C&ESAR 2025 by DGA
32nd Computer & Electronics Security Application Rendezvous

TRUST-AWARE VERTICAL INTRUSION DETECTION FOR IOT VIA EVOLUTIONARY GRAPH NEURAL NETWORKS (V-IDS)

MYRIA BOUHADDI AND KAMEL ADI

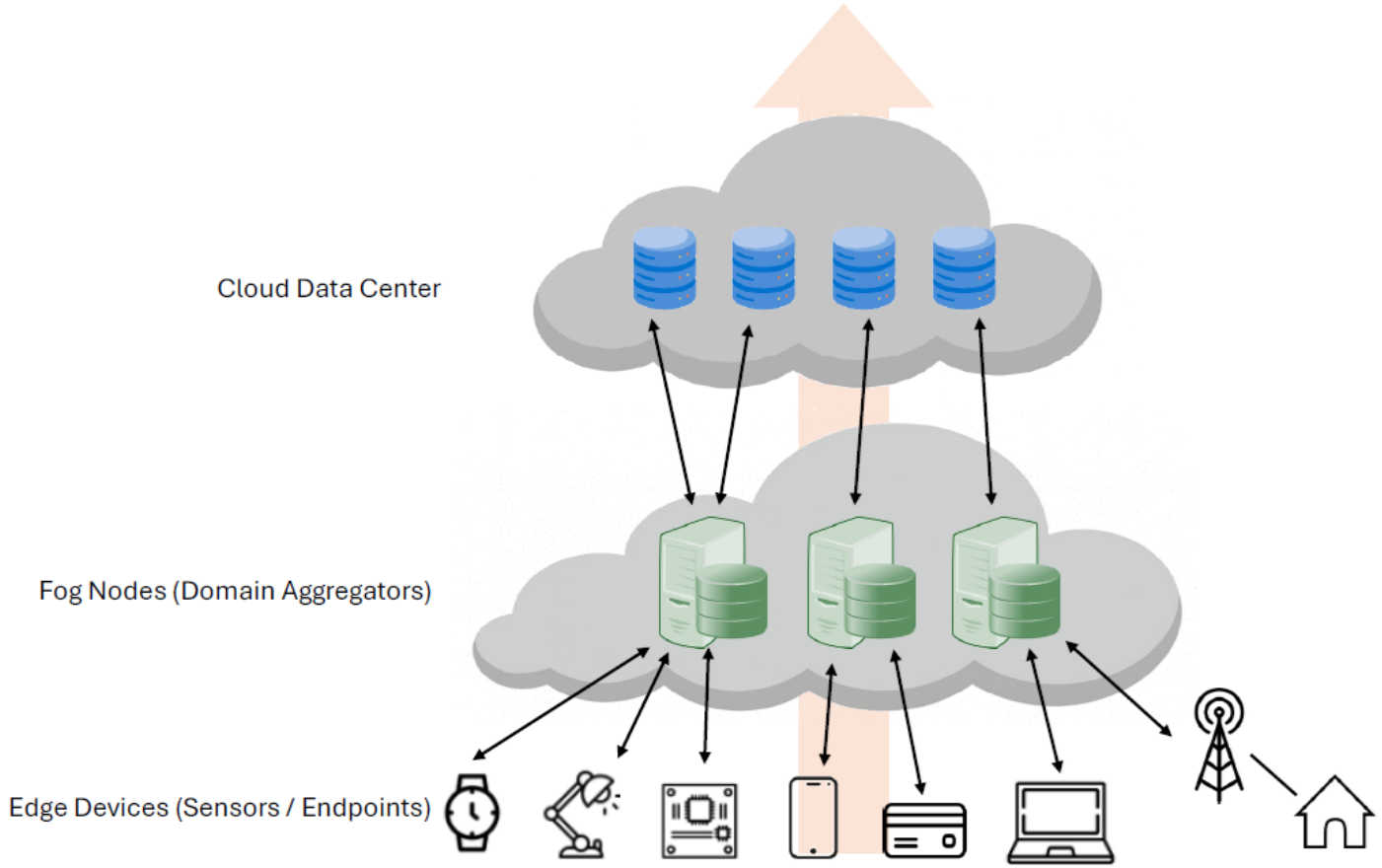
COMPUTER SECURITY RESEARCH LABORATORY, UNIVERSITY OF QUEBEC IN OUTAOUAIS, GATINEAU, QUEBEC, CANADA

MYRIA.BOUHADDI@UQO.CA, KAMEL.ADI@UQO.CA

Outline

- Context and motivation
- Problem statement
- Proposed framework
- Experimental evaluation
- Conlusion and future work

FROM SMART HOMES TO SMART CITIES , AND NEW THREATS



"The same device that measures temperature can, tomorrow, be used to exfiltrate industrial secrets."

