IDS using Reinforcement learning

Under Dr. Kamalakanta Sethi Sir

Team members: Chandra Shekar PV

Dheeraj

Samhitha

Problem Statement

- To design an effective deep reinforcement learning-based IDS that can efficiently learn from its environment and make accurate decisions in real-time while minimizing false positives and negatives.

Introduction: What is an IDS?

- An IDS(Intrusion Detection System) analyzes the data packets from the network and the system-level applications to detect any malicious activity.
- An IDS detects an attack as soon as possible and takes appropriate action.
- It can deal with both insider and outsider attacks

IDS Architecture

- Agent like logger; it gathers data for analysis.
- It is also known as sensor.
- Director: It is like the analyzer, it would analyze the data obtained from the agents according to its internal rules.
- Notifier: The notifier is the component of the IDS that alerts the security team when a security breach or attack is detected

Different types of IDS system:

- Based on the monitoring environment IDS are classified as
- Host based IDS
- Network Based IDS

- Based on the Detection model IDS are classified as:
- IDS using Signature detection
- IDS using Anomaly detection

- Based on the Architecture IDS are classified as:
- Centralized IDS
- Distributed IDS

Motivation:

- Due to the recent advancements in the Internet of Things (IoT) technologies, the detection and prevention of intrusions in enterprise networks have become a crucial and challenging task.
- An IDS system is designed to detect potential security threats that might go unnoticed by other security measures.
- It helps to identify intrusions and security breaches in real time.

Challenges:

- **False positives and false negatives**: IDSs must accurately detect threats without generating too many false alarms or missing real threats.
- **Attack diversity:** Hackers use a wide range of tactics and techniques to infiltrate systems, and IDSs must be able to detect and respond to these various methods.
- **High-performance requirements:** IDSs must be able to analyze large volumes of data in real-time to detect threats as quickly as possible.

The nascent stage of the research: Traditional machine learning techniques

- The support vector machine (SVM), is among the most successful and widely used machine learning algorithms used in intrusion detection systems.
- SVMs are well-suited for detecting attacks because they can handle high-dimensional data, are robust to noise and outliers, and can generalize well to new data.
- These traditional machine learning techniques can be used to build a basic IDS that can detect some types of attacks.
- However, they have limitations, and more advanced techniques, such as deep learning, may be necessary to build a more robust and effective IDS.

The limitations posed by the machine learning technique's:

- **Data quality and quantity:** ML algorithms require large amounts of high-quality data to accurately learn patterns and make predictions.
- **Feature engineering:** Feature engineering involves selecting and extracting the most relevant features from the data to train the ML model.
- **Adversarial attacks:** Attackers may try to evade IDS by using adversarial attacks, such as injecting malicious code into network packets that can fool the ML algorithms.

Reinforcement Learning:

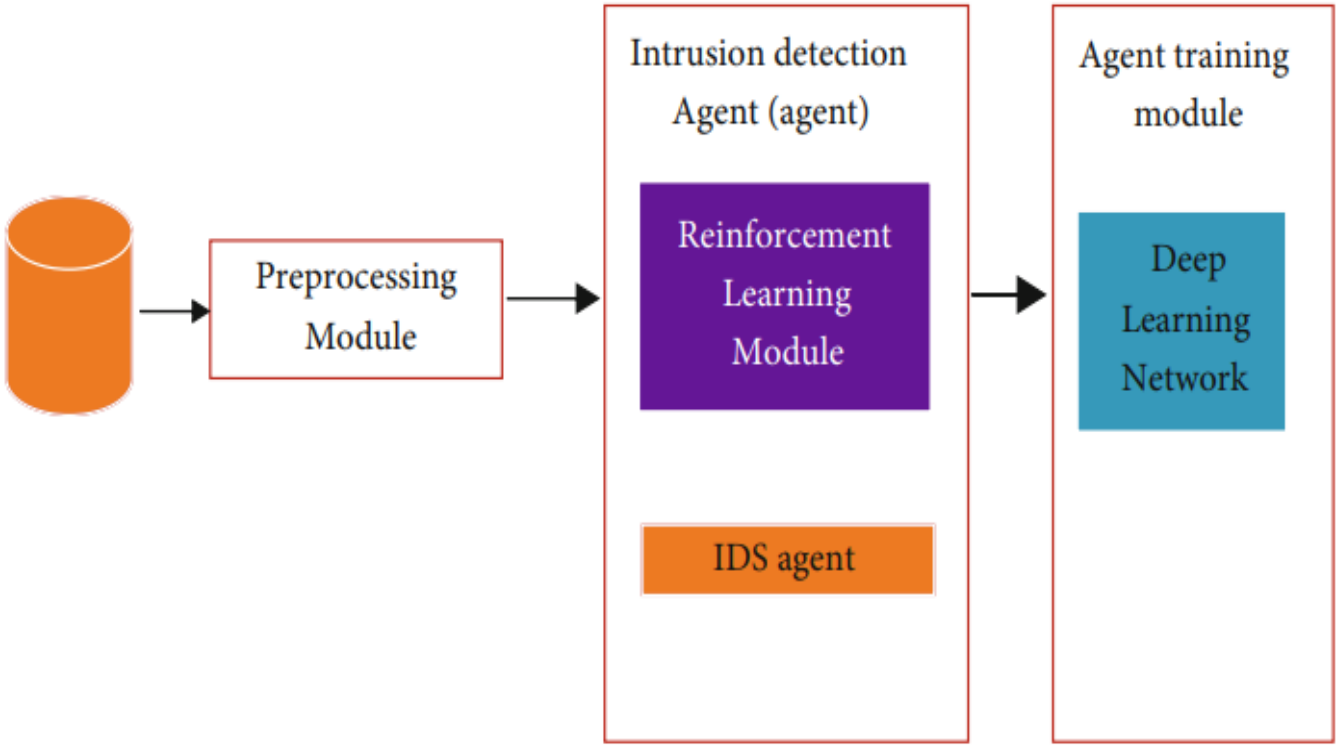
- Reinforcement Learning (RL) is a type of machine learning in which an agent learns to make decisions in an environment to maximize a cumulative reward.
- In RL, the agent does not have access to a labeled dataset like supervised learning.
- RL can be made model free which gives edge over machine learning
- RL has been applied to a wide range of applications, including autonomous driving, game playing, robotics, and finance

Reinforcement Learning to the rescue:

- **Continuous learning:** RL can continuously learn and update its policy as new data becomes available, leading to more robust and up-to-date IDS.
- **Feature engineering:** RL can learn relevant features automatically through trial and error, reducing the need for expert feature engineering.
- **Adversarial attacks:** RL can be used to train IDS that are more robust to adversarial attacks by incorporating these attacks into the training process.
- We will be using Deep reinforcement learning as the solution to our problem statement.

Literature Review-I: **Intrusion Detection System for Industrial Internet of Things Based on Deep Reinforcement Learning**

- Due to its complexity and openness, the Industrial Internet of Things faces increasing network security threats.
- As a result, conventional intrusion detection technology cannot satisfy the network threat.
- The proposed model here presents a near-end strategy optimization method for the IDS based on DRL.
- This method combines deep learning's observation capability with reinforcement learning's decision-making capability for efficient detection.

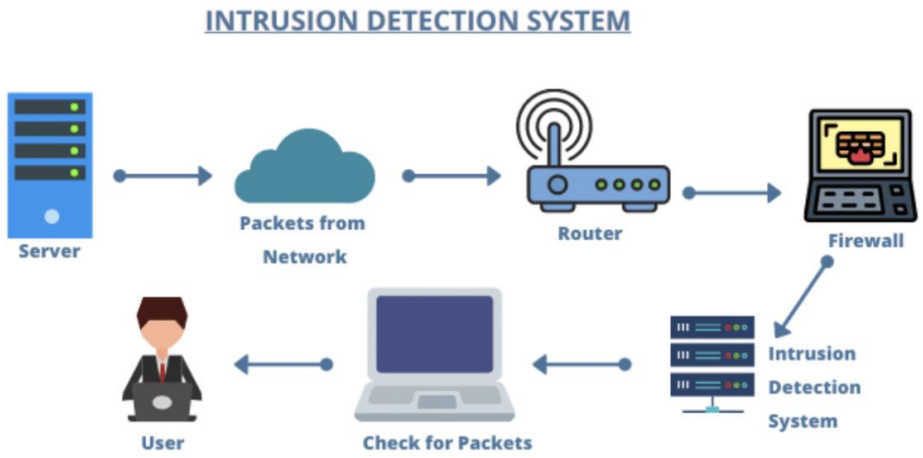


Proposed model for reinforcement learning based IDS for IOT data.

