University of Glasgow

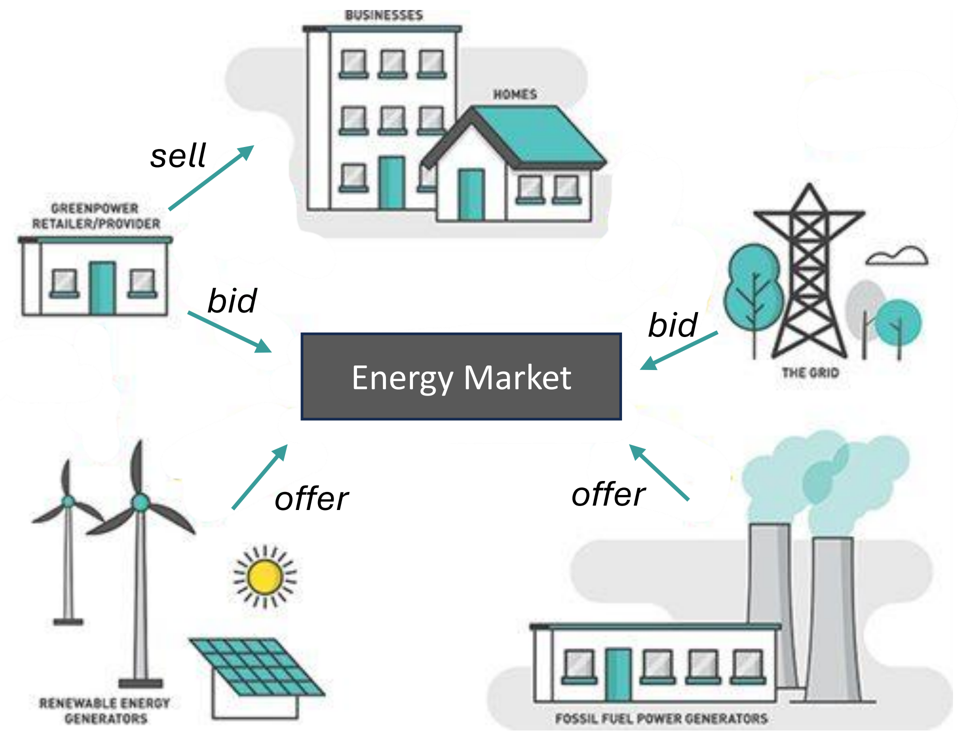
Knowledge & Data Engineering Systems

Incremental Unsupervised Detection of Financially Motivated Attacks in Energy Markets

Ghadeer Alsharif, Christos Anagnostopoulos and Angelos Marnerides

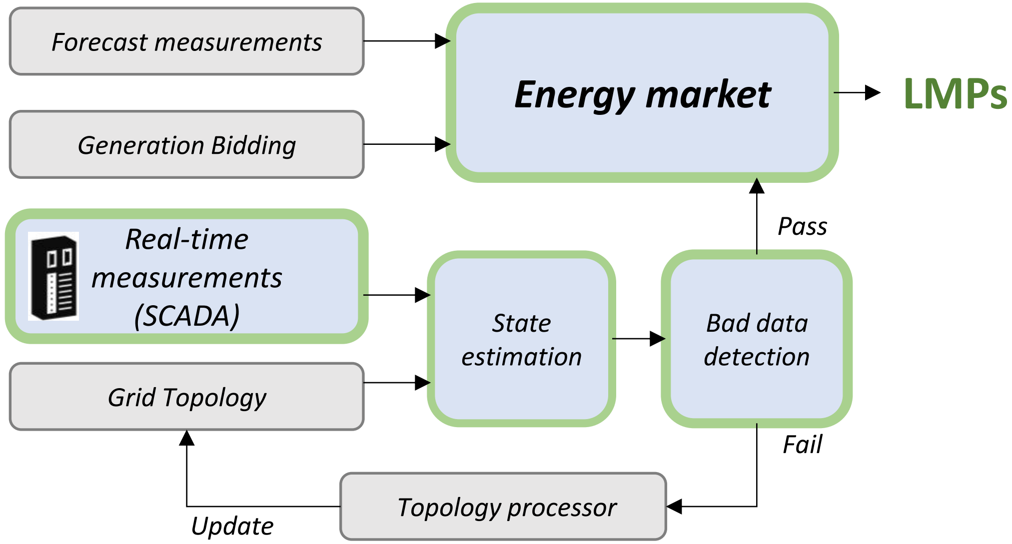
Introduction

- **The Evolution of the Electricity Market:**
  - The electricity industry has undergone a transition towards a competitive framework where participants can bid and offer energy within a dynamic pool.
  - This shift has been driven by the adoption of *Locational Marginal Prices (LMPs)* as the primary mechanism for determining market dynamics.