IOT ATTACKS ARE RAPIDLY INCREASING

- **32.7 million** IoT cyberattacks in **2018** → **112 million in 2022** *(+243% in four years)*
- Over **1.7 billion** IoT attacks detected in **2024** (Kaspersky)
- Around **820,000** IoT attack attempts **per day** expected in **2025**
- More than **50% of IoT devices** contain **critical vulnerabilities**
- **1 in 3** global data breaches now involves an **IoT device**

IOT SECURITY WEAKNESSES AND EMERGING ATTACK VECTORS

Weak security defaults: default passwords, outdated firmware

Resource constraints: limited CPU/RAM → weak/no encryption

Insecure protocols: MQTT, CoAP, UPnP, Telnet

Poor patching & maintenance: long-lasting exploitable flaws

Layered architecture: edge-fog-cloud blind spots

High heterogeneity: diverse devices, inconsistent security

WHY EXISTING IDS FAIL IN MODERN IOT ENVIRONMENTS

Traditional IDS are **flat**, centralized, or focus only on single-layer events.

No global correlation across Edge–Fog–Cloud → multi-stage attacks stay hidden.

Existing GNN-based IDS use **static topologies** and **fixed trust weights**.

They assume all nodes are equally reliable – even compromised ones.

Result: fragmented visibility, high false positives, delayed or missed detection.

TOWARD ADAPTIVE VERTICAL DETECTION AND TRUST REASONING

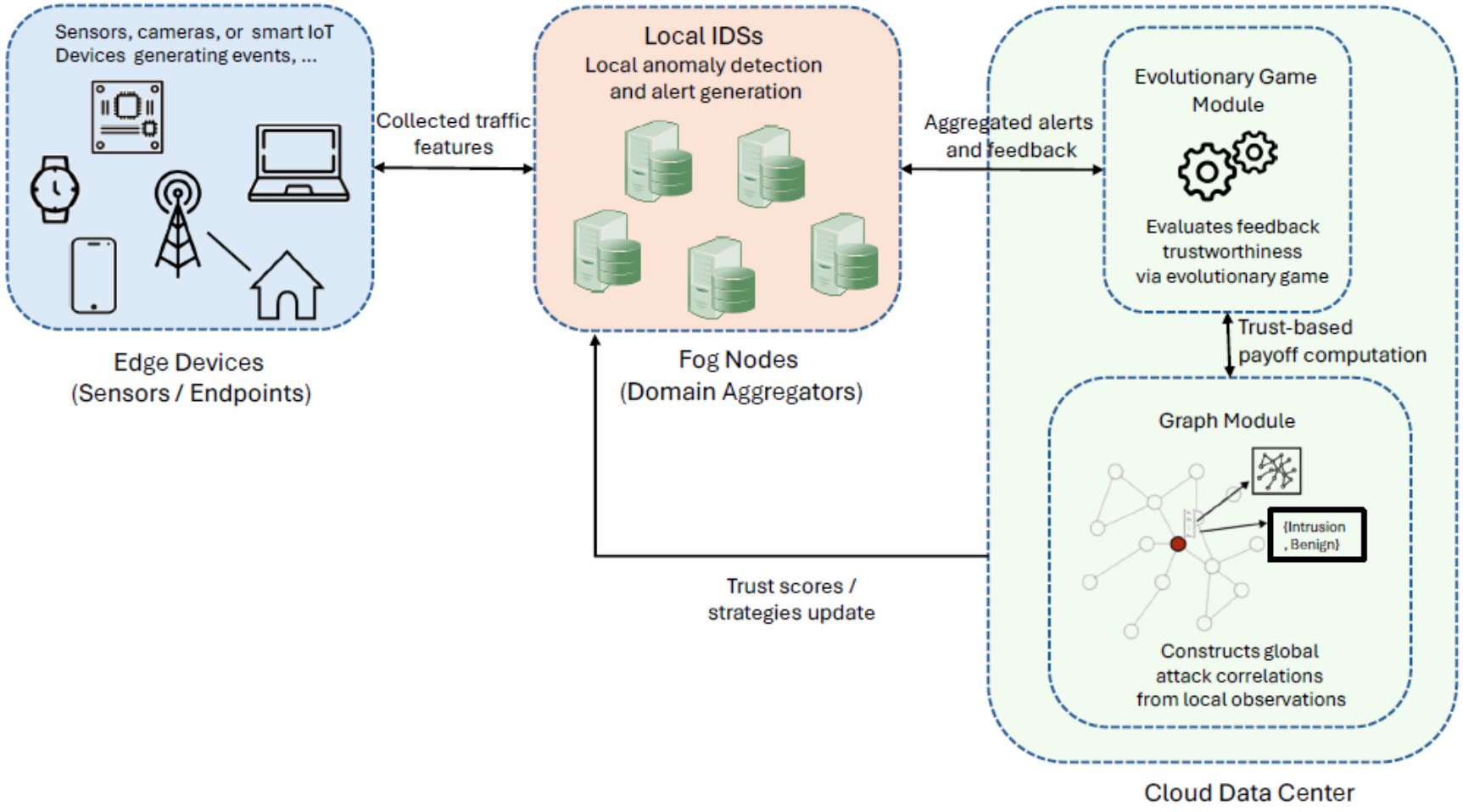
Correlates alerts across Edge, Fog, and Cloud layers
→ enabling true multi-level IoT visibility

