



SINAPSE Project

Intelligent Cybersecurity for CNS

SESAR Research project - CNS for ATM (“Intelligent CNS Network”), ATM Excellent Science & Outreach phase

EngageKTN’s Workshop on Vulnerabilities and global security of the CNS/ATM system , 10 Nov. 2020



Founding Members



The Team



Agenda

Overview – ALTYS Technologies

- Project idea
- Technological building blocks

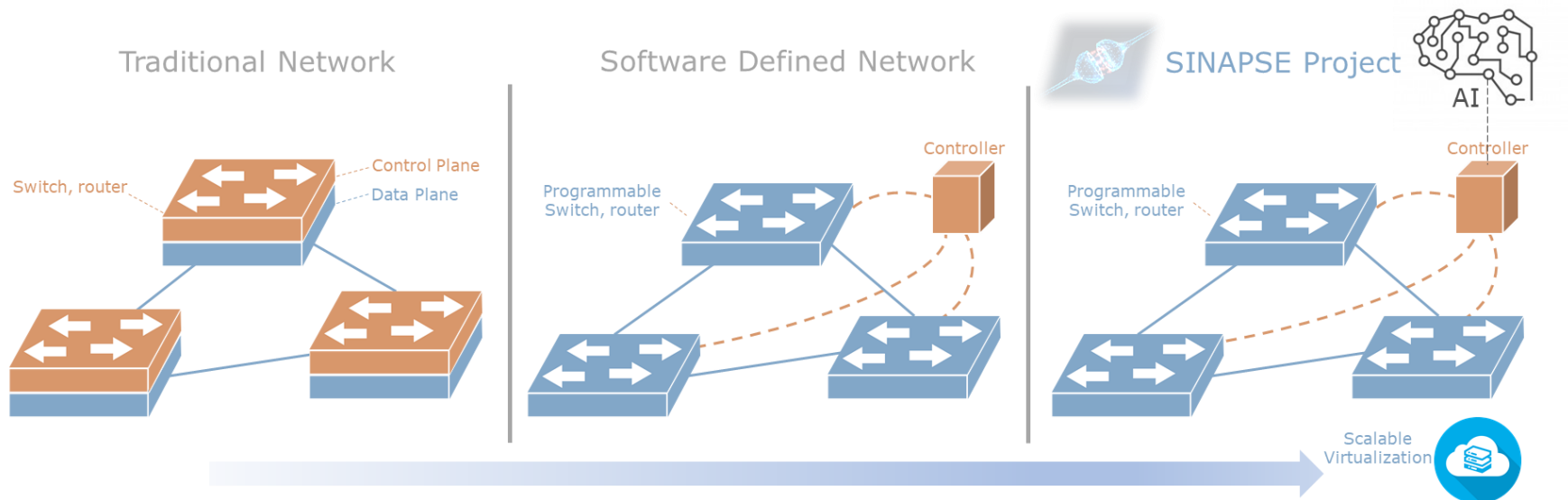
Cybersecurity Focus – University of Bradford

- Cybersecurity Architecture for CNS network
- Resilient Intrusion Detection & Prevention System (IDPS) for SDN powered by AI
- Securing AI from Cybersecurity Attacks
- Protecting AI against malicious AI-powered Cybersecurity Attack

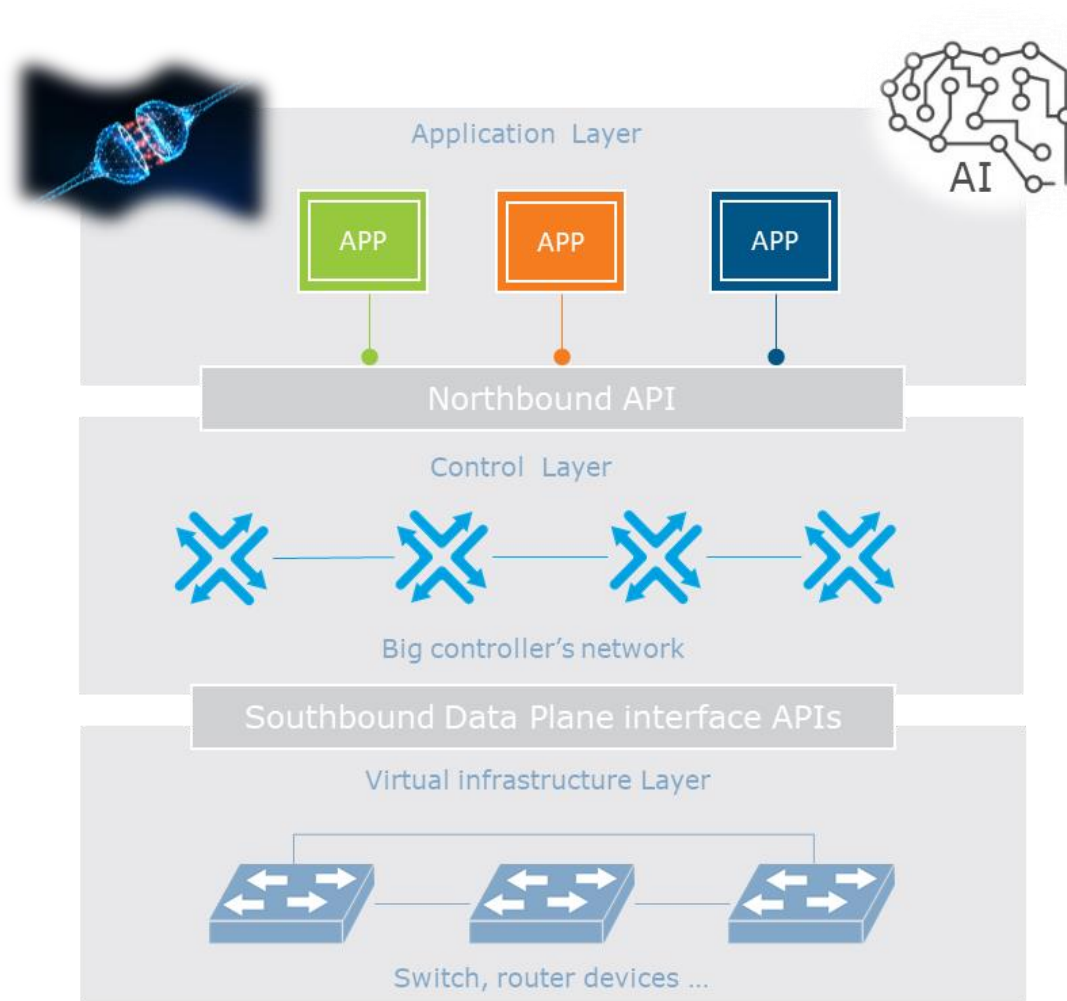
Project objectives

Intelligent & secured Aeronautical Datalink Communications network based on Software Defined Networking (**SDN**) augmented with Artificial Intelligence (**AI**)

- Predict and prevent safety services outages (e.g. ATN CPDLC)
- Optimize networking (e.g. QoS prediction and path selection)
- Intelligent Cybersecurity functions



Project objectives





Cybersecurity Architecture

Securing the aircraft / datalink / Ground



Founding Members



EUROPEAN UNION



EUROCONTROL

Security Architecture

Aircraft segment:

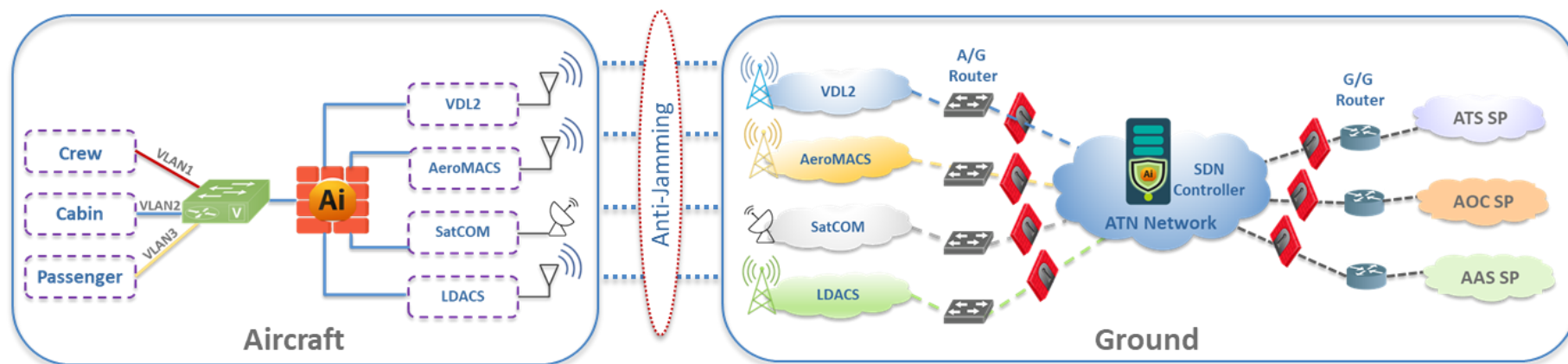
- Logical segregation of safety-critical and non-safety critical traffic domains
- Onboard router with AI-powered security gateway

Ground Segment:

- SDN controller for network management & Control
- IPDS powered by AI to secure SDN controller

Datalinks

- AI-based Anti-jamming





AI-powered Cyber Security Solutions

Resilient Intrusion Detection System (IDS) for SDN powered by AI

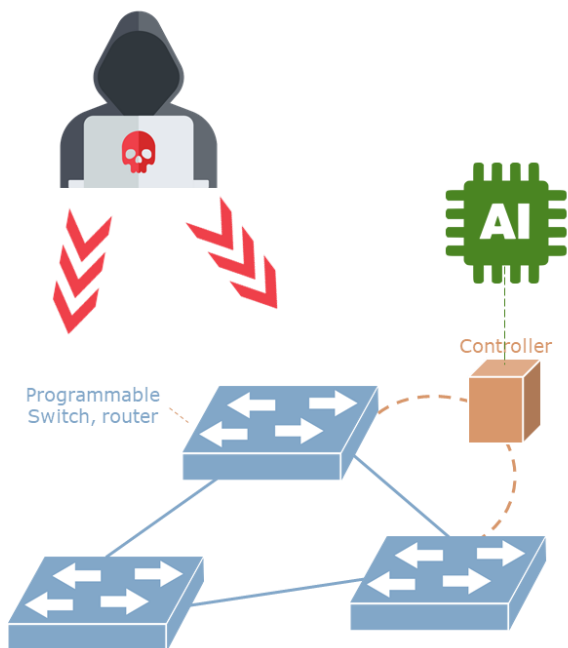


Founding Members

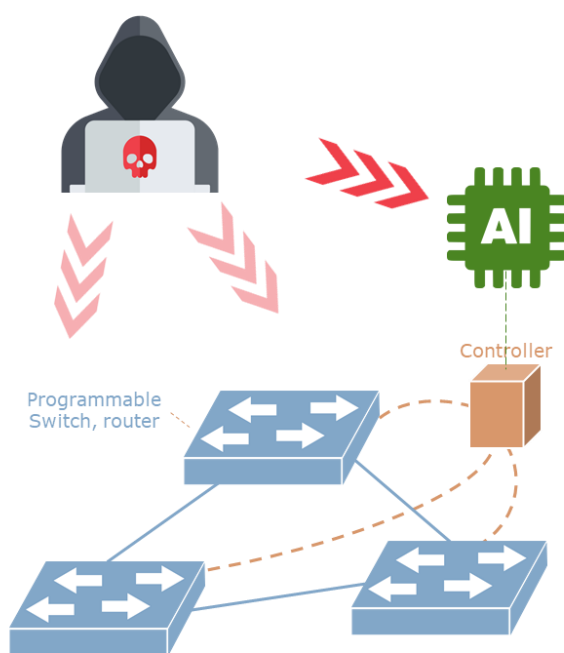


Proposed Solutions

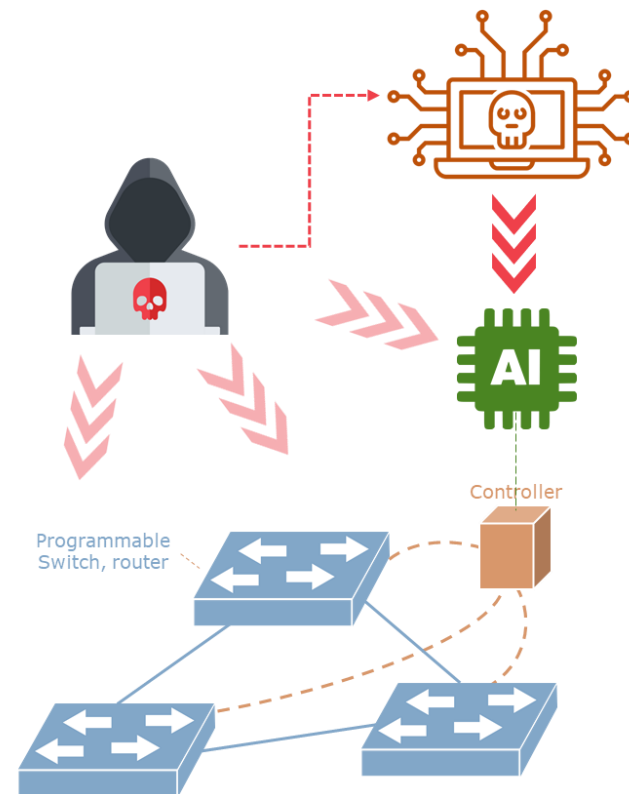
Level 1 – Securing the SDN Controller using AI



