Detection of Primary User Emulation Attack in Cognitive Radio Network

Under the guidance of:

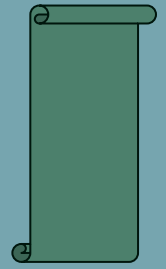
Dr. Wangjam Niranjan Singh
(*Assistant Professor*)

Team :

Rishav Raj
Snehasish Das
Debraj Dutta Gupta
Sumir Das

Contents

- Introduction
- Problem Statement
- Literature Review
- Methodology
- Simulation
- Result & Findings
- Conclusion
- References



Introduction

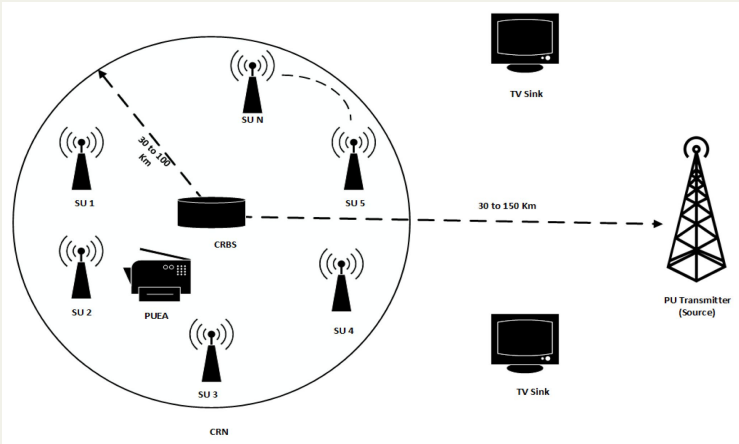
Introduction to Cognitive Radio Networks (CRNs)

What are CRN's ?

Cognitive Radio Networks (CRNs) are advanced wireless communication systems that intelligently allow unlicensed users to access underutilized licensed frequency bands without interfering with primary users, optimizing spectrum utilization to meet the growing demand for spectrum resources.

Key Characteristics :-

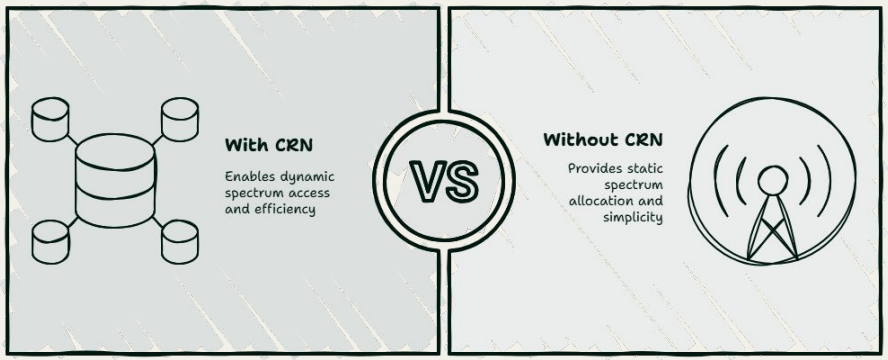
- Dynamic spectrum Access
- Real-time Environment Adaptation
- Intelligent decision making
- Secondary User Accomodation

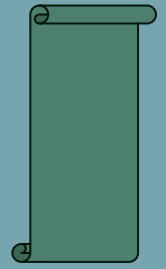


CRBS :- Cognitive Radio Base Station(**30MHz-3GHz**)

Spectrum With CRN and Without CRN

- **Traditional networks treat spectrum as a fixed resource**, leading to congestion in some bands and wastage in others.
- **CRN introduces intelligence**, allowing devices to find and use available spectrum dynamically without waiting for manual allocation.
- **CRN transforms spectrum usage from rigid to flexible**, enabling smarter, more efficient wireless communication.





Problem Statement

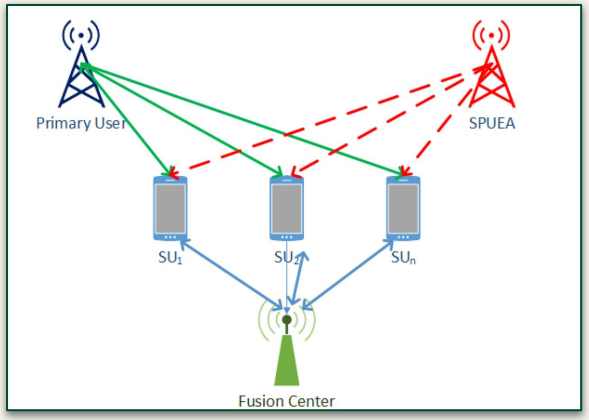
Security Challenges

The Shadow Threat: Primary User Emulation Attack

A malicious Secondary User (mSU) mimics the signal characteristics of a legitimate Primary User (PU).

Goal:

- To deceive other SUs into believing the PU has returned, forcing them to vacate the spectrum.
- Disrupts the opportunistic access of legitimate SUs, leading to performance degradation.
- Can severely impact the efficiency and reliability of CRNs.



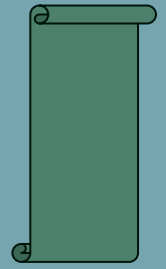
Why is PUEA a Significant Concern?

High Stakes: The Impact of PUEA

- **Denial of Service (DoS) for SUs:** Prevents legitimate SUs from accessing available spectrum.
- **Resource Wastage:** Underutilized spectrum due to the attacker's false presence.
- **Trust Erosion:** Undermines the cooperative nature of cognitive radio networks.
- **Difficulty in Detection:** Attackers can employ sophisticated techniques to mimic PU signals accurately.

Objective

- Develop and evaluate **clustering-based methods** (**K-Means**, **Agglomerative** and **DBSCAN Clustering**) for **detecting Primary User Emulation Attacks (PUEA)** in **Cognitive Radio Networks**.
- **Identify key statistical features** that **effectively distinguish** between **legitimate Primary Users** and **emulated attackers.**
- **Compare algorithm performance** across varying **attack scenarios** and **PUEA intensities (10–50%)**, using critical metrics like **Detection Rate** and **False Detection Rate**.
- **Provide optimization insights** and **visualization tools** to **enhance real-world PUEA detection strategies**, focusing on the **impact of attacker proximity**.