Integrates a dynamic trust mechanism
→ based on **evolutionary game theory**

Injects trust into a Graph Neural Network
→ for structural and temporal reasoning

Remains robust under adversarial and noisy conditions

A VERTICAL VIEW OF INTRUSION DETECTION



LOCAL DETECTION & METRIC EXTRACTION AT FOG NODES

- Each Fog node F_i monitors its Edge devices $\mathcal{E}_i$
  and extracts structured security metrics from raw detection events:

$$\phi_i(t) = \left[A_i(t),\ H_i(t),\ \Delta_i(t),\ R_i(t)\right]$$

Where:

- A_i – *Anomaly intensity*
  Average anomaly score across all events in $\mathcal{D}_i(t)$.
- H_i – *Event-type entropy*
  Diversity of observed event types (Shannon entropy).
- Δ_i – *Temporal dispersion*
  Std deviation of inter-arrival times between events.
- R_i – *Detection rate*
  Number of events per device per time window.

Global Fusion at Cloud Level

Step 2 – Global Correlation using a Graph Neural Network (GNN)

- The cloud constructs a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ from all Fog nodes.
- **Nodes** = Fog entities; **Edges** encode connectivity or behavioural similarity.
- Initial edge weights w_{ij} reflect **baseline trust** / communication links.
- ⟶ **At this stage, we have the global structure… but trust is still static.**

WHY WE NEED ADAPTIVE TRUST BETWEEN NODES

Some Fog nodes may become **compromised, faulty, or misconfigured**.

→ Their incorrect alerts can **poison the global decision process**.

→ Treating all nodes equally leads to **propagation of errors**.

→ IoT ecosystems involve **millions of heterogeneous devices** – some *will* behave abnormally.

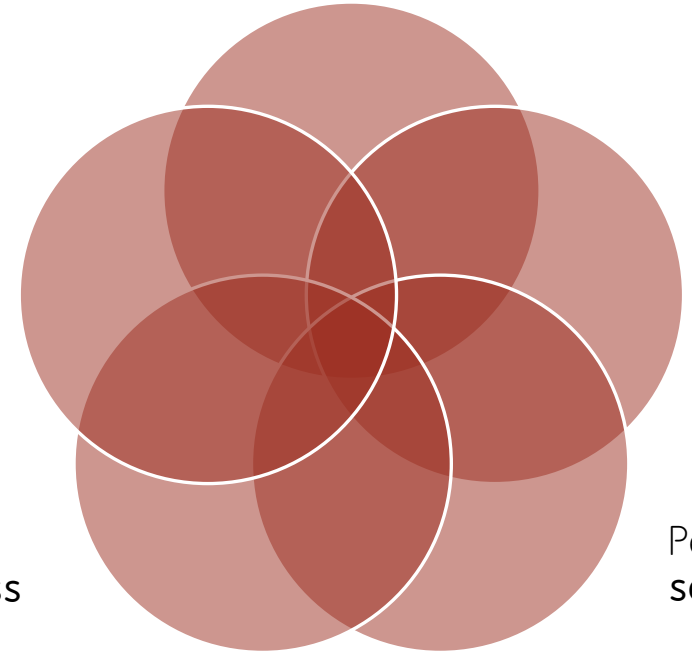
→ We need a mechanism that **continuously evaluates and updates trust**.