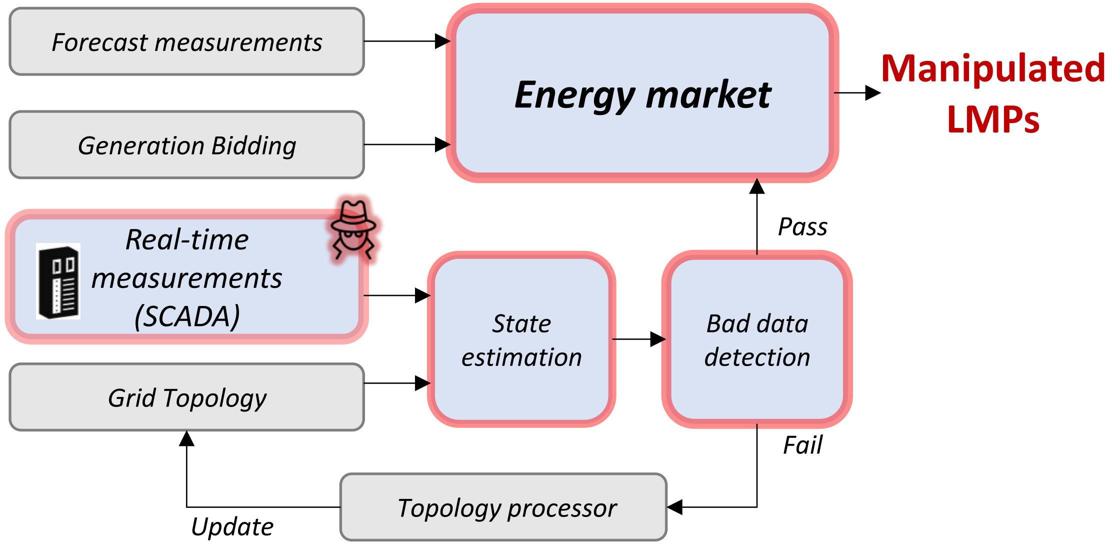
Introduction

- **The Evolution of the Electricity Market:**
  - LMPs reflect the marginal cost of supplying an electricity unit at specific locations within the grid, at any given point in time.
  - LMPs facilitate efficient resource allocation, congestion management, and market equilibrium



Research Problem

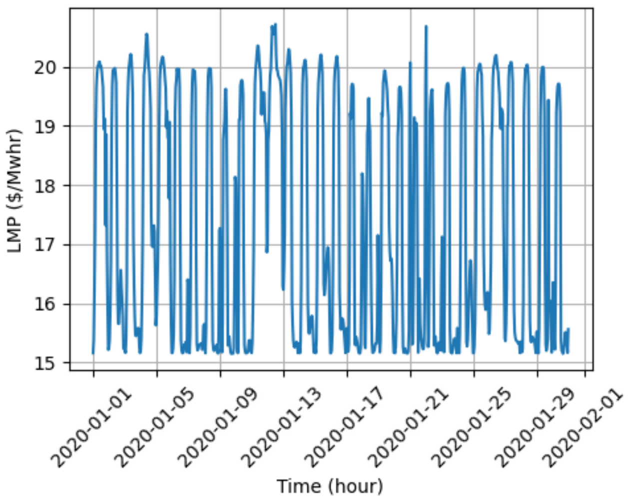
- **Stealthy False Data Injection Attacks in the Energy Market:**
  - Malicious actors target data transmitted from Remote Terminal Units (RTUs) to the SCADA system.
  - **Objective**: Manipulate market outcomes for financial gain.
  - **Persistence**: Attacks designed to persist over an extended period for long-term gains.
  - **Impact**: Manipulation of state estimation results, skewing LMPs.
  - **Consequences**: Financial losses, inefficient resource allocation, and reduced system efficiency.

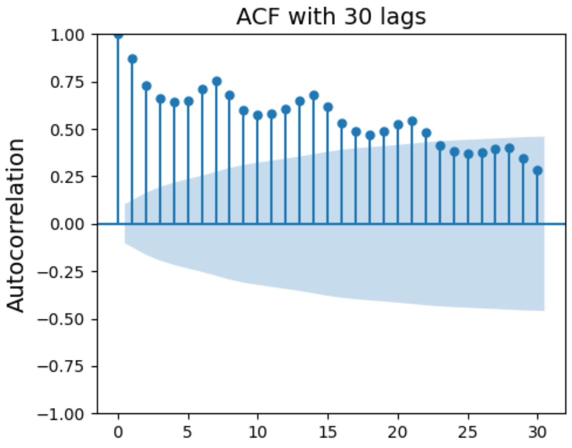


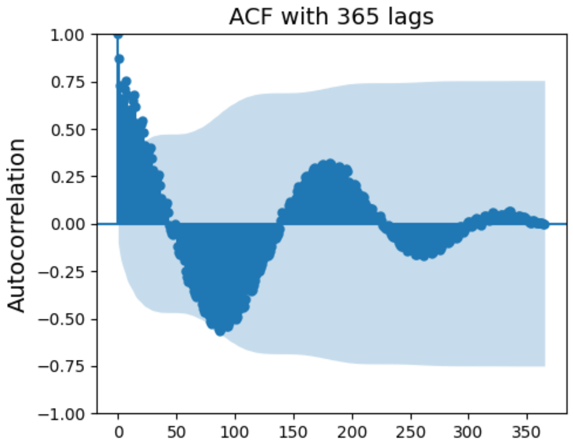
Challenges

Why these kind of attacks are difficult to detect?

1. Complex System Interdependencies with High Uncertainty
2. Subtle Price Variations.
3. Non-Stationary LMP Characteristics

