COMPSCI 402 – Artificial Intelligence

Graph Anomaly Detection

Shouju Wang. <sw599@duke.edu>

Overview

Abstract

Introduction

Survey

Discussion

Abstract

- AI Impact & Complexity:
  - Rapid advancements in AI.
  - Impact on human lives.
  - Concerns about privacy and transparency.
- Human-Centered AI (HCAI):
  - Emergence of HCAI.
  - Focus on human-AI interaction.
  - Translating qualitative statements to technical requirements.
- Trustworthy AI Systems:
  - Importance of trustworthiness.
  - Emphasis on data preprocessing and anomaly detection.
- Anomaly Detection:
  - Role in enhancing AI trustworthiness.
  - Classification of current methods.
  - Graph Anomaly Detection & GCNs.

Introduction

AI's Impact on Society

Issues of Bias and Non-Inclusivity

Human-Centered AI (HCAI) and trustworthy AI

The importance of Data anomaly detection

AI, like other significant technological breakthroughs in human history, has had a profound impact on our society.
start from around 1960.

AI's impact

Issues of Bias and Non-Inclusivity

much AI-based technology ignores human-centered aspects and has produced biased and unfair outcomes. These include but are not limited to age, ethics, education, society class, gender, language, culture, emotions, personalities, and many others.

From the perspective of Human-centered AI (HCAI) and trustworthy AI, they focus on the exploration of how contemporary and future AI systems can efficiently interact within a society that comprises both artificial and human agents

Human-Centered AI (HCAI) and trustworthy AI

Relationship between HCAI and trustworthy AI

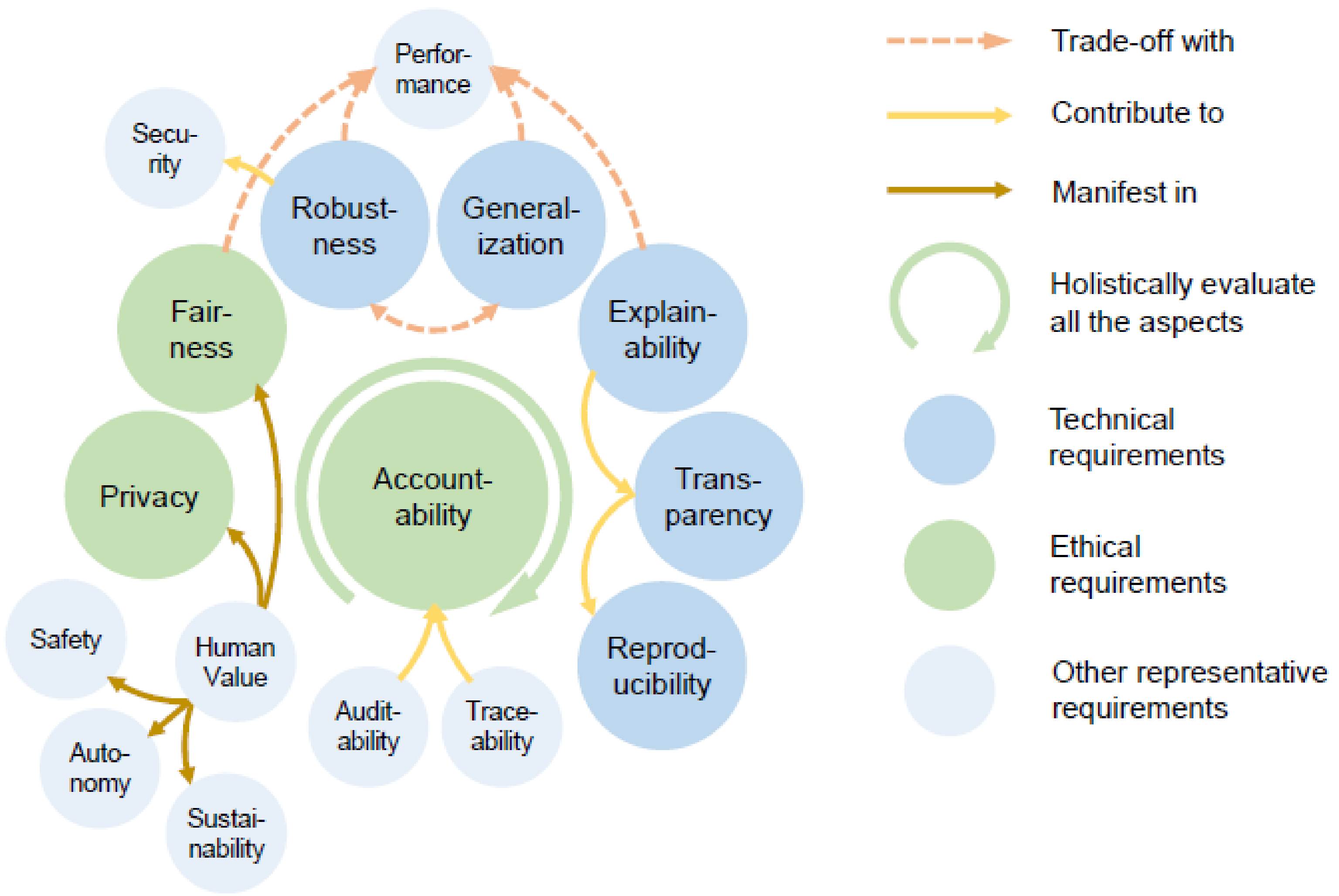
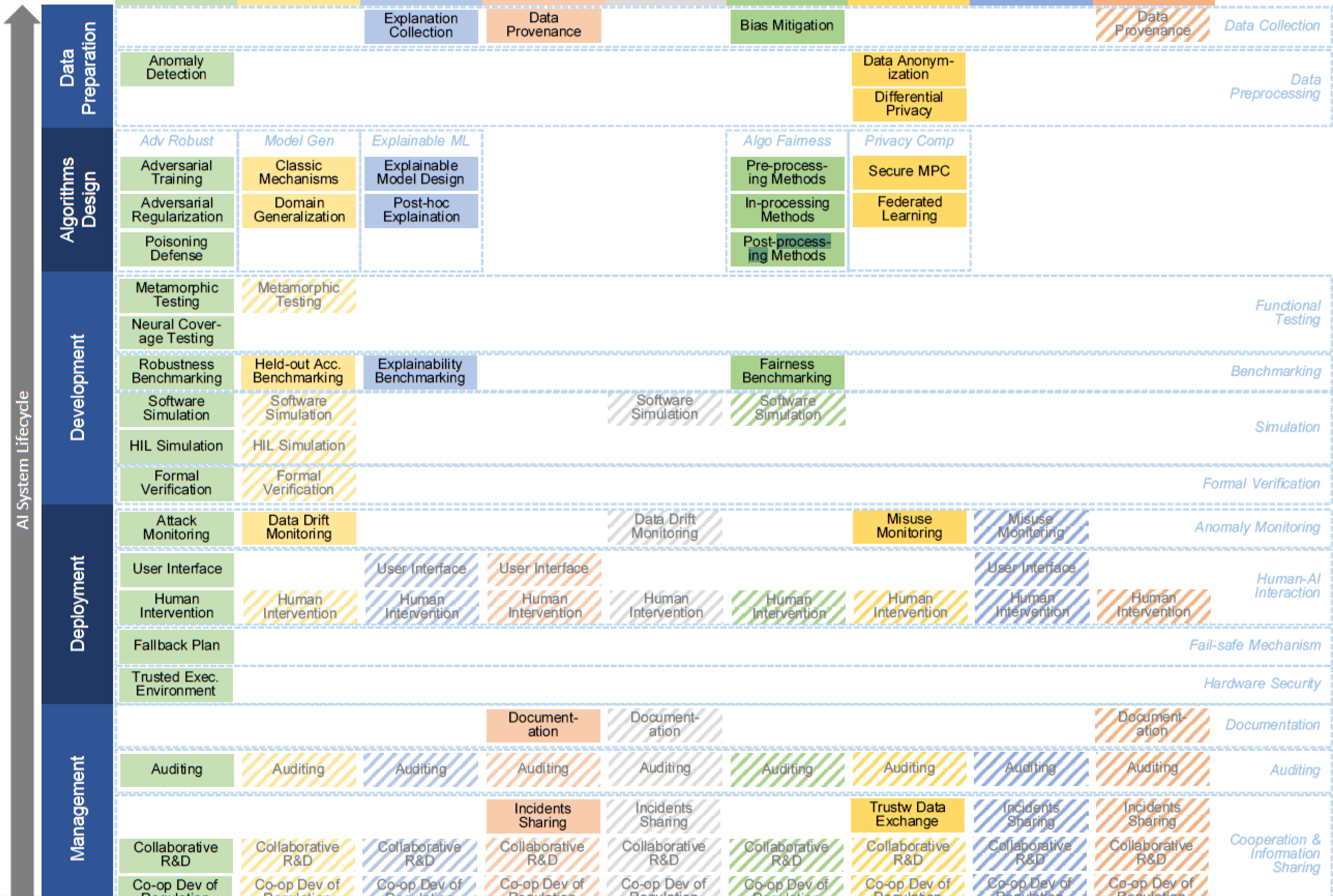


Fig. 1. The relation between different aspects of AI trustworthiness discussed in this survey. Note that implicit interaction widely exists between aspects, and we cover only representative explicit interactions.


AI System Lifecycle
Data Preparation
Algorithms Design
Development
Deployment
Management
Explanation Collection
Data Provenance
Bias Mitigation
Data Provenance
Data Collection
Anomaly Detection
Data Anonym-ization
Differential Privacy
Data Preprocessing
Adv Robust
Model Gen
Explainable ML
Algo Fairness
Privacy Comp
Adversarial Training
Classic Mechanisms
Explainable Model Design
Pre-process-ing Methods
Secure MPC
Adversarial Regularization
Domain Generalization
Post-hoc Explaination
In-processing Methods
Federated Learning
Poisoning Defense
Post-process-ing Methods
Metamorphic Testing
Metamorphic Testing
Neural Cover-age Testing
Functional Testing
Robustness Benchmarking
Held-out Acc. Benchmarking
Explainability Benchmarking
Fairness Benchmarking
Benchmarking
Software Simulation
Software Simulation
Software Simulation
Software Simulation
HIL Simulation
HIL Simulation
Simulation
Formal Verification
Formal Verification
Formal Verification
Attack Monitoring
Data Drift Monitoring
Data Drift Monitoring
Misuse Monitoring
Misuse Monitoring
Anomaly Monitoring
User Interface
User Interface
User Interface
User Interface
Human Intervention
Human Intervention
Human Intervention
Human Intervention
Human Intervention
Human Intervention
Human Intervention
Human Intervention
Human Intervention
Human-AI Interaction
Fallback Plan
Fail-safe Mechanism
Trusted Exec. Environment
Hardware Security
Document-ation
Document-ation
Document-ation
Documentation
Auditing
Auditing
Auditing
Auditing
Auditing
Auditing
Auditing
Auditing
Auditing
Auditing
Incidents Sharing
Incidents Sharing
Trustw Data Exchange
Incidents Sharing
Incidents Sharing
Collaborative R&D
Collaborative R&D
Collaborative R&D
Collaborative R&D
Collaborative R&D
Collaborative R&D
Collaborative R&D
Collaborative R&D
Collaborative R&D
Cooperation & Information Sharing
Co-op Dev of
Co-op Dev of
Co-op Dev of
Co-op Dev of
Co-op Dev of
Co-op Dev of
Co-op Dev of
Co-op Dev of
Co-op Dev of

The importance of Data anomaly detection

As a very important stage of data preprocessing, anomaly detection is primarily because machine learning models are highly sensitive to outliers, making data cleaning through anomaly detection a valuable method to enhance their performance.