→ *"Without adaptive trust, a single unreliable node can distort the perception of the entire system."*

THE POWER OF EVOLUTIONARY DYNAMICS IN CYBERSECURITY

Capture **temporal consistency** in node behaviour.

Provide **stable, convergent trust dynamics** (Evolutionarily Stable Strategies – ESS).



Enable **distributed, autonomous trust adaptation** without central control.

Naturally **suppress unreliable or malicious behaviours**.

Perform **peer-based selection of reliable nodes** (trust emerges from interaction).

INSPIRATION FROM NATURE : EVOLUTIONARY ADAPTATION FOR TRUST

- Nodes behave like agents in a population.
- Honest / cooperative behaviour ⟶ **reinforced**.
- Unreliable or inconsistent behaviour ⟶ **penalized** and loses influence.
- Replicator Dynamics adjusts trust levels based on performance over time.
- "Trust evolves – it is not assigned once and for all."

EVOLUTIONARY GAME THEORY FOR TRUST MODELING

- Nodes act as players adapting their strategies over time.
- Fitness = consistency & correctness of their detections.
- Cooperative (honest) nodes ⟶ higher payoff ⟶ trust increases.
- Unreliable nodes ⟶ lower payoff ⟶ trust decays automatically.
- Replicator Dynamics adjust trust levels based on performance.

➤ Trust becomes an emergent, self-adjusting property – not a fixed rule.

FROM UTILITY TO EVOLUTIONARY DYNAMICS

- Node utility: $u_i = \sum_{j \in \mathcal{N}(i)} w_{ij}\, \mathbf{sim}(\varphi_i, \varphi_j)$
- Average utility: $\bar{u} = x_H u_H + x_U u_U$
- Replicator equation: $\dot{x}_s = x_s \left(u_s - \bar{u}\right)$
- Node replicator coefficient: $r_i = u_i - \bar{u}$

STEP 3 – TRUST-WEIGHTED MESSAGE PASSING

- We incorporate the trust scores into the GNN message-passing process:

$$\tilde{\varphi}_i = r_i \cdot \varphi_i, \qquad \tilde{w}_{ij} = r_i \cdot r_j \cdot w_{ij}$$

$$h_i^{(l+1)} = \sigma\left(\sum_{j \in \mathcal{N}(i)} \tilde{w}_{ij} \, W^{(l)} h_j^{(l)} \right)$$

We have:

- High-trust nodes ⟶ stronger influence in the graph.
- Low-trust or inconsistent nodes ⟶ attenuated messages.
- The GNN progressively **filters out unreliable contributors**.

"Trust acts as an adaptive volume control on each node's voice in the graph."

STEP 4 – END-TO-END VERTICAL IDS PIPELINE

- Edge ⟶ Fog: local data collection + lightweight anomaly metrics
- Fog ⟶ Cloud: transmit summary vectors $\phi_i(t)$
- Compute node utilities u_i + trust/replicator coefficients r_i
- Construct a trust-weighted graph for GNN reasoning
- Run GNN inference ⟶ fuse alerts across layers
- Output global intrusion decisions with confidence scores

EXPERIMENTAL EVALUATION: GOALS & METHODOLOGY

Assess robustness of the Vertical IDS under

- noisy environments
- compromised Fog nodes
- coordinated / stealthy attacks

Validate trust dynamics

- Does the evolutionary game penalize malicious nodes?
- Does the trust-weighted GNN reduce their influence?

Compare against baselines

- Flat IDS
- Horizontal-only GNN
- GNN without trust adaptation

SIMULATING ADVERSARIAL BEHAVIOUR IN IOT FOG NETWORKS

Scenario 1 – Low-level corruption: 10% of Fog nodes generate **systematic false alerts**.