- The system extracts the most appealing feature set using a feature selection method based on LightGBM.
- Here, we construct an intrusion detection system based on the deep reinforcement learning PPO2 algorithm.
- The intrusion detection system is effective and has defeated 99.9% of different kinds of cyber assaults.
- Precision, recall rate, F1 score, and other indicators, outperforms current DL based models and other DRL models.

Literature review – II: **A context-aware robust intrusion detection system: a reinforcement learning-based approach**

- Constant growth of usage of networks
- Novel attacks increasing day by day
- The techniques till now don't provide high accuracy and have less false positive rate.
- The breakout point : Defense against adversarial attacks

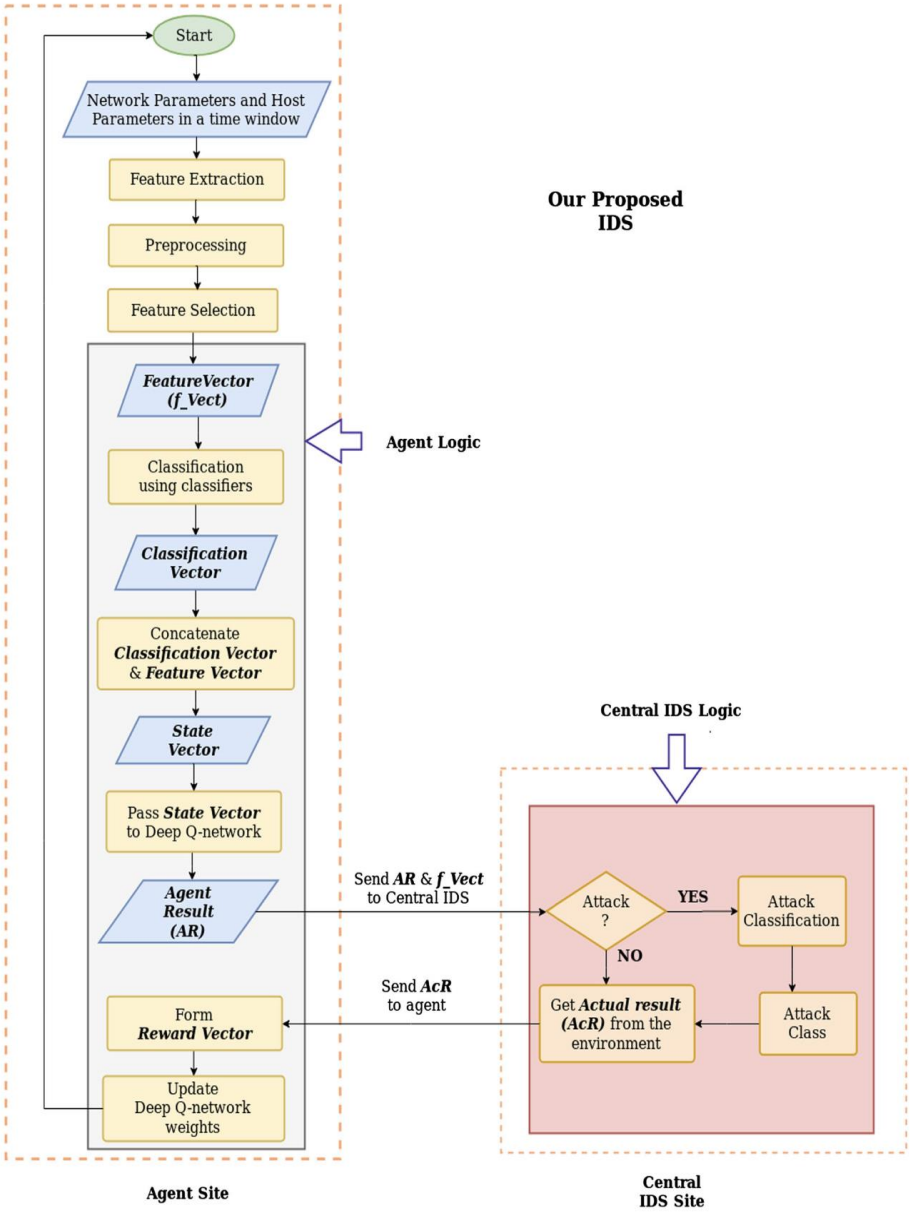


link

The proposed model:

- The dataset has been pre-processed using one hot encoding and L2 Normalization.
- Feature Engineering : reduce the features

Datasets	# total features	# selected features
NSL-KDD	41	36
UNSW-NB15	49	19
AWID	154	22