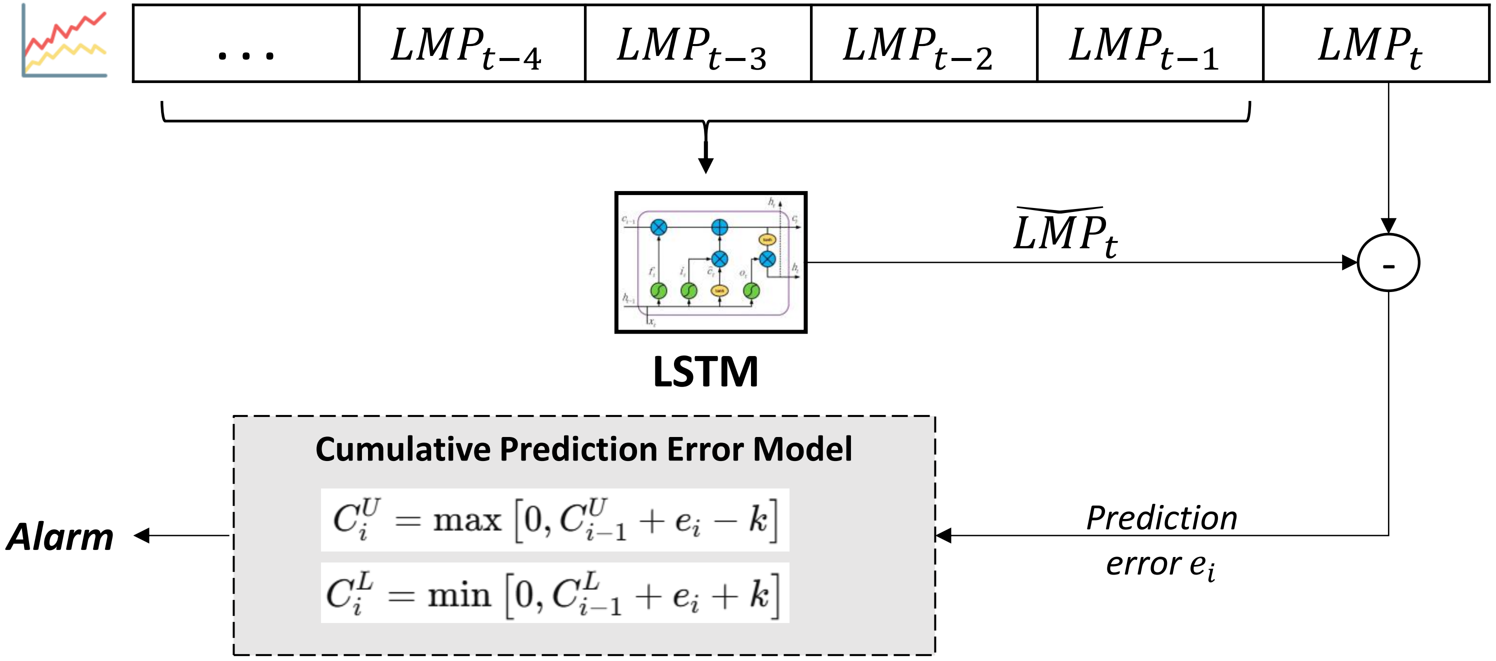






Cumulative Prediction Error Model

Design of the Cumulative Prediction Error Model:

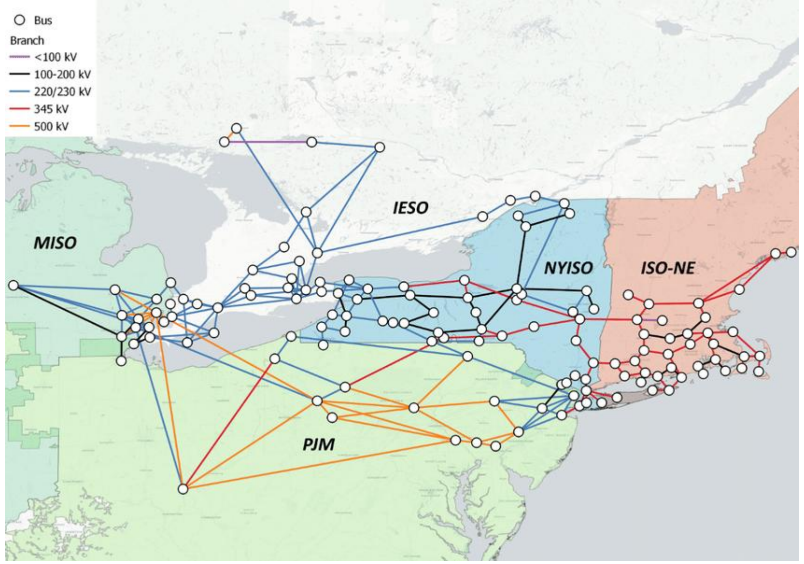


FDIA Simulation

1. **Simulation benchmark:** NPCC test system provided in [1].
2. **Attack vector: T**ransmission line ratings attack [2] at line 109 targeting Bus/node 115.

Algorithm 1 FDIA Generalized Process

Input: Power system case $\mathcal{P}$, nominal attack vector $\mathbf{a}_{\text{nom}}$, attack magnitude α, attack time indices $\mathcal{T}_a$.
Output: $\mathcal{S}$: Time series of LMPs, labels, and timestamps
function LMPATTACKSIMULATION($\mathcal{P}, \mathbf{a}_{\text{nom}}, \alpha, \mathcal{T}_a$)
  Initialize $\mathcal{S} \leftarrow \emptyset$
  for each timestep t **do**
    $\mathbf{l}_t \leftarrow$ GETLOADPROFILE($\mathcal{P}, t$) ▷ *Load vector for all buses at time t*
    if $t \in \mathcal{T}_a$ **then**
      $\mathbf{a}_t \leftarrow \alpha \cdot \mathbf{a}_{\text{nom}}$, $y_t \leftarrow 1$ ▷ *FDIA present*
    else
      $\mathbf{a}_t \leftarrow \mathbf{a}_{\text{nom}}$, $y_t \leftarrow 0$ ▷ *No FDIA*
    end if
    $\lambda_t \leftarrow$ RUNOPF($\mathcal{P}, \mathbf{l}_t, \mathbf{a}_t$)
    $\mathcal{S} \leftarrow \mathcal{S} \cup \{(\lambda_t, y_t, t)\}$
  end for
  return $\mathcal{S}$
end function

