6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India

Anomaly Detection in Multiplex Networks

Ruchi Mittal\textsuperscript{a}, M.P. S Bhatia\textsuperscript{b}

\textsuperscript{a}Research scholar, Netaji Subhas Institute of Technology, New Delhi-110075, India
\textsuperscript{b}Professor, Netaji Subhas Institute of Technology, New Delhi-110075, India

Abstract

Detecting anomalies in social is a vital task, with numerous high impacted social networks such as WWW, Facebook, Twitter and so on. There are multiple of techniques have been developed for detecting outliers and anomalies in graph data. More recently, the area of multiplex networks has extended a considerable attention among researchers for more concrete results. A Multiplex network is a network, which contains multiple systems of the same set of nodes and there exists various types of the relationship among nodes. In this paper, we discover the anomalies across numerous multiplex networks. By anomalies or outliers means nodes, which behave abnormal or suspicious in the system. Compared to single layer networks, the outliers’ nodes may found into many layers of the multiplex network and find anomalies in the multiplex network is still untouched. From this study, we propose a new metric called cross-layer anomaly detection (CAD). The CAD is a measure, which detects the anomalies in the multiplex network. For experiments, we make use of two real-world multiplex networks. We compare the results of our proposed metric with other similar methods, and we get encouraging and similar results.

© 2018 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the scientific committee of the 6th International Conference on Smart Computing and Communications.

Keywords: Multiplex Network; Anomaly Detection; multiple Layers; Edges; Nodes;

* Corresponding Author.
Email: ruchi.mittal138@gmail.com
1. Introduction

It is interesting to find out the nodes, which shows the least appearance in a given network. A network is nothing but a collection of nodes joined together by edges [1]. Many real-life applications consist of network type structure where individuals act as nodes and relationship among them serves as edges. Finding individuals, which holds suspicious behavior or have the least appearance of the network is an exciting task and called as anomaly detection. For example, detecting networks intrusion or network failure [2], credit card fraud [3], telecommunications fraud [4] and so on.

To all networks, there is an assumption that only one type of interaction exists between any two nodes. Sometimes this assumption may ignore the multiple interactions or relationship among entities of the network, which doesn’t lead to refined results. A system formed by various interactions among entities is called a multiplex network [5, 6]. A multiplex network contains multiple layers; in which each segment represents one type of communication among entities. For example: in social networks, similar entities interact with others via Facebook, Twitter, LinkedIn and so on. Existing graph theory concepts cannot be directly applied to such networks, as there exist cross-layer interaction between entities. In Fig. 1, we show a sample multiplex network with two layers, where two type of communication between nodes exist.

Fig. 1. A Sample multiplex network with two-layer architecture.

The combined concepts of data mining and graph theory are widely used to study the various features of the network. For example, using anomaly detection methods, one can find the suspicious nodes in the network. Anomaly detection is a branch of data mining, which is concerned with discovering rare occurrences in datasets [7]. In general, data objects are inter-related, and one can easily map this into graphs or networks. The multiple paths lying among two data object may efficiently capture the long-range relationship and helps to spot the suspicious object in the network.

There are various methods defined for anomaly detection in networks such as distance-based anomaly detection [8], density based anomaly detection [9], distribution-based anomaly detection [10], clustering-based anomaly detection [11] and so on. Depending on the application, one can apply the anomaly detection method to find out the outlier nodes. For example, Clustering based method first find out the cluster in the network and then find out the nodes, which have least interaction.

In this paper, we propose a methodology for anomaly detection in the multiplex network. Here, we used the famous Gaussian model [12] along with other defined features of a multiplex network to detect anomalous nodes in the network. The formulation for Gaussian model for the simple network is as follow:

\[
p(x; \mu, \sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}
\]

(1)

Here, \(x = \{x^1, x^2, \ldots, x^m\}\) is the training set, \(\mu\) is the mean and \(\sigma^2\) is the variance. In figure 2, we present a sample network, in which nodes inside the red circle are the anomalous nodes of the network.
دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات