Temasek Defence Systems Institute

Temasek Defence Systems Institute

A Network Intrusion Detection System on an Integrated Satellite-Terrestrial Network Based on Unmanned systems using Decision Tree Machine Learning

Author: Yap Kok Siong Jason (DSO National Laboratories)

Thesis advisors: Prof. Preetha Thulasiraman, ECE Dept., (Naval Postgraduate School)

Introduction

In recent years, there has been a surge in interest in Integrated Satellite-Terrestrial Networking (ISTN) architectures based on unmanned or autonomous systems. Over the last several years, developing interoperable networking protocols to connect satellite networks with terrestrial networks has been an ongoing topic of research. In addition, investigations on how to establish secure networking to prevent cyber-attacks against ISTNs is also of interest.

Objectives

Our goal was also to build a NIDS using the Decision Tree machine learning algorithm while identifying the critical location of NIDS in the ISTN architecture.

The contributions of this thesis are as follows:

- Identification of the placement of NIDS for a proposed cohesive ISTN architecture with various unmanned systems.
- Incorporation of NIDS with Network Control Center (NCC) and a Network Management Center (NMC), which is comprised of a data collector, feature extractor, classifier, anomaly detector, and response administrator to allow the network architecture to react according to the cyber-attack threat.
- Use of valid integrated satellite-terrestrial communication network security datasets from an open-source thesis to perform cyber-attack detection using Decision Tree machine learning.
- Proof that different attacks can be grouped together based on objectives, and that supervised machine learning using the decision tree algorithm can segregate the various classes of attack traffic from benign traffic.

Decision tree implementation

DT is one of the most popular algorithms in ML. The benefits of DT are that it can quickly learn from a dataset by studying information about the system's crucial features that reveal malicious activity.

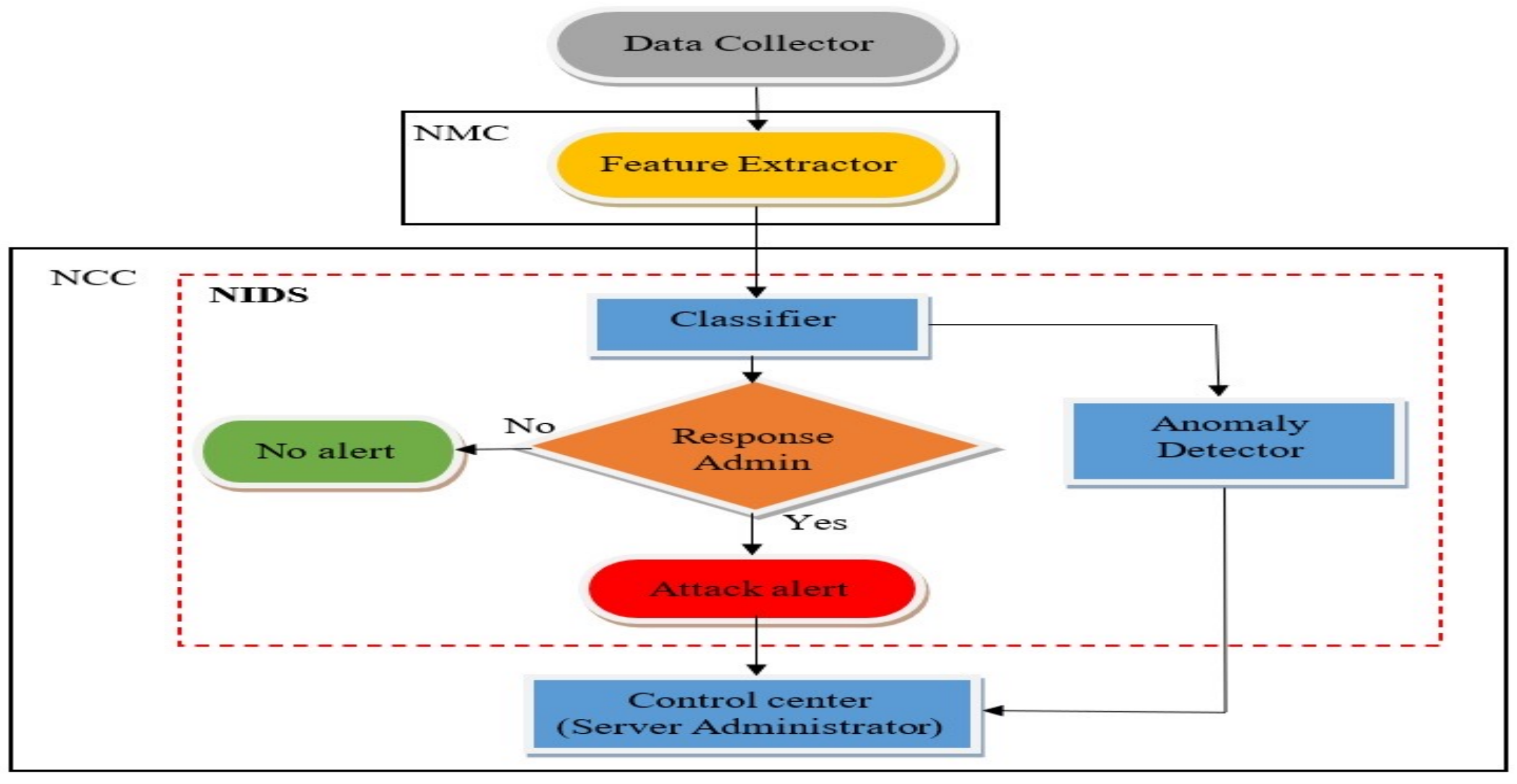
It uses a non-parametric approach that is not dependent on probability distribution assumptions and is distribution-free [29]. It can promote to check on any advancement of attack signatures and different activities that have occurred while perceiving the data patterns.