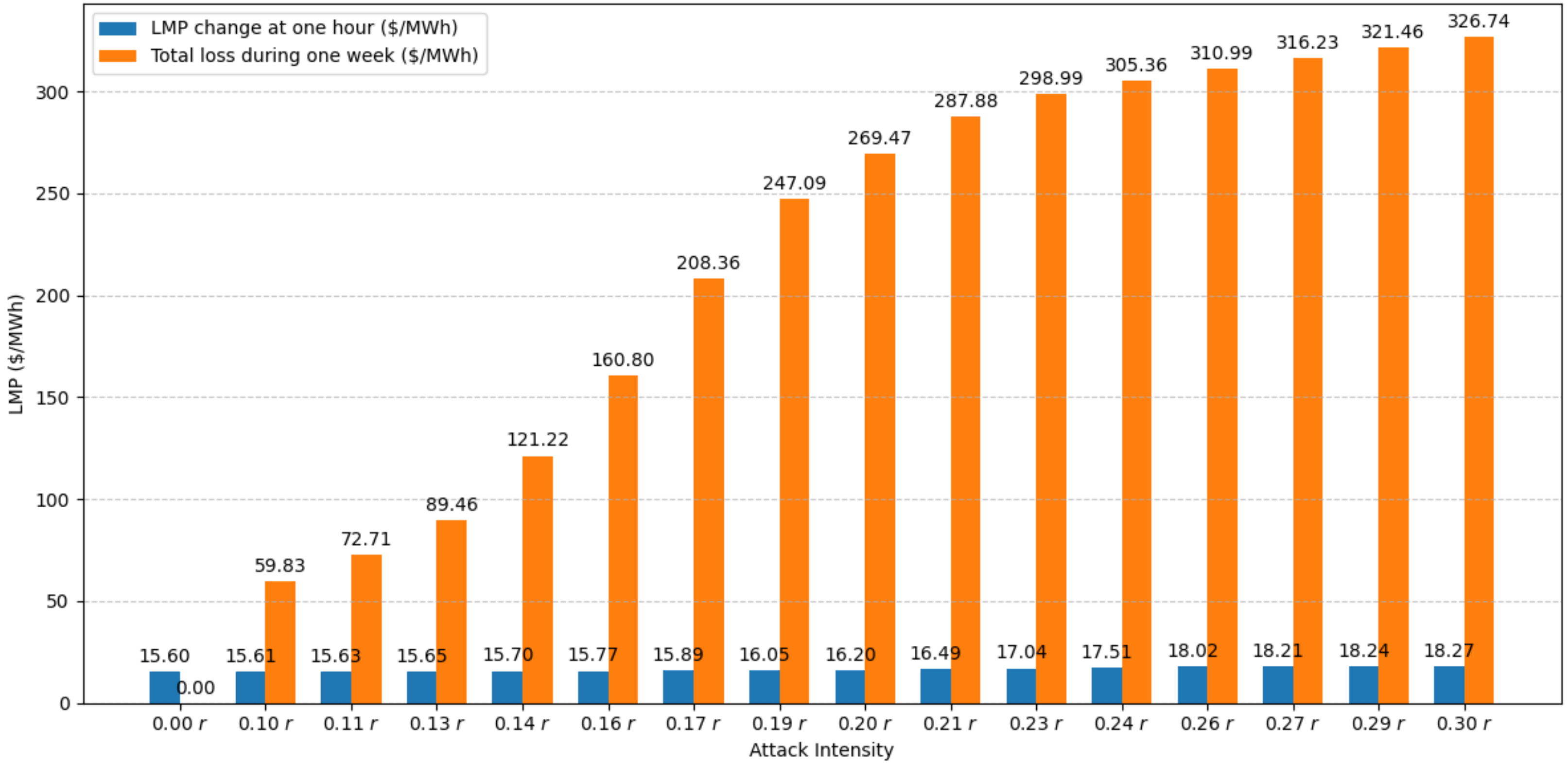


NPCC system [1]

[1] Zhang, Q. and Li, F., 2023. A Dataset for Electricity Market Studies on Western and Northeastern Power Grids in the United States. Scientific Data, 10(1), p.646.
[2] Ye, H., Ge, Y., Liu, X. and Li, Z., 2015. Transmission line rating attack in two-settlement electricity markets. IEEE Transactions on Smart Grid, 7(3), pp.1346-1355.

