NetSim™

AI/ML for Communication Networks

Traffic Estimation
Load Balancing
Throughput Prediction
Resource Allocation
Link Adaptation
Power Control
Beamforming
Interference Estimation
Signal Strength Prediction
Network Attacks Detection

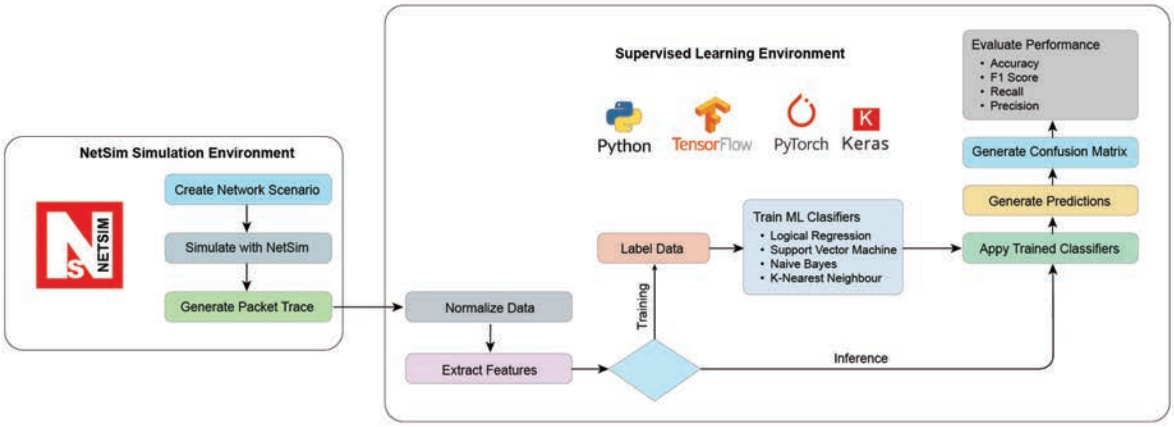
Introduction

NetSim can be used in combination with ML techniques to develop advanced models for a wide range of applications. These include:

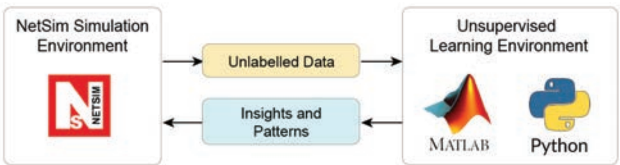
1. Traffic estimation, Load balancing, Throughput prediction
2. Resource allocation, Link adaptation
3. Power control, Beamforming, Interference estimation, Signal strength prediction.
4. Detection of Network attacks using classifiers