Scenario 2 – Mixed malicious activity: 20% of nodes behave **maliciously** and inject **random noise** into their reports.

Scenario 3 – Coordinated adversaries: A group of Fog nodes cooperates to **mimic legitimate patterns** while pushing false information.

Goal: Stress-test the **trust mechanism** under realistic and stealthy adversarial conditions.

DATASET AND SIMULATION PARAMETERS

Dataset: UNSW-NB15 (2.5M records, 9 attack categories).

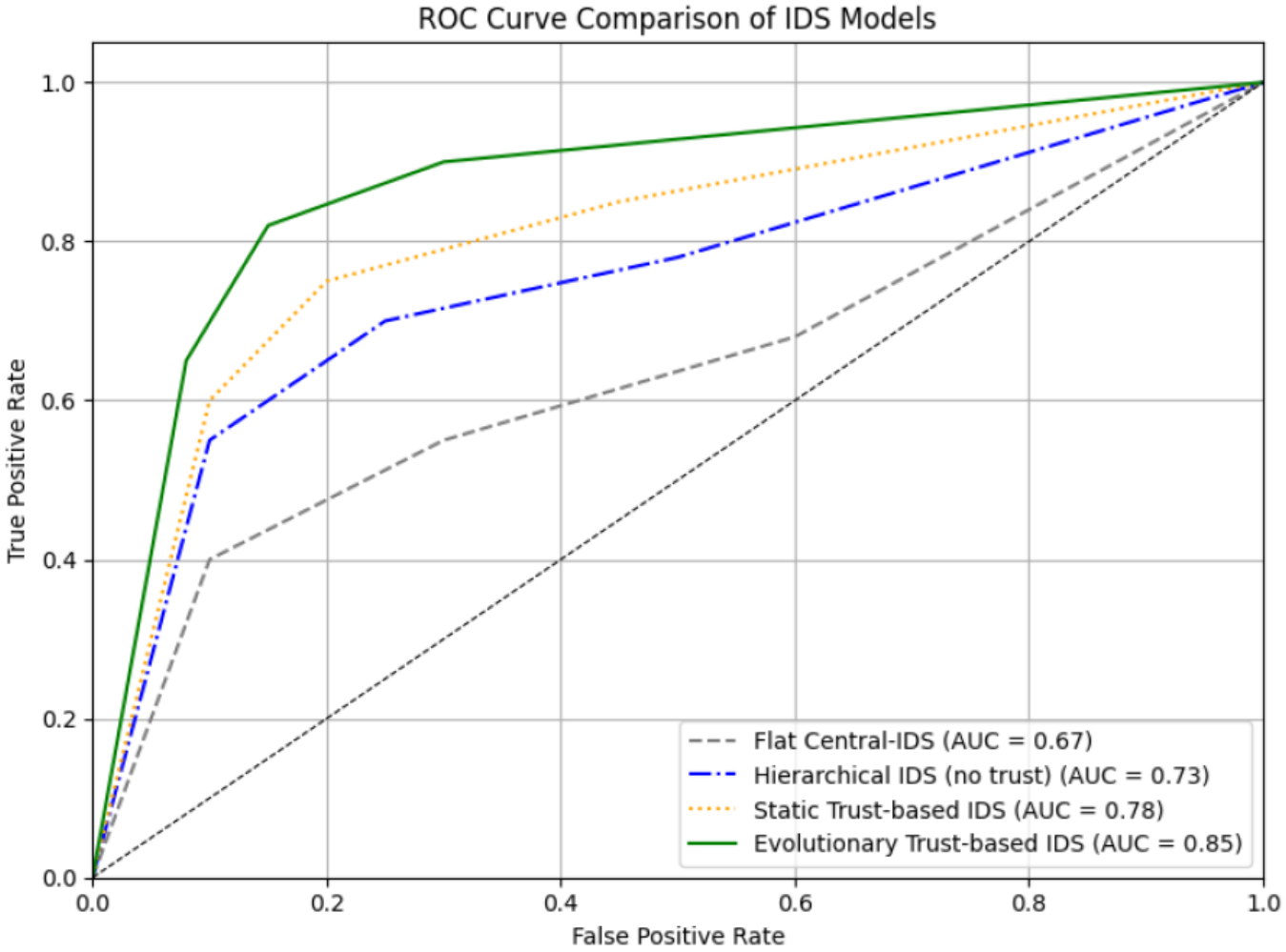
IoT environment: 3-tier **Edge** → **Fog** → **Cloud** topology.