Experiment Results

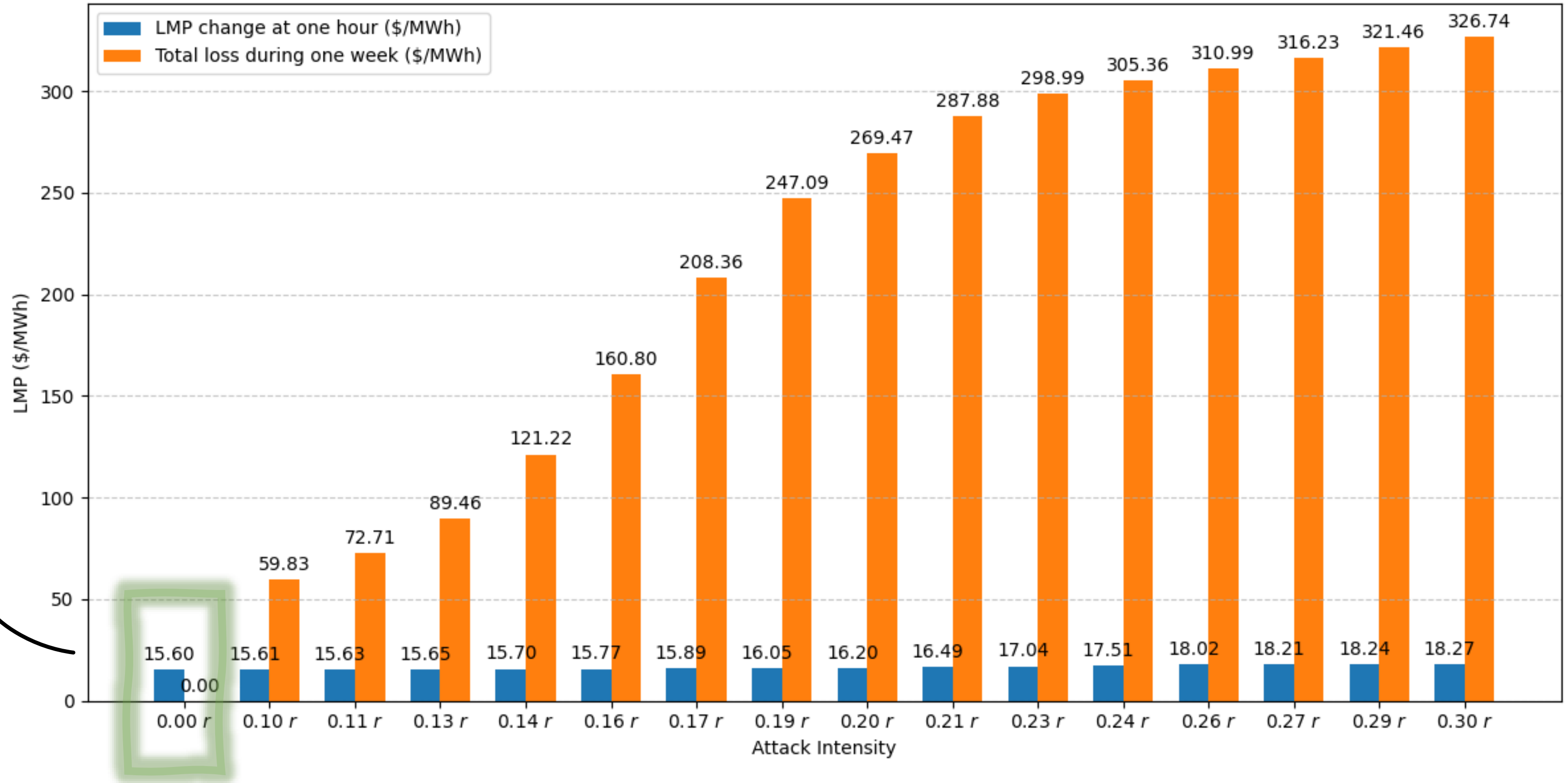
1- Impact of Attack Intensity on LMP Change ($/MWh) and Total Loss ($) During a Week



Experiment Results

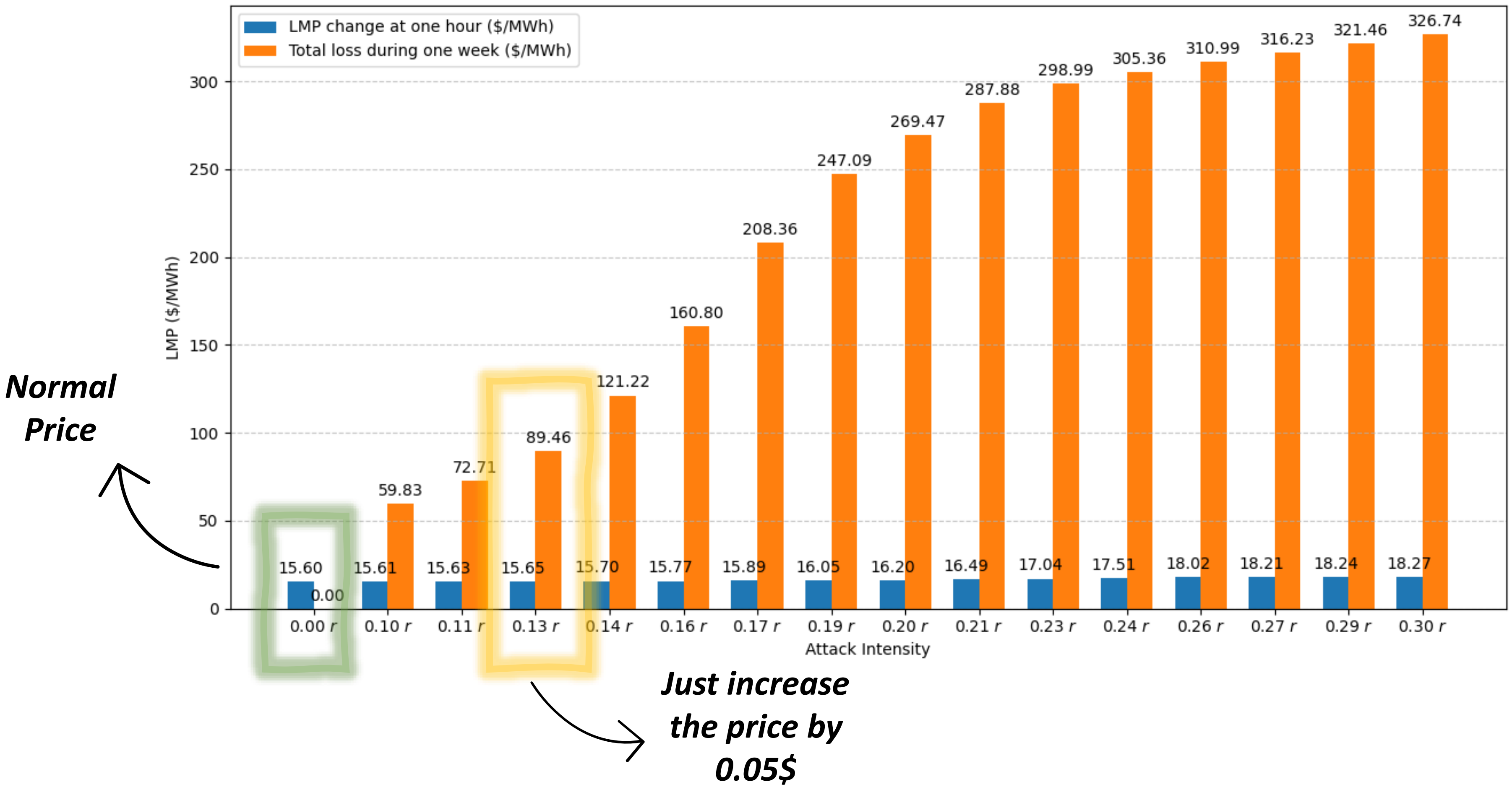
1- Impact of Attack Intensity on LMP Change ($/MWh) and Total Loss ($) During a Week

