2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

A Group Formation Game for Local Anomaly Detection

Zixin Ye, Tansu Alpcan, Christopher Leckie

Abstract— This paper studies strategic group formation for local anomaly detection with potential applications to Cognitive Radio Networks (CRN) and the Internet-of-Things (IoT). The problem comprises multiple local anomaly detection tasks which use machine learning (ML) models and partial data. We consider a two-layer network structure with anomaly detectors in the lower layer acting as local anomaly detectors and central nodes at the upper layer as data aggregators, which train the ML models used by local anomaly detectors. The problem is addressed using a strategic (non-cooperative) game formulation, where all central nodes and detectors are players. The players interactively learn one or multiple optimal machine learning models for their dynamically identified local anomaly detection problems. The game is next formulated as a successive optimization problem and solved using the player's best responses to compute a Nash equilibrium. Under mild conditions, we prove that this group formation game is also an exact potential game. Experimental results are consistent with theoretical ones and show fast convergence to the solution.

I. INTRODUCTION

Multi-agent Cyber-Physical networks have become increasingly pervasive with well-known applications in Cognitive Radio Networks (CRN) [1] and the Internet of Things (IoT). The nodes of such networks usually have high-performance storage/computing units acting as independent decision-makers. Moreover, the network structure is often hierarchical, with multiple central nodes as aggregators and numerous network users/devices as operators. A CRN consists of software-defined-radio devices (mobile phones, autonomous vehicles) supported by multiple central nodes (base stations, cloud centers). Instead of being passively controlled, all devices proactively acquire services from the central nodes according to their preferences. However, the behaviors of independent decision-makers have made anomaly detection more challenging in the cyber-physical network. On the one hand, agents are usually reluctant to share local information with others due to privacy concerns. On the other hand, each agent's anomaly detection problem may not be identical, e.g., it may have its local definition of normal data and anomalies depending on the ambient environment. Therefore, rather than handling one unified anomaly detection problem, solutions for a set of Local Anomaly Detection (LAD) tasks are more relevant yet demanding in multi-agent cyber-physical networks.

Numerous works tackle LAD problems in multiple disciplines. [2], [3] formulated the LAD as Contextual Anomaly Detection in an IoT network. [4], [5] modeled LAD as Correlated Anomaly Detection, which is defined by a set of local anomaly detection problems embedded with a correlation graph. However, most previous works establish their solutions under a collective and collaborative framework, e.g., either anomaly detectors are instructed by a central controller or collaborate with others. Moreover, domain knowledge or the environment's meta-information is usually assumed, e.g., spatial-temporal information. We argue that those conditions may not be satisfied in a multi-agent system because 1) multiple service providers (central nodes) exist in the network to deliver private service; 2) anomaly detectors are independent, whose decisions are made for their interests; 3) meta-information of either data or detectors may not be easily shared due to data privacy. Therefore, a game-theoretic approach is more suitable for addressing the LAD problems. Note that these LAD problems are not a priori known to the anomaly detectors or central nodes.

Our game is designed in a simple two-layer network as a bipartite graph. The game takes central nodes and anomaly detectors as players, which concurrently learn multiple machine learning (auto-encoder) models for all the LAD problems they jointly identify. Unlike many previous game-theoretic methods, our game 1) only models the training stage where no attackers or anomalies exist; 2) is non-cooperative, with information-sharing only between the anomaly detectors and central nodes. Each central node learns an ML model with data from all connected detectors, forming a local training group. Then, each detector optimizes its connection strategy toward central nodes by combining the best model for its LAD problem. The game evolves with the player's best response dynamics, which entail model training and optimal group formation.

This paper aims to fill a research gap in addressing local anomaly detection problems in multi-agent networks. Based on a review of the most recent and relevant work presented in Section II, the main contributions of this paper are:

- a novel non-cooperative connection/group formation game that supports a distributed learning scheme to identify and solve all LAD problems at once;
- the proposed distributed learning scheme does not

This work was supported in part by the Australian Research Council Linkage Project under the grant LP190101287 and Northrop Grumman Mission Systems' University Research Program.

Z. Ye and T. Alpcan are with Department of Electrical Engineering and C. Leckie is with the School of Computing and Information Systems, University of Melbourne, Parkville, Australia zixin4@student.unimelb.edu.au

rely on any meta-information of anomaly detectors and domain knowledge of their environments;
- the best response dynamics of our proposed game are solved through iterative optimization;
- under a mild condition, the game is shown to be an exact potential game.

II. RELATED WORK

Anomaly detection [6] identifies anomalies outside of normal/expected behaviors. However, the definition of anomalies can be either global or local. For example, a person driving at 100km/h on the highway can be considered normal but anomalous in the residential area, and vice versa for him/her driving at 50km/h. Driving at 800km/h can be undoubtedly globally anomalous in most circumstances. As a result, local anomaly detection becomes necessary to tackle local anomalies, containing multiple definitions of anomalies and normal data conditioned on some meta-information of the anomaly detectors. Contextual anomaly detection shares a significant intersection with the LAD, where meta-information from either network activities or agents is learned along with the anomaly estimators. [2], [3] applied feature engineering and data mining towards contextual information, e.g., learnable feature matrices or parameters of a joint distribution. Another method of modeling the LAD problem to estimate the correlation of the local problems, work in [5] analyzed the correlation against the geo-location and time of normal patterns. While [4] proposed a model-free method to solve multiple LAD problems at once based on estimating a local-problem similarity graph. [7], [8] proposed a collaborative learning framework that captivates local anomaly features into the central model. [9], [10] integrated privacy-preserving methods by only exchanging model parameters between learners. Our game-theoretic framework is similar to the work in [11]. However, assumptions of a mesh network structure and the coalition of players are assumed in these works. In particular, [12] applied a split-and-merge strategy for users to search for their best learning partners as a group, while again, it is based on a coalition formation game aiming for one central problem.

III. Problem Definition

We define a set of local anomaly detection problems on a multi-agent cyber-physical network consisting of multiple anomaly detectors and central nodes. Each anomaly detector faces a local anomaly detection problem, whose definition of anomalies depends on what is normal in its local environment. Each central node holds a deep-learning model trained for anomaly detection tasks. All detectors choose to connect one or multiple central nodes to use their deep-learning models for local anomaly detection tasks. In return, they must share their local data with the connected central nodes for their models' training dataset. All anomaly detectors and central nodes are independent agents/entities not affiliated with each other and only aim to maximize their own utilities. Central nodes facilitate information sharing between anomaly detectors, which do not have direct connections to each other.

TABLE I: Mathematical Notation

A_i, A^j	j^{th} column, i^{th} row of A
$\mathbb{Z}, \mathbb{R}$	space of integers, real numbers
$\mathbf{w} \in \mathbb{R}^n$	a n-dimension vector
Δ^m	M-dimensional Simplex
$\lvert \cdot \rvert$	size of a vector/matrix/set
$\mathcal{V} := \{v_1, \cdots, v_N\}$	set of anomaly detectors
$\mathcal{C} := \{c_1, \cdots, c_M\}$	set of central nodes
$\mathcal{A} \subset \mathbb{R}^{N \times M}$	set of valid connection matrices
$A \in \mathcal{A}$	connection matrix
$W \in \mathcal{W}$	set of machine learning parameters of $\mathcal{C}$
$\mathbf{w}_{c_k} = W_k$	machine learning parameters at $c_k \in \mathcal{C}$
$f_{c_k}(\cdot; \mathbf{w}_{ck})$	machine learning model at $c_k \in \mathcal{C}$
$U_{v_i} : \mathcal{A} \to \mathbb{R}$	utility function of $v_i \in \mathcal{V}$
$U_{c_k} : \mathcal{W} \to \mathbb{R}$	utility function of $c_k \in \mathcal{C}$

Problem 1: Based on the network learning model and the assumptions above, to which central nodes should the anomaly detectors (devices) connect? In other words, what is the best way for them to share their data and select central ML models to solve their local anomaly detection tasks?

IV. Local Anomaly Detection on a Network

This section presents the network and local anomaly detection models and relevant notation.