Survey

Definition and
Taxonomy of anomaly

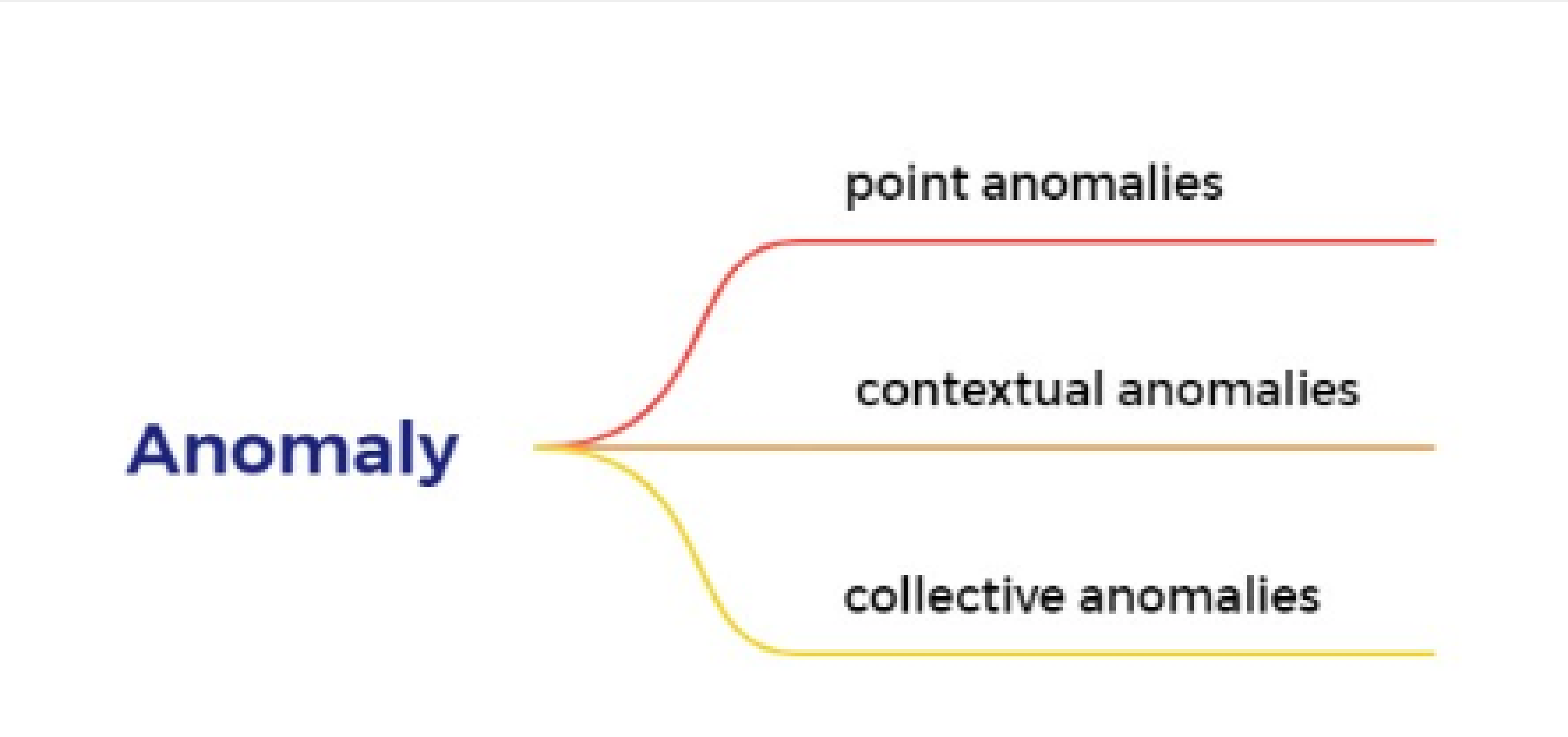
Brief introduction to
graph anomaly
detection

Techniques used for
graph node anomaly
detection.

Detailed
GNC Based Techniques

Definition and Taxonomy of anomaly

Anomalies are commonly denoted as abnormalities, deviants, or outliers.



The application of graph-based anomaly detection spans a wide array of fields, including social activities, e-commerce, and numerous others. Traditional detection methods often neglect the intricate interconnections between objects.