Types of ML techniques supported in NetSim

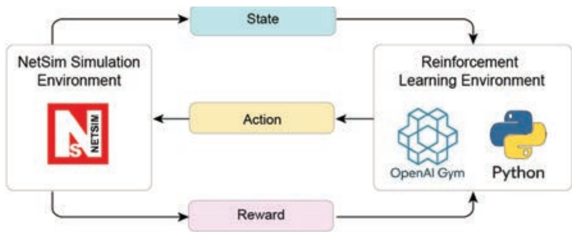
Supervised Learning



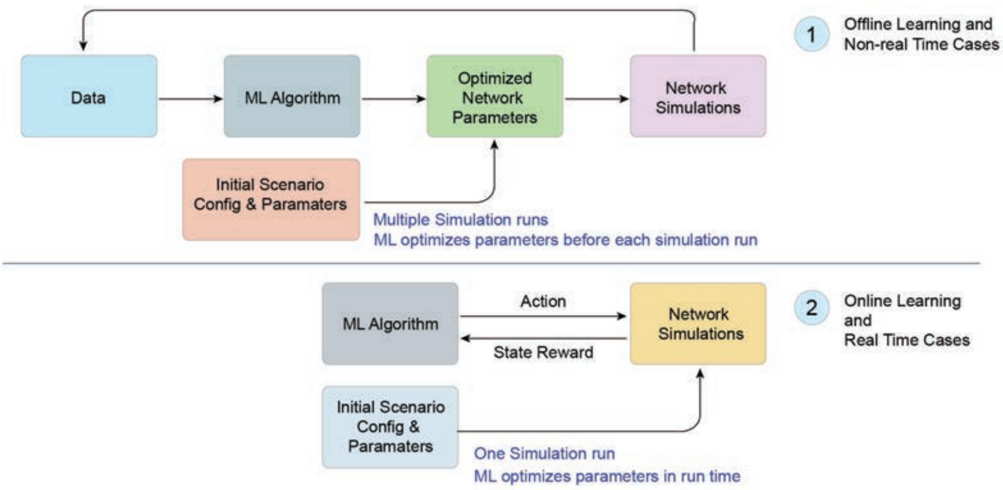
Unsupervised Learning



Reinforcement Learning



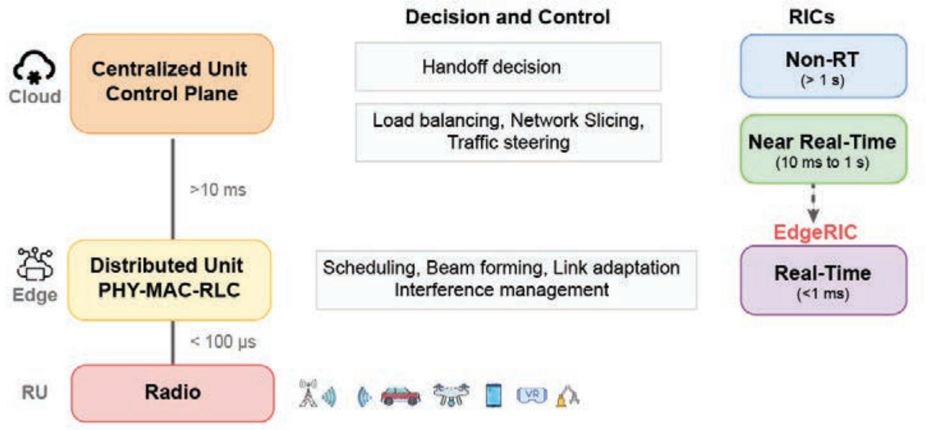
NetSim-ML Integration Frameworks



ML Category	Operation Mode	Example Use Case
Unsupervised Learning	Online	IoT/WSN Clustering for Energy Optimization
Supervised Learning	Offline	VANET Sybil Attack Detection IoT Rank Attack Detection
Reinforcement Learning	Online	5G/6G Delay Aware Scheduling 5G/6G Downlink Power Control

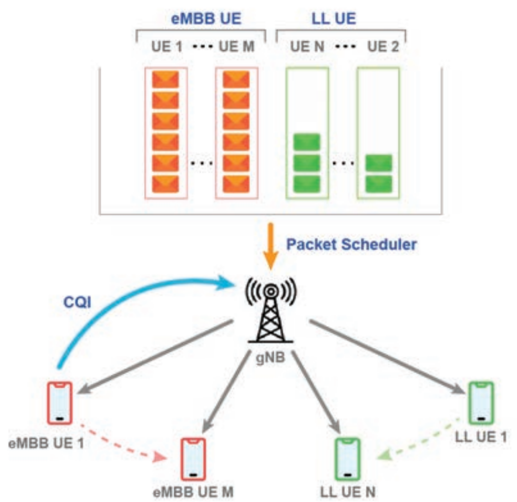
AI/ML in 5G/6G RAN

- Users can interface their AI/ML algorithms with NetSim
  - Train AI models using detailed network telemetry data, down to TTI time scale.
  - Enable AI-driven inference i.e., decisions and predictions
- Applications
  - Develop and test your x-Apps and r-Apps
  - Supports Non-Real-time (> 1s), Near Real-Time (10ms – 1s) and Real-Time (< 10 ms) RIC feedback loops
- Algorithms
  - Online Machine Learning
  - Reinforcement Learning
    - Q-learning, PPO, DQN, A2C
    - Interface to OpenAI Gymnasium RL framework
- Alignment with 3GPP TR 37.817 standards for:
  - Radio Measurements
  - KPIs
  - Interaction time scales



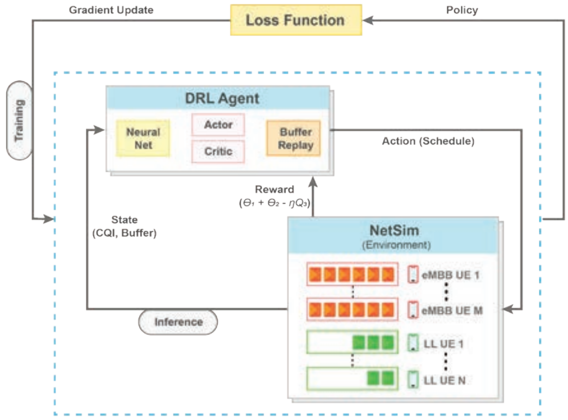
Use Case 1: Delay Aware Scheduling using Reinforcement Learning

- *N* delay sensitive (URLLC) UEs with arrival rates λ_1, λ_2, …, λ_N and mean delay bounds $d_1, d_2, \ldots, d_N$
- *M* high throughput (eMBB) UEs, with full buffer backlog traffic
- Each UE sees a different transmission channel due to distance based pathloss and time-varying Rayleigh fading
- Packets are queued for transmission and at every slot and the scheduler should assign resources to each UE
- Goal: Maximize the sum throughput of eMBB UEs while meeting the delay constraints of the low latency UEs
- This is the classical *opportunistic scheduling* problem without delay constraints; the delay constraints make the problem a much more complex *Markov Decision Problem (MDP)*



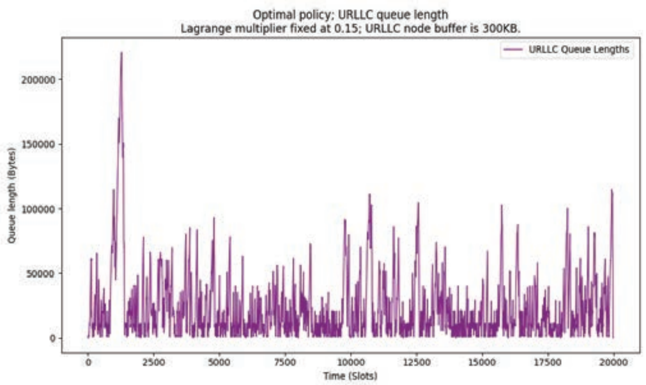
Scenario model in NetSim and the reward function

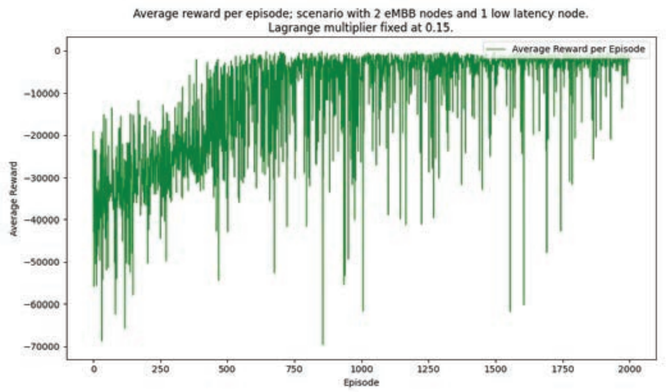
- **UEs:** 2 eMBB UEs and 1 Low Latency (LL) UE
- **States**:
    - Channel Quality Indicator (CQI) of all nodes Queue length at LL node
    - NetSim passes states to RL algorithm
- **Actions**: Fractional allocation of resources per UE per slot.
    - Action constraint: sum of allocation fractions should be 1, which represents total PRBs in a slot
    - Scheduling:{(0, 0, 1), (0, 1, 0), (1, 0, 0), (0, 0.5, 0.5), (0.5, 0. 0.5), (0.5, 0.5, 0)},
    - These fractions were chosen to reduce the action space; any set of fractional combinations that sum to 1 can be set
    - RL returns actions
- **Reward**: $R = \theta_1 + \theta_2 - \eta \cdot Q_3$
    - Units: θ_1, θ_2 in Mbps, Q_3 in Bytes
    - NetSim passes reward and next state

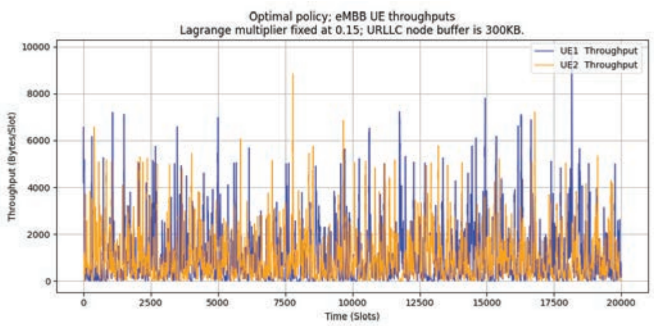


System Parameters			
Parameter	Value	Parameter	Value
UEs	2 eMBB UEs , 1 LL UE	Pathloss Model	Log Distance
gNB	1 gNB serving 3 UEs	Pathloss Exponent	3
Band and BW	n78; 100 MHz	Fading Model	Rayleigh
eMBB Traffic Model	Full buffer UE1, UE2	Coherence Time	30 ms
LL Traffic Model	2 Mbps Download	MCS	Chosen for Zero BLER
Scheduling	RL based at each TTI		

Queue length, Throughputs and the RL Training Curve







Fixed LM	Avg. eMBB1 Thpt. (Mbps)	Avg. eMBB2 Thpt. (Mbps)	Avg. URLLC Q Length (Bytes)	Avg. Delay (ms)
0.075	20.21	17.96	63031.41	31.5
0.15	15.96	15.22	35141.51	17.70
0.30	11.64	12.57	14907.28	7.45

Use case 2: Downlink Power Control using Reinforcement Learning

- Due to the broadcast nature of wireless communication, signals interfere with each other; Interference degrades the performance of the 5G RAN
- We use Reinforcement Learning (RL) for downlink (DL) power control to mitigate interference, boost SINR and maximize sum throughput

- Optimization Problem: Received Signal to Interference plus Noise Ratio (SINR) of link i in slot t is a function of power allocation $p = [p_1, ..., p_n]^T$

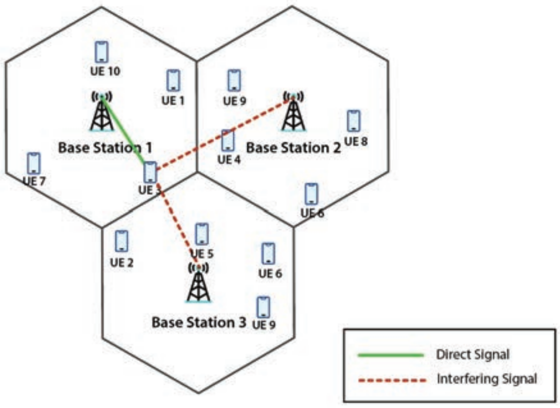
$$\gamma_{i(t)}\,(p) = \frac{g_{ii}^t P_i}{\sum_{j \neq i} g_{ji}^t P_j + \sigma^2}$$

where $g_{ii}^{\,t}$ is time varying due to mobility and fading.

  - The objective is to maximize a weighted sum-rate utility function. The dynamic power allocation problem in time slot (t) is formulated as:

$$\text{maximize} \sum_{i=1}^{M} R_i\,(t)$$

where $R_i\,(t)$ is a function of $\gamma_i^{(t)}\,(p)$, since the instantaneous rate (MCS) can be obtained from 3GPP SE-MCS tables, and spectral efficiency (SE) is dependent on SINR.



Reinforcement Learning

- Environment:
  - The 5G cellular network (see next slide for details)
  - Fading channel
  - Association doesn’t change
  - Scheduling is Round Robin
- Agent
  - Centralized oracle. Controls power in each gNB
- State:
  - Vector of received SINRs at the UEs
  - SINRs discretized into 4 buckets
  - State changes every coherence time
- Action: Power Control i.e., power-up, power-down, power-hold
  - A control of ΔP_i applied to gNB_i
  - $\Delta P_i \in \{0\ dB, \pm 1\ dB, \pm 3\ dB\}$
  - Transmit power limits: [27, 46] dBm
  - Agent applies power control every $N{=}3$ frames (30 ms)
  - Power is adjusted after fading gain is taken into account
- Reward function:
  - Sum throughput
  - Throughput is obtained every $N{=}3$ frames i.e., time between two consecutive actions

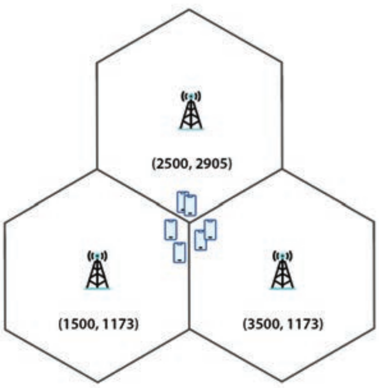
The Q Table

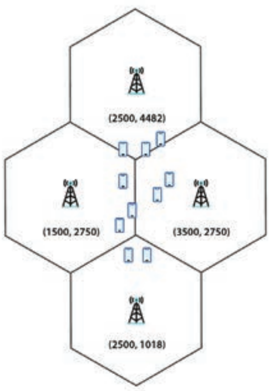
States:
SINR buckets = 4
No. of states = 4^6 = 4096

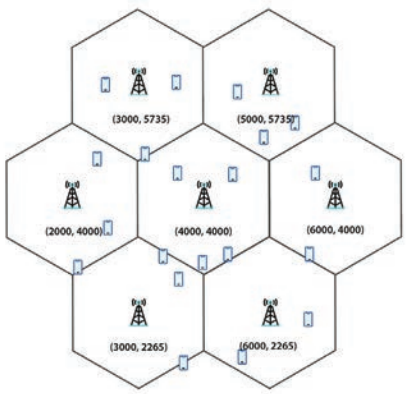
Actions:
Power control options = 5
No. of gNBs = 3
No. of Actions = 5^3 = 125

Q table size = $S \times A \approx 500k$

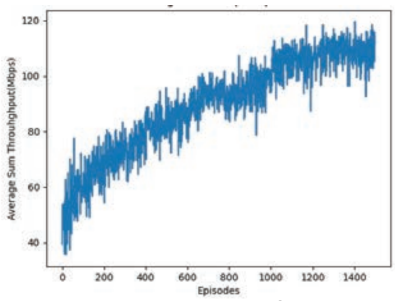
Test Scenarios



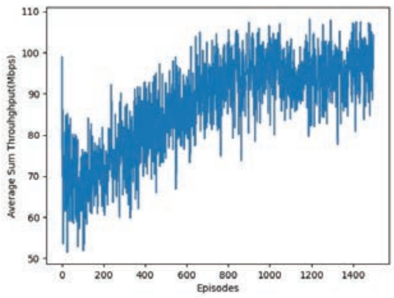




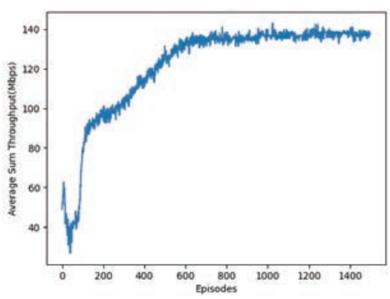
RL yields 1.5x to 2.5x performance improvement