Level 2 – Securing AI from Cybersecurity Attacks

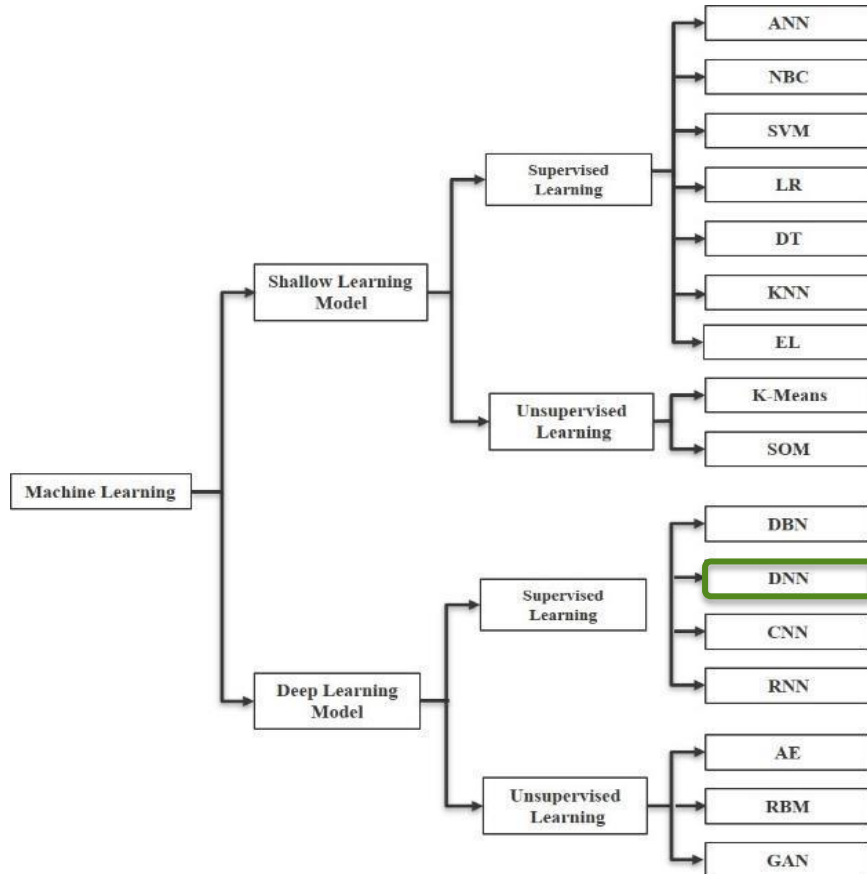


Level 3 – Protecting AI against malicious AI powered Cybersecurity Attack



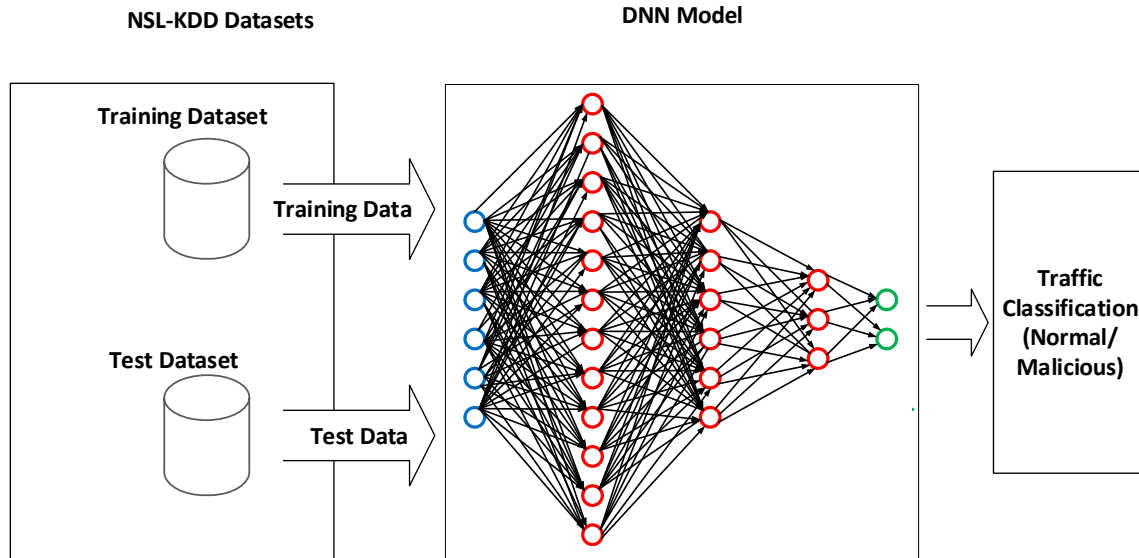
Level 1 - Securing the SDN Controller using AI

AI based IDPS using machine learning (ML) algorithm



- **AI Training Data Set**
 - NDSL-KDD
- **Supervised Deep Learning**
 - Data size
 - Decision boundary
 - Feature Engineering
- **Supervised Deep Learning Models**
 - DBN: Image, video & motion-capture data
 - **DNN: Tabular data**
 - CNN: Image data (pictures, video, etc.)
 - RNN: Sequential data (time series, text and audio)