Brief introduction to graph anomaly detection

types of graphs

Plain Graph

A static, undirected graph G is formally denoted as G = {V, E}

Attributed Graph

A static attributed graph, symbolized as G = {V, E, X}

types of graphs

Dynamic Graph

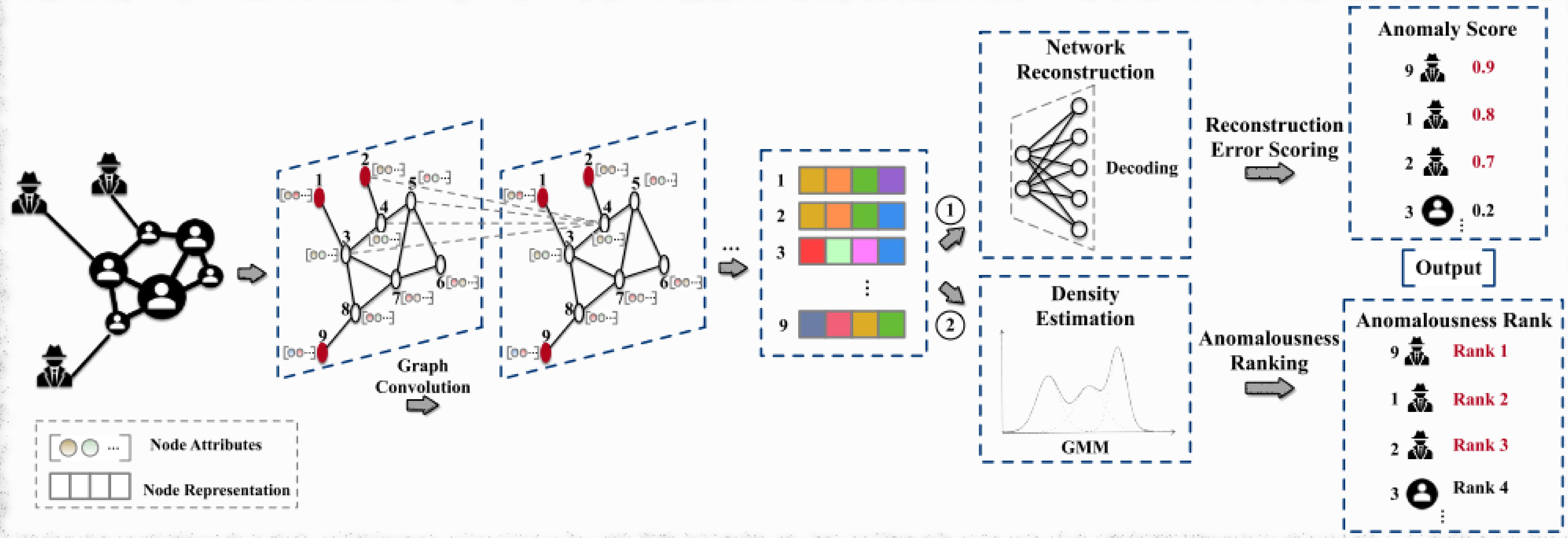
A dynamic graph, referred to as G(t), is characterized by a collection of elements {V(t), E(t), Xv(t), Xe(t)}