A. Two-layer Network Structure

Our communication network structure is formulated as a bipartite graph $\{\mathcal{V}, \mathcal{C}, \mathcal{A}\}$, where $\mathcal{V} := \{v_1, \cdots, v_N\}$ represents the set of anomaly detectors, $\mathcal{C} := \{c_1, \cdots, c_M\}$ represents the set of central nodes, and $\mathcal{A} := \{A \in \mathbb{R}^{N \times M} | A_i \in \Delta^M, \forall i = 1, \cdots, N\}$ represents the connection (communication link) matrix from $\mathcal{V}$ to $\mathcal{C}$. A valid matrix $A \in \mathcal{A}$ is a row-wise stochastic matrix whose (i, j) entry represents the communication probability/frequency between v_i and c_j. If $\mathcal{A}$ is assumed to be in an integer space, it implies every anomaly detector exclusively connects to a central node and implements its ML model. We argue that such an integer connection is equivalent to a group formation, where anomaly detectors connected to the same central node serve as a group and share one central service.

B. Distributed Anomaly Detection

As an anomaly detector v_i connecting to the central node c_i, it agrees to share its local data as part of the c_i's ML model training. However, anomaly detectors are usually constrained with limited resource capacity to implement a large-scale ML training task. Therefore, training the ML models at the central nodes with powerful computing and storage resources has become a convincing scenario, e.g., virtual private cloud (VPC) in IoT or Radio Resource Unit (RRU) in CRN. Accordingly,

anomaly detectors deploy the trained ML models from the connected central nodes for their local anomaly detection. Such a machine learning scheme has been widely adopted in many real-world edge computing tasks supported by cloud services. In our paper, independent agents with imperfect information implement this distributed anomaly detection.

1) Locally Observed Data: we denote the locally observed dataset of v_i as $D_{v_i} \in \mathbb{R}^{n_i \times d}$, where n_i represents the number of data points in D_{v_i} and d is the number of features of the data. Similarly, we denote a data point in D_{v_i} as $\mathbf{x} \in \mathbb{R}^d$. The dataset D_{v_i} represents all data observed by v_i, e.g., each anomaly detector has a limited ownership or detection range of all network patterns. We denote $D := \cup_{v_i \in \mathcal{V}} D_{vi}$ as aggregate data from all local datasets, the total number of which is n if the local data of any two random anomaly detectors have no overlaps, then $n = \sum_{i=1}^{N} n_i$.

2) Anomaly Detection Model Training Using Auto-encoders: This paper uses the auto-encoder structure as the ML model to detect local anomalies. The auto-encoder structure is a deep learning structure compatible with a semi-supervised learning task. The structure aims to minimize the distance between the input data and its output, i.e., reconstruction error. In the inference stage, the distance (reconstruction loss) is expected to be much more significant for anomalies. We denote the auto-encoder held at c_k as $f_{c_k}(\cdot, \mathbf{w}_{c_k})$, where the function f_{c_k} is concatenated by two deep neural networks: an encoder $E : \mathbb{R}^d \to \mathbb{R}^l$ and a decoder $E : \mathbb{R}^l \to \mathbb{R}^d$. Consequently, $f_{c_k}(\mathbf{x}; \mathbf{w}_{c_k}) = (E \circ D)(\mathbf{x}; \mathbf{w}_{c_k})$, where $(E \circ D) : \mathbb{R}^d \to \mathbb{R}^d$ is the symbol of composite function, $\mathbf{x} \in \mathbb{R}^d$ is the input data and $\mathbf{w}_{c_k}$ is the model's parameters.

3) Anomaly Estimation Using Auto-encoders: in the estimation stage, each anomaly detector selects the auto-encoders from the connected central nodes to score its local data as a potential anomaly. We first denote the anomaly-scoring function of a local anomaly detector v_i as $f_{v_i} : \mathbb{R}^d \to \mathbb{R}^d$. We choose this function to be a linear mixture (ensemble) model from all central models weighted by A_i:

$$f_{v_i}(\mathbf{x}, A_i) = \sum_{k=1}^{M} A_i^k \cdot f_{c_k}(\mathbf{x}; \mathbf{w}_{c_k}). \tag{1}$$

This anomaly-scoring function combines the auto-encoder scores from all connected central nodes by v_i's connection vector A_i. To determine if a data point $\mathbf{x} \in D_{v_i}$ is an anomaly, a threshold-based method is used based on the sum of squared errors between $\mathbf{x}$ and $f_{v_i}(\mathbf{x}, A_i)$. Under a threshold $\epsilon_{v_i} \in \mathbb{R}$, any data $\mathbf{x} \in D_{v_i}$ will be counted as the anomaly if $||f_{v_i}(\mathbf{x}, A_i) - \mathbf{x}||_2^2 \geq \epsilon_{v_i}$. In our work, ϵ_{v_i} is determined by the 50 percentile of the Euclidean error of all local data, denoted by the percentile function q for each v_i as:

$$\epsilon_{v_i} = q(\{||f_{v_i}(\mathbf{x}, A_i) - \mathbf{x}||_2^2 | \mathbf{x} \in D_{v_i}\}, 0.5). \tag{2}$$