Level 1 - Securing SDN Controller using AI

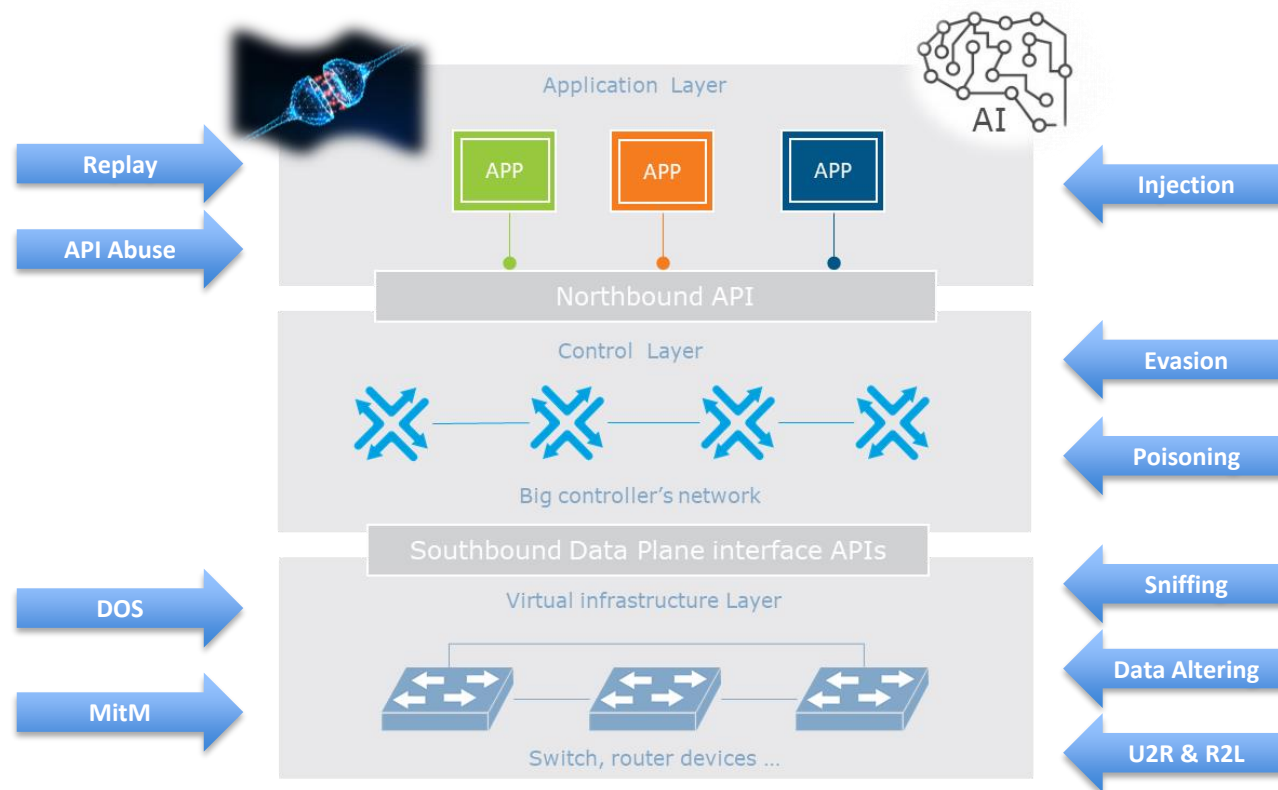


- **Input Parameters (Neurons)**
 - Average packet per flow
 - Duration
 - Protocol type
 - Service
 - Rate of flows
 - Rate of ports
- **Output (Classification)**
 - Malicious Traffic
 - Non-Malicious Traffic
- **Performance Metrics**
 - Learning rate
 - Loss rate
 - Accuracy rate

Level 2 - Securing AI from Cybersecurity Attacks

Poisoning Attacks - Malicious altering of training dataset

Countermeasure - Data Sanitising



AI Model - Performance Metrics (reminder)

Mean Square Loss (MSE)
$$MSE = 1/N \sum_{(x,y) \in D} (y - \text{prediction}(x))^2$$

Accuracy (A)
$$A = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision Rate (P)
$$P = \frac{TP}{TP + FP}$$

Recall Rate (R)
$$R = \frac{TP}{TP + FN}$$

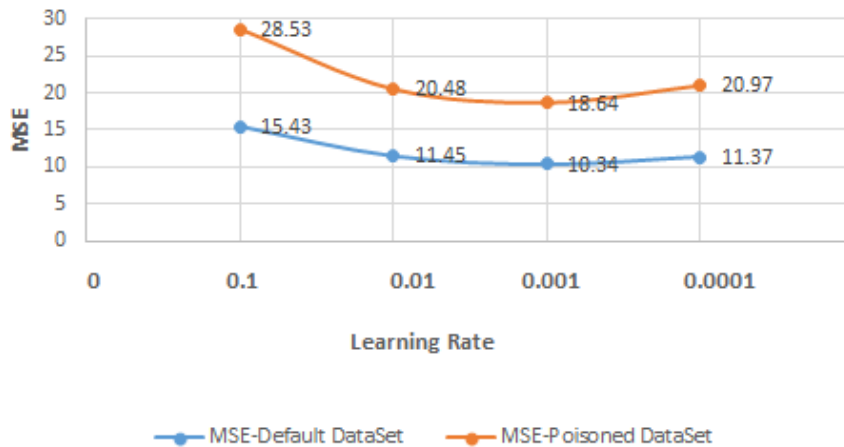
		TRUE CONDITION	
PREDICTED CONDITION		CONDITION POSITIVE	CONDITION NEGATIVE
	PREDICTION POSITIVE	TRUE POSITIVE (TP)	FALSE POSITIVE (FP)
	PREDICTION NEGATIVE	FALSE NEGATIVE (FN)	TRUE NEGATIVE (TN)