Literature Review

Literature Review

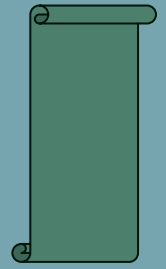
SL. No.	Author	Date of Publication	Title	Contribution	Methodology	Drawback
1	Dinu Mary Alias,Ragesh G. K	30 Jun, 2010	Cognitive Radio Networks: A Survey	Dynamic spectrum access improves spectrum efficiency. Paper provides overview of cognitive radio functions and techniques.	Centralized sharing Distributed sharing.	Licensed users returning causes unlicensed users to vacate spectrum. Spectrum mobility can occur due to various factors.
2	Khaled Mohammed Saifuddin, Kazi Fahid Reza, Masud An Nur Islam Fahim, Sk. Shariful Alam	01 Sep, 2017	Detection of Primary User Emulation Attack in Cognitive Radio Environment	Different methods to model the communication channels and improve the signal measurement accuracy . Outliers in localization procedures are filtered out to improve the detection accuracy of PUE attacks	Filter and cyclostationary feature detection , spectrum decision and channel parameters , and shadow senders.	security issues in DSA—those related to spectrum access and software protection

Literature Review

SL. No.	Author	Date of Publication	Title	Contribution	Methodology	Drawback
3	Ishu Gupta,O. P. Sahu	01 Feb, 2018	An Overview of Primary User Emulation Attack in Cognitive Radio Networks	In this paper, a general overview of cognitive radio security issues has been given with main focus on Primary User Emulation Attacks	Discussed about: energy detection,cyclostationary feature based detection and matched filter detection	These method also fails if the attacker transmit during these quiet periods,this technique also fails especially when the Pus are TV systems
4	Khatereh Akbari,Jamshid Abouei	01 May, 2018	Signal Classification for Detecting Primary User Emulation Attack in Centralized Cognitive Radio Networks	an effective sequential scheme to identify the PUE attack in CRNs. The PUE detection process was performed in the CR base station to make the final decision about the presence or absence of the real PU or PUE attacker by wideband spectrum sensing	the Bayesian nonparametric clustering approach based on the Dirichlet Process Mixture Model (DPMM) is used for clustering and determining the number of detected PUs.	Terms of the run time, even though the N-Uniform had the worst performance from the PU detection rate and the clustering accuracy points of view

Literature Review

SL. No.	Author	Date of Publication	Title	Contribution	Methodology	Drawback
5	Bishal Chhetry, Ningrinla Marchanga	21 Jun, 2021	Detection Of Primary User Emulation Attack (PUEA) In Cognitive Radio Networks Using One-Class Classification	One-class classification is used for detecting PUEA.	classification algorithms are investigated, viz., Isolation Forest, Support Vector Machine, MCD and LOF.	All of the techniques, SVM performs the worst with inconsistent performance. Isolation Forest (IF) performs better than SVM but not as good as MCD and LOF
6	Amar Taggu and Ningrinla Marchang	05 Jul, 2022	A Density-based Clustering Approach to detect Colluding SSDF Attackers in Cognitive Radio Networks	Proposed a DBSCAN-based technique for detecting Colluding SSDF attacks. Demonstrated effectiveness when attacker percentage is below 50%.	Density-Based Spatial Clustering of Applications with Noise (DBSCAN) Performance comparison with Agglomerative Clustering Detection (ACD)	Colluding SSDF attacks are harder to detect. Attacks are more harmful due to collaboration.



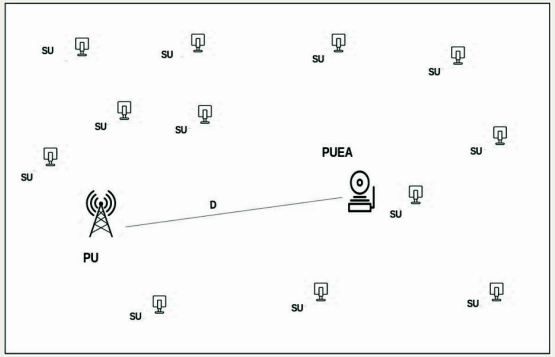
Methodology

Step 1

Network Scenario Simulation and Feature Extraction

Network Scenario Simulation

- Extract Statistical Features
  - Mean
  - Variance
  - Median
  - Lower Quartile
  - Upper Quartile
- Simulate Network Scenarios
  - Scenario A (D is large)
  - Scenario B (D is medium)
  - Scenario C (D is small)
- Calculate Received Powers
  - Received Power from PU
  - Received Power from PUEA



$$P_r = P_t r^{-\alpha} e^{a\beta}$$

Step 2

Manhattan Distance Matrix Calculation

Identify Scenarios and Cases

Determine the scenarios and cases for analysis

Compute Manhattan Distance Matrix

Calculate the distance matrix using feature columns

Save Distance Matrices

Store the matrices for future clustering and visualization

Step 3

PU

How to combine PU and PUEA feature matrices?

10% Mix
Provides a small-scale integration, useful for initial testing.

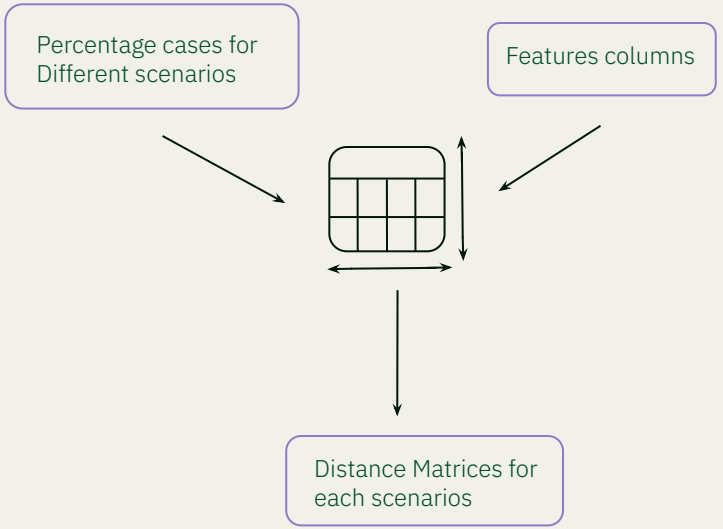
20% Mix
Offers a moderate integration level, balancing detail and manageability.

30% Mix
Allows for a more significant integration, enhancing data diversity.

And so on...

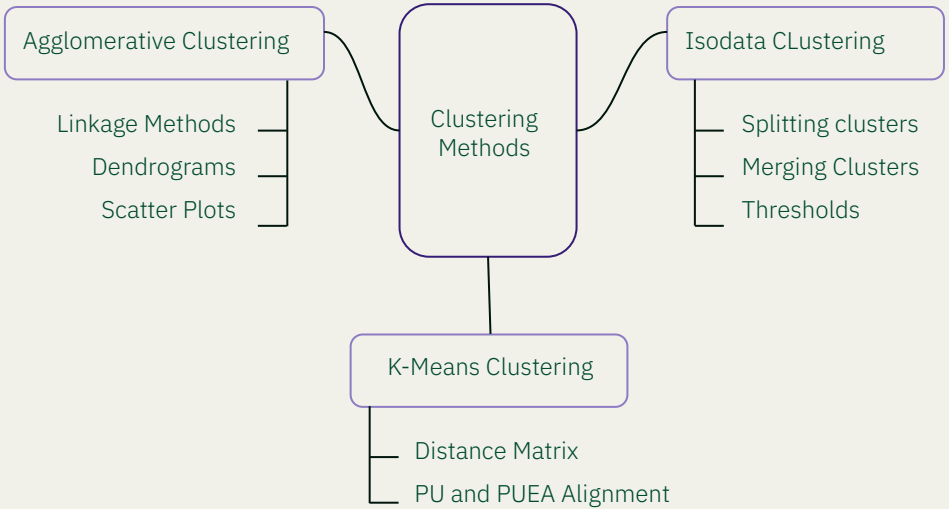
Step 4

Manhattan Distance Matrix for Clustering and Visualization



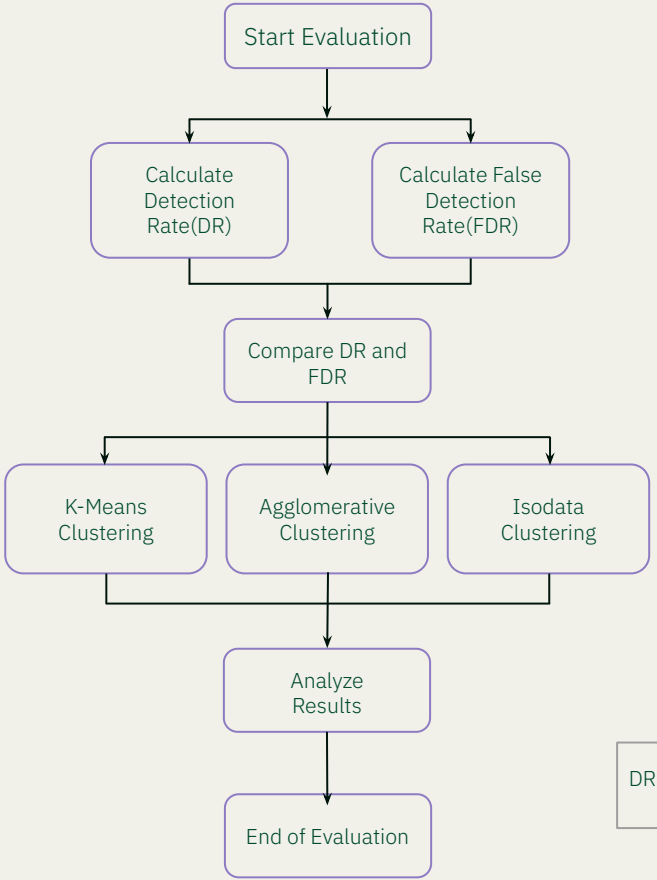
Step 5

Clustering Methods and Their Characteristics



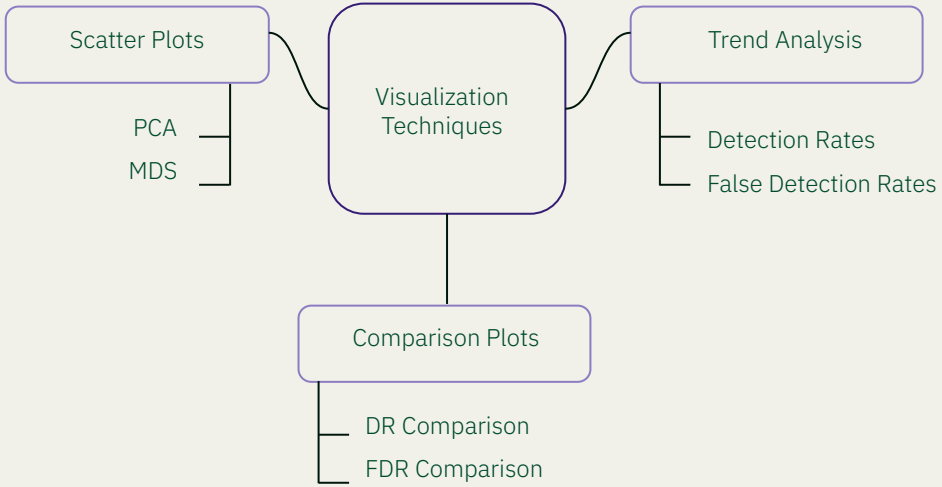
Step 6

Evaluation of Clustering Methods



Step 7

Visualization Techniques in Clustering Evaluation



$$DR = \frac{\text{No. of correctly detected PUEA}}{\text{Total no. of attacker}}$$

$$FDR = \frac{\text{No. of PU detected as PUEA}}{\text{Total no. PU}}$$

Different types of Clustering Algorithm

DBSCAN

Density-Based Spatial Clustering of Applications with Noise

Key Features

- Identifies clusters of arbitrary shape
- Natural outlier detection
- No pre-defined number of clusters

Agglomerative

Hierarchical Clustering with Bottom-up Approach

Key Features

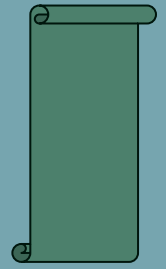
- Hierarchical structure analysis
- Multiple linkage criteria
- Dendrogram visualization

K-Means

Partition-Based Clustering with Centroid

Key Features

- Simple and fast convergence
- Works well with spherical clusters
- Pre-defined number of clusters (K)



Simulation

Key Characteristics of Primary User Signals (for Detection)

$$P_r = P_t r^{-\alpha} e^{a\beta}$$

Identifying the Legitimate: PU Signal

- **Pr** is the received power
- **Pt** is the transmitted power
- **r** is the distance between the transmitter and receiver
- **α** is the path loss exponent
- **e** is Euler's number (approximately 2.71828)
- **a** and **β** are constants or coefficients

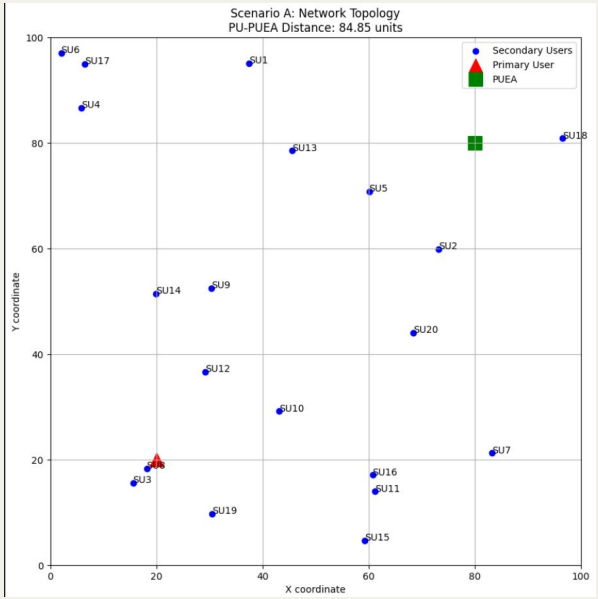
Our Simulation Parameters:-

- **Transmit Power**:
  - PU: 20 dB
  - PUEA: 30 dB
- **Path Loss Model**:
  - Formula: 10 × path_loss_exp × log10(distance)
  - Path Loss Exponent: Uniform random between 2-6 (varies by secondary user)
- **Shadowing**:
  - Log-normal shadowing: Uniform random between 4-12 dB (varies by secondary user)

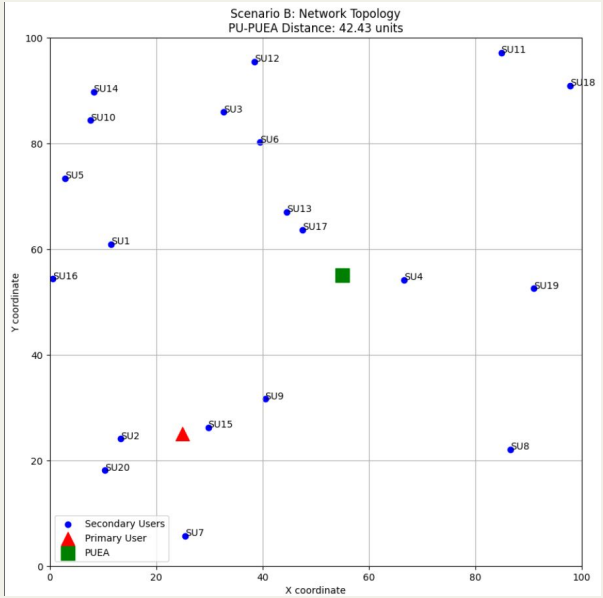
For Our Simulation

- **Setup Network Topology**
  - Define three scenarios: Far distance (A), Medium distance (B), Close distance (C)
  - Place Primary User and PUEA at different distances
  - Distribute Secondary Users randomly across the area
- **Signal Propagation Modeling**
  - Calculate path loss using distance-based model
  - Apply random shadowing effects
  - Generate received power measurements at Secondary Users
- **Time Slot Simulation**
  - Run simulation for 500 time slots for each scenario
  - Collect received power measurements for each Secondary User

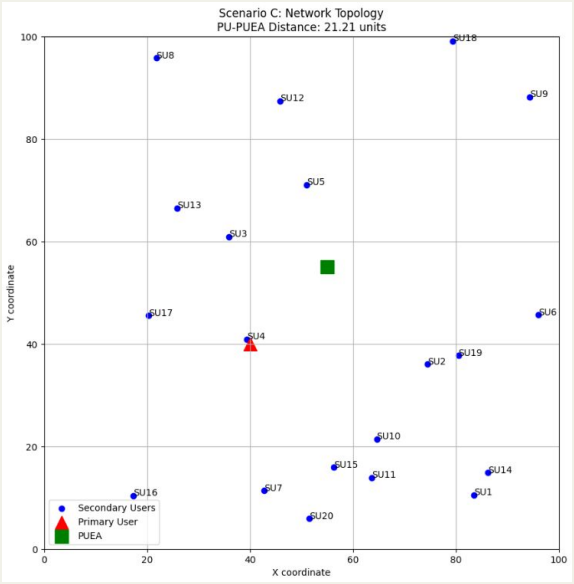
Our three scenarios:



PU Position: (20, 20)
PUEA Position: (80, 80)
PU-PUEA Distance: 84.85 units



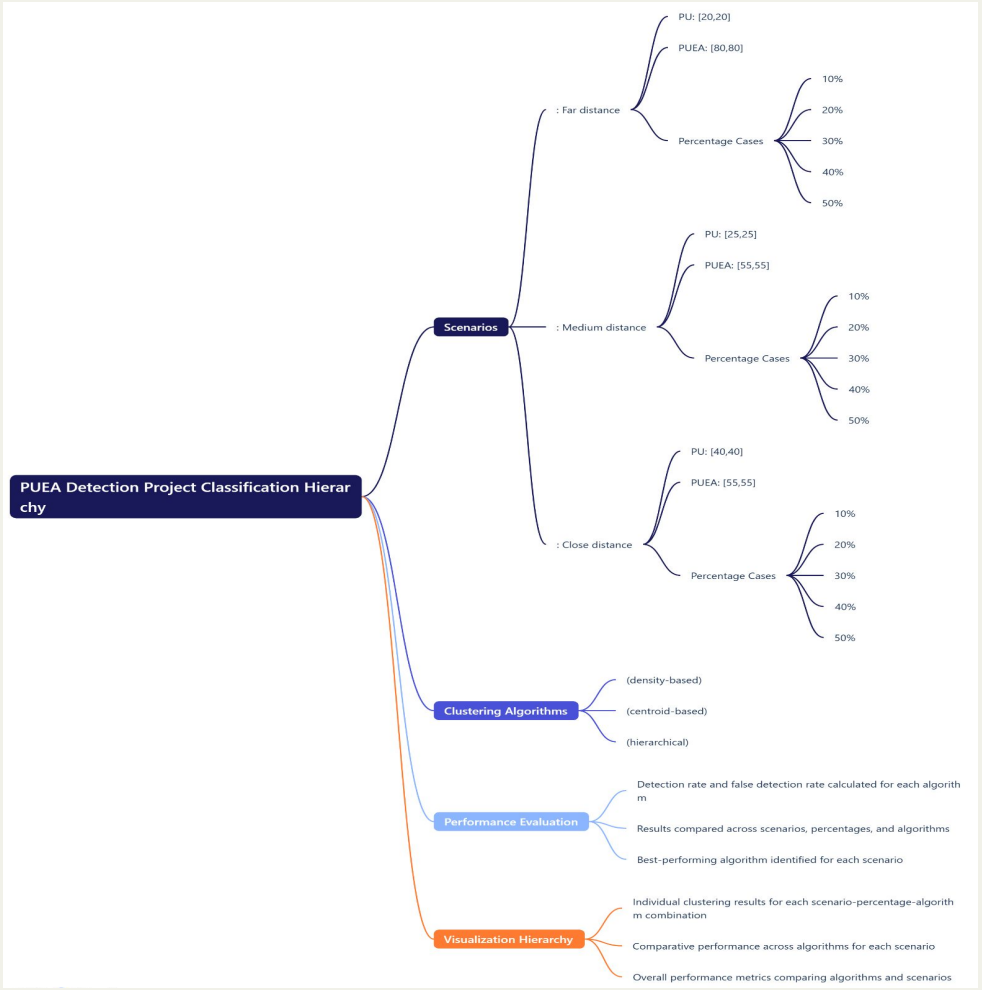
PU Position: (25, 25)
PUEA Position: (55, 55)
PU-PUEA Distance: 42.43 units



PU Position: (40, 40)
PUEA Position: (55, 55)
PU-PUEA Distance: 21.21 units

Generating Our Dataset...

It creates different scenarios with varying distances between PU and PUEA, extracts statistical features (mean, variance, median, lower quartile, and upper quartile) from these measurements, and creates multiple test cases with different percentages of PUEA presence (10%, 20%, 30%, 40%, and 50%) to evaluate the effectiveness of various clustering algorithms in distinguishing between legitimate and malicious signals.


PUEA Detection Project Classification Hierarchy
Scenarios
: Far distance
PU: [20,20]
PUEA: [80,80]
Percentage Cases
10%
20%
30%
40%
50%
: Medium distance
PU: [25,25]
PUEA: [55,55]
Percentage Cases
10%
20%
30%
40%
50%
: Close distance
PU: [40,40]
PUEA: [55,55]
Percentage Cases
10%
20%
30%
40%
50%
Clustering Algorithms
(density-based)
(centroid-based)
(hierarchical)
Performance Evaluation
Detection rate and false detection rate calculated for each algorithm
Results compared across scenarios, percentages, and algorithms
Best-performing algorithm identified for each scenario
Visualization Hierarchy
Individual clustering results for each scenario-percentage-algorithm combination
Comparative performance across algorithms for each scenario
Overall performance metrics comparing algorithms and scenarios

Example Time slot Matrix for D1= 56.57 (for PU)

	User	Mean	Variance	Median	Upper Quartile	Lower Quartile
TS1	PU	—	—	—	—	—
TS2	PU	—	—	—	—	—
TS3	PU	—	—	—	—	—
⋮	⋮	⋮	⋮	⋮	⋮	⋮
TS19	PU	—	—	—	—	—
TS20	PU	—	—	—	—	—

We get statistical deviation features of receive power of PU in One case

Example Time slot matrix for D1= 56.57 (for PUEA)

	User	Mean	Variance	Median	Upper Quartile	Lower Quartile
TS1	PUEA	—	—	—	—	—
TS2	PUEA	—	—	—	—	—
TS3	PUEA	—	—	—	—	—
⋮	⋮	⋮	⋮	⋮	⋮	⋮
TS19	PUEA	—	—	—	—	—
TS20	PUEA	—	—	—	—	—

We get statistical deviation features of receive power of PUEA in One case

	User	Mean	Variance	Median	Upper Quartile	Lower Quartile
TS1	PU	—	—	—	—	—
TS2	PU	—	—	—	—	—
TS3	PU	—	—	—	—	—

	User	Mean	Variance	Median	Upper Quartile	Lower Quartile
TS1	PUEA	—	—	—	—	—
TS2	PUEA	—	—	—	—	—
TS3	PUEA	—	—	—	—	—

80 % of PU's Time slots

20 % of PUEA's Time slots

Replace that % of time slots with its PUEA statistical features.

	User	Mean	Variance	Median	Upper Quartile	Lower Quartile
TS1	PU	—	—	—	—	—
TS2	PU	—	—	—	—	—
TS3	PU	—	—	—	—	—
TS6	PUEA	—	—	—	—	—

Forming the required dataset.