C. Summary of Model's Assumptions

For convenience, we formally summarize all assumptions of our network learning model mentioned above: (A1) to make all possible group formations achievable, the hypothetical number of aggregators, M, should be no less than the number of detectors, N, i.e., $M \geq N$; (A2) all central nodes are reachable and exclusive for anomaly detectors, i.e., $A \in \mathbb{Z}^{N \times M}, \forall A \in \mathcal{A}$; (A3) local datasets are disjoint, i.e., $D_{v_i} \cap D_{v_j} = , \forall i \neq j$; (A4) LAD is formulated as a semi-supervised learning task;

V. Game-theoretic Framework

We propose a non-cooperative game for the network learning process for several realistic reasons. First, anomaly detectors solving LAD problems are selfish: they only aim to maximize local performance with potential privacy concerns. Second, central nodes may belong to different service entities with competitive relationships and no information-sharing contract. Even if they belong to the same entity, central nodes' cooperation can be very expensive, e.g., synchronization of database replicas and real-time communication across two regions. Third, the game does not require domain knowledge of the network environment, e.g., no meta-information (domain knowledge) is required from observed data points and anomaly detectors, e.g., temporal-spatial information of the anomaly detectors and how data points are generated.

A. Game Definition

Our game is played at the training time and is defined as a tuple:

$$\mathcal{G} = \{\{\mathcal{V}, \mathcal{C}\}, \{\mathcal{A}, \mathcal{W}\}, \mathcal{U}\}. \tag{3}$$

The set of players is the union of anomaly detectors $\mathcal{V}$ and central nodes $\mathcal{C}$.The connection matrix $A \in \mathcal{A}$ is a strategy profile of all anomaly detectors $\mathcal{V}$. The set of auto-encoders parameters $W \in \mathcal{W}$ is a strategy profile of all central nodes. For any strategy profile (A, W), where $A \in \mathcal{A}$ and $W \in \mathcal{W}$, A_i is the connection strategy of v_i while $W_k = \mathbf{w}_{c_k}$ denotes the learning parameters of the auto-encoder owned by c_k. Lastly, $\mathcal{U}$ denotes the set of utility functions for both anomaly detectors U_{v_i} and central nodes U_{c_k}. For convenience, we also denote the strategy profile against a player v_i with the notation $-v_i$, e.g., A_{-i}, U_{-v_i}.

B. Utility Functions

1) Utilities of Anomaly Detector Players: The utility function of v_i is simply the sum-of-squared errors between the input data and its estimated output:

$$U_{v_i}(A_i, W, D_{v_i}) = \sum_{\mathbf{x} \in D_{v_i}} || \sum_{k=1}^{M} A_i^k \cdot f_{c_k}(\mathbf{x}; \mathbf{w}_{c_k}) - \mathbf{x}||_2^2. \tag{4}$$

2) Utilities of Central Node Players: Based on the learning network model, each central node c_k trains its own auto-encoder $f_{c_k}(\cdot; \mathbf{w}_{c_k})$ with local data shared by all connected anomaly detectors. The utility function of c_k is the training loss function conditioned on the current connection (data-querying) strategy (A).

$$U_{c_k}(\mathbf{w}_{c_k}, A, D) = \sum_{v_i \in \mathcal{V}} \sum_{\mathbf{x} \in D_{v_i}} ||A_i^k (f_{c_k}(\mathbf{x}; \mathbf{w}_{c_k}) - \mathbf{x})||_2^2. \tag{5}$$

Even without the integer constraint on $\mathcal{A}$, the ensemble estimation function and both utility functions are still valid for continuous action space, e.g., f_{v_i} becomes an ensemble model from all f_{c_k} weighted by a connection probability A_i^k.