As a result, the value of various security frameworks is increased by examining the layout of intrusion detection information [17]. Unlike other classification algorithms, the decision tree uses non-linear relationships between parameters that does not influence the performance results.

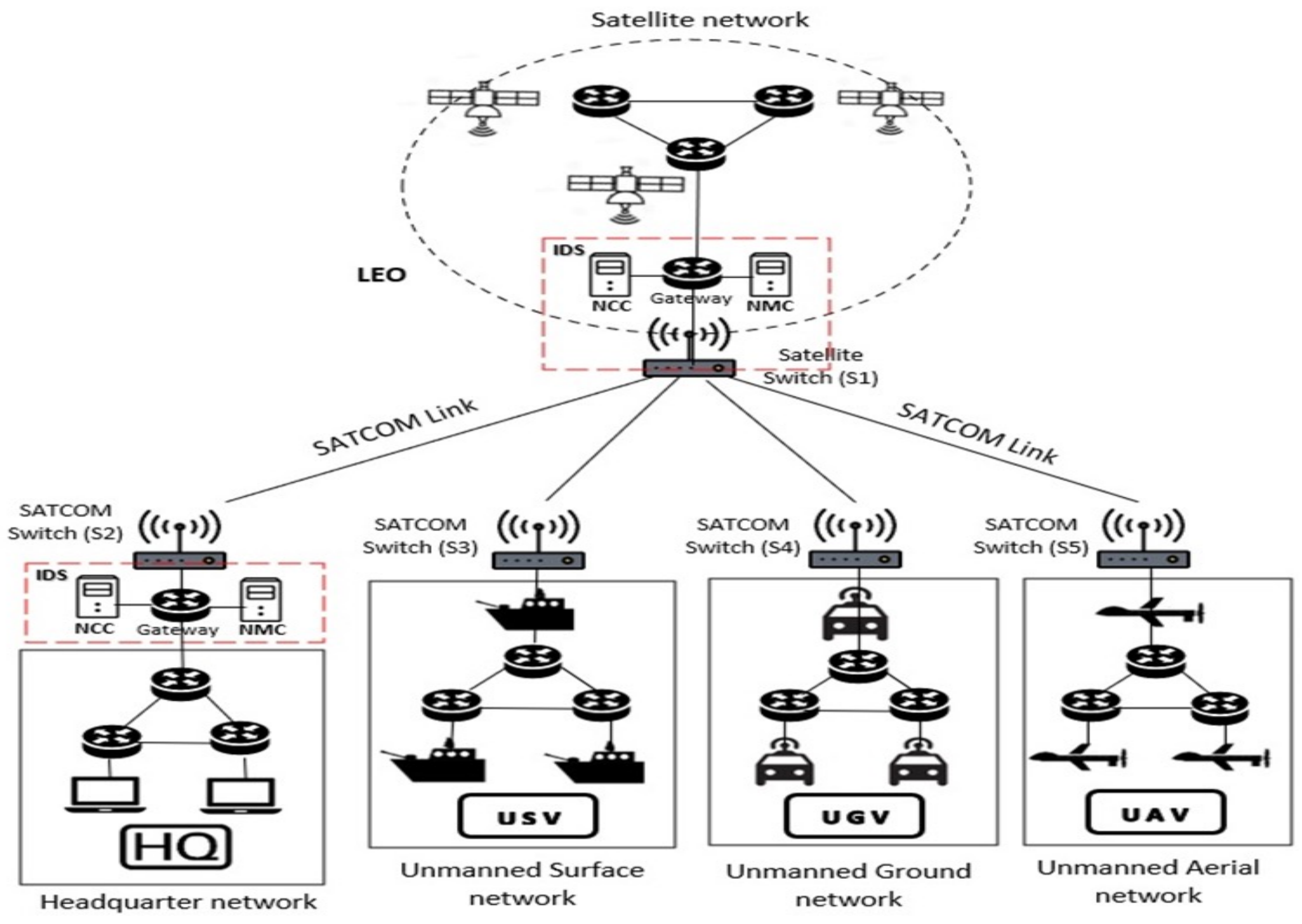
It also gives a rich arrangement of rules, which are simple, straightforward and require a shorter training period. The DT can also be easily integrated with the technologies in real-time applications.

Proposed security architecture

Our proposed security system includes a classifier and an anomaly detector which can identify both known and unknown threats quickly. This system should be able to initiate particular reactions in order to safeguard the network's integrity, isolate the regions under attack, and promptly notify the server authorities. The NIDS is identified within the flow chart.



Hence, NIDS is deployed at two key locations in the network. One is in the HQ, while the other is at the satellite network shown. We understand that if the HQ or satellite network system fails, we will be unable to establish connection with the mission's many unmanned systems. These two locations are essential and critical to the entire network.



Summary of anaysis

The overall accuracy for the simulation runs for DT (Fine) machine learning algorithm using three different split criterions. The results show that MDRS performs the best when it comes to detecting either benign-terrestrial or benign-satellite attacks

Experiments	Split criterion		
Using Decision Tree (Fine)	Gini's diversity index (GDI)	Twoing rule (TR)	Maximum deviance reduction selection (MDRS)
Benign -Terrestrial Network Attack	98.6%	98.6%	**99.6%**
Benign - Satellite Network Attack	98.1%	98.1%	**98.3%**
Benign – Combined	**91.7%**	91.0%	91.2%

For the simulation runs for DT (Fine) machine learning algorithm using three different split criterions with an increasing number of splits from 100 to 200.

Experiments	Split criterion		
Using Decision Tree (Fine)	Gini's diversity index (GDI)	Twoing rule (TR)	Maximum deviance reduction selection (MDRS)
Benign – Combined	**93.3%**	93.2%	93.0%

Future Work

1. Implement other supervised Machine Learning algorithms
2. Generate and obtain more datasets for ISTN

Reference:

[17] S. C. L. Shilpashree. S, Nayana G Bhat, Sunil Kumar G, "Decision Tree: A Machine Learning for Intrusion Detection," International Journal of Innovative Technology and Exploring Engineering (IJITEE), April 2019.

[29] "Advantages of a Decision Tree for Classification." Python Learn Python Programming. https://pythonprogramminglanguage.com/what-are-the-advantages-of-using-a-decision-tree-for-classification/ (accessed.

NUS National University of Singapore