Example Dataset

Similarly , we form datasets for each %cases of PUEA

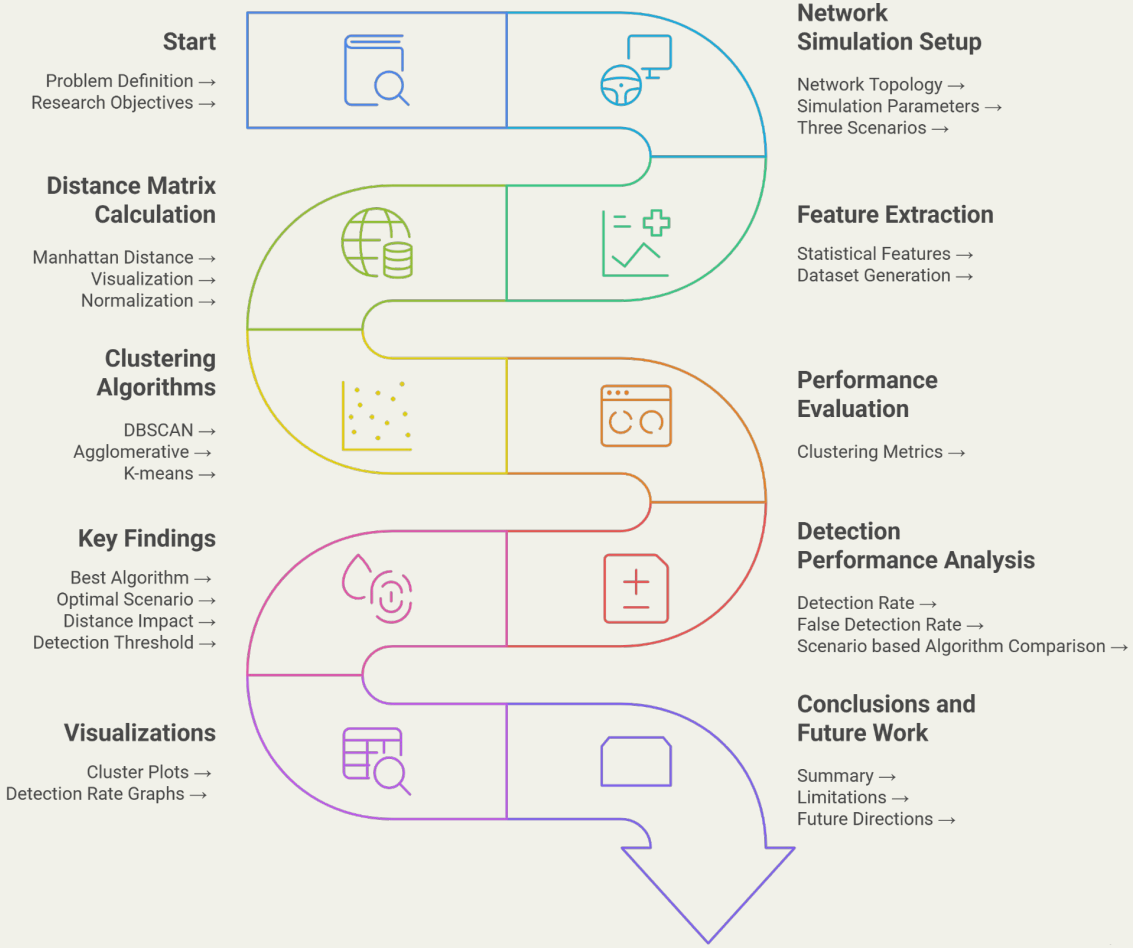
	User	Mean	Variance	Median	Upper Quartile	Lower Quartile
TS1	PU	—	—	—	—	—
TS2	PU	—	—	—	—	—
TS3	PUEA	—	—	—	—	—
⋮	⋮	⋮	⋮	⋮	⋮	⋮
TS19	PUEA	—	—	—	—	—
TS20	PU	—	—	—	—	—

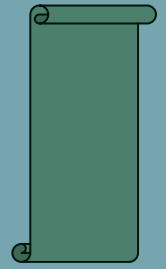
Manhattan Distance:

This measures the distance as the sum of the absolute differences between the coordinates of the points

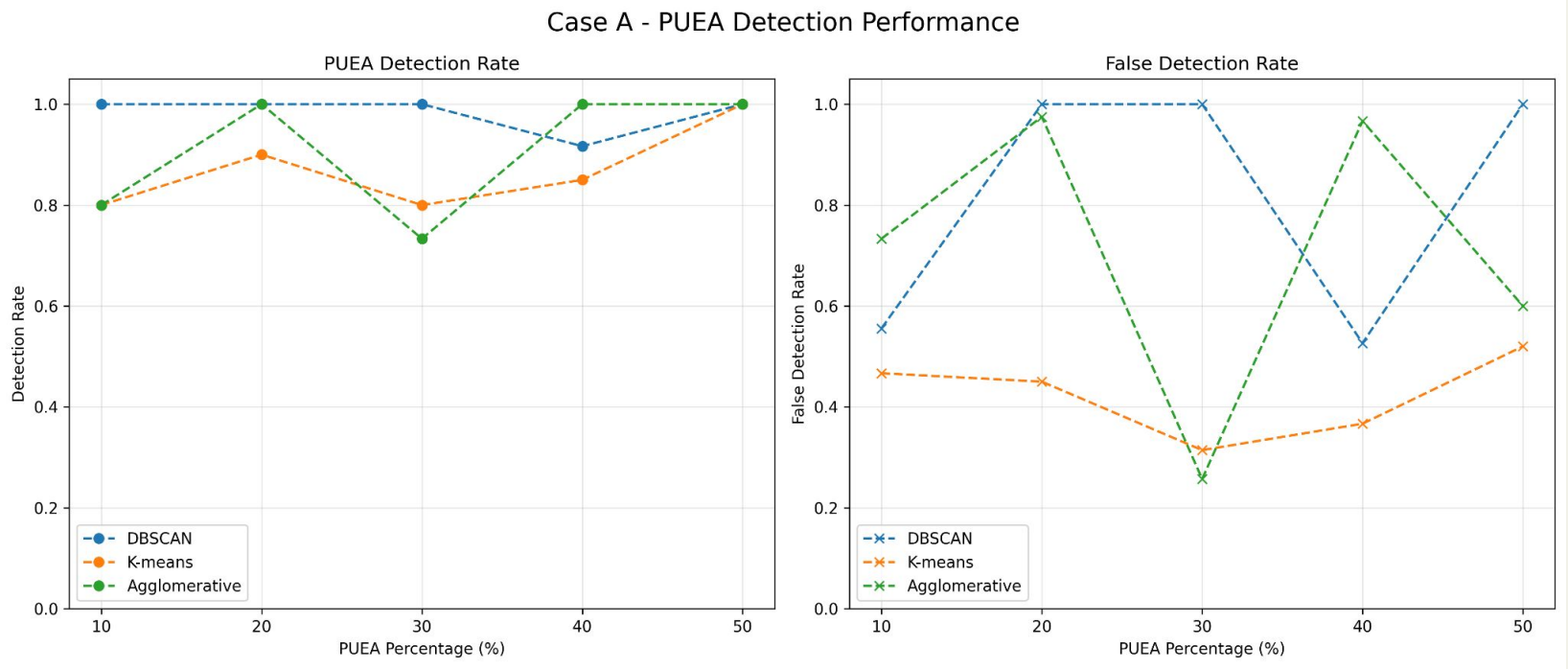
$$M_{i,j} = \sum_{k=1}^{n} |x_{i,k} - x_{j,k}|$$

