



Co-Membership-based Generic Anomalous Communities Detection

Shay Lapid¹ · Dima Kagan¹ · Michael Fire¹

Accepted: 7 December 2022 / Published online: 5 January 2023

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract

Nowadays, detecting anomalous communities in networks is an essential task in research, as it helps discover insights into community-structured networks. Most of the existing methods leverage either information regarding attributes of vertices or the topological structure of communities. In this study, we introduce the Co-Membership-based Generic Anomalous Communities Detection Algorithm (referred as to *CMMAC*), a novel and generic method that utilizes the information of vertices co-membership in multiple communities. *CMMAC* is domain-free and almost unaffected by communities' sizes and densities. Specifically, we train a classifier to predict the probability of each vertex in a community being a member of the community. We then rank the communities by the aggregated membership probabilities of each community's vertices. The lowest-ranked communities are considered to be anomalous. Furthermore, we present an algorithm for generating a community-structured random network enabling the infusion of anomalous communities to facilitate research in the field. We utilized it to generate two datasets, composed of thousands of labeled anomaly-infused networks, and published them. We experimented extensively on thousands of simulated, and real-world networks, infused with artificial anomalies. *CMMAC* outperformed other existing methods in a range of settings. Additionally, we demonstrated that *CMMAC* can identify abnormal communities in real-world unlabeled networks in different domains, such as Reddit and Wikipedia.

Keywords Anomaly detection · Anomalous community detection · Anomalous subgraph detection · Complex networks analysis · Social networks analysis

✉ Shay Lapid
lapidshay@gmail.com

Dima Kagan
kagnadi@post.bgu.ac.il

Michael Fire
mickyfi@post.bgu.ac.il

¹ Software and Information Systems Engineering, Ben-Gurion University of the Negev, Beer-Sheva, Israel

1 Introduction

We live in a networked world where almost everything can be represented as a network, including online social networks (OSNs) [12], a virus outbreak [54], food recipes [61], and a city's water supply system [20]. One attribute of complex networks is the formation of communities [29], which are clusters of relatively densely connected vertices with respect to the rest of the network [29]. For instance, a group of OSN users who share a common subject of interest [44], a team of coworkers, exposing each other to virus transmission [31], a family of ingredients from a certain cuisine [2], or a city neighborhood corresponding to its water supply system [14]. Analyzing such a community-structured network can help us gain meaningful insights into the objects represented by communities. For example, the detection of OSN communities promoting violent extremism and radicalization [9], finding a group with a high potential to cause a pandemic outbreak [65], recommending recipe-enhancing ingredients substitution [61], and locating a neighborhood likely to suffer from a water supply breakdown [52].

The ability to detect anomalous communities is crucial to the deduction of insights from community-structured networks [36]. Such insights could help humanity cease a pandemic by an early reveal of a virus' hot spots [28], identify groups of fake profiles spreading fake news [15], or prevent targeted violence toward minorities by uncovering hatred-inciting communities in an online social network [43].

Over the last two decades, both industry and academic researchers proposed various solutions to address the problem of anomaly detection in networks [3, 25, 39, 40, 50, 51], aiming to utilize them to gain insights into the analyzed networks. Altshuler et al. [5] demonstrated that by applying an anomaly detection algorithm on call recording logs of a country's mobile network, they could classify events appearing in a particular time period as emergencies or not. While the majority of the conducted studies are mainly focused on uncovering anomalous vertices, only a handful focus on detecting anomalous communities [7, 13, 33, 45, 48, 53, 59, 70].

Most of these methods fail in scenarios where the anomalous communities are concealed properly in the background network, having similar properties as the rest of the communities. For example, methods based on density and fraction of cross-boundary edges, such as *Conductance* [30], tend to achieve poor results as the anomalous communities become either more sparse or harder to separate from other communities.

In this study, we introduce a novel generic network analysis and machine-learning-based algorithm to detect anomalous communities in complex networks. Motivated by Kagan et al. [40], demonstrating anomalous vertices could be determined by the number of improbable edges they have, we have hypothesized a community composed of many unexpected vertices, has a higher chance of being anomalous.