Our Proposed IDS
Start
Network Parameters and Host Parameters in a time window
Feature Extraction
Preprocessing
Feature Selection
FeatureVector (f_Vect)
Agent Logic
Classification using classifiers
Classification Vector
Concatenate Classification Vector & Feature Vector
State Vector
Pass State Vector to Deep Q-network
Agent Result (AR)
Send AR & f_Vect to Central IDS
Central IDS Logic
Attack ?
YES
Attack Classification
NO
Get Actual result (AcR) from the environment
Attack Class
Send AcR to agent
Form Reward Vector
Update Deep Q-network weights
Agent Site
Central IDS Site

Results and observations:

Action	Accuracy (%)	FPR (%)
Model before adversarial attack	81.80	2.6
Model after adversarial attack	78.44	5.8
Model after applying DAE	80.05	6.8

Literature Review - III: **Deep Q-Learning based Reinforcement Learning Approach for Network Intrusion Detection.**

- An RL agent is capable of enhancing its capabilities over time through self-learning without any supervision .
- The state explosion problem.
- Most of the Approaches:

  Can’t deal with large datasets.

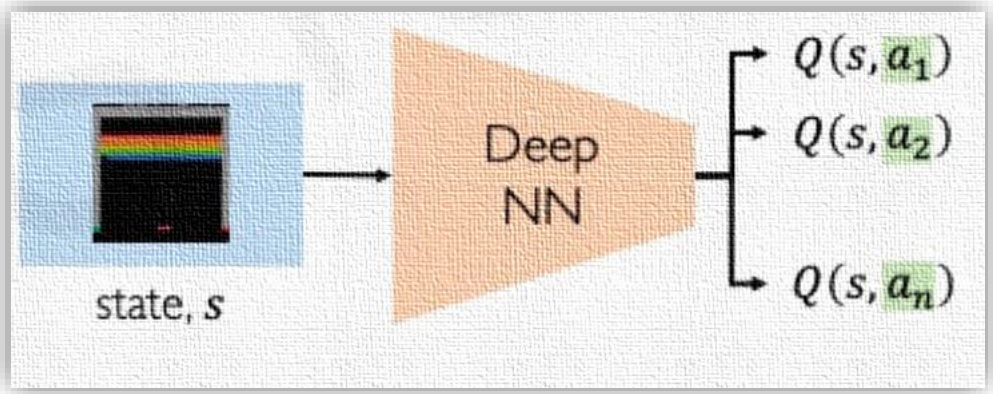
  Can’t detect the legitimate traffic with good accuracy.
- Deep reinforcement learning (DRL) :

  Can deal with Unmanageable huge number of state spaces.

We leverage a deep neural network as a function approximator for the Q-function.

A target Q value is obtained by adding the current reward and the next state's Q-value multiplied by the value of discount factor (λ).

Link



$$Loss = \frac{1}{n}\sum_{n}\left(\underbrace{Q(s,a)}_{\text{Prediction}} - \underbrace{r + \gamma Q(s',a')}_{\text{Target}}\right)^2$$