AI Model - Performance Results

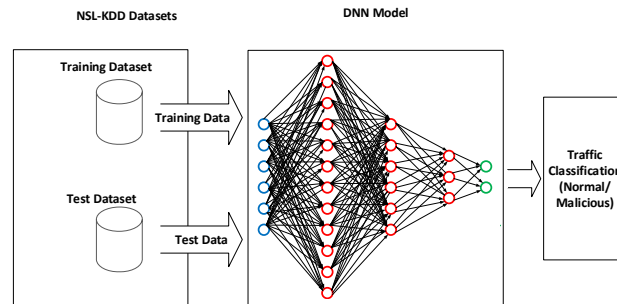
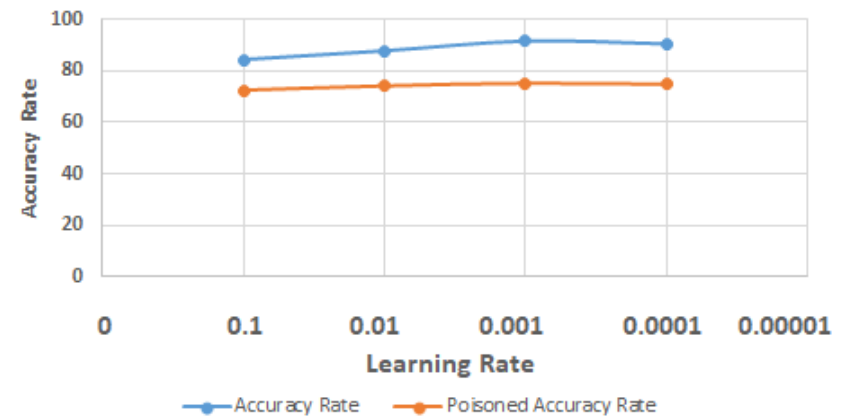
$$MSE = 1/N \sum_{(x,y) \in D} (y - prediction(x))^2$$

$$A = \frac{TP + TN}{TP + TN + FP + FN}$$

Mean Square Loss



Accuracy Rate Using Default & Poisoned Datasets

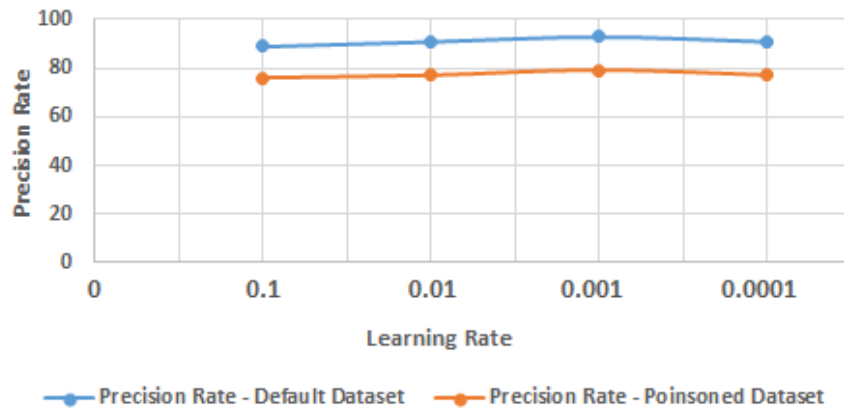


AI Model - Performance Results

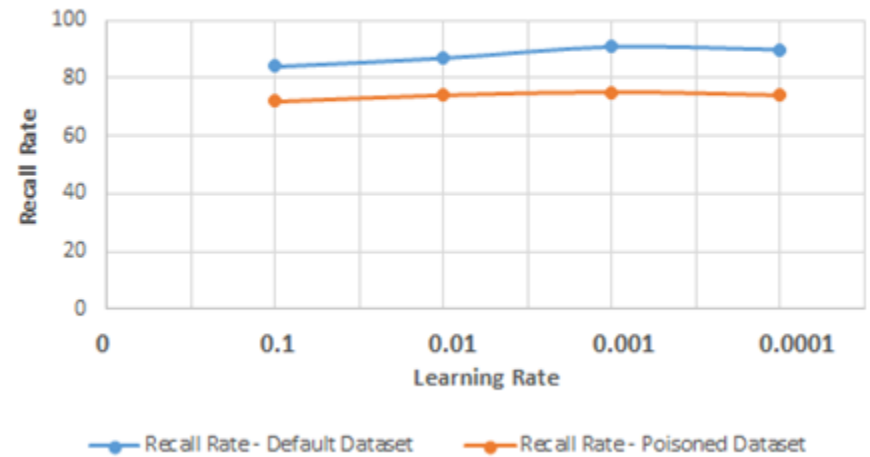


Degradation of Model performance == Indicators of attacks

Precision Rate Using Default and Poisoned Datasets



Recall Rate Using Default and Poisoning Datasets



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

$$R = \frac{TP}{TP + FN}$$

Level 3 – Protecting AI against malicious AI powered Cybersecurity Attacks





Investigate possible countermeasures, against malicious AI attacks to proposed ML- algorithm, **Evasion Attacks**

- Intelligent attacks on AI model classifiers
- Understand AI model classification and then inject undetected pattern

Countermeasures for malicious AI

- Avoid complex Model Architecture
- Simulate attacks to train AI Model

Poisoning vs. Evasion Attacks on AI

Attacks	Stage	Sabotage
Poisoning 	Training	Poisoning of training datasets for the purpose of creating backdoors in the target AI model <ul style="list-style-type: none">• Backdooring• Trojaning
Evasion 	Production	Adversarial programming to achieve Evasion in terms of increasing: <ul style="list-style-type: none">• False negative• False positive



SINAPSE Project

Getting in touch with us



Founding Members



EUROPEAN UNION

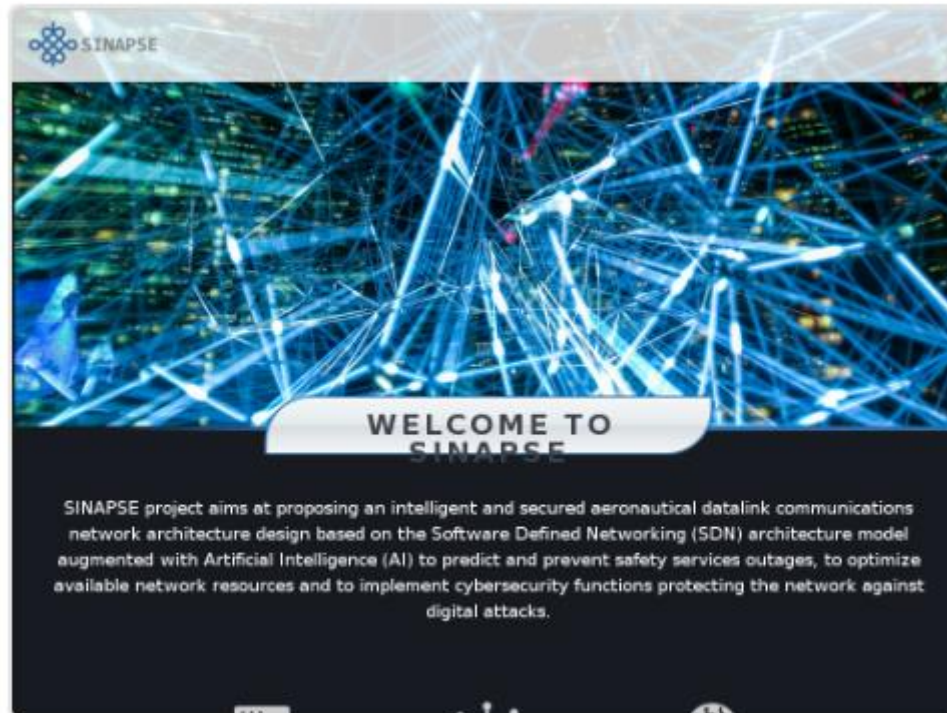


EUROCONTROL

Getting in touch with us



<http://sinapse-s2020.eu>





SINAPSE Project

Thank you very much for your attention!



This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 783270



Founding Members



The opinions expressed herein reflect the author's view only.

Under no circumstances shall the SESAR Joint Undertaking be responsible for any use that may be made of the information contained herein.