The approach we employ to test our hypothesis undergoes a classification problem. We predict the affiliation probability of vertices to their communities, and aggregate the resulting probabilities to determine the "normality" of each community. We adopt a novel concept of utilizing the information of vertices' co-membership between communities, by formulating the aforementioned classification problem as a link-prediction problem in a new utility network, in which vertices are connected to community-representing vertices if they belong to the corresponding communities in the original network. More simply stated, we create a new network encapsulating the information of co-membership and then applies an anomaly detection algorithm to it.

The two significant advantages of our method are: (a) It utilizes only information of vertices' co-membership to communities, which makes it agnostic to the density of communities. It can only be affected by the fraction of cross-boundary edges they contain, and specifically, to improve as it increases; and (b) the co-membership information is converted to a network, of which only its structural features are extracted and utilized, which makes it independent of a specific domain. Our method succeeds in cases when communities are hard to separate from the background. Additionally, it is generic, unlike most of the studies in this field (see Sect. 2.2).

To evaluate our algorithm, we utilized two types of labeled datasets (see Sect. 4.1): (a) *Fully simulated random generated networks*, infused with anomalous communities; and (b) *real-world networks* infused with anomalous communities, that is, forcibly connecting randomly generated anomalous communities to other real communities in the real-world data. Additionally, we applied our method to two unlabeled real-world networks collected from Reddit¹ and Hebrew Wikipedia² revisions information. The results demonstrate that our method successfully identifies anomalous communities in all cases. In the first two cases, where simulated data or real-data perturbation are involved, causing them to be labeled datasets, our algorithm outperformed the baselines when the anomalous communities were sparse, small, and contained many cross-boundary connections. In the first unlabeled case, Reddit, our algorithm was able to identify two communities (subreddits) that presented peculiar activity, such as an utter failure of collaboration. In Wikipedia, where we depict an article as a community and the Wikipedians (editors) who edit it as vertices, our algorithm uncovered articles tainted with political agenda or violent content due to trolling.

The key contributions of our study are threefold:

- We have developed a novel generic algorithm for uncovering anomalous communities in complex networks and demonstrated that our algorithm could uncover real-world anomalous communities.
- We present a novel random network generation algorithm, which generates a random community-structured network, infused with anomalous communities. The algorithm includes the ability to control the number, size, and type (network generating algorithm) of the normal communities and the infused anomalous communities. The algorithm is well-suited to conduct research in the field of anomalous community detection in networks.
- We have developed and published online an open-source code of this study's framework as well as the labeled datasets we created and utilized throughout this study to facilitate future research in the field of anomalous community detection in complex networks.

The remainder of this paper is organized as follows: Sect. 2 provides a brief overview of previous studies on anomalous vertices detection in networks, and on anomalous subgraphs and communities detection in networks. In Sect. 3, we describe in detail our anomalous community detection method and our anomaly-infused community-structured random network generator. In Sect. 4 we describe the collection and creation of the networks' datasets used to evaluate our algorithm, and the experiments performed to evaluate it. In Sect. 5, we report our study's results. In Sect. 6, we analyze the evaluation results and insights and discuss our algorithm's limitations. Lastly, in Sect. 7, we present our conclusion and offer future research directions.

¹ <https://www.reddit.com>.

² <https://he.wikipedia.org>.

2 Related Work

Detecting anomalies in network-based data is an essential task for countless applications and areas [4]. In recent times, the ability to detect anomalous communities in networks, rather than stand-alone anomalies, became a high-impact task as well [48]. The following section surveys studies on anomalous vertices detection and anomalous communities detection in networks.

2.1 Anomalous Vertices Detection

Research and technology in the field of anomaly detection in networks have significantly evolved in the last two decades [4]. Noble and Cook [50] were one of the first to study anomaly detection in network-based data. Their method assumed infrequently occurring substructures indicate anomalous behavior, while normal substructures reoccur much more often. Jimeng et al. [39] proposed a method for detecting anomalous vertices in bipartite networks, where they calculated relevance scores between vertices and aggregated the results to one score per vertex, where a low score indicated an anomaly. Papadimitriou et al. [51] presented a method to identify anomalies in a web network by comparing consecutive pairs of snapshots of the network by calculating similarity measures between them, where scores that were too low or high indicated an anomaly. In the same year, Akoglu et al. [3] proposed OddBall, a feature-based method to detect outliers in weighted networks. They chose pairs of features extracted from a vertex's *egonet*, whose patterns obey power-laws. Vertices with significant deviation from the patterns are considered outliers. Fire et al. [25] presented a method for detecting fake profiles on online social networks based on anomalies in a fake user's social structure, namely the topology of the network. The method followed the intuition a fake profile randomly connects to other users in the network. Kagan et al. [40] proposed a generic unsupervised algorithm able to detect anomalous vertices based on network topological features alone, with the idea a vertex with many improbable edges has a higher likelihood of being anomalous. Ding et al. [21] introduced an interactive deep-learning-based approach, which allows the system to proactively communicate with the end-user to mitigate the lack of labeled data and enhance the anomaly detection performance. Recently, Gutiérrez-Gómez et al. [34] proposed MADAN, a parallelized method to rank and localize outlier vertices within their contexts, at different scales of a network, where they utilize heat kernel to smoothen signals around vertices at each scale, and the remaining highly concentrated signals after smoothing point to anomalous vertices.