Link

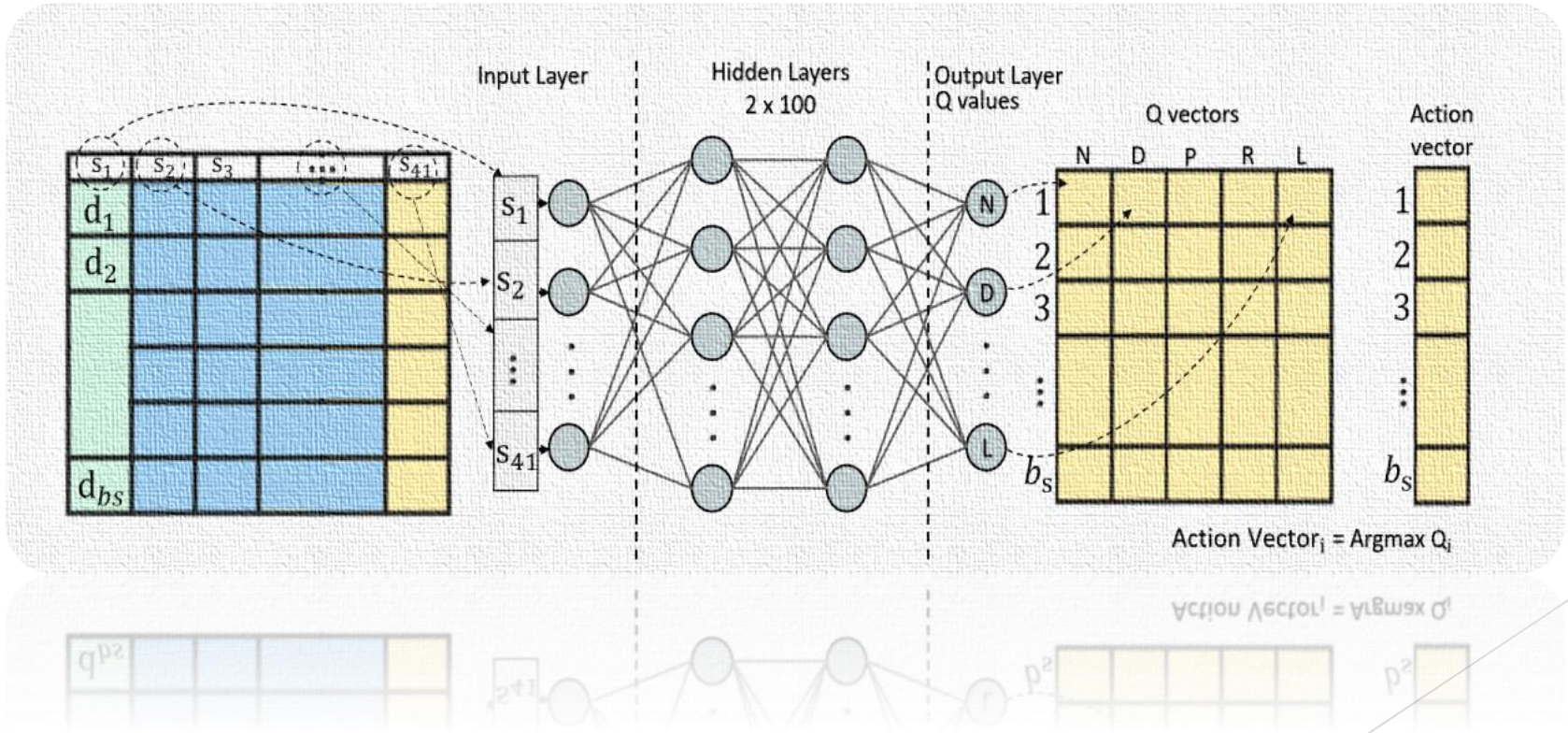
Bellman Equation

$$Q(s,a) = R(s) + \gamma \max_{a'} Q(s',a')$$

$Q(s,a)$: x — $R(s) + \gamma \max_{a'} Q(s',a')$: y

$Q(s,a)$ = Return if you
- start in state s.
- take action a (once).
- then behave optimally after that.

- The exploration helps the agent to select either a random action with a probability of e or an action, greedily based on the value function with the greatest value with a probability of 1 − e.
- 41 features as the inputs of DQN such that Si = Fi for training and prediction using DQN.



