University of Glasgow

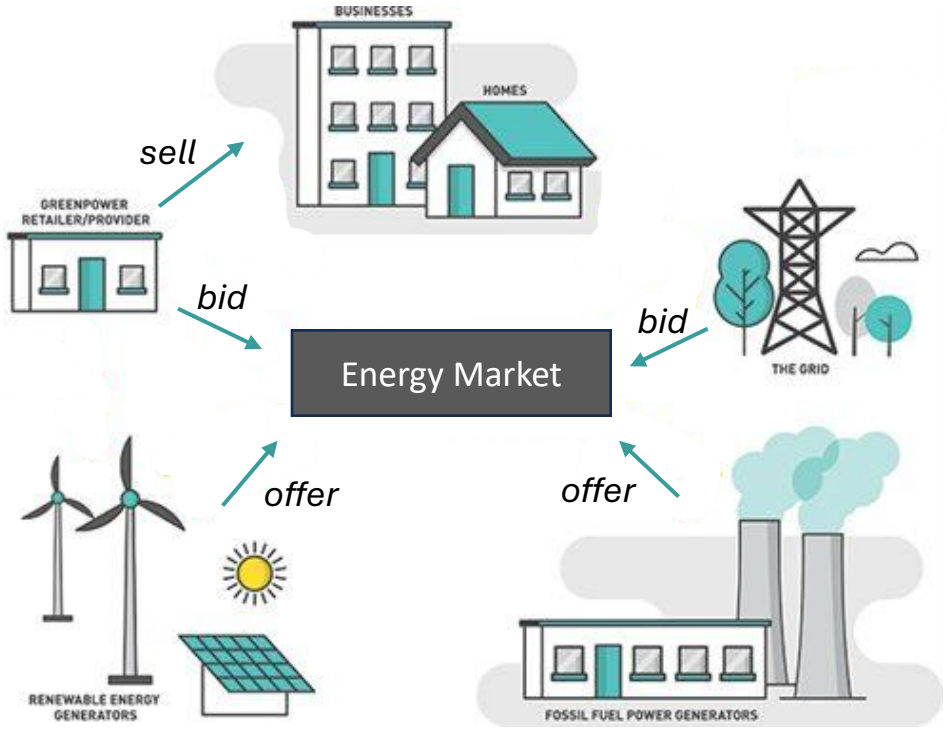
Knowledge & Data Engineering Systems

Drift-aware Unsupervised Detection of Stealthy FDIA Towards Energy Market

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.

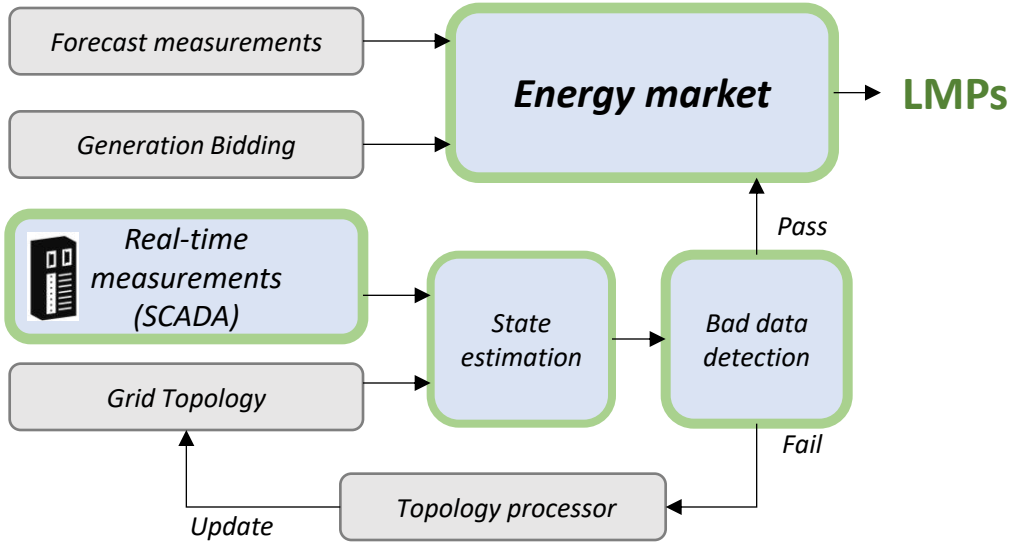


University of Glasgow

Introduction

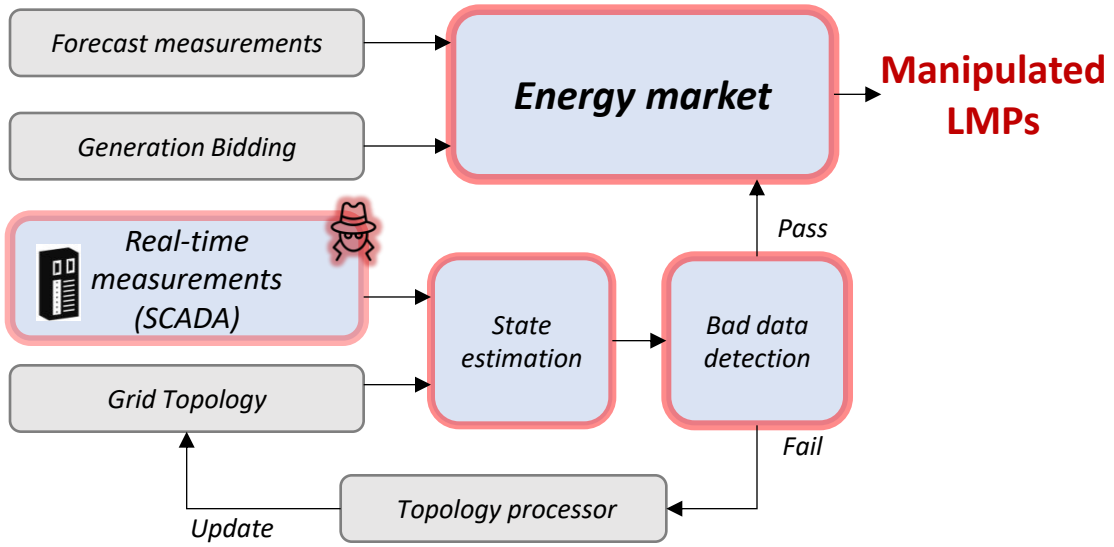
Knowledge & Data Engineering Systems

- **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



Motivation

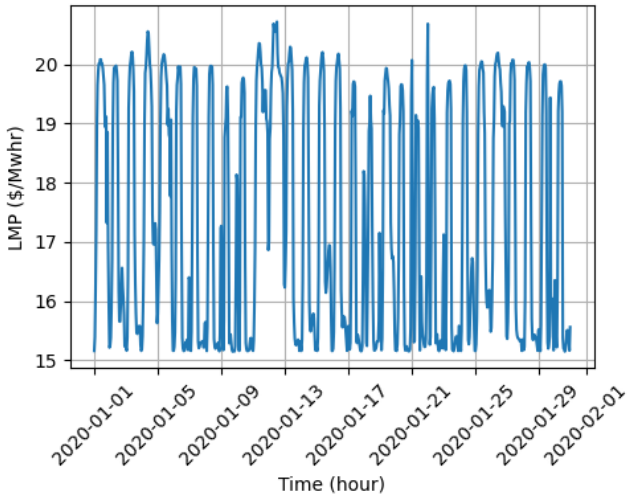
- **Stealthy False Data Injection Attacks in the Energy Market:**
  - Malicious actors target data transmitted from Remote Terminal Units (RTUs) to the SCADA system.
  - **Objective**: Manipulate market outcomes for financial gain.
  - **Persistence**: Attacks designed to persist over an extended period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

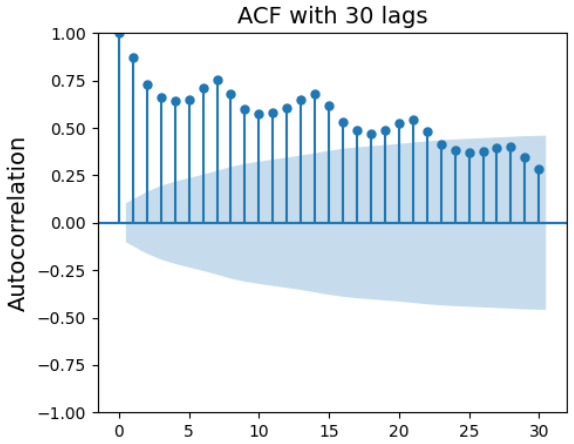


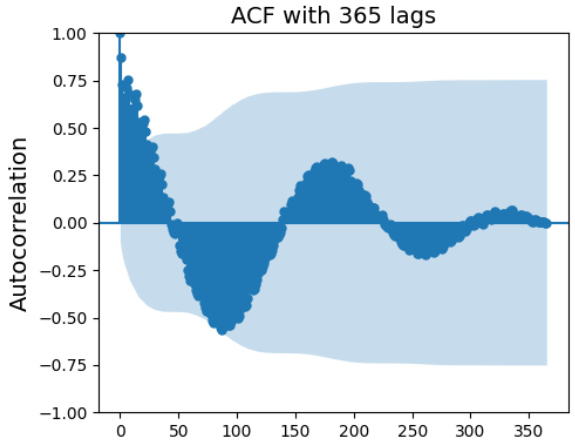
Challenges

***CH1**: LMP attacks are designed to avoid detection, with attackers subtly influencing energy prices.*

***CH2**: The inherent uncertainty in power systems results in non-stationarity of energy prices. This yields the key statistical properties of LMP to drift over time.*







University of Glasgow

Knowledge & Data Engineering Systems

Research Gap

1. *Focus on attack strategies development rather than detection mechanisms.*
2. *Existing defense approaches secure measurement units but:*
   - *Assume PMUs are attack-proof (ignoring GPS spoofing, etc.)*
   - *Protecting only select measurements reduces redundancy; lowers estimation accuracy.*
3. *Current anomaly detection frameworks:*
   - *Depend on model-based approaches (predefined system models).*
   - *Vulnerable to stealthy FDIAs and novel attacks outside assumed conditions.*

University of Glasgow

Contribution

Knowledge & Data Engineering Systems

*We propose a **data-driven**, online **Change Ponit Detection** framework for detecting stealthy FDIAs in LMP time series:*