Normal Price



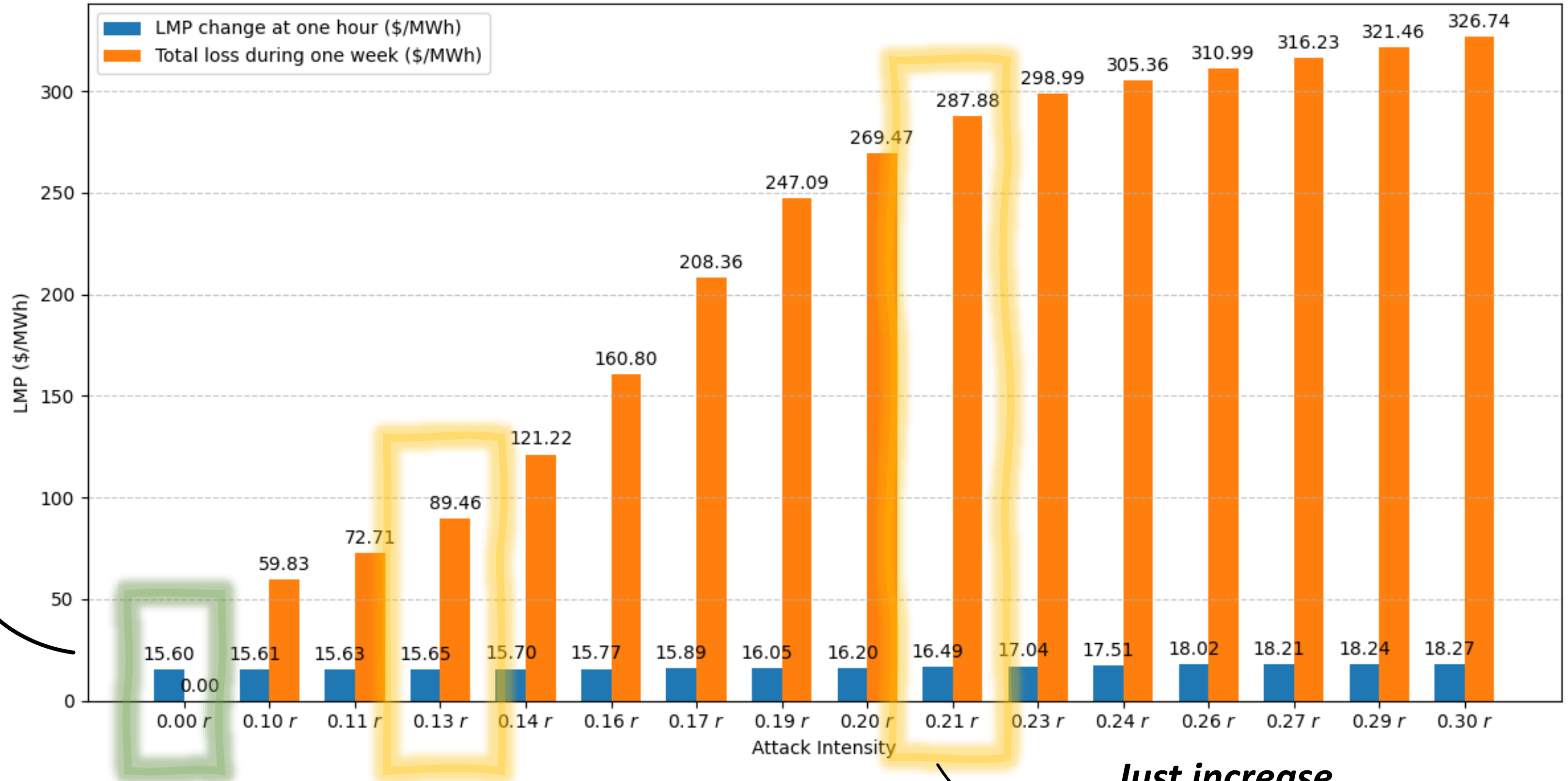
Experiment Results

1- Impact of Attack Intensity on LMP Change ($/MWh) and Total Loss ($) During a Week