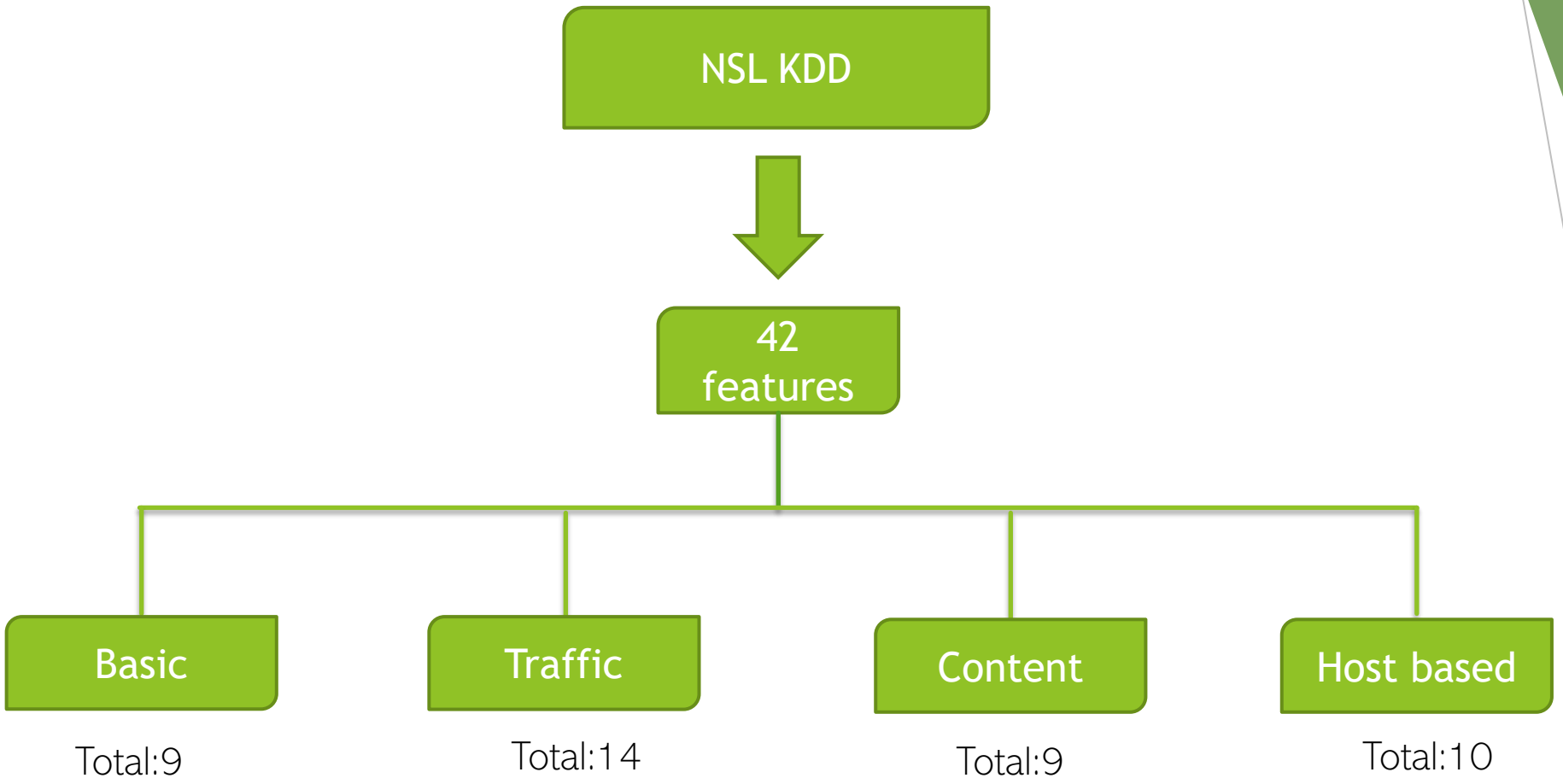
Results and Observations:

Metric	Discount Factors		
	$\gamma = 0.001$	$\gamma = 0.1$	$\gamma = 0.9$
Precision	0.7784	0.6812	0.6731
Recall	0.7676	0.7466	0.758
F1 score	0.8141	0.7063	0.6911
Accuracy	0.7807	0.7473	0.7578

Metric	Attack Categories			
	Normal	DoS	Probe	R2L
Accuracy	0.8094	0.9247	0.9463	0.8848
F1 score	0.8084	0.9237	0.9449	0.8370
Precision	0.8552	0.9249	0.9441	0.8974
Recall	0.8093	0.83	0.9247	0.8848

NSL-KDD DATASET

- Network Intrusion Detection dataset.
- Very Popular for Performance evaluation.
- Contains 41 Features and 1 label
- Total 5 attack Classes
  - Normal
  - Denial of service
  - Probe
  - Root to local
  - Unauthorized to root



Also, There are 4 categorical features,
One-Hot Encoding is performed on them

References:

- **Intrusion Detection System for Industrial Internet of Things Based on Deep Reinforcement Learning**

  Authors - Sumegh Tharewal , Mohammed Waseem Ashfaque , Sayyada Sara Banu , Perumal Uma , Samar Mansour Hassen , and Mohammad Shabaz

- **A context-aware robust intrusion detection system: a reinforcement learning-based approach.**

  Authors - Kamalakanta Sethi E. Sai Rupesh · Rahul Kumar ·

  Padmalochan Bera Y. Venu Madhav

- **Deep Q-Learning based Reinforcement Learning Approach for Network Intrusion Detection.**

  Authors– Hooman Alavizadehi, Jylian Jang-Jaccard and Hootan Alavizadeh

Future work:

- Data pre-processing by doing feature engineering and normalizing the features using L2 normalization and performing one hot encoding.
- Building a ML based IDS initially and developing it further into a deep reinforcement learning model using the concepts of Deep learning and Reinforcement learning.
- We would try to extend the model to the IoT devices.
- Furthermore, we would optimize the model to give the best possible results.