C. Best Response Dynamics

1) Cost Minimization by Players: for each player v_i, the local problem of minimizing its utility is

$$u^*_{v_i,W} = \min_{A_i \in \mathbb{Z}^M} U_{v_i}(A_i, W, D_{v_i}) \text{ s.t. } A_i \in \mathcal{A} \tag{6}$$

where $u^*_{v_i,W}$ is the optimal value acquired by v_i conditioned on $W \in \mathcal{W}$. Notice that $u^*_{v_i,W}$ is attainable if $||\mathbf{w}_{c_k}||_2^2 \leq \infty$ since (4) is convex on $A \in \mathcal{A}$. With the integer constraint on the actions, solving (6) becomes as easy as finding c_k that minimizes the local losses, i.e., an argmin process.

2) Training Loss Minimization by Central Nodes: in the training process, central nodes minimize their training loss by gradient descent algorithms. We have

$$l^*_{c_k,A} = \min_{\mathbf{w}_{c_k} \in \mathbb{R}^{|W_k|}} U_{c_k}(\mathbf{w}_{c_k}, A, D) \tag{7}$$

where $l^*_{c_k,A}$ is the optimal value attained by c_k conditioned on $A \in \mathcal{A}$. We assume (7) is differentiable but non-convex, whose local optima can be acquired by the gradient-descent algorithms. The best response dynamics show that finding the optimal solutions for either (6) and (7) depends on the other problem's optimal solution. However, the non-convexity of (7) makes the global optima acquirement non-trivial.

D. Network Training Algorithms

Based on the best responses (6) and (7), a distributed algorithm is proposed to solve our game. It is distributed since all players search for their best responses by solving a local optimization problem. The interaction ends with successive optimizations between the network's lower (Algorithm 1) and upper (Algorithm 2) layers.

Using Algorithm 1, each anomaly detector concurrently updates the best response by finding the central node minimizing its local losses in Algorithm 1, e.g., $\arg\min_{A_i} U_{v_i}(A_i, W, D_{v_i})$.

For central nodes, their auto-encoders concurrently update the model parameters with available training data and a gradient-descent solver, e.g., ADAM. The operations iterate between Algorithm 1 and all models' training updates, while a stopping condition needs to be defined to terminate the iteration. Since all algorithms run at the player level, it does not have a central framework, and players in the same layer update their actions in parallel, which brings a favorable run time in a large-scale network.

Algorithm 1: Best Connection Search for v_i

Input: Network Parameters $\mathcal{C}, W, D_{v_i}, \{f_{c_k}\}_{c_k \in \mathcal{C}}$
Output: Connection Strategy A_i
Update $\{\mathbf{w}_{c_k}, f_{c_k}\}_{c_k \in \mathcal{C}}$
function $\arg\min_{A_i}(\mathcal{C},\ W,\ D_{v_i},\ \{f_{c_k}\}_{c_k \in \mathcal{C}})$
  Step 1: Return the A_i that minimize (6)
  Step 2: Update central node connection by A_i

VI. Theoretical Analysis

This section studies several properties of the game $\mathcal{G}$ (3) and its best response dynamics. We first prove $\mathcal{G}$ is an exact potential game, then we show the sufficient condition of attaining the global optimum of its potential function.

A. Exact Potential Game

We start with the following definition.

Definition 6.1 (Exact Potential Game): The game $\mathcal{G}$ defined in Section V-A by (3) is an exact potential game, if there is a potential function $\Phi_D : \mathcal{A} \times \mathcal{W} \rightarrow \mathbb{R}$ such that i) for each Player $v_i \in \mathcal{V}$, $\forall A_{-i} \in \mathcal{A}_{-i}, W \in \mathcal{W}, \forall A_i^{'}, A_i^{''} \in \mathcal{A}_i$, $\Phi_D(A_i^{'}, A_{-i}, W) - \Phi_D(A_i^{''}, A_{-i}, W) = U_{v_i}(A_i^{'}, W, D_{v_i}) - U_{v_i}(A_i^{''}, W, D_{v_i})$; ii) for each Player $c_k \in \mathcal{C}$, $\forall \mathbf{w}_{-c_k} \in \mathcal{W}_{-k}, A \in \mathcal{A}, \forall \mathbf{w}_{c_k}^{'}, \mathbf{w}_{c_k}^{''} \in \mathcal{W}_k$, $\Phi_D(\mathbf{w}_{c_k}^{'}, \mathbf{w}_{-c_k}, A) - \Phi_D(\mathbf{w}_{c_k}^{''}, \mathbf{w}_{-c_k}, A) = U_{c_k}(\mathbf{w}_{c_k}^{'}, A, D) - U_{c_k}(\mathbf{w}_{c_k}^{''}, A, D)$.

