FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 503-511 | e-ISSN: 2347-470X

# A Smart Secure model for Detection of DDoS Malicious Traces in Integrated LEO Satellite-Terrestrial Communications

**Lakshmisree Panigrahi[1], Binod Kumar Pattanayak[2*], Bibhuprasad Mohanty[3], Saumendra Pattnaik[4], and Ahmad Khader Habboush[5]**

*[1]Department of Computer Science and Engineering, Institute of Technical Education & Research, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, India; laxmishreepanigrahi@soa.ac.in*
*[2]Department of Computer Science and Engineering, Institute of Technical Education & Research, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, India; binodpattanayak@soa.ac.in*
*[3]Department of Electronics and Communication Engineering, Institute of Technical Education & Research, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, India; bibhumohanty@soa.ac.in*
*[4]Department of Computer Science and Engineering, Institute of Technical Education & Research, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, India; saumendrapattnaik@soa.ac.in*
*[5]faculty of Information Technology, Jerash University, Jerash, Jordan; ahmad_ram2001@jpu.edu.jo*

*__Correspondence:__ Binod Kumar Pattanayak; binodpattanayak@soa.ac.in

**ABSTRACT-** For many researchers, defense against DDoS attacks has always been a major subject of attention. Within the LEO Satellite-Terrestrial (LSTN) network field, distributed denial of service (DDoS) attacks is considered to be one of the most potentially harmful attack techniques. For the facilitation of network protection by the detection of DDoS malicious traces inside a network of satellite devices, machine learning algorithms plays a significant role. This paper uses modern machine learning approaches on a novel benchmark Satellite dataset. The STIN and NSL-KDD datasets has been used to detect network anomalies. The pre-processing of data has been performed effectively and a host of ML methods have been applied to classify the outputs into normal, regular node or untrustable /malicious node. We have evaluated the analysis results in presence of attacks as well as without presence of attacks, supervised machine learning techniques basic measurements like accuracy, True positive, False positive etc. Our proposed trust model shows better accuracy, nearby 98% and we have shown that our proposed machine learning based security model performs better to get rid of DDoS attacks on integrated LEO satellite-terrestrial networks without compromising on the packet routing efficiency. We are able to improve routing speed and improve network security against distributed denial of service (DDoS) attacks by integrating an ensemble-based trust model trained on NSL-KDD+STIN+Exata Simulated resultant dataset with ACO for routing decisions. In dynamic network scenarios, as trustworthiness is an essential criterion in route decision-making, this proposed approach signifies resilient and adaptable routing.

**Keywords:** Satellite Communication, Security, anomaly detection, LEO, GEO, machine learning, supervised learning, trust models.

**ARTICLE INFORMATION**

**Author(s)**: Lakshmisree Panigrahi, Binod Kumar Pattanayak, Bibhuprasad Mohanty, Saumendra Pattnaik and Ahmad Khader Habboush;

**Received**: 28/02/2024; **Accepted**: 24/04/2024; **Published**: 30/05/2024;
**e-ISSN**: 2347-470X;
**Paper Id**: IJEER 2802-25;
**Citation:** 10.37391/IJEER.120223
**Webpage-link**:
https://ijeer.forexjournal.co.in/archive/volume-12/ijeer-120223.html

**Publisher's Note:** FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

## 1. INTRODUCTION

The Satellite networks are the key to staying connected, no matter where we go. Compared to GEO and MEO satellites, LEO satellites orbits are closer to earth and their size is relatively smaller, hence the rocket needed to launch the LEO satellites are cheaper and also smaller. LEO technology is used for the things which require, maritime operations disaster relief or global mobile communication. LEO satellite orbit in low altitude and lower the altitude less time taken in traveling of signals which results to almost no delay [1,2]. Low Earth Orbit (LEO) satellites revolve around the earth, along their own orbit. A constellation of Low Earth Orbit (LEO) Satellites is the alternative solution for internet broadband connectivity for the rural area. LEO satellites orbits from approximately 160 to 2,000km above the earth's surface. They constantly revolve and communicates with each other by forming a constellation of satellites compared to Geostationary Earth Orbit (GEO) that operates at approximately 35,786 km from Earth. In LEO orbit Telecommunications, imaging, and spy satellites operate. The Hubble Telescope and the International Space Station are well-known objects in LEO. Companies site the satellites into orbit in an unparalleled frequency to build a mega constellations of communication satellites in LEO [3]. Constellations of LEO

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 503-511 | e-ISSN: 2347-470X

satellites like Starlink, OneWeb and Kuiper, are the most widespread [4] as summarized below table1[5].

**Table1. LEO satellite constellations Data**

| Name | Orbital planes | Satellites |
|---|---|---|
| Iridium Next | 6 | 66 |
| OneWeb | 18 | 648 |
| Starlink | 72 | 1594 |
| Starlink VLEO | 83 | 7518 |
| Kuiper (part 1) | TBD | 784 |
| Kuiper (part 2) | TBD | 1296 |
| Kuiper (part 3) | TBD | 1156 |
| Telesat (polar) | 6 | 72 |
| Telesat (inclined) | 9 | 45 |

LEO objects orbit around the planet have high speeds. Generally, LEO satellites complete one full revolution around the earth once every two hours, whereupon LEO satellites travel in and out of range, which leads to another shared characteristic of satellites that is LEO constellations. Since LEO satellites are always traveling, it would not be possible to rely on only one satellite for any form of stable coverage. As their distance is less their coverage is also confined to a small area. Hence the constellation of satellites has to work together to provide stable coverage.