Implementation: PyTorch + PyTorch-Geometric, **50 epochs**, Adam optimizer.

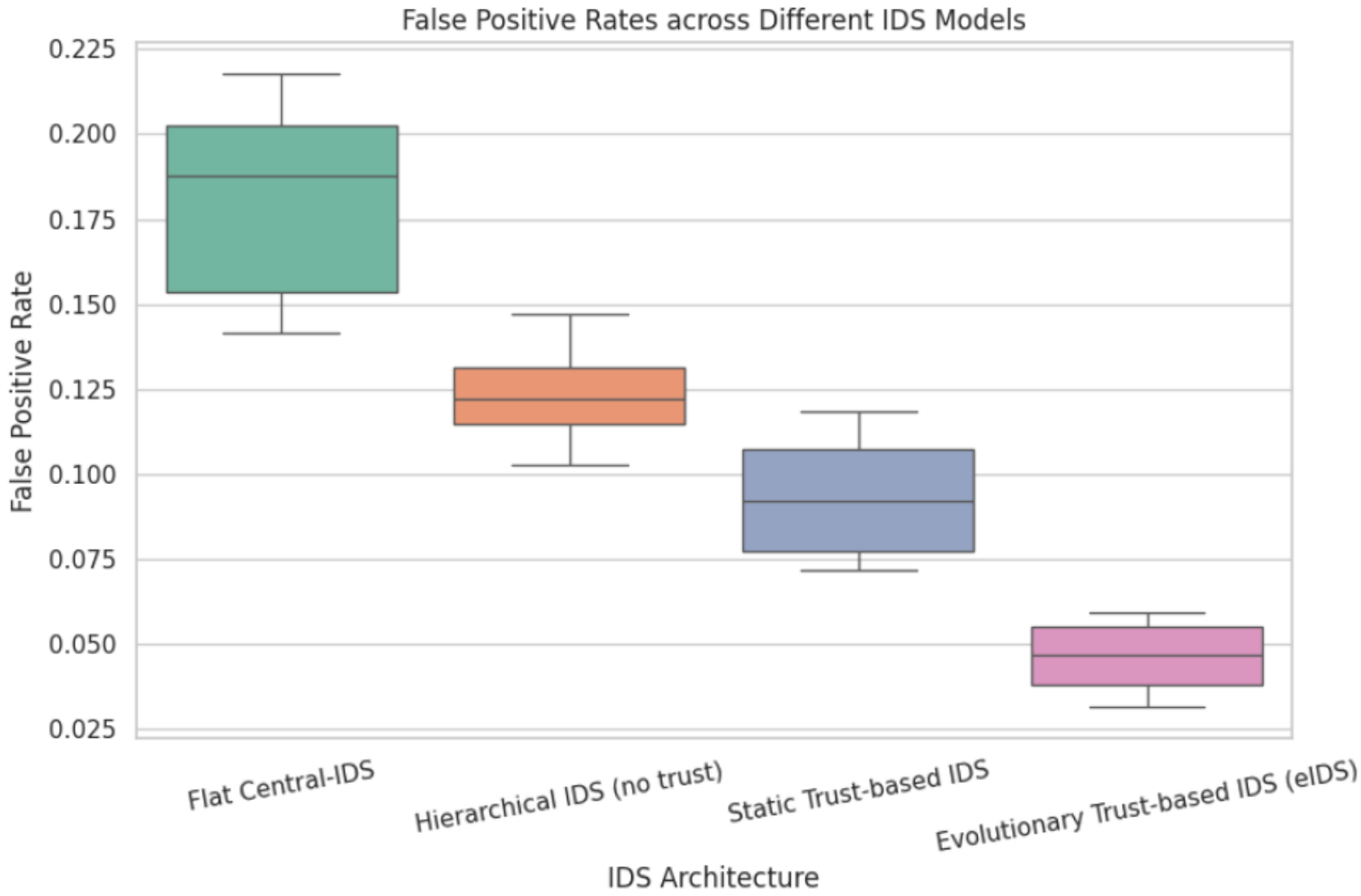
Evaluation focus: accuracy **and** resilience under adversarial stress.