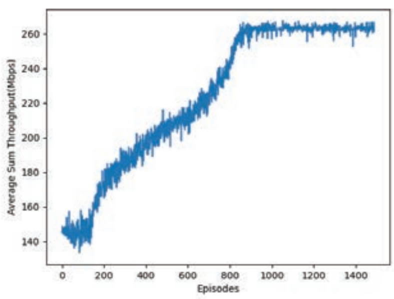
3 gNBs 6 UEs; RL algorithm: Q learning



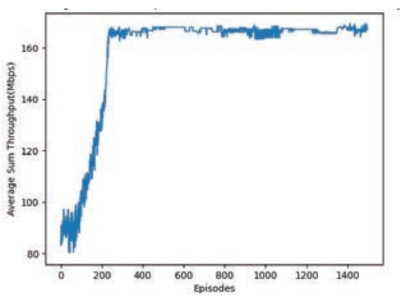
4 gNBs 11 UEs; RL algorithm: Q learning



3 gNBs 6 UEs; RL algorithm: PPO



7 gNBs 20 UEs; RL algorithm: PPO



4 gNBs 11 UEs; RL algorithm: PPO

Scenario	Avg. Sum Thpt. (Mbps)	
	Without RL	With RL (PPO)
3 gNBs 6 UEs	55	140
4 gNBs 11 UEs	80	165
7 gNBs 20UEs	181	265

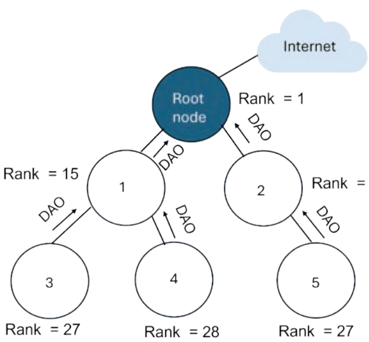
AI/ML in IoT security

- IoT networks are subject to a variety of attacks
  - Spoofing attacks, denial of service attacks, jamming and eavesdropping
- Supervised learning can be used to label the network traffic or app traces of IoT devices to build the classification model

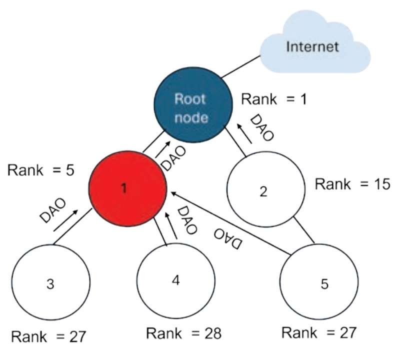
Use case #3: Detecting network attacks in RPL based IoT using classifiers

Rank attack in RPL using NetSim

- Normal RPL process:
  - Transmitter broadcasts DIO during DODAG formation
  - Receiver updates parent list, sibling list, and rank
  - Receiver sends DAO message with route information
- Malicious node behavior:
  - Receives DIO but doesn't update its rank
  - Advertises a fake (lower) rank
  - Other nodes update their rank based on this fake information
- Attack impact:
  - Nodes choose malicious node as preferred parent due to lower rank
  - Malicious node drops packets instead of forwarding
  - Result: Zero network throughput



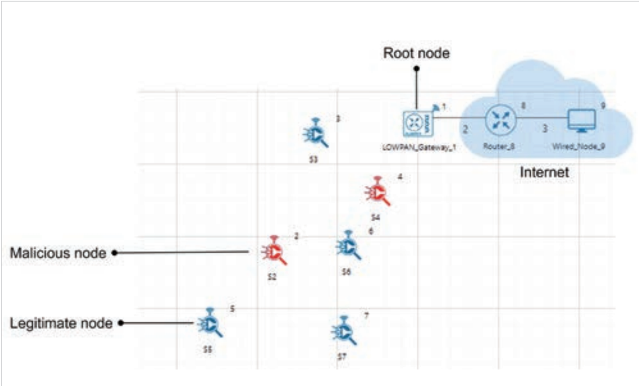
All nodes in the network choose their parent based on link quality



Nodes 3, 4, and 5 choose parent as malicious node 1 due to its lower rank

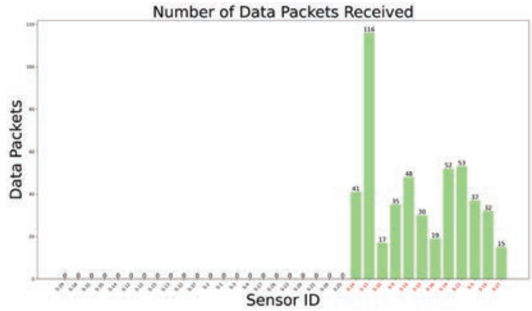
Attack scenarios - Training data generation

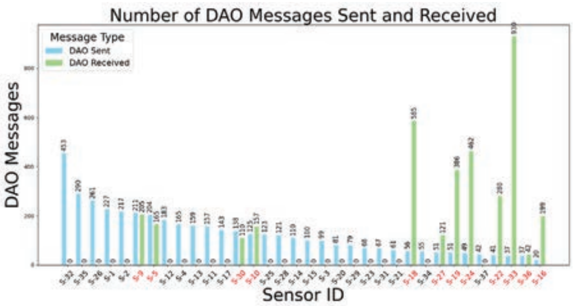
- Created 8 scenarios with varying node counts (6 to 39)
- Malicious node count: 2, 4, 5, 6, 8, 10, 12, and 14
- Simulations run with 3 random seeds for each scenario
- Enabled packet trace for all scenarios
- Feature Extraction
  - DAO Sent
  - DAO Received
  - DIO Sent
  - DIO Received
  - Data Packets Received
- Used a python script to calculate the number of DAO, DIO, and data packets received by each sensor from packet trace.