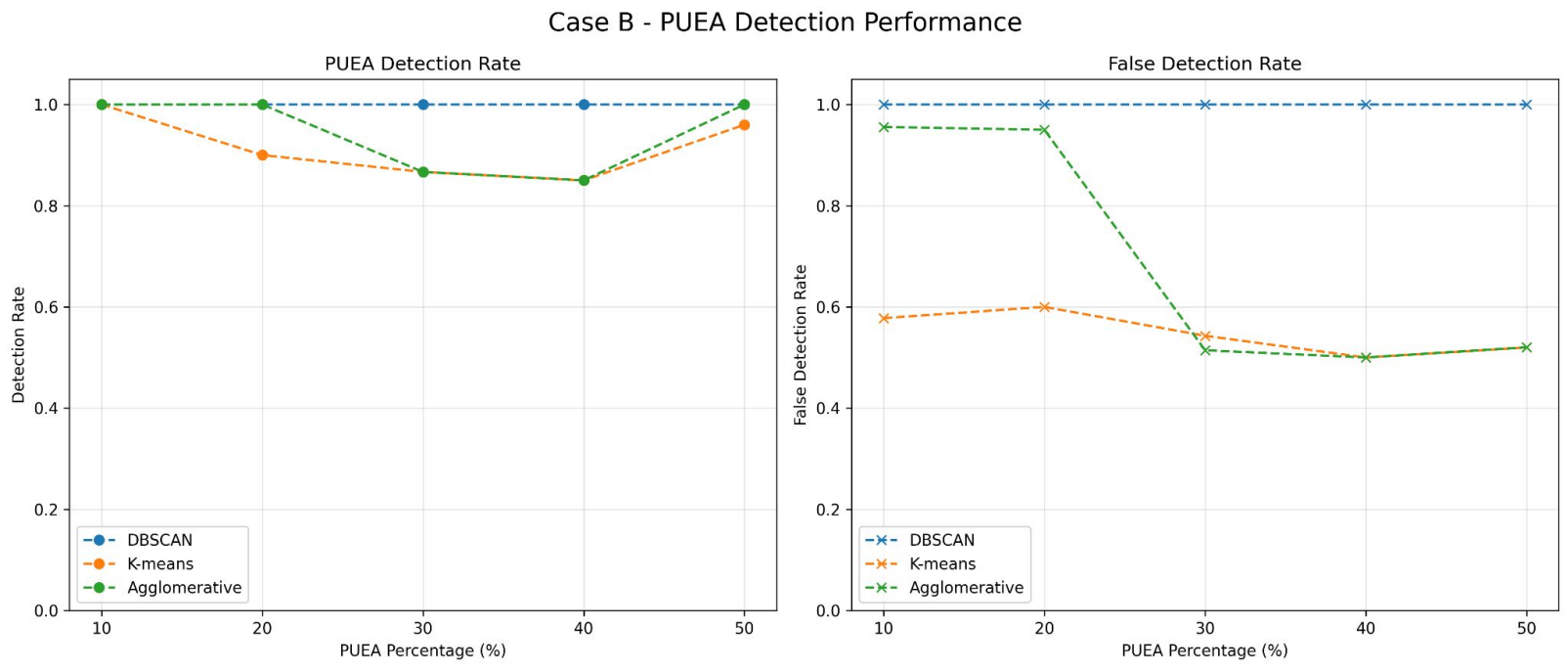
	TS1	TS2	TS3	.....	TS19	TS20
TS1	0	—	—	—	—	—
TS2	—	0	—	—	—	—
TS3	—	—	0	—	—	—
⋮	⋮	⋮	⋮	⋮	⋮	⋮
TS19	—	—	—	—	0	—
TS20	—	—	—	—	—	0

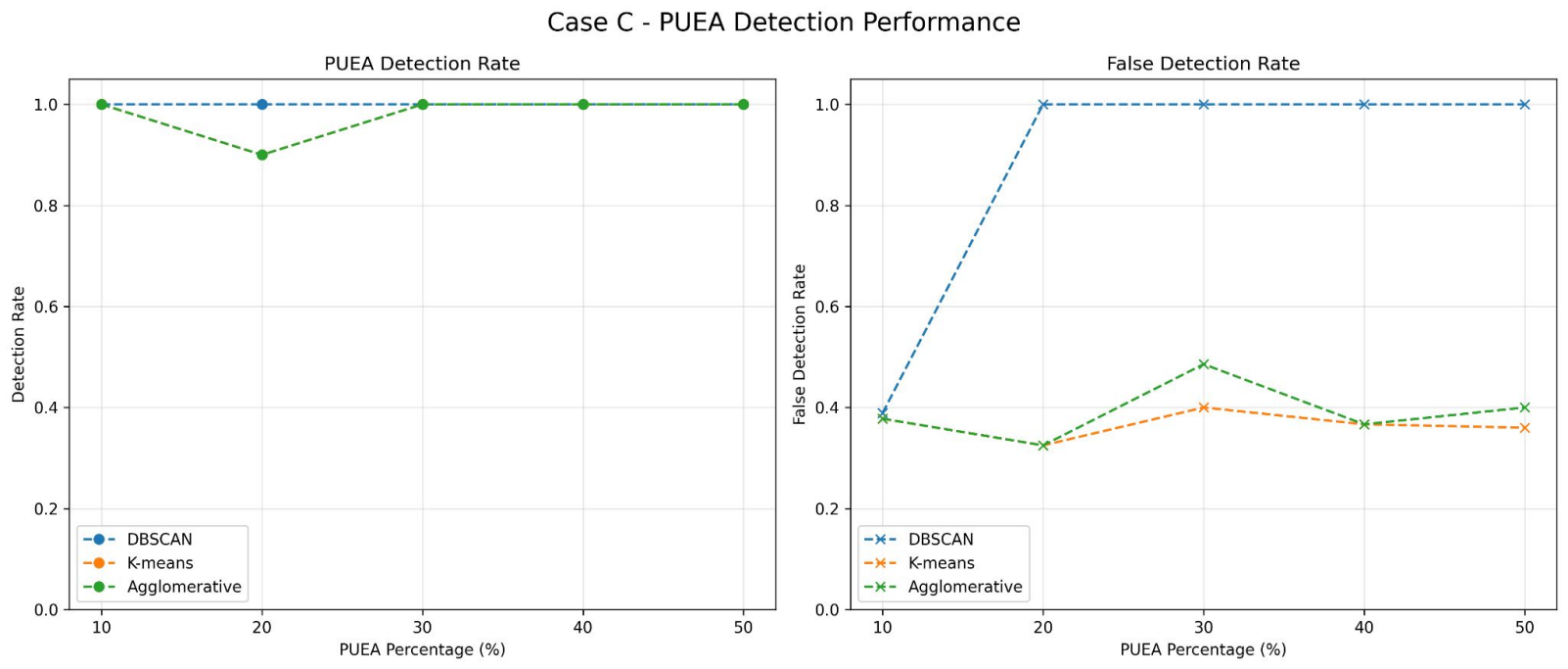

Start
Problem Definition →
Research Objectives →
Distance Matrix Calculation
Manhattan Distance →
Visualization →
Normalization →
Clustering Algorithms
DBSCAN →
Agglomerative →
K-means →
Key Findings
Best Algorithm →
Optimal Scenario →
Distance Impact →
Detection Threshold →
Visualizations
Cluster Plots →
Detection Rate Graphs →
Network Simulation Setup
Network Topology →
Simulation Parameters →
Three Scenarios →
Feature Extraction
Statistical Features →
Dataset Generation →
Performance Evaluation
Clustering Metrics →
Detection Performance Analysis
Detection Rate →
False Detection Rate →
Scenario based Algorithm Comparison →
Conclusions and Future Work
Summary →
Limitations →
Future Directions →