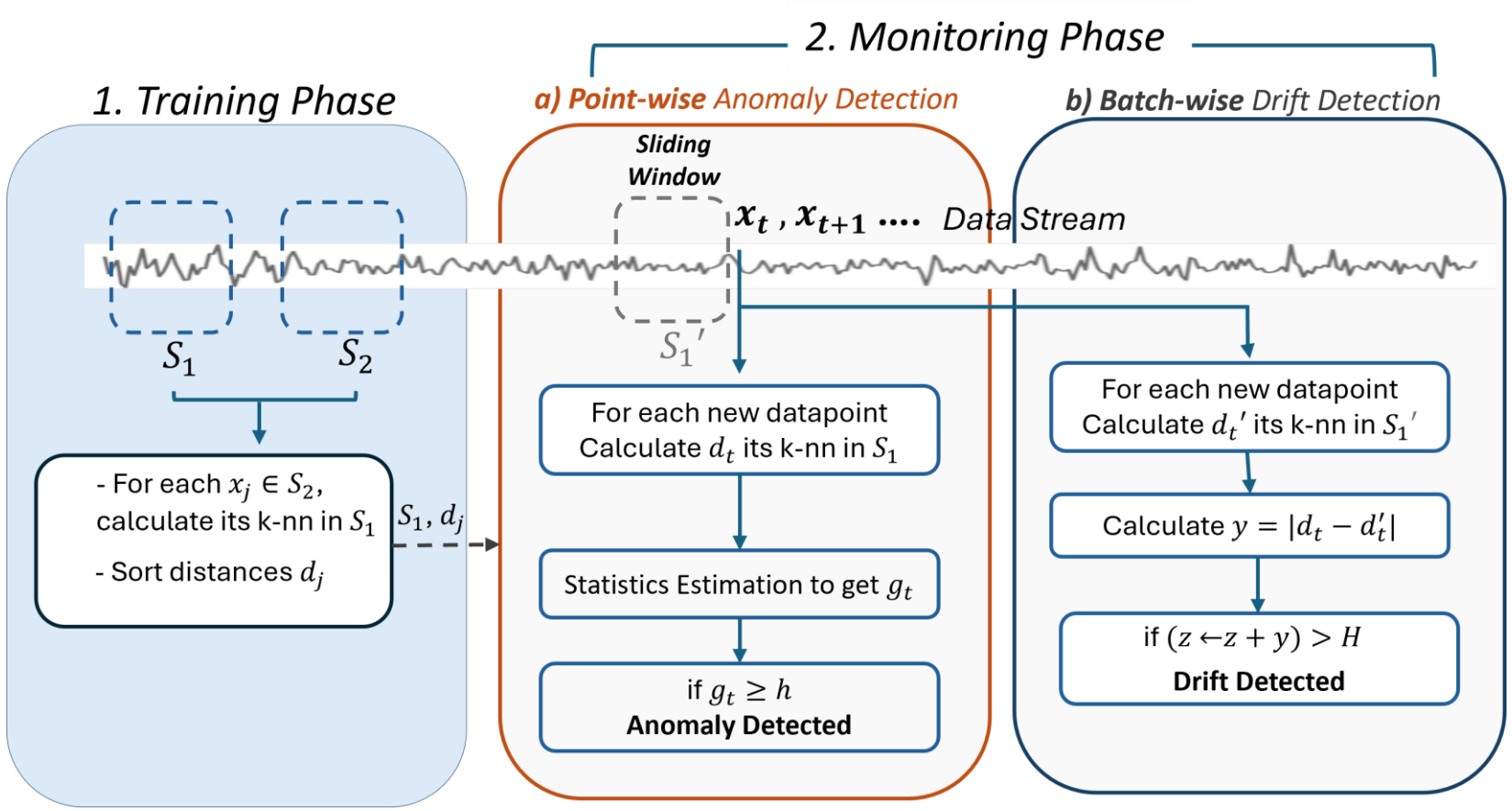
1. *Novel framework for detecting LMP manipulation via market-level models.*
2. *Generalized CPD approach; no assumptions on data distribution.*
3. *Adaptive anomaly detection distinguishing deliberate attacks from normal evolving LMP patterns.*

University of Glasgow

Knowledge & Data Engineering Systems

Methodology

Drift-aware Unsupervised Anomaly Detection Framework:



University of Glasgow

Methodology

Knowledge & Data Engineering Systems

Point-wise Anomaly Detection Model:

Algorithm 1 GEMAD: Anomaly Detection Model

Input: S_1, d_j and parameters: k, α, λ, h.
Initialization: the reference set $S'_1 \leftarrow S_1$.
for each new point x_t: **do**
    Get the k-NNs of x_t from S_1 and compute d_t.
    $\hat{p}_t = \frac{1}{N_2} \sum_{x_j \in S_2} \mathbb{I}\{d_j > d_t\}$, $\hat{s}_t = \log\left(\frac{\alpha}{\hat{p}_t}\right)$
    $g_t \leftarrow \max\{0, \lambda.g_{t-1} + \hat{s}_t\}$
    if $g_t \geq h$ **then**
        Alarm
    else
        Label x_t as $normal$, $S'_1(t) \leftarrow S'_1(t-1) \cup \{x_t\}$
    end if
end for