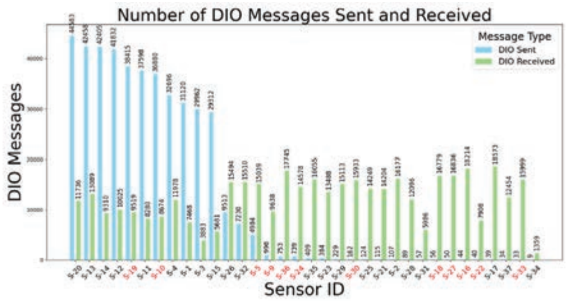


Data processing and Feature Visualization

- Data extraction from packet trace to Excel using Python script
- Total dataset: 534 sensors, 5 features each
- Feature normalization process:
  - Calculate max value for each feature across all sensors
  - Divide each sensor's value by the max to get 0-1 range
- Manual labeling: 1 for non-malicious, 0 for malicious







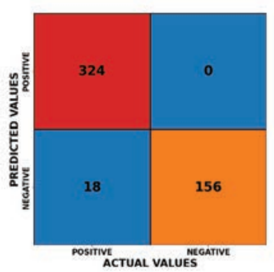
Feature visualization: 5, 9, 10, 16, 18, 19, 22, 24, 27, 30, 33 and 36 malicious nodes

Detection of Malicious: ML based Classifiers used

- K-Nearest Neighbor classifier
- Naive Bayes classifier
- Support Vector Machine classifier
- Logistic Regression classifier

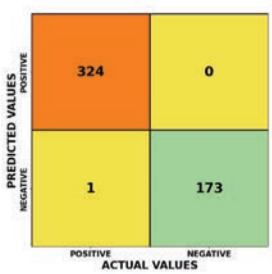
Confusion Matrix: Accuracy, Precision, F1 Score, Recall

CONFUSION MATRIX FOR LOGISTIC REGRESSION CLASSIFIER



Metric	Value
Accuracy	0.9980
Precision	0.9969
Recall	1.0000
F1 Score	0.9985

CONFUSION MATRIX FOR SUPPORT VECTOR MACHINE CLASSIFIER



Metric	Value
Accuracy	0.9639
Precision	0.9474
Recall	1.0000
F1 Score	0.9730

Comparison and Future Work

Key Observations

- High Precision (>94%): Low false positive rate; malicious classifications are likely correct.
- Near-Perfect Recall (≥99.69%): Classifiers rarely miss malicious nodes.
- Robust F1 Scores (>0.97): Well-balanced performance in identifying threats and avoiding false alarms.

Classifier	True Positive	True Negative	False Positive	False Negative	Accuracy	Precision	Recall	F1 Score
Naive Bayes	323	174	0	1	0.9980	1.00	0.9969	0.9985
KNN	324	164	10	0	0.9799	0.9701	1.000	0.9484
Logistic Regression	324	156	18	0	0.9639	0.9474	1.000	0.9730
SVM	324	173	1	0	0.9980	0.9969	1.000	0.9985

Use Case #4: Sybil attacks in VANETs using Machine Learning

Understanding Sybil Attacks in VANETs

- Critical security threat where malicious vehicles create multiple fake identities ("ghost vehicles")
- Attackers can manipulate traffic data and compromise road safety applications
- Potential impacts include:
  - False traffic congestion reports
  - Compromised safety-critical applications
  - Increased risk of accidents

Detection Method Using NetSim

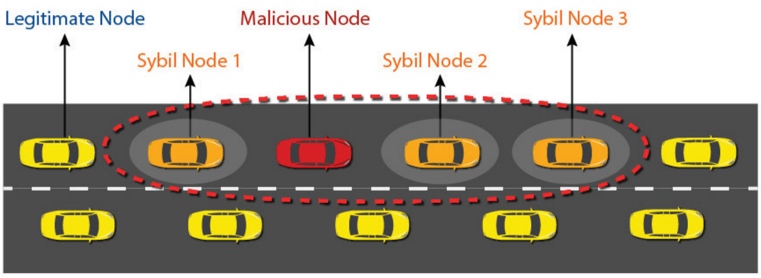
- Leverages RSSI (Received Signal Strength Indicator) measurements between nodes
- Key detection principle: Multiple fake identities from same physical location have similar RSSI patterns
- Network setup includes:
  - Combination of legitimate nodes, malicious nodes, and sybil nodes
  - Multiple roadside units (RSUs) for signal measurement
  - IEEE 802.11p and IEEE 1609 standards implementation