Experiment Results

1- Impact of Attack Intensity on LMP Change ($/MWh) and Total Loss ($) During a Week



Normal Price

Maliciously increase the price by 0.05$

Just increase the price by 0.89$

Experiment Results

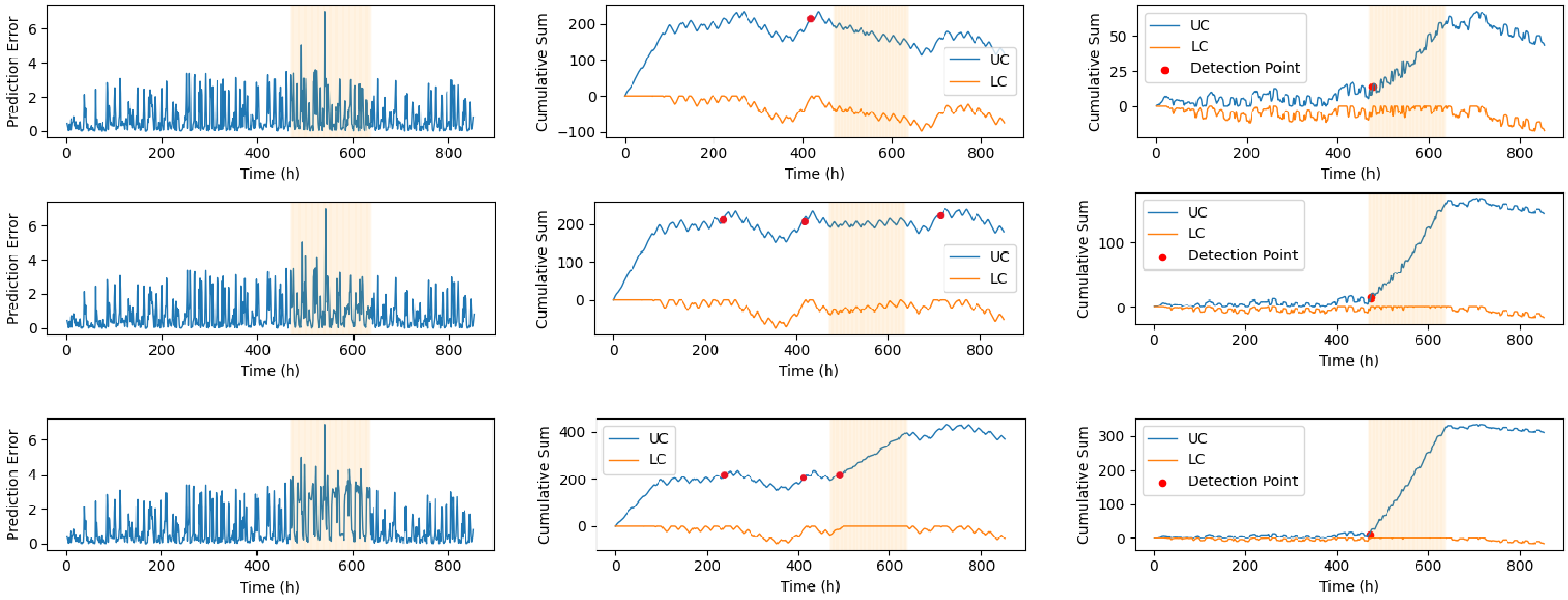
2. Comparing the **Visibility of LMP Manipulation** across different models at various attack intensities

a) Baseline 1 : Prediction Error ***b) Baseline 2: Cumulative Sum*** ***c) Our model: Cumulative Prediction Error***