University of Glasgow

Methodology

Knowledge & Data Engineering Systems

Batch-wise Drift Detection Models:

Algorithm 2 CAD Drift Detection

Input: Threshold H.
Initialization: $z \leftarrow 0$, S_1' from GEMAD (Algorithm 1).
for each new point x_t: **do**
    Call GEMAD to label x_t and obtain d_t.
    if x_t is $normal$: **then**
        Get the k-NNs of x_t from S_1' and compute d_t'.
        $y = |d_t - d_t'|$, $z = z + y$
        if $z \geq H$ **then**
            Drift detected; reset z and retrain model
        end if
    end if
end for

Algorithm 3 CKL Drift Detection

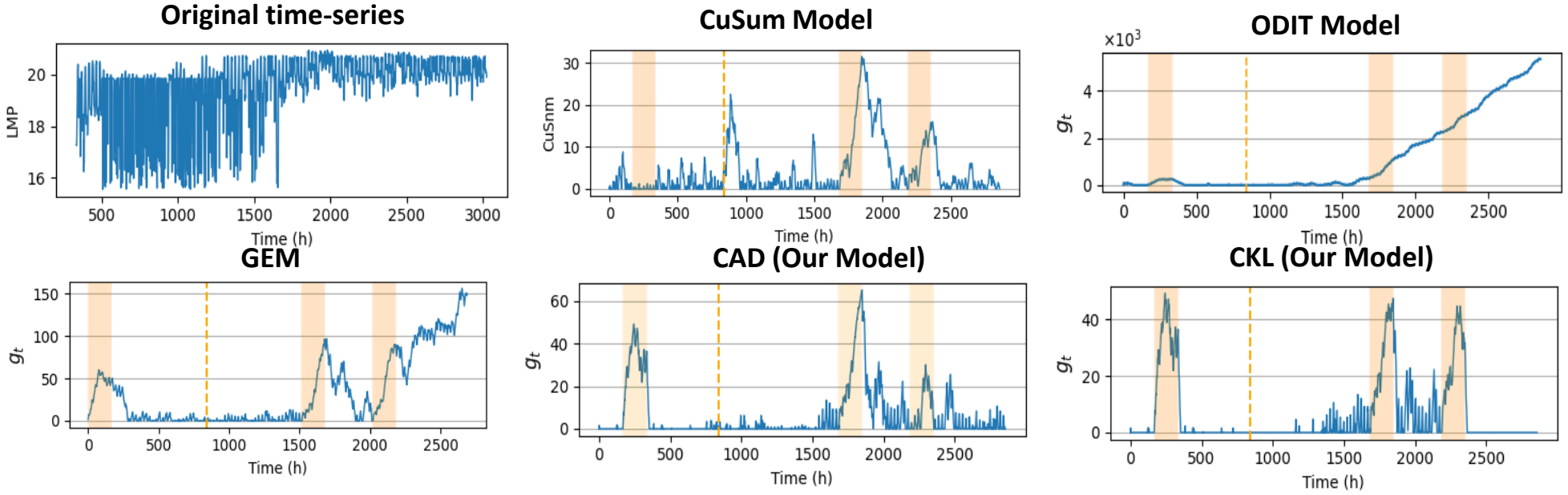
Input: Threshold H, tolerance θ, window size w
Initialization: $z \leftarrow 0$, S_1' from GEMAD (Algorithm 1).
for each new point x_t: **do**
    Call GEMAD to label x_t and obtain d_t.
    if x_t is $normal$: **then**
        Append p_t to P and get the k-NNs of x_t from S_1'.
        Compute d_t' and p_t' in (7), (9), append p_t' to P'
        if len$(P') = w$ **then**
            $D_{KL}(P\|P')$ in (12), $z \leftarrow z + |D_{KL} - \theta|$
            if $z \geq H$ **then**
                Drift detected; reset y and retrain model
            end if
        end if
    end if
end for