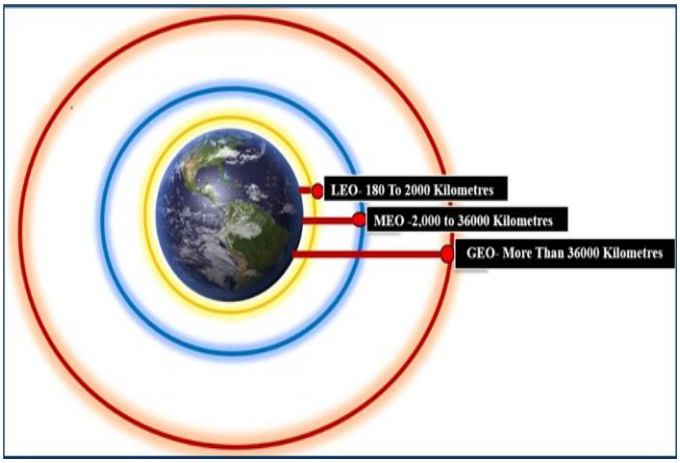


**Figure1**. Different types of satellite Network *w.r.t* Altitude

LEO satellites are closer to Earth than GEO satellite, hence, the round-trip lag, to and from the satellite is shorter. LEO satellites are helpful in making real-time communication like voice calls. The disadvantage of LEO satellites is that, a number satellites are required to cover a particular surface area. Satellites in LEO orbits revolve around earth numerous times each day, so when a satellite files over an area the next satellite should supersede, to take over the communication after the first satellite has driven over the area. This also builds on to the network complexity as various ground stations have to communicate with every passing satellite using different frequencies so that there is no confusion between different satellites communications that are faster and have lower latency than a GEO satellite. Compared with conventional geostationary satellites, low-orbiting orbit (LEO) satellites move closer to the Earth, resulting in lower latency as well as more rapid data transfer rates. The balance integration of LEO satellite constellations with terrestrial (ground-based) communication networks is commonly referred to as integrated LEO (Low Earth Orbit) terrestrial networks. These networks incorporate the strengths of both satellite and terrestrial technologies and provide wide area coverage and connectivity. Communications can be extended to remote or underserved areas where terrestrial infrastructure is either inadequate or nonexistent by integrating such LEO constellations of satellites with the terrestrial networks, such as fiber optics, 5G infrastructure, or modern cellular networks. There are various obstacles in the way of integrating LEO satellites with terrestrial networks. Some of the critical challenges are: Complexity of Dynamic Routing, Ease changes in behavior, Cooperation, regulating the latency, system maintaining security, its capacity to be scaled, Cluster Managing of the satellites, Regulatory Issues, the payloads whose services regenerating, Energy Use, Compatibility of User Equipment, Redundancy and Reliability, Spectrum Managing, the environmental Aspects, and Cost on the infrastructure.

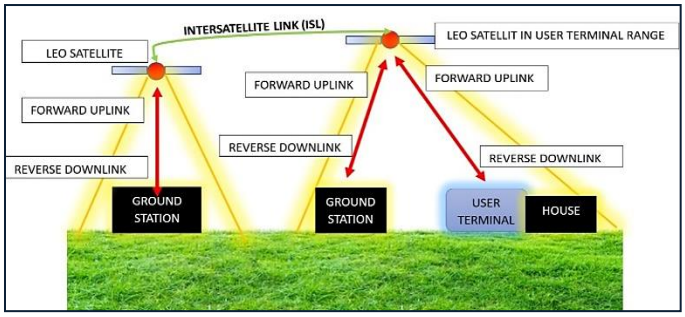


**Figure 2.** LSTN satellite communication Scenario

A Denial of Service (DoS) assault is a malevolent attempt to impede an intended system's accessibility, like a website or application, for authorized users. Attackers typically produce a lot of packets or requests, which potentially overwhelm the system users are trying to access. For initiating a Distributed Denial of Service (DDoS) assault, the attacker gets to use several hacked or controlled sources. In Low Earth Orbit Satellite-Terrestrial Networks (LSTN), designing a trust model for DDoS attack detection requires selecting important characteristics that characterize particular characteristics of the network's behavior. There are a number of steps accountable for developing an integrated trust strategy for satellite and terrestrial transmission networks to defend against attacks such as DDoS using machine learning techniques. With the overall prescience around space technologies, “security by obscurity” for space systems is extinct, the attack surface has expanded as the satellites have become more software dependent. Many techniques exist to operate the satellites or the ground-based systems that convey instructions to the orbiting satellites. Space systems have improved in complication, mostly recognized as a “black box” of badly understood but coordinated space-cyber. The aforementioned brings about potential danger since, in contrast to other anti-satellite systems, cyberattacks are cheaper

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 503-511 | e-ISSN: 2347-470X

to launch. The methods to attack space system depends on the entry point or target. A space system consists of the ground segment, the link segment, and the space segment. The techniques depend on which segment is targeted to be attacked. Attacks can not only be small cyber-attacks but also a huge attack, targeting an entire constellation of satellites. A cyber-attack is favored more by adversaries to develop and leverage in time of conflict. Satellites boundaries are often thought to be the radio frequency link in particular, or the ground system in general. If the boundary has been broken through, the few internal protection which exists within the satellite, an adversary can control it without facing obstruction — alike to the premature days of traditional cybersecurity when firewalls were only shield to protect from attacks. To protect the satellites from intrusion, the biggest challenge is to aware them on the threats and the development of an onboard cyber technology which fits in range of the size, weight, power, and computational limitations of the satellite. Aerospace engineers have a strong fancy to use what has worked in past; therefore, to make the changes to implement, "security on board" is required to evolve. There are several phases and factors to take into account while developing a trust model for satellite network DDoS attack detection. Creating a trust architecture that functions effectively for DDoS detection requires constant monitoring, adding new data, and making adjustments for dynamic attack patterns. It is a challenging practice that may require for the coordination with professionals with satellite communication network protection. There are a lot of options to set up a secure system for satellites. There is need of Additional funds from government and companies to expand security solutions that can work inside the impression of a inmtegrated satellite network and have the resilience to find, react and protect.