Based on this definition of the exact potential game, we state that

$$\Phi(A, W; D) = \sum_{v_i \in \mathcal{V}} \sum_{\mathbf{x} \in D_{v_i}} ||\sum_{k=1}^{M} A_i^k \cdot f_{c_k}(\mathbf{x}; \mathbf{w}_{c_k}) - \mathbf{x}||_2^2. \tag{8}$$

The exact potential function measures the total sum-of-squared losses of local estimation from all anomaly detectors in $\mathcal{G}$.

Theorem 1 (Exact Potential Game): The game $\mathcal{G}$ (3) is an exact potential game if $\mathcal{A} \subseteq \mathbb{Z}^{N \times M}$, i.e. if the connection matrices have only integer entries.

Proof: We omit the proof due to the space limitations. ■

Theorem 2 (Convergence): The best response dynamic of the game $\mathcal{G}$ (3) converges to a Nash Equilibrium if the perfect solver exists for (6) and (7).

We omit the proof here since it has been proved as the Theorem 1 of [13]. Furthermore, [14] shows that every pure Nash Equilibrium of an exact potential game is equivalent to a local optimum of the potential function. Theorem 2 assumes an ideal situation as the assumption

of "perfect solvers" does not exist, particularly for solving (7).

B. Connection to Collaborative Learning

The exact potential function (8) is the sum of the estimation loss of the local training data from all anomaly detectors. Therefore, the game $\mathcal{G}$ also offers us a central problem formulation, where all players collaborate together to minimize the sum of their local estimation loss. Firstly, this section will formulate this central optimization problem in (9) with all players' actions as the decision variables. Secondly, this section will also show sufficient conditions to attain the global optimum of this central optimization problem by the non-cooperative best-response dynamics.

$$\Phi^* = \min_{A \in \mathbb{Z}^{N\times M}, W} \quad \Phi(A, W; D), \tag{9a}$$

$$\text{s.t.} \quad A_i \in \Delta^M, i = 1, \cdots, N, \tag{9b}$$

C. Global Optimum Attainment Without Collaboration

This section discusses the sufficient conditions of acquiring the global optimum in (9) from the best response dynamics of $\mathcal{G}(3)$. We start with the definition of the global optimum of the central optimization problem and assuming we have a way to find them.

Definition 6.2 (Optimal Solutions of the Global Problem): An optimal solution of (9) is defined as $A^* \in \mathcal{A}, W^* \in \mathcal{W}$ where $W_k^* = \mathbf{w}_{c_k}^*, k = 1, \cdots, M$.

Assumption 2.1 (Perfect Central Solver): We assume there exists a perfect solver for (9) which acquires the optimal solution (A^*, W^*).

Next, we define two primal decomposition forms of our central problem (9), similar to the definition of dual decomposition in Section 2.2. of [15].

Definition 6.3 (Primal Decomposition): The central problem (9) has a primal decomposition by $\mathcal{V}$ if $\exists \phi_{v_i}(A_i)$ such that $\Phi(A, W; D) = \sum_{v_i \in \mathcal{V}} \phi_{v_i}(A_i)$. In addition, the central problem (9) has a primal decomposition by $\mathcal{C}$ if $\exists \phi_{c_k}(W_k)$ such that $\Phi(A, W; D) = \sum_{c_k \in \mathcal{C}} \phi_{c_k}(W_k)$.

1) Primal Decomposition by Anomaly Detectors:

Theorem 3: For each v_i, 1) its utility function (6) is a primal decomposition component of the potential function (9a) and A_i^* is its best response conditioned on W^*; 2) if $A_i^{'}$ is its best response conditioned on W^*, then $(A^{'}, W^*)$ is also optimal for (9).

2) Primal Decomposition by Central Nodes:

Theorem 4: For each c_k, 1) its utility function (7) is a primal decomposition component of the potential function (9a) and W_k^* is its best response conditioned on A^*; 2) if $W_i^{'}$ is an optimal solution of (7) conditioned on A^*, then $(A^*, W^{'})$ is also optimal for (9).