0.1r

0.2r

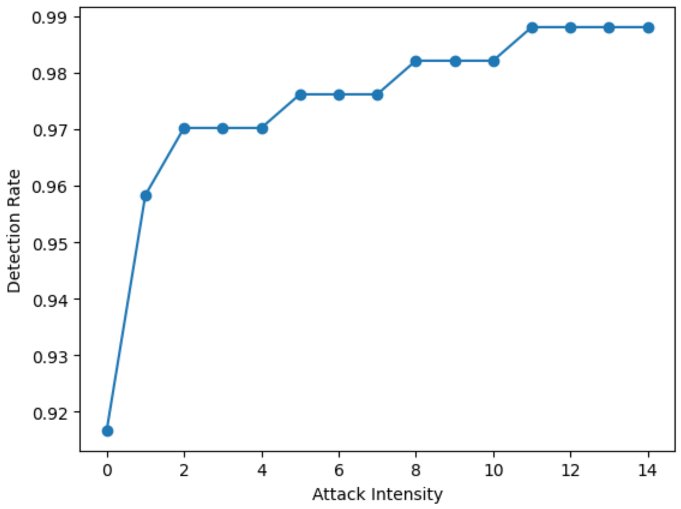
0.3r



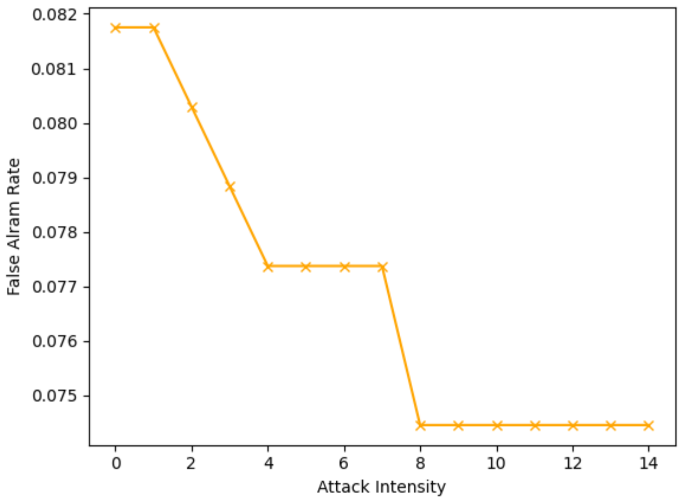
Experiment Results

3. Detection Performance of our model over different attack intensity:

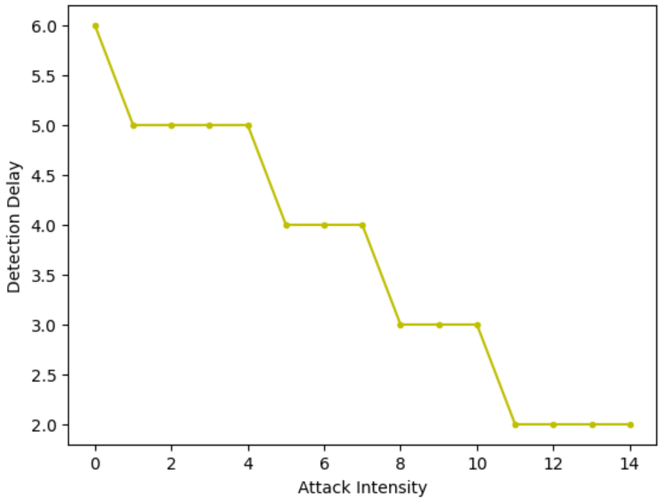
a) Detection Rate



b) False Alarm



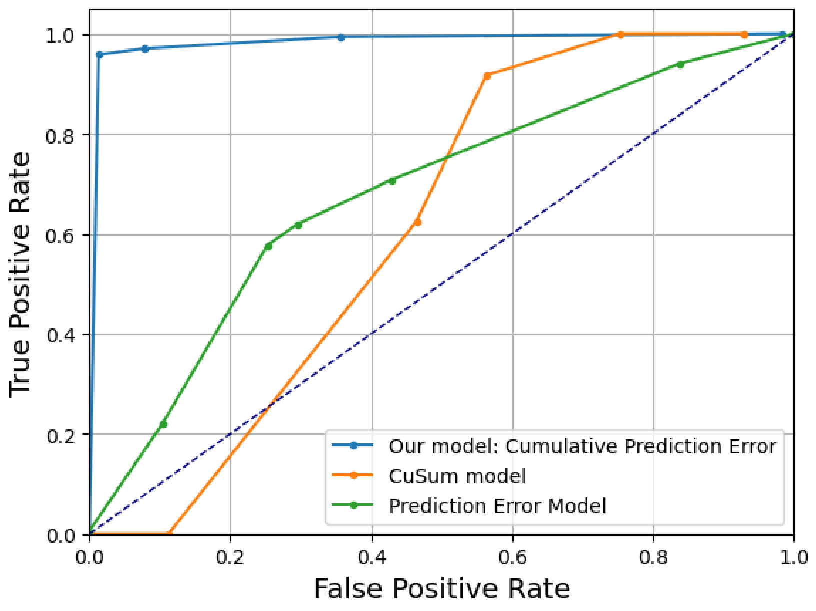
c) Detection Delay



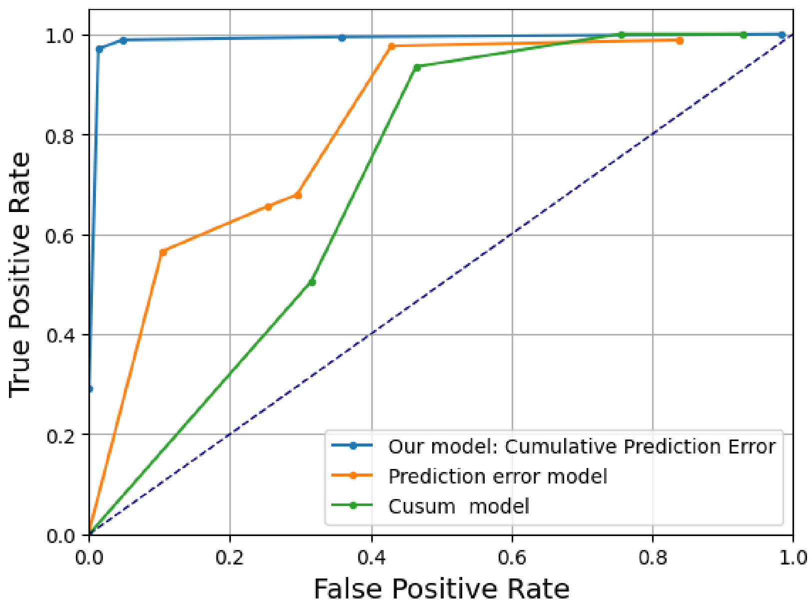
Experiment Results

4. Detection Performance over different threshold

a) Attack intensity 0.15r



b) Attack intensity 0.3r



Conclusion

Our model effectively meets the research objectives by accurately detecting financially motivated attacks:

1. *Achieved an average AUC of 0.94 and an F1-score of 0.85, indicating robust detection capability.*
2. *Enables a quick detection of LMP anomalies within a few time steps.*
3. *Relies just on the LMP time-series without requiring additional data sources.*

Conclusion

Research Limitations:

1. *The designed model is univariate, focusing exclusively on analyzing a single time-series variable (LMP data).*
2. *Unable to determine whether LMP anomalies are caused by technical issues or malicious activities.*

University of Glasgow

Knowledge & Data Engineering Systems

Thank you!