Results (ROC and AUC)

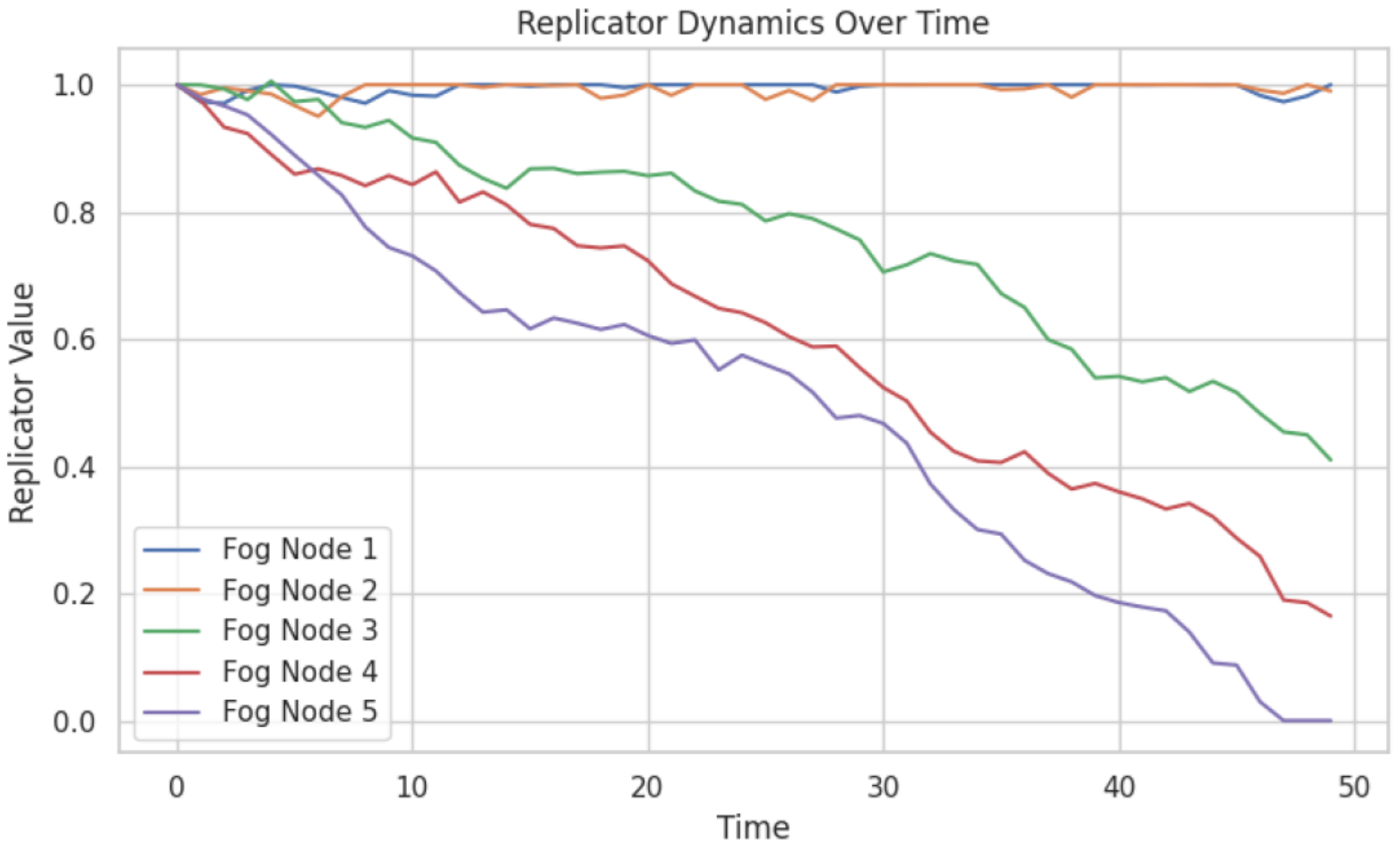
Global Detection Performance



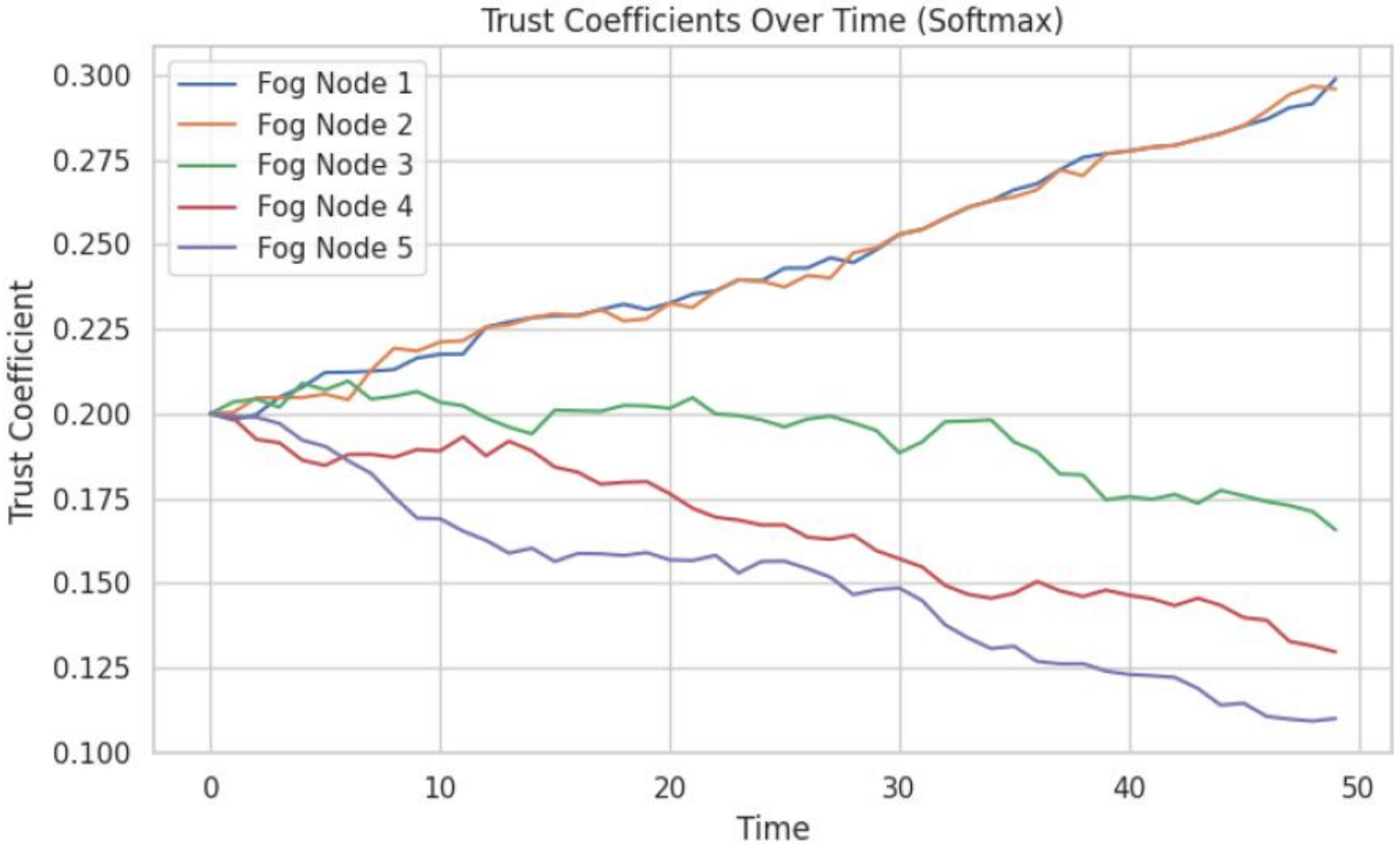
REDUCING FALSE ALARMS THROUGH ADAPTIVE TRUST



HOW TRUST EMERGES OVER TIME



TRUST CONVERGENCE ACROSS FOG NODES



Conclusion and future work

Toward Adaptive & Trust-Aware IDS for IoT

V-IDS provides **multi-layer intrusion detection** with **evolving trust**.

Combining **GNN + Evolutionary Games** improves **robustness** under adversarial drift.

Next steps: Edge–Fog–Cloud deployment, scalability experiments, federated trust learning.

Thank You! Questions?

MYRIA.BOUHADDI@UQO.CA