2.2 Anomalous Subgraphs and Communities Detection

In recent years, due to the increase in volume and sophistication of cyber-threats [37], the ability to detect a group of entities whose linkage is abnormal regarding the other network's edges, namely, the detection of anomalous communities, has become a necessity and a valuable field of research [48].

Singh et al. [59] were the first to address the problem of anomalous subgraph detection rather than single anomalous vertices detection, by utilizing an approach from the field of signal processing, by detecting signal in noise—to detect un-hinted anomalous subgraphs in a background network. More specifically, they applied sparse principal component analysis to the network's modularity matrix and checked for substantial deviation in the results compared to the expected results of a random subgraph. The method was tested on a simulated network.

Miller et al. [48] studied a similar direction by adopting another method from the field of signal processing and proposed several algorithms based on the spectral properties of the principal eigenspace of a network's residuals matrix. The algorithms analyze the residuals, comparing the residuals of an observed random subgraph to its expected value to find outliers and were able to demonstrate the detection of small, highly anomalous subgraphs, in real-world networks. In the same year, Gupta et al. [33] proposed SODA. Given a set of queried subgraphs, which are a subset of a network, Gupta et al. classified them as anomalous or not, and constructed an attribute-based classifier utilizing linear programming methods, namely, SIMPLEX. They used the classifier to predict the edge existence probability between each pair of vertices in each queried subgraph. They gave each subgraph an "outlierness" score based on the number of unexpected existing edges and the number of missing expected edges. Subgraphs with "outlierness" scores above some threshold were classified as anomalous subgraphs. Gupta et al. have achieved a precision score of 0.881 on a real-world dataset infused with generated anomalous subgraphs. As they lacked a labeled real-world dataset, they manually checked the highest-ranked subgraphs and reported to find interesting outliers.

Bridges et al. [13] proposed GBTER, a generalized version of the BTER model [57], which is a generative model that simulates a real-world community-structured network, assuming each vertex belongs to a single community. Additionally, they used a method of computing the probability distribution of a network given a generative model, which could derive the probabilities of the network's subgraphs. Bridges et al. [13] used the GBTER model to simulate a normal network and a network infused with an anomalous community, and compared the anomaly-infused network probability distribution to the expected distribution of the normal network. The comparison was used to detect the existence of an anomaly in the network, and by examining the probabilities of the subgraphs, they detected the anomalous subgraph. Bridges et al. [13] have achieved an AUC score of 0.936 in an experiment conducted on a small simulated network.

Yu et al. [69] proposed GLAD, a generative approach incorporating ideas from both MMSB and LDA models, that enables the utilization of two forms of data acquired from a network: (1) point-wise, i.e., a single vertex's attributes, and (2) pair-wise, i.e., the relationships between vertices. GLAD learns the parameters of the distributions that describe the latter two forms of data. Then, they rank the communities by their similarity to the learned distributions. They achieve accuracy ranging from 0.8 to 1 on a synthetic dataset and 0.25–0.45 on a real-world DBLP dataset, where publications of a specific conference are treated as normal communities and publications of other conferences are considered anomalous.

Zhao et al. [70] referred to the task of detecting an anomalous subgraph as an optimization problem that tries to find a subset of vertices that maximizes overall abnormalities. The main contribution of the research was the introduction of parallel computation of such a problem. Kumar et al. [42] studied sockpuppetry in discussion communities, where they discovered sockpuppets behave differently from benign users. One example they discovered was the more clustered ego-networks are, the more likely they are to interact with each other. In the same year, Zheng et al. [71] presented ELSIEDET, a three-stage sybil detection