Techniques on anomaly node detection

Graph Type	Approach	Category	Objective Function	Measurement	Outputs
Static Graph - Plain	[77]	NR	$\sum_{(i,j)\in E} \lVert \mathbf{Z_i} - \mathbf{Z_j} \rVert^2 + \alpha \sum_{(i,j)\notin E} (\lVert \mathbf{Z_i} - \mathbf{Z_j} \rVert - 1)^2$	Anomaly Score	$\sum_{k=1}^{d} \frac{y_i^k}{y_i}$
	DCI [105]	NR	$\frac{1}{K} \sum_{k=1}^{K} \mathcal{L}_{DCI}^{k}$	Anomaly Prediction	Predicted Label
	NAC [88]	RL	Cumulative reward	-	Anomalies
Static Graph - Attributed	ALAD [106]	Non-DP	$\min_{W,H} \lVert A - WW^T \rVert_F^2 + \alpha \lVert X - WH \rVert_F^2 + \gamma(\lVert W \rVert_F^2 + \lVert H \rVert_F^2)$	Anomaly Score	$\frac{\mathbf{W}_{n,c}}{\sum_c \mathbf{W}_{n,c}} cos(\mathbf{A}_{n*}, \mathbf{H}_{c*})$
	Radar [41]	Non-DP	$\min_{W,R} \lVert X - W^T X - R \rVert_F^2 + \alpha \lVert W \rVert_{2,1} + \beta \lVert R \rVert_{2,1} + \gamma tr(R^T L R)$	Residual Analysis	Residual Value
	ANOMALOUS [107]	Non-DP	$\min_{W,\tilde{R}} \lVert X - XWX - \tilde{R} \rVert_F^2 + \alpha \lVert W \rVert_{2,1} + \beta \lVert W^T \rVert_{2,1} + \gamma \lVert \tilde{R}^T \rVert_{2,1} + \varphi tr(\tilde{R} L \tilde{R}^T)$	Residual Analysis	Residual Value
	SGASD [108]	Non-DP	$\min_{\mathbf{w},\mathbf{c}} \frac{1}{2} \sum_{i=1}^{m} \mathbf{c_i}(V_{i,*}\mathbf{w} - y_i)^2 + \frac{\lambda_1}{2} \lVert \mathbf{w} \rVert_2^2 + \lambda_2 \sum_{i=0}^{d} \sum_{j=1}^{n_i} \lVert \mathbf{c}_{G_j^i} \rVert_2$	Anomaly Prediction	Predicted Label
	DONE [82]	DNN	$\alpha_1 \mathcal{L}_{str}^{Recs} + \alpha_2 \mathcal{L}_{attr}^{Recs} + \alpha_3 \mathcal{L}_{str}^{Hom} + \alpha_4 \mathcal{L}_{attr}^{Hom} + \alpha_5 \mathcal{L}^{Com}$	Anomaly Scores	o_i^s, o_i^a, o_i^{com}
	DOMINANT [93]	GCN	$(1-\alpha)\mathcal{R}_S + \alpha \mathcal{R}_A$	Anomaly Score	$(1-\alpha)\lVert \mathbf{a}_i - \hat{\mathbf{a}}_i \rVert_2 + \alpha \lVert \mathbf{x}_i - \hat{\mathbf{x}}_i \rVert_2$
	ALARM [94]	GCN	$\sum_{i=1}^{n} \sum_{j=1}^{n} -[\gamma A_{ij} \log \hat{A}_{ij} + (1 - A_{ij}) \log(1 - \hat{A}_{ij})] + \mathcal{L}_a$	Anomaly Score	$(1-\alpha)\lVert \mathbf{a}_i - \hat{\mathbf{a}}_i \rVert_2^2 + \alpha \lVert \mathbf{x}_i - \hat{\mathbf{x}}_i \rVert_2^2$
	SpecAE [98]	GCN	$\mathbb{E}[dis(X, \hat{X})] + \mathbb{E}[dis(X, \hat{X})] + \lambda_1 \mathbb{E}(E(Z)) + \lambda_2 KL$	Density Estimation	Anomalousness Rank
	Fdgars [99]	GCN	$\mathcal{L}_{GCN}$	Anomaly Prediction	Predicted Label
	GraphRfi [100]	GCN	$\mathcal{L}_{rating} + \lambda \mathcal{L}_{fraudster}$	Anomaly Prediction	Predicted Label
	ResGCN [109]	GCN	$(1-\alpha)\lVert A - \hat{A} \rVert_F^2 + \alpha \lVert X - \hat{X} - \lambda R \rVert_F^2$	Anomaly Score	$\lVert R_{i,:} \rVert_2$
	GraphUCB [101]	RL	Expert Judgment	-	Anomalies
	AnomalyDAE [110]	GAT	$\alpha \lVert (A - \hat{A}) \odot \boldsymbol{\theta} \rVert_F^2 + (1 - \alpha) \lVert (X - \hat{X}) \odot \boldsymbol{\eta} \rVert_F^2$	Reconstruction Loss	Anomalousness Rank