Theorem 3 shows that having an optimal W^* of collaborative optimization (9) is a sufficient condition of acquiring an optimal A^* of (9) by the best response dynamics of $\mathcal{G}$, and vice versa in Theorem 4. However, finding an optimal W^* or A^* as the precondition (initial condition) of the best response dynamics can be difficult. Therefore, attaining the global optimum of the central problem is not generally guaranteed by the best response dynamics with a random initial condition. Nevertheless, we will show in the simulation section that the best response dynamics empirically return a near-optimal outcome of the collaborative optimization problem.

VII. Simulations

A. Simulation Setup

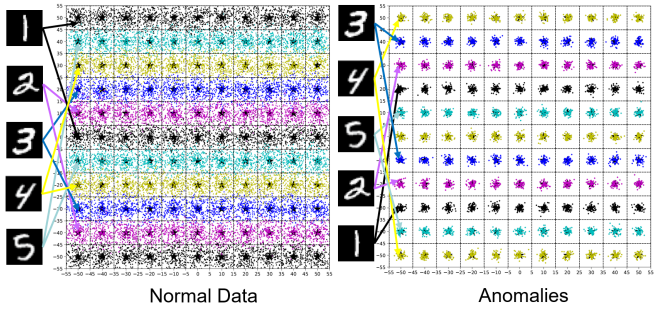
1) Distributed MNIST Data Generation: in this paper, we use our synthetic data generator to create MNIST data points in a 2-dimensional space. This is due to lack of equivalent wireless network datasets. As shown in Figure 1 (a), the generator randomly creates color-coded data points based on a Gaussian-mixture Model (GMM). Anomaly detectors are located in different areas with a limited detection range (dash-line grid). All data points falling into an anomaly detector's (v_i) detection range forms its local data D_{v_i}. We assign each data point with a random MNIST figure whose color represents an MNIST digit. For example, black data are only drawn from the MNIST figures with digit one.

2) Defining Normal Data and Anomalies: We utilize the data point's color to specify locally normal data and anomalies for each anomaly detector v_i. As shown at the left-hand side Figure 1 (a), locally normal data of v_i is defined as all digits observed in its detection range. Similarly, the local anomalies of v_i are digits that never emerge. For instance, the anomaly detector at the bottom-left corner observes 2 (purple) and 1 (black) as its locally normal data. Therefore, any MNIST data with digits 3, 4, and 5 will be counted as anomalies, e.g., on the right-hand side of Figure 1 (a).

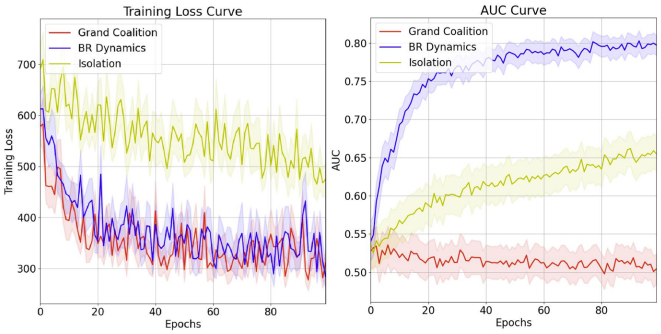
B. Simulation Results

In Figure 1 (b), the simulation of the best response dynamics is compared with two other learning schemes: 1) all anomaly detectors learning as a grand coalition (red) and learning their local problems independently (yellow).

1) Training Loss: The average training loss of the overall central node's model is shown on the left-hand side, consistently decreasing on average. Due to the semi-supervised learning framework, learning in a grand coalition has a training loss as small as that of the best dynamics responses. This is because the grand coalition learning creates a global anomaly detection model which takes all locally normal data as its training data, i.e., one auto-encoder minimizes the self-mapping SSE of all network data. Nevertheless, the training-loss curve reflects a decent loss-minimization outcome from the best response dynamics, similar to the grand coalition.



(a)



(b)

Fig. 1: (a) shows 121 anomaly detectors (stars) with their detection range in dash lines are presented. Note that the detectors do not know their location and how MNIST digit classes are distributed in the matrix. 5-digit classes of the MNIST data are used to generate locally normal data (left) and anomalies (right) based on a GMM; (b) shows the simulation results from our game-theoretic learning process (blue). The left figure shows the training loss, and the right shows the AUC values over 100 epochs. A comparison of isolated (yellow) methods and grand-coalition learning (red) is also presented.