University of Glasgow

Experiments

Knowledge & Data Engineering Systems

1- Detection Performance Comparison



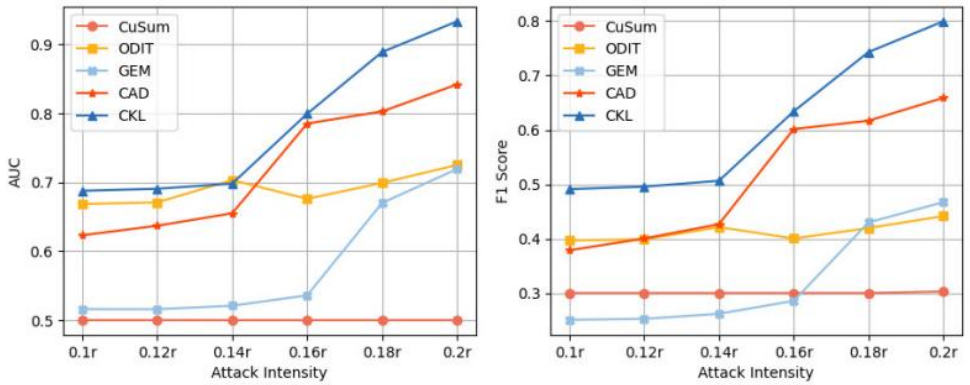
Metric	CuSum		ODIT		GEM		CAD (Our Model)		CKL (Our Model)	
	Before	After	Before	After	Before	After	Before	After	Before	After
DR	0.119	0.9642	0.988	1.000	0.9107	0.8244	0.9821	0.9136	0.9821	0.9519
Precision	0.0826	0.2250	0.3023	0.2250	0.5751	0.2591	0.9166	0.4342	0.9166	0.5955
F1-score	0.0976	0.3648	0.4630	0.3096	0.7050	0.3943	0.9482	0.5886	0.9482	0.7422
AUC	0.3388	0.6503	0.6133	0.5546	0.7872	0.6504	0.9776	0.8401	0.9776	0.9156
FAR	0.4413	0.6634	0.7614	0.8906	0.3363	0.5234	0.0269	0.2334	0.0269	0.1208

Experiments

2- *Impact of Diverse Attack Intensity*

Attack intensity	No FDIA	$0.1r$	$0.12r$	$0.14r$	$0.16r$	$0.18r$	$0.2r$
LMP ($/Mwhr)	15.6	15.61	15.64	15.7	15.77	16.03	16.2
Total illegal profit in a week ($/Mwhr)	0	59.83	81.08	121.22	160.8	227.7	269.47

TABLE III: LMP values under different attack intensities



3- *Detection Efficiency Comparison*

Method	CAISO dataset		Synthetic dataset	
	FAR	**Updates**	**FAR**	**Updates**
No drift detection	0.3306	0	0.3123	0
Fixed update (weekly)	0.0404	24	0.0841	18
CAD Model	0.0188	12	0.1483	6
CKL Model	0.0059	11	0.0947	3

Conclusion & Future work

Key Achievements:

- Novel market-level approach for stealthy FDIA detection.
- Concept drift–aware, adaptive detection model.
- High detection reliability with minimal false alarms.

Future Work:

- Extend the framework by integrating spatial clustering of buses to enhance detection accuracy.
- Design an optimized model update strategy that determines when and what to update after drift detection.


University of Glasgow
Knowledge & Data Engineering Systems
Thank you!
Ghadeer Alsharif
g.alsharif.1@research.gla.ac.uk
LinkedIn