Skysong Innovations
Advancing the Arizona State University Knowledge Enterprise

1475 N. Scottsdale Road, Suite 200
Scottsdale, AZ 85287-3538
Phone: 480 884 1996 Fax: 480 884 1984

Case ID:M21-188P^
Published: 2/18/2022

Inventors

Kaize Ding

Huan Liu

Contact

Shen Yan
shen.yan@skysonginnovations.com

Inductive Anomaly Detection for Attributed Networks

-Background In a variety of real-world applications (e.g., social spam detection, financial fraud detection, and network intrusion detection), detecting anomalies from networked data plays a vital role in keeping malicious behaviors or attacks at bay. With the increasing usage of attributed networks for modeling information systems, anomaly detection has fundamentally become a learning task, aiming to accurately characterize and detect anomalies (i.e., abnormal nodes) whose patterns (relating to structure and attributes) deviate significantly from the majority reference nodes.

Anomaly detection on attributed networks is predominately carried out in an unsupervised manner and can be further divided into two settings based on how new data is handled: (1) transductive and (2) inductive. The former performs anomaly detection on a single, fixed attributed network that includes new nodes, while the latter anticipates how to handle newly observed nodes or (sub)networks with a previously learned model. Transductive anomaly detection methods require retraining of the model when new data arrives, which tends to be computationally expensive. Although graph neural networks have become a focus for inductive anomaly detection, two main challenges persist: (1) Existing graph neural networks are not tailored for anomaly detection and are thus ineffective at characterizing node abnormality, and (2) unseen anomalies that emerge in newly added data can jeopardize the detection capability of previously learned models. Invention Description Researchers at Arizona State University have developed an unsupervised framework for inductive anomaly detection that is built on graph differentiative layers, wherein anomaly-aware node representations are first learned through an autoencoder network. Then, a generative adversarial network is trained to broaden the model for handling newly added data. Specifically, the generator provides informative potential anomalies, while the discriminator learns a decision boundary that differentiates between potential anomalies and normal data. As such, this innovation bypasses the computational costs associated with transductive models and effectively detects anomalies among newly added nodes. Potential Applications • Attributed networks • Cyber security • Fraud detection Related Publication: Inductive Anomaly Detection on Attributed NetworksFaculty Profile of Professor Huan Liu