Result & Findings


Case A - PUEA Detection Performance
PUEA Detection Rate
Detection Rate
PUEA Percentage (%)
DBSCAN
K-means
Agglomerative
False Detection Rate
False Detection Rate
PUEA Percentage (%)
DBSCAN
K-means
Agglomerative


Case B - PUEA Detection Performance
PUEA Detection Rate
Detection Rate
PUEA Percentage (%)
DBSCAN
K-means
Agglomerative
False Detection Rate
False Detection Rate
PUEA Percentage (%)
DBSCAN
K-means
Agglomerative


Case C - PUEA Detection Performance
PUEA Detection Rate
Detection Rate
PUEA Percentage (%)
DBSCAN
K-means
Agglomerative
False Detection Rate
False Detection Rate
PUEA Percentage (%)
DBSCAN
K-means
Agglomerative

Key Observations:

Case A:

- **PUEA Detection Rate**:

  DBSCAN maintains near-perfect detection at 10%, 20%, and 30%, dropping slightly at 40% before recovering at 50%

  K-means shows the most variability, with detection rates between 0.8-1.0

  Agglomerative clustering shows a notable dip at 30% PUEA percentage

- **False Detection Rate**:

  DBSCAN and Agglomerative show highly variable false detection rates that oscillate dramatically

  K-means maintains the lowest false detection rate (0.3-0.5) across all PUEA percentages.

Case B:

- **PUEA Detection Rate**:

  DBSCAN maintains a perfect 1.0 detection rate across all PUEA percentages

  K-means and Agglomerative both show a downward trend until 40%, then recover at 50%

- **False Detection Rate**:

  DBSCAN shows a constant 1.0 false detection rate (very poor performance)

  K-means and Agglomerative show improving false detection rates as PUEA percentage increases.

Case C:

- **PUEA Detection Rate**:

  DBSCAN maintains perfect 1.0 detection across all percentages

  Agglomerative drops slightly at 20% but recovers to 1.0 for the remainder

  K-means maintains consistent high performance (not fully visible but appears stable)

- **False Detection Rate**:

  DBSCAN performs very poorly with near 1.0 false detection for most percentages

  K-means and Agglomerative maintain relatively low false detection rates (0.3-0.5).

Key Findings:

Algorithm Performance:

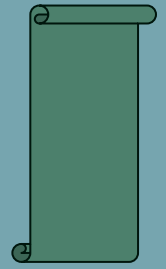
- DBSCAN consistently achieves the highest PUEA detection rates across all cases but suffers from extremely high false detection rates in Cases B and C
- K-means shows the most balanced performance with moderate-to-high detection rates and generally lower false detection rates
- Agglomerative clustering performs well in detection but shows higher volatility in false detection rates.

PUEA Percentage Impact:

- Detection performance generally improves at higher PUEA percentages for K-means and Agglomerative clustering
- False detection rates tend to stabilize or decrease at higher PUEA percentages for K-means and Agglomerative clustering.

Best Overall Algorithm:

- K-means offers the best balance between detection and false detection rates across all three cases
- While DBSCAN has superior detection rates, its extremely high false detection rates make it impractical for real-world deployment
- Agglomerative clustering shows promise but with higher variability than K-means.



Conclusions

Conclusion - Securing the Cognitive Future

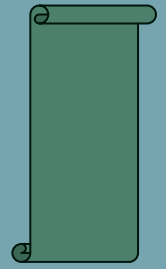
Our analysis of DBSCAN, K-means, and Agglomerative clustering for PUEA detection highlights key trade-offs between detection accuracy and false alarm rates.

- K-means offers the best balance, delivering reliable detection with manageable false alarms, making it the most practical for real-world use.
- DBSCAN achieves very high detection but suffers from consistently high false alarm rates, limiting its effectiveness.
- Agglomerative clustering performs well but shows greater variability, especially in false alarms.
- Detection improves at higher PUEA intensities (40–50%), indicating better algorithm performance as attack severity increases.
- Performance differences across Cases A, B, and C emphasize the need to consider environmental factors when choosing an algorithm.

We recommend K-means as the primary method, fine-tuned for specific network conditions, possibly supported by ensemble techniques to enhance overall detection reliability.

Future Directions

- **Robust Detection**: Develop hybrid models, integrate deep learning, and enhance resilience against adversarial attacks.
- **Adaptive and Efficient Systems**: Implement real-time tuning and optimize for IoT and resource-limited networks.
- **Cross-Domain Applicability**: Validate detection methods across different network types.



References

[1] Dinu Mary Alias and Ragesh G. K, “Cognitive Radio Networks: A Survey,” 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET).

[2] Khaled Mohammed Saifuddin, Kazi Fahid Reza, Masud An Nur Islam Fahim, Sk. Shariful Alam, ”Detection of Primary User Emulation Attack in Cognitive Radio Environment,”2017 6th International Conference on Informatics, Electronics and Vision & 2017 7th International Symposium in Computational Medical and Health Technology (ICIEV-ISCMHT).

[3] Ishu Gupta and O. P. Sahu, “An Overview of Primary User Emulation Attack in Cognitive Radio Networks,” 2018 Second International Conference on Computing Methodologies and Communication (ICCMC).

[4] Khatereh Akbari,Jamshid Abouei,”Signal Classification for Detecting Primary User Emulation Attack in Centralized Cognitive Radio Networks,”Electrical Engineering (ICEE), Iranian Conference.

[5] Bishal Chhetry, Ningrinla Marchanga,”Detection Of Primary User Emulation Attack (PUEA) In Cognitive Radio Networks Using One-Class Classification,” Research Gate.

[6]Amar Taggu and Ningrinla Marchangi,”A Density-based Clustering Approach to detect Colluding SSDF Attackers in Cognitive Radio Networks,”2022 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC).

END OF PRESENTATION

Thank You!