Machine Learning Approach

- Feature extraction from RSSI measurements:
  - RSSI power at each RSU
  - RSSI differences between vehicles
  - RSSI similarity patterns

Multiple classifier comparison

- Random Forest
- K-Nearest Neighbor
- XGBoost
- Decision Tree



Detection Performance

- High accuracy across all classifiers (95-97%)
- XGBoost classifier achieved best overall results: 97% accuracy, 80% precision, 87% recall, 0.83 F1 score
- System effectively distinguishes between legitimate and sybil nodes in diverse scenarios

Network Clustering in IoT/WSN for Energy Optimization

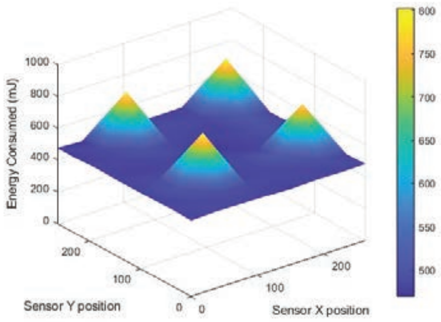
Network clustering is an optimization strategy for IoT and WSN to extend the network lifetime. Using the NetSim - MATLAB interface, users can implement advanced clustering algorithms that dynamically adapts to changing network conditions while optimizing energy consumption.

Clustering Architecture and Implementation

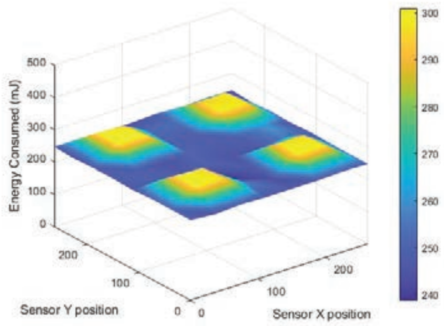
1. Algorithm Support:
   - k-Means and Fuzzy c-Means Clustering:
     - » Groups sensors dynamically based on position and proximity.
     - » Elects cluster heads using metrics like distance to centroids or remaining energy
   - Self-Organizing Map (SOM) Neural Networks:
     - » Creates clusters by training a neural network with sensor positions as input.
     - » Dynamically selects cluster heads based on power consumption and distance to cluster centroids.
2. Cluster Head Election:
   - Algorithms consider factors like:
     - » Distance: Sensors closer to the cluster centroid are preferred.
     - » Residual Energy: Sensors with higher remaining energy are prioritized to balance power consumption.
3. Integration with MATLAB:
   - NetSim interfaces with MATLAB for clustering calculations and visualizations.
   - Outputs include cluster IDs, cluster sizes, and cluster head details for all nodes.
4. Energy Optimization:
   - Prevents rapid depletion of cluster head nodes by balancing energy usage across the network.
   - Metrics like energy consumed in transmission, reception, idle, and sleep states are monitored.

Benefits of Dynamic Clustering in NetSim

- Enhanced Energy Efficiency: Uniform energy consumption across nodes extends network lifetime.
- Adaptability: Periodic re-clustering adjusts to changing conditions in real-time, making it ideal for mobile and dynamic environments.
- Scalability: Supports large-scale sensor networks by simplifying routing and resource allocation.
- Advanced Visualization:
  - Graphs for energy consumption and SOM topology.
  - Real-time updates on cluster configurations and sensor states.



Cluster heads are selected based on distance without considering energy consumption. This results in higher energy consumption for specific cluster heads, leading to spikes in the energy usage pattern.



Cluster head selection considers both distance and energy consumption, distributing the load more evenly among cluster heads. This leads to a balanced energy consumption pattern across the network.

NetSim's integration with MATLAB allows researchers to customize clustering algorithms for specific applications, making it a powerful tool for designing and analysing IoT and WSN systems.

Under Development: Federated Learning in 5G/6G Networks

Documentation and codes for all uses cases are available at:

https://tetcos.com/machine-learning-netsim.html

Select list of research publications featuring AI/ML with NetSim

1. DETONAR: Detection of Routing Attacks in RPL-Based IoT (https://ieeexplore.ieee.org/document/9415869)
2. Reinforcement-Learning-based IDS for 6LoWPAN (https://ieeexplore.ieee.org/document/9724461)
3. ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things (https://ieeexplore.ieee.org/document/8777504)
4. Q-Learning Relay Placement for Alert Message Dissemination in Vehicular Networks (https://www.sciencedirect.com/science/article/pii/S1877050922006342)
5. Adaptive Hybrid Heterogeneous IDS for 6LoWPAN (https://arxiv.org/abs/2205.09170)
6. Exploring cybersecurity issues in 5G enabled electric vehicle charging station with deep learning (https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/gtd2.12275)
7. Adversarial RL-Based IDS for Evolving Data Environment in 6LoWPAN (https://ieeexplore.ieee.org/document/9916285)
8. Advancing 6G Network Performance: AI/ML Framework for Proactive Management and Dynamic Optimal Routing (https://ieeexplore.ieee.org/document/10522874)
9. An Intelligence-Based Framework for Managing WLANs: The Potential of Non-Contiguous Channel Bonding (https://ieeexplore.ieee.org/abstract/document/10500831)
10. Learning-Based Road Link Quality Estimation for Intelligent Alert-Message Dissemination (https://ieeexplore.ieee.org/abstract/document/10271590)
11. Malicious Node Detection in VANETs via Enhanced DSR and ML (https://ieeexplore.ieee.org/abstract/document/10532957)
12. Performance Analysis of 5G DDoS Attack using Machine Learning (https://digitalcommons.memphis.edu/etd/2201/)
13. SIGMAML: SNR-Guided 5G Mobility Management using Machine Learning Algorithms (https://ieeexplore.ieee.org/abstract/document/10667970)
14. Intelligent QoS Agent Design for QoS Monitoring and Provisioning in 6G Network (https://ieeexplore.ieee.org/abstract/document/10279078)
15. A Novel Two-Step Bayesian Hyperparameter Optimization Strategy for DoS Attack Detection in IoT (https://ieeexplore.ieee.org/abstract/document/10467454)
16. Flexibly Controlled 5G Network Slicing (https://ieeexplore.ieee.org/abstract/document/10019226)

500+ CUSTOMERS ACROSS 30+ COUNTRIES

NUS National University of Singapore

MULTIMEDIA UNIVERSITY
Malaysia

LEEDS BECKETT UNIVERSITY

Fukushima Renewable Energy Institute, AIST
Japan

Universitas Miguel Hernández

NORTH-WEST UNIVERSITY
YUNIBESITI YA BOKONE-BOPHIRIMA
NOORDWES-UNIVERSITEIT
South Africa

BSNL Connecting India
Bharat Sanchar Nigam Ltd., India

INL Idaho National Laboratory
USA

Dirgantara Indonesia
Indonesian Aerospace

University of Udine
Italy

INTI International University & Colleges
LAUREATE INTERNATIONAL UNIVERSITIES
Spain

Indian Institute of Space Science and Technology

verizon
USA

GIST Gwangju Institute of Science and Technology
South Korea

NTIS National Company of Telecommunications & Information Security
الشركة الوطنية لحماية الاتصالات والمعلومات

ihp
Innovations for High Performance Microelectronics (IHP), Germany

MBDA
France

IIT, Kharagpur

Technische Hochschule Ingolstadt
Germany

UNIWERSYTET SZCZECIŃSKI
Poland

PHILIPS
Philips
Netherlands

DRDO-CABS

UTP UNIVERSITI TEKNOLOGI PETRONAS
Malaysia

IIT, Kanpur

Cranfield University
UK

UNIVERSIDADE DE VIGO
Spain

IIT Bombay

DRDO-ISSA

LEEDS BECKETT UNIVERSITY
UK

STAFFORDSHIRE UNIVERSITY

DIRGANTARA INDONESIA
INDONESIAN AEROSPACE (IAe)

UCLM UNIVERSIDAD DE CASTILLA-LA MANCHA
Spain

DRDO-CAIR

A·P·U ASIA PACIFIC UNIVERSITY OF TECHNOLOGY & INNOVATION
Malaysia

University of South Australia

UNIVERSITY OF MICHIGAN
USA

BITS Pilani Dubai Campus

PEARSON Education

Al-Nahrain University
Iraq

University of Wisconsin Eau Claire
USA

UPNM National Defence University of Malaysia

UCB UNIVERSIDAD CENTRAL DE BAYAMON

جامعة السلطان قابوس
Sultan Qaboos University
Oman

IIT, Delhi

DAIICT
India

The University Of Sheffield

UTHM Universiti Tun Hussein Onn Malaysia

TSI TRANSPORT AND TELECOMMUNICATION INSTITUTE
Latvia

iiit-b International Institute of Information Technology Bangalore

VIT Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

IIT, Roorkee

IM INFOCOMM MEDIA DEVELOPMENT AUTHORITY
Singapore

सीडैक CDAC
Hyderabad, India

IIT Bhubaneswar
Indian Institute of Technology Bhubaneswar

Military Technological College
Egypt

KUET

Contact Us

- Interested in getting an evaluation of NetSim? Have a few questions about NetSim before starting an evaluation?
- We are happy to tell you more about our product, support, pricing, customers, and company.
- Have specific simulation requirements not listed on our brochure or webpage? We can likely model them with minor code modifications. Please just email us the details

youtube.com/tetcos | facebook.com/tetcosnetsim | twitter.com/tetcos

www.tetcos.com | linkedin.com/company/tetcos | sales@tetcos.com

TETCOS LLP #214, 7th Main, 39th A Cross, Jayanagar 5th Block, Bangalore Pin - 560 041, India.

Sales : +91 80 2663 0624 Tech Support : +91 76760 54321