	SemiGNN [111]	GAT	$\alpha \mathcal{L}_{sup} + (1-\alpha)\mathcal{L}_{unsup} + \lambda \mathcal{L}_{reg}$	Anomaly Prediction	Predicted Label
	AEGIS [112]	GAN	$\mathcal{L}_{AE} + \mathcal{L}_{GAN}$	Anomaly Score	$1 - D(\mathbf{z}_i)$
	REMAD [113]	NR	$\mathcal{L}_{res} + \beta \lVert R^T \rVert_{2,1}$	Residual Analysis	Residual Value
	CARE-GNN [27]	NR	$\mathcal{L}_{GNN} + \lambda_1 \mathcal{L}_{Simi}^{(1)} + \lambda_2 \mathcal{L}_{reg}$	Anomaly Prediction	Predicted Label
	SEANO [114]	NR	$-\sum_{i\in V_L} \log p(y_i \mid \mathbf{x}_i, \bar{\mathbf{x}}_{N_i}) - \sum_{i\in V} \sum_{v' \in C_i} \log p(v' \mid \mathbf{x}_i, \bar{\mathbf{x}}_{N_i})$	Anomaly Score	Discriminator's Output
	OCGNN [115]	NR	$\frac{1}{\beta K} \sum_{v_i \in \mathbf{V}_{tr}} [\lVert g(X, A; W)_{v_i} - c \rVert^2 - r^2]^+ + r^2 + \frac{\lambda}{2} \sum_{l=1}^{L} \lVert W^{(l)} \rVert^2$	Location in Embedding Space	Distance to Hypersphere Center
	GAL [67]	NR	$\max\{0, \max_{y_{v'} \neq y_u} g(u, v') - \min_{y_v = y_u} g(u, v) + \Delta_{y_u}\}$	Anomaly Prediction	Predicted Label
	CoLA [116]	NR	$-\sum_{i=1}^{N} y_i \log(CLM(v_i, \mathcal{G}_i)) + (1 - y_i) \log(1 - CLM(v_i, \mathcal{G}_i))$	Anomaly Score	$\frac{\sum_{r=1}^{R} (s_{i,r}^{(-)} - s_{i,r}^{(+)})}{R}$
	COMMANDER [117]	NR	$-\mathcal{L}_D + \mathcal{L}_C + \mathcal{L}_R$	Anomaly Score	$\tilde{y}_i \lVert \bar{\mathbf{x}}_i - \mathbf{x}_i \rVert_2^2$
	FRAUDRE [118]	NR	$\sum_{i=1}^{n} f^*(y_i, \mathbf{h}_i^{(final)} \mathbf{W}_2)$	Anomaly Prediction	Predicted Label
	Meta-GDN [119]	NR	$(1 - y_i) \cdot \lvert dev(v_i) \rvert + y_i \cdot \max(0, dev(v_i))$	Anomaly Score	$\mathbf{u}_s^T \mathbf{o}_i + b_s$
Dynamic Graph - Plain	NetWalk [84]	DNN	$\gamma \mathcal{L}_{AE} + \mathcal{L}_{Clique} + \lambda \lVert W \rVert_F^2 + \beta KL$	Anomaly Score	Nearest Distance to Cluster Centers
Dynamic Graph - Attributed	MTHL [120]	Non-DP	$min_{\mathcal{P}}\, f(\mathcal{P})$	Anomaly Score	Distance to Hypersphere Centroid
	OCAN [121]	GAN	$\mathcal{L}_{LSTM-AE} + \mathcal{L}_{GAN}$	Anomaly Score	Discriminator's Output

* Non-DP: Non-Deep Learning Techniques, DNN: Deep NN Based Techniques, GCN: GCN Based Techniques, RL: Reinforcement Learning Based Techniques.
* GAT: GAT Based Techniques, NR: Network Representation Based Techniques, GAN: Generative Adversarial Network Based Techniques.

Detailed GNC-Based Techniques



Discussion

1. Challenges in graph detection

2. Outlook and future research opportunities towards graph detection

Outlook and future research opportunities

Less anomaly detection research in edge and sub-graph detection.

Dynamic Graphs Detection

Anomaly Detection in Huge Graphs

Challenges in Detecting Adversarial Anomalies

Multi-faceted Anomaly Detection

End

Thank you