2) AUC Curve: The testing dataset contains locally normal data and local anomalies for each anomaly detector. The testing curve is generated on the right-hand side with the average AUC values computed from all anomaly detectors in every training epoch. The AUC curve reflects the average anomaly-detection performance of each detector on its local data. Since the anomaly data is chosen from the same digits (1,2,3,4,5) as the normal data and due to lack of prior knowledge, the grand coalition centralized model struggles to identify local anomalies, which causes the AUC to fluctuate around 0.5. In contrast, the average AUC curve from the best response dynamics increases above 0.8 thanks to each anomaly detector's optimal group formation/connection. The isolated learning also induces increasing AUC values, whose rate is significantly lower than the best response dynamics.

VIII. Conclusion

We proposed a novel non-cooperative game of identifying and solving local anomaly detection problems in the multi-agent-cyber-physical network. Using autoencoders as the anomaly detection models, all models can be efficiently trained by the players' best response dynamics to tackle different LAD problems. Each anomaly detector finding the best central nodes to interact with is equivalent to an optimal group formation of learning multiple local models simultaneously. Our game is proved to be an exact potential game in which all players aim to minimize total LAD losses. The best response dynamics also guarantee convergence towards a local optimum of the potential function, which is equivalent to the Nash Equilibrium of the game under ideal conditions. The simulation result reflects essential properties of the best response dynamics, significantly outperforming other benchmark methods.

References

[1] J. Mitola and G. Maguire, "Cognitive radio: making software radios more personal," IEEE Personal Communications, vol. 6, no. 4, pp. 13–18, 1999.

[2] M. A. Hayes and M. A. Capretz, "Contextual anomaly detection framework for big sensor data," Journal of Big Data, vol. 2, p. 2, Feb 2015.

[3] X. Yu, H. Lu, X. Yang, Y. Chen, H. Song, J. Li, and W. Shi, "An adaptive method based on contextual anomaly detection in internet of things through wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 16, no. 5, p. 1550147720920478, 2020.

[4] K. Bai, A. Zhang, Z. Li, R. Heano, C. Wang, and L. Carin, "Collaborative anomaly detection," 2022.

[5] Z. Chen, X. Yu, Y. Ling, B. Song, W. Quan, X. Hu, and E. Yan, "Correlated anomaly detection from large streaming data," in 2018 IEEE International Conference on Big Data (Big Data), pp. 982–992, 2018.

[6] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Comput. Surv., vol. 41, jul 2009.

[7] Y. Mirsky, T. Golomb, and Y. Elovici, "Lightweight collaborative anomaly detection for the iot using blockchain," Journal of Parallel and Distributed Computing, vol. 145, pp. 75–97, 2020.

[8] A. H. Ahmed, M. A. Riegler, S. A. Hicks, and A. Elmokashfi, "Rcad: Real-time collaborative anomaly detection system for mobile broadband networks," in Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, KDD '22, (New York, NY, USA), p. 2682–2691, Association for Computing Machinery, 2022.

[9] M. Katzef, A. C. Cullen, T. Alpcan, C. Leckie, and J. Kopacz, "Privacy-preserving collaborative sdr networks for anomaly detection," in ICC 2021 - IEEE International Conference on Communications, pp. 1–6, 2021.

[10] M. Katzef, A. C. Cullen, T. Alpcan, and C. Leckie, "Generative adversarial networks for anomaly detection on decentralised data," Annual Reviews in Control, vol. 53, pp. 329–337, 2022.

[11] S. Liu, T. Li, and Q. Zhu, "Distributed machine learning with strategic network design: A game-theoretic perspective," 2020.

[12] W. Saad, Z. Han, T. Basar, M. Debbah, and A. Hjorungnes, "Coalition formation games for collaborative spectrum sensing," IEEE Transactions on Vehicular Technology, vol. 60, pp. 276–297, jan 2011.

[13] B. Swenson, R. Murray, and S. Kar, "On best-response dynamics in potential games," SIAM Journal on Control and Optimization, vol. 56, no. 4, pp. 2734–2767, 2018.

[14] D. Monderer and L. S. Shapley, "Potential games," Games and Economic Behavior, vol. 14, no. 1, pp. 124–143, 1996.

[15] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein. 2011.