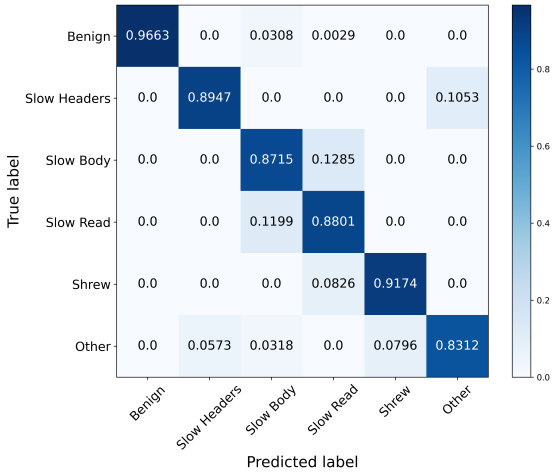

Figure 8: Confusion Matrix of AlexNet-RF at the MEO node

recognition accuracy for both normal traffic and Shrew attacks, and over 87% accuracy for the other three types of attack traffic. 12.85% of Slow Body attack traffic is misclassified as Slow Read. This indicates that the model has confusion in distinguishing between the Slow Body and Slow Read attack types. The false-negative issue for Benign traffic also requires further optimization to reduce false alarms for normal traffic.

5 Conclusions and Future Work

This paper studies DDoS attack and defense scenarios in multilayer satellite networks. Using multiple types of low-rate DDoS attacks as a case study, we propose an ensemble model combining AlexNet and Random Forest for detecting anomalous traffic in satellite networks. The ensemble model achieves recognition accuracy of over 87% for abnormal traffic types. Considering the differences between satellite networks and terrestrial network protocols, we designed a DTN-based tunnel to facilitate the conversion between the IP stack and the BP stack. The proposed scheme is highly portable, and the low-rate DDoS attack dataset used closely resembles

real-world conditions, making it deployable in actual satellite network environments. In the future, we will select entry classifier nodes for MEO satellites with the objective of minimizing path delay and deploy the model to enhance its scalability in large-scale satellite networks and scenarios with increased traffic.

6 Acknowledgments

- This paper is supported by National Key R&D Program of China under Grant No. 2018YFA0701604 and NSFC under Grant No. 62341102.

References

[1] ZHU Hui, CHEN Siyu, LI Fenghua, WU Heng, ZHAO Haiqiang, and WANG Gang. User random access authentication protocol for low earth orbit satellite networks. *Journal of Tsinghua University (Science and Technology)*, 59(1):1–8, 2019.

[2] Yan Zhang, Yong Wang, Yihua Hu, Zhi Lin, Yadi Zhai, Lei Wang, Qingsong Zhao, Kang Wen, and Linshuang Kang. Security performance analysis of leo satellite constellation networks under ddos attack. *Sensors*, 22(19):7286, 2022.

[3] Muhammad Usman, Marwa Qaraqe, Muhammad Rizwan Asghar, and Imran Shafique Ansari. Mitigating distributed denial of service attacks in satellite networks. *Transactions on emerging telecommunications technologies*, 31(6):e3936, 2020.

[4] Vinton Cerf, Scott Burleigh, Adrian Hooke, Leigh Torgerson, Robert Durst, Keith Scott, Kevin Fall, and Howard Weiss. Delay-tolerant networking architecture. Technical report, 2007.

[5] Wei Guo, Jin Xu, Yukui Pei, Liuguo Yin, Chunxiao Jiang, and Ning Ge. A distributed collaborative entrance defense framework against ddos attacks on satellite internet. *IEEE Internet of Things Journal*, 9(17):15497–15510, 2022.

[6] Mark Manulis, Christopher P Bridges, Richard Harrison, Venkkatesh Sekar, and Andy Davis. Cyber security in new space: analysis of threats, key enabling technologies and challenges. *International Journal of Information Security*, 20:287–311, 2021.

[7] Melek Onen and Refik Molva. Denial of service prevention in satellite networks. In *2004 IEEE International Conference on Communications (IEEE Cat. No. 04CH37577)*, volume 7, pages 4387–4391. IEEE, 2004.

[8] Zhe Tu, Huachun Zhou, Kun Li, Man Li, and Aleteng Tian. An energy-efficient topology design and ddos attacks mitigation for green software-defined satellite network. *IEEE Access*, 8:211434–211450, 2020.

[9] Kun Li, Huachun Zhou, Zhe Tu, Weilin Wang, and Hongke Zhang. Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning. *IEEE Access*, 8:214852–214865, 2020.

[10] Satellite Tool Kit (STK). http://www.agi.com, 2018. [EB/OL].

[11] CICFlowMeter. https://www.github.com/ISCX/, 2017. [Online].

[12] Keith Scott and Scott Burleigh. Bundle protocol specification. Technical report, 2007.

[13] Lijuan Li, Man Li, HJ Bi, and HC Zhou. Multi-type low-rate ddos attack detection method based on hybrid deep learning. *Chin. J. Netw. Inf. Secur*, 8:73–85, 2022.

[14] Tcpdump. https://www.tcpdump.org/, 2019. [Online].

[15] Fei Long. *Satellite network robust QoS-aware routing*. Springer, 2014.

[16] Yuankai Guo, Yangyang Li, and Yuan Xu. Study on the application of lstm-lightgbm model in stock rise and fall prediction. In *MATEC Web of Conferences*, volume 336, page 05011. EDP Sciences, 2021.

[17] Wen Hu and Yuxue Shi. Prediction of online consumers' buying behavior based on lstm-rf model. In *2020 5th International Conference on Communication, Image and Signal Processing (CCISP)*, pages 224–228. IEEE, 2020.