## 2. RELATED WORK

Depending on the behavior and protocols use, the traffic of Low Earth orbit satellite constellation networks (LSCNs) can change a lot. Because of accessibility to public network, it is not any way guaranteed for an ideal network in terms of security. That means we have to deal with security concerns during transmission of messages within that of a satellite network traffic. Despite the accomplishment of ML approach and associated software, the privacy protection of information and associated gadgets is required. The paper [6] shows a complete survey on the implementation of Federated Learning in different features of anomaly detection. Compared to terrestrial networks, LSCNs have periodicity and regularity. However, although these characteristics bring convenience to the research of LSCNs, they also make LSCNs extremely vulnerable to several types of threats and attacks [23]. A Denial of Service (DOS) attack is the act of overwhelming the resources of a victim computer or network so that the victim cannot service requests from other legitimate clients. According to the Survey Paper on Security problems in Satellite Communication Network infrastructure [7], we summarize the different types of attacks as in *figure 3* below.

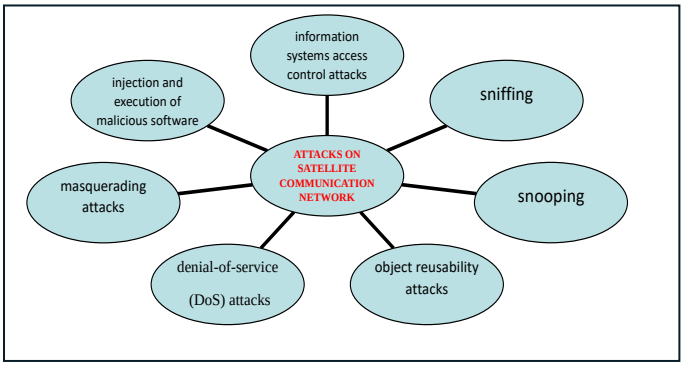


**Figure 3**. Different types of attacks on satellite networks

The common problem for protecting the data of satellites, Telemetry & command and control system stations include information systems access control attacks, order and implementation of malware attacks, impersonate attacks, sniffing, snooping, denial-of-service (DoS) attacks and object durability of malicious attacks. In paper [10], a space-time graph model is constructed to recognize the key nodes in LSCNs, and a DDoS attack and selected as the principal method to attack the key nodes. Study [11] suggests an ensemble model RFMLP that combines random forest (RF) and multilayer perceptron (MLP) for the growing identification of attack performance. Various ML models using SVM has been proposed with different advantageous features [14,15]. Priorly, Different feature extraction and machine learning hybridized with Deep learning methods have been done to maintain effectiveness and security of networking systems [20-22].

Trust plays a very important role in case of satellite networks. There are several put-to-point cases that can show the above. Some of the main reasons for using trust as an important factor in case of small satellite based smart satellite security may be small capability of devices in terms of computation and resource itself. Secondly, there are huge number of satellite devices and hence it is very difficult to handle them. Thirdly, many times there is chances of cyberattacks, Paper [8] put forward a safe routing system which is established on node trust for low Earth Orbit satellite network, called SLT, which calculates the direct trust, indirect trust and combines trust value between satellite nodes through D-S evidence theory and aggregate the low cost OPSPF routing protocol with the trust evaluation. The integrated LEO-terrestrial network is able to adapt to the dynamic threat landscape during DDoS attacks by merging dynamic traffic routing with a trust model. Dynamic routing in an environment involving integrated Leo satellite networks and terrestrial networks involves figuring out the most efficient paths for transmitting data based on to existing network conditions, such as connection availability, congestion, and QoS requirements. The Dynamic traffic scheduling and optimal routing protocol with cross layer design [18] along with scenario-based routing technique [19] have been used to pick the energy efficient nodes and to communicate the information smoothly. To be able discover the most suitable paths for data transmission, dynamic routing in integrated Leo satellite and terrestrial networks continuously analyses network topology and connection requirement data. Dynamic routing methods

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 503-511 | e-ISSN: 2347-470X

assure dependable and efficient network communication by updating to varying network conditions. By assigning trusted components a priority as they routing, the trust model creates an infrastructure for effective decision-making that ensures the network's availability and resilience in the presence of adverse contexts. New methods and models have potentially emerged in the domain of trust models against attacks using DDoS for Low Earth Orbit (LEO) satellite integrated Intelligent routing architectures.

## 3. EXPERIMENTAL ANALYSIS

For integrating a trust model into dynamic traffic routing under DDoS attacks, datasets with features relevant to satellite network behavior and including annotations for normal and DDoS attack instances that can potentially be used for training and evaluating trust model for DDoS detection has been taken in our work. In our proposed network structure, we implemented Ant Colony Optimization (ACO) to pick the shortest path while concurrently utilizing an ensemble-based trust model with the NSL-KDD+STIN+Exata-CDOS datasets to detect and avoid DDoS attacks along all of those routes. ACO, or Ant Colony Optimization, is a metaheuristic technique that focuses inspirations coming from ants' foraging behaviours. It can be tuned for dynamic routing within terrestrial and integrated Leo satellite networks.

This is how we combined these elements:

***a) ACO for Shortest Path Routing:***

- *Utilizing ACO in the network topology to choose the shortest path routing choices.*
- *Deciding on the nodes and edges in the network, in addition to the pheromone levels and heuristic data (reliability, bandwidth, and distance) attributed to each.*
- *Guiding the ants (routing agents) toward the best routes by iteratively exploring and updating pheromone trails depending on path quality and heuristic data using ACO.*

***b) Preparing Effective Dataset for Trust Model Based on Adaboost Ensemble:***

- *To produce an extensive dataset for DDoS attack detection and prevention, preprocessed, Simulated the Exata CDOS and joined the NSL-KDD, STIN, Resultant simulated Exata datasets different relevant fields like the followings:*
  ***Source IP Address**: The packet sender's IP address.*
  ***Destination IP Address:** The packet recipient's IP address.*
  ***Source Port:** The packet sender's port number.*
  ***Destination Port:** The packet recipient's port number.*
  ***Protocol:** TCP, UDP, ICMP, and other transport layer protocols which are are utilized.*
  ***Packet Length:** The packet's total bytes in length.*
  ***Time Stamp:** The instant of packet transmission or reception.*
  ***packet Type:** the particular kind of packet (routing, data, control, etc.).*
  ***Packet Content:** the data in the payload or actual contents of the packet.*
  ***Packet Sequence Number:** The packet's sequence number.*
  ***Routing Algorithm Employed:** The packet's routing algorithm (Here, ACO).*
  ***Routing Metrics:** Information utilized to measure routing, such as hop count,*

  *Etc…*
- *Using the combined dataset, design and train an Adaboost ensemble model for forecasting the probabilities of DDoS attacks. Then we evaluate the ensemble model's efficiency using relevant measures, including F1-score, accuracy, precision, and recall.*
- *Then Incorporating the trained ensemble model in the routing decision-making procedure for assessing the reliability of routes and staying clear of routes that are likely to be targeted by denial-of-service attacks.*

***c) Integration:***

- *To direct the ants toward routes with a lesser risk of DDoS attacks, we have incorporated the ensemble-based trust model predictions as additional information to supplement the ACO algorithm.*
- *Applying trust scores coming from the ensemble model into the ACO algorithm's pheromone update rule, reinforcing high-trust paths and discouraging low-trust paths.*
- *When picking a routing strategy, examining the trade-offs between reliability and the shortest path in length, maintaining the right balance between the network efficiency and security requirements.*

We have used NSL-KDD and STIN dataset. Also, proposed model uses EXata/Cyber Denial of Service for DDos Attack Simulation. NSL-KDD dataset contains approximately 41 features referring to traffic input. The label column of NSL-KDD [13] contain multiple categories (whether it is normal or attack) and the scores of the labels. The above Label is parted into different kind of attacks like Dos and non-attacks or normal. There are Around 125,000 instances. STIN security dataset [12] contains types of malicious attack from both earthbound and satellite networks. STIN dataset contains the malicious attacks for satellites (SAT20). The STIN (Space-Terrestrial Internetworking) contains SAT20 and TER20 datasets referring to the satellite and terrestrial attacks respectively. We used both the dataset so we can get normal situations with the attack scenarios during on integrated satellites networks. The EXata/Cyber package [25] is a group of infrastructure for emulation and simulation. A wide range of assault methodologies are used by the Cyber Library, that include radio jamming, eavesdropping, distributed denial of service (DDoS) attacks, three different types of attacks are provided by EXata/Cyber's DOS Attack model:

• ***Basic:*** In this scenario, a considerable amount of UDP traffic is sent to the intended target host or network from the attacker(s). Both of CPU power and network buffer memory are used by this network traffic.

• ***TCP SYN:*** In this case, the the target computer receives TCP SYN packets from the attacker(s). The transport layer buffer

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 503-511 | e-ISSN: 2347-470X

RAM is used up by the victim computer establishing a new TCP connection every time it sends a TCP SYN packet.

CubeSat functions in Low earth orbit (LEO). Like other LEO satellites it is small in size and its weight is constructed to a certain limit hence boosting solar energy harvesting and restricting DC-to-DC converters will be a tough task. We have used multiport converter inside our satellites which need single inductor and low number of components, which reduces overall dimensions of system [9]. There are various phases and factors that has been taken into consideration while designing the system of trust for satellite network DDoS attack detection. A high-level procedure for guiding the development of our proposed LSTN network trust model is as in the following working steps.

**Algorithm: Steps of Our Proposed Trust Model**

***Data Collection:***

• Preparing a dataset that it reflects the way a satellite communication network operates. Features such as source-destination addresses, packet sizes, traffic patterns, and so on needs to be added in this dataset.

• Addition of labels concerning the dataset that indicate the both attacks through DDoS and regular patterns of activity.

***Data Preprocessing:***

• Bringing numerical features to the same scale, normalize or standardize them.

• Handling of outliers and values that are missing in the dataset.

***Splitting the Dataset:***

• Split the dataset in to training and testing sets to enable to accurately evaluate the effectiveness of the model.

***Feature Selection/Engineering:***

• Checking out the dataset and select necessary characteristics.

• Developing novel features that may encompass specific characteristics of DDoS attacks within satellite networks.

***Trustworthiness Score Calculation:***

• Establish a trustworthiness score for every network entity, including nodes and devices.

• Determine or forecast each entity's trustworthiness score based on the features those have been chosen.

***Model Selection:***

• Select a statistical or machine learning model that works well for trust modelling. Depending on how intricate the trust ties are, this could involve neural networks, ensemble approaches, or regression models.

***Model Training:***

• Make use of past data to train the trust model. To help the model, use labeled data that shows which examples are trustworthy and which are not.

***Assessment of the Model (Model Evaluation):***

• Assessing the trust model's effectiveness using a different validation or test set. Depending on the particular requirements, use measurements like area under the ROC curve, F1 score, precision, and recall.

## 3.1. Preprocessing

Before using the NSL-KDD, STIN and Exata Output datasets, the null values and non-useful fields needed to be cleaned. The libraries used for data cleaning were Pandas, Sci-Kit Learn (sklearn), NumPy. Pandas was used to read the data text files and convert the objects into appropriate data types so the models could be applied on them. After reading both the dataset, we joined both the dataset by using Pandas built-in functions and created a new dataset containing features of both datasets. Then we used, the function fillna() to replaces all empty or non-existent data or NULL values with an appropriate specified value . To discover duplicates, we used the duplicated () method of Pandas. Then To remove duplicates, the drop_duplicates () method has been used. Shannon entropy Method has been used to measure the imbalancing of the resulted joined dataset. Then after knowing less Shannon entropy i.e, imbalanced dataset, SMOTE was used to balance the Dataset. SMOTE is statistical method to tackle unbalanced data in dataset. SMOTE was used to maintain the equilibrium of fully trust,weakly trust and untrust values i.e attackers and normal/non-attackers. The above method may give the optimum accuracy. The dataset has been splitted into X_train, X_test, y_train and y_test with test size of 0.2 (80% for training and 20% for testing). Feature extraction have been done to reduce the number of feature components to 2 from the joint dataset. Feature Extraction aims to minimize number of features in a dataset by forming new features from the original one (then ditch the actual ones). Feature Extraction techniques advantages are:

- Improve the accuracy
- Overfitting risk reduction
- Training speed increased
- Enhance the visualization of data
- Increase in explainability model

Autoencoders, Principal Component Analysis (PCA), LBA (Local Binary Pattern), t-distributed Stochastic Neighbor Embedding (t-SNE), Locally Linear Embedding (LLE), Linear Discriminant Analysis (LDA), Independent Component Analysis (ICA) are some important Feature Extraction techniques. To analyze EEG and fMRI Independent Component Analysis is used. PCA is one of the most used linear dimensionality reduction techniques. But For Image dataset, LBP (Local Binary Pattern) achieves better performance with different sizes of datasets compared to PCA (Principal Component Analysis) [17]. we have used A Random Forest Classifier PCA for the feature extraction purpose. PCA set of features led to 98% classification accuracy. Then we did feature scaling so that all features are contributing equally and no features is dominating over another.

## 3.2. Proposed Algorithms

After going through the paper [16] on the evaluation of tree-based ensemble machine learning methods, we evaluated the different ensemble methods and find out that the Adaboost ensemble method provides relatively higher accuracy as compare to other ensemble methods. Hence, we opted Adaboost as the ensemble method to use for our trust model. The comparison of accuracies of different ensemble ML methods for our two datasets have been proved through boxplots. From the boxplot, we found that the accuracy score of Adaboost is higher. Adaboost or Adaptive Boosting is a boosting machine learning technique where multiple weak learners are combined

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 503-511 | e-ISSN: 2347-470X

by a classifier through a weighted linear combination. First Adaboost chooses a training subset randomly, then it trains the model by accurate prediction of the previous training. for training the model the adaboost needs certain parameters like base_estimator, n_estimators and learning_rate. base_estimator is a weak leaner used for training the model. n_estimators is the number of weak learners to train repetitively. Learning_rate is the weight of the weak learners. this process continues until the full training dataset is fitted or until it has reached its specified maximum number of estimators.

We have proposed a ML adapted STIN+NSL-KDD algorithm to combine trust and ML in presence of an effective dataset. As Usual, two key points have to be considered, efficiency of identifying traffic and synchronization of processing time. Due to the limited resources of the satellite network, the complexity of the training model will greatly affect the Training time of the satellite nodes. The basic procedure of our proposed basic ML model has been summarized in the following Flowchart.

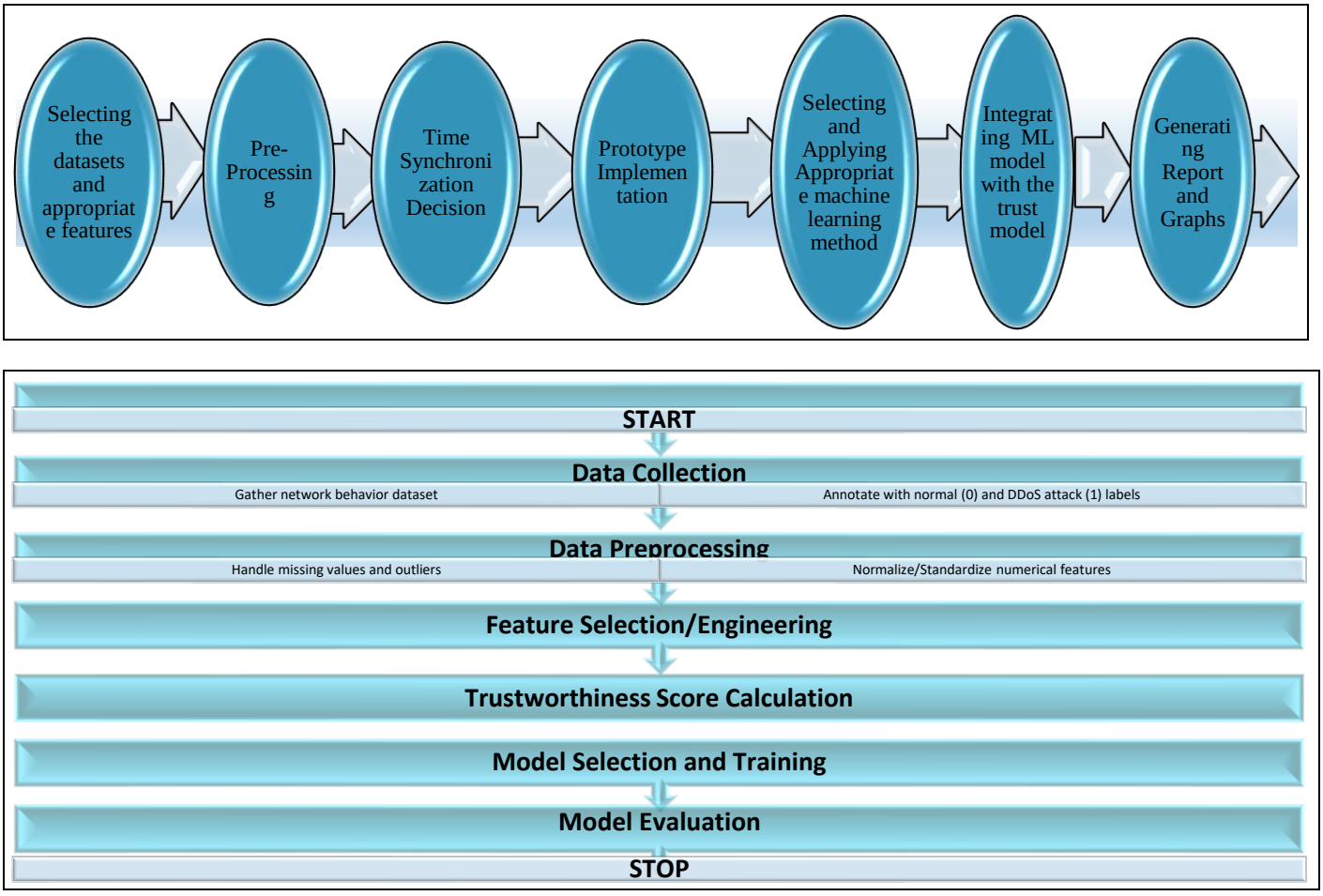


**Figure 4.** Steps of working alongwith Flowchart of our proposed ML method

The main phases for developing a holistic trust model for DDoS detection in terrestrial and satellite-based networks using machine learning are displayed in the above diagram. A decision or process has been denoted by each oval shape, and the execution flow is represented by arrows.

We have created a Ada-boost model by declaring the Ada-boost classifier in which our base_estimator is SVC (Support Vector Classifier), n_estimators is 50 and Learning Rate is 1. To train Adaboost Classifier we used fit () and fitted the X_train and y_train into it. Then we predicted the response for test dataset with respect to the training dataset that we give to the Adaboost Classifier.

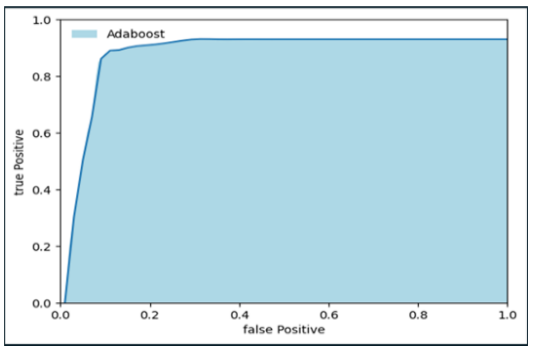


**Figure 5.** AUC ROC curve of our proposed method

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 503-511 | e-ISSN: 2347-470X

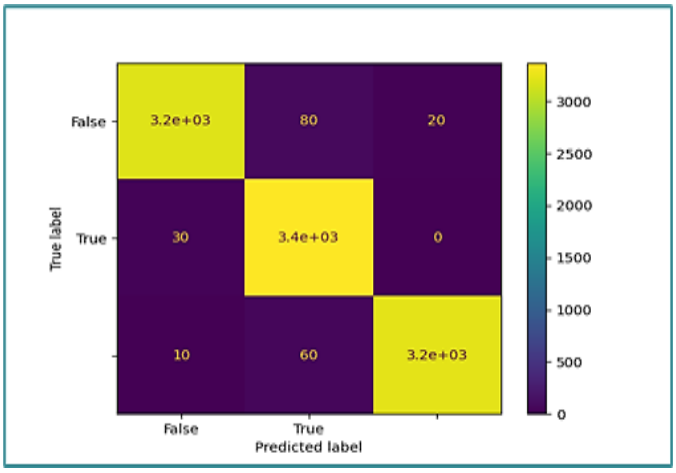


**Fig6.** Confusion Matrix

**Table 2. Classification Report of our proposed method**

| | PRECISION | RECALL | F1-SCORE | SUPPORT |
|---|---|---|---|---|
| **Class1: Not trustable** | 0.98 | 0.97 | 0.97 | 3300 |
| **Class 2: Weakly trustable** | 0.97 | 0.99 | 0.98 | 3400 |
| **Class3: Fully trustable** | 0.99 | 0.98 | 0.98 | 3300 |
| **accuracy** | | | 0.98 | 10000 |
| **macro avg** | 0.98 | 0.98 | 0.98 | 10000 |
| **Weighted avg** | 0.98 | 0.98 | 0.98 | 10000 |

we used the metrics module for accuracy calculation for sklearn. Calculating the accuracy from Adaboost confusion matrix we get accuracy of nearby 98%. We found the accuracy by comparing the predicted values to the actual test values. Our accuracy is 98% or above. Hence, it can be concluded that by using the attack dataset combination and applying pre-processing, we have got a very good machine learning model that can very well, even not optimally identify and classify between malicious and non-malicious sources.

## 3.3 Trust Score Calculation

Determining initial trust ratings and modifying them in various stages of the routing choice necessitates taking into account a number of different elements, including the reputation of the node, past performance, network conditions, and immediate observations. In the context of the ensemble-based trust model and integrated ACO routing, the following steps can be taken to set initial trust scores and update them in defense against DDoS attacks:

### 3.3.1. Determining the Initial Trust Scores of Network Components

• ***Node features:*** Determine the initial trust scores by looking at the nodes' basic features, like their security features, reliability, and reputation. Low initial trust scores can be attributed to nodes with recognized flaws or instances previously.

• ***Historical analysis Behavior:*** In order to assess the initial trustworthiness of nodes and routes, cover the past behavior data from the NSL-KDD+STIN dataset. Low trust scores may be assigned to nodes that have a history of malicious activity or conventional DDoS attacks.

• ***Desired Reliability:*** To determine initial trust scores, focus into account desired reliability measures like nodes uptime, bandwidth availability, and latency. Outstanding trustworthy nodes could start on with higher trust scores.

### 3.3.2. Trust Score Updating

***1. Observations and Feedback:*** Keep an eye on network instances and accumulate input from DDoS attack detections and options for routing. Refresh trust scores in response to real-time observations of things like DDoS attack instances, network congestion, and successfully completed routes.

***2. Reputation Managerial Behavior:*** Over time, update trust scores according to nodes' and routes' reputations. Nodes with declining performance or security events may see a reduction in trust scores, while nodes that continuously behave trustworthy and enhance routing may see an increase in trust scores.

***3. Ensemble Model Estimations:*** To dynamically update trust ratings, use the ensemble-based trust model's predictions. The trust scores of nodes and routes that the ensemble model flags as possible sources or targets of DDoS assaults may be modified accordingly.

***4. Pheromone Updating Rule:*** The ACO algorithm's pheromone update rule have used trust scores. Pheromone trails can be made stronger or less powerful according to how trustworthy the routes are; paths with higher trust scores have been promoted, while those with lower trust scores should be avoided.

Here, in terms of TCP SYN DDoS attacks we have compared our model with that of other 2 routing models [24] as well as traditional ACO based SP (shortest Path) model. As shown in *fig. 7*, We computed the average path delay of 4 routing models under in the presence of different types of DDoS malicious traffics like, the traditional Syn_DDoS and UDP_DDoS. Node delay time and propagation time cover the most part of path delay. assuming that the time for communication processing and evaluation in the above scenario and a routing node's forwarding delay is 10 ms. The propagation delay is defined as the proportion of path distance and speed of light. Avarage Path delay of ACO-SP is lowest since it is the nearby optimal shortest path found by ACO algorithm. The path delay of our

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 503-511 | e-ISSN: 2347-470X

proposed model is higher than the ACO-SP since it is considering trust as a measure to find out the next hop in the routing path, but it is lower than the TR and HR algorithms that shows even if we have used trust in the aim for secure routing, routing speed has not been compromised. This has been summarized in *table 3*. Additionally, we realize that the targeted node in the routing process need to be the one that should be avoided the most because the addressed node's usual traffic will be adversely impacted the lower AR is calculated by the TR and SP algorithms, while a higher AR is gained by our proposed (P) and HR algorithms.

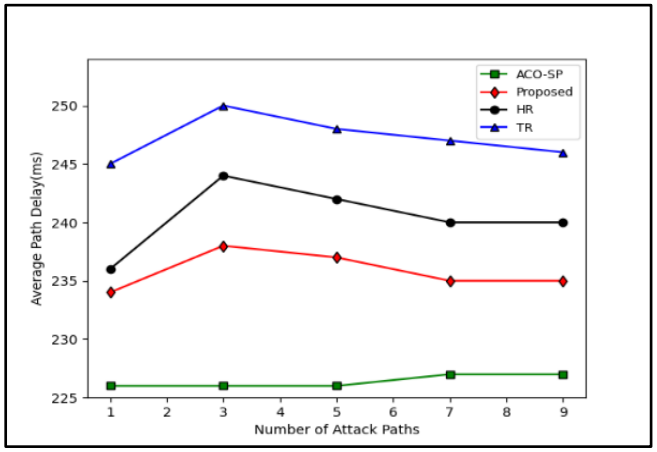


**Figure 7.** Average path delays of 4 different algorithms

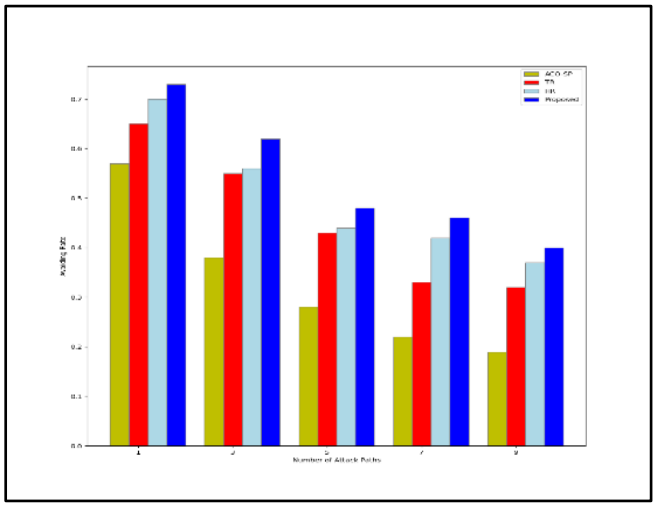

**Figure 8.** Avoiding Rates of 4 different algorithms

**Table 3. Comparison of our proposed model with other models**

| Model | Average Path Delay(ms) |
|---|---|
| HR | About 2% higher than that of ACO-SP algorithm |
| TR | About 3% higher than that of ACO-SP algorithm |
| ACO-SP | Around 225 to 230 |
| Proposed | About 1% higher than that of ACO-SP algorithm |

Thus, our proposed learn model can be used for the design of secured and trust models for LSTN communications.

## 4. CONCLUSIONS

For the continuous operation of a satellite network, a routing protocol should have to take care some of main features. Fault tolerance is one of those main features. In any way or situation, like lack of energy, sensor malfunction, physical defect, creation of path break, the network should sustain itself and should not create transmission problem in between the source and destination. our performance should be improved with respect to longevity, robustness, and overloading. To do so, network's all the alternative paths have to be maintained as highly important and guaranteed ones with the help of control messages. We have proposed in our model one trust-based attack resistant protocol that can work quite well as compared to some existing variant models of SATCOM. We have taken some parameters as mentioned in our previous sections. Still there remains lots of measurements to be done by comparing with other existing protocols also in terms of other parameters. We should do Fine-Tuning: If the model's performance is not satisfactory grade, Trying experiment with various models, modifying the hyperparameters, or enhancing feature engineering, Deployment: After ensuring satisfaction with the model's performance, putting it into use within the satellite network configuration, Continuous Monitoring and Updating: maintaining updated on the network and get the latest data and utilizing the latest data to update the model in a regular basis in order to cope with changing attack patterns. Mostly, we can extend our simulation work with very large-scale as well as heterogeneous datasets. Hence, our future task with regard to our proposed model is to extend the above for very large-scale networks and simulating with a comparison of many existing variant models with different types of measurement parameters, particularly Fault Tolerance and QoS measurements. Also, Real-time monitoring, through alerting and mitigation continuous improvement has to be observed in the proposed model. We have to Include constraints in the ACO algorithm, like link capacity, network congestion, and quality of service requirements. If we are successfully able to do so, then it is high chance that our proposed model can be applied in real satellite-enabled applicable areas.

## REFERENCES

[1] Lin, Z., Lin, M., Champagne, B., Zhu, W. P., & Al-Dhahir, N. (2020). Secure beamforming for cognitive satellite terrestrial networks with unknown eavesdroppers. IEEE Systems Journal, 15(2), 2186-2189.
[2] Lin, Z., Lin, M., Champagne, B., Zhu, W. P., & Al-Dhahir, N. (2020). Secure and energy efficient transmission for RSMA-based cognitive satellite-terrestrial networks. IEEE Wireless Communications Letters, 10(2), 251-255.
[3] Boley, A. C., & Byers, M. (2021). Satellite mega-constellations create risks in Low Earth Orbit, the atmosphere and on Earth. Scientific Reports, 11(1), 10642.
[4] Del Portillo, I., Cameron, B. G., & Crawley, E. F. (2019). A technical comparison of three low earth orbit satellite constellation systems to provide global broadband. Acta astronautica, 159, 123-135.
[5] Rossi, A., Petit, A., & McKnight, D. (2020). Short-term space safety analysis of LEO constellations and clusters. Acta Astronautica, 175, 476-483.
[6] Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., ... & Gadekallu, T. R. (2022). Federated learning for intrusion detection system: Concepts, challenges and future directions. Computer Communications.

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 503-511 | e-ISSN: 2347-470X

[7] Shah, S. M. J., Nasir, A., & Ahmed, H. (2014). A survey paper on security issues in satellite communication network infrastructure. International Journal of Engineering Research and General Science, 2(6), 887-900.
[8] Li, H., Shi, D., Wang, W., Liao, D., Gadekallu, T. R., & Yu, K. (2022). Secure routing for LEO satellite network survivability. Computer Networks, 211, 109011.
[9] Muhaidheen, M., Muralidharan, S., & Vanaja, N. (2022). Multiport Converter for CubeSat. International Journal of Electrical and Electronics Research, 10(2), 290-296.
[10] Zhang, Y., Wang, Y., Hu, Y., Lin, Z., Zhai, Y., Wang, L., ... & Kang, L. (2022). Security Performance Analysis of LEO Satellite Constellation Networks under DDoS Attack. Sensors, 22(19), 7286.
[11] Ashraf, I., Narra, M., Umer, M., Majeed, R., Sadiq, S., Javaid, F., & Rasool, N. (2022). A deep learning-based smart framework for cyber-physical and satellite system security threats detection. Electronics, 11(4), 667.
[12] Li, K., Zhou, H., Tu, Z., Wang, W., & Zhang, H. (2020). Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning. IEEE Access, 8, 214852-214865.
[13] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009, July). A detailed analysis of the KDD CUP 99 data set. In 2009 IEEE symposium on computational intelligence for security and defense applications (pp. 1-6). Ieee.
[14] Aburomman, A. A., & Reaz, M. B. I. (2016). A novel SVM-kNN-PSO ensemble method for intrusion detection system. Applied Soft Computing, 38, 360-372.
[15] Aburomman, A. A., & Reaz, M. B. I. (2016, October). Ensemble of binary SVM classifiers based on PCA and LDA feature extraction for intrusion detection. In 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC) (pp. 636-640). IEEE.
[16] Ampomah, E. K., Qin, Z., & Nyame, G. (2020). Evaluation of tree-based ensemble machine learning models in predicting stock price direction of movement. Information, 11(6), 332.
[17] Divya, C. D., & Rajendra, A. B. (2020). Review on Prevailing Difficulties Using IriS Recognition. In Computational Vision and Bio-Inspired Computing: ICCVBIC 2019 (pp. 656-661). Springer International Publishing.
[18] Jenila, L., & Canessane, R. A. (2022). Cross Layer Based Dynamic Traffic Scheduling Algorithm for Wireless Multimedia Sensor Network. IJEER, 10(2), 399-404.
[19] Manhar, A., & Dembla, D. Improved Hybrid Routing Protocol (IHRP) in MANETs Based on Situation Based Adaptive Routing.
[20] Behera, B. B., Mohanty, R. K., & Pattanayak, B. K. (2022). Attack Detection and Mitigation in Industrial IoT: An Optimized Ensemble Approach. Specialusis Ugdymas, 1(43), 879-905.
[21] Ballav, B., Rana, G., & Pattanayak, B. K. (2015, December). Investigating the effect of Black Hole attack on Zone Based Energy Efficient Routing Protocol for Mobile Sensor Networks. In 2015 International Conference on Information Technology (ICIT) (pp. 113-118). IEEE.
[22] Swain, J., Pattanayak, B. K., & Pati, B. (2021). A systematic study and analysis of security issues in mobile ad-hoc networks. In Research anthology on securing mobile technologies and applications (pp. 144-150). IGI Global.
[23] Zhu, H.; Chen, S.Y.; Li, F.H.;Wu, H.; Zhao, H.Q.;Wang, G. User random access authentication protocol for low earth orbit satellite networks. J. Tsinghua Univ. (Sci. Technol.) 2019, 59, 1–8. [CrossRef]
[24] K. Li, H. Zhou, Z. Tu, W. Wang and H. Zhang, "Distributed Network Intrusion Detection System in Satellite-Terrestrial Integrated Networks Using Federated Learning," in IEEE Access, vol. 8, pp. 214852-214865, 2020, doi: 10.1109/ACCESS.2020.3041641.
[25] https://www.keysight.com/us/en/assets/3122-1407/data-sheets/EXata-Cyber-Attack-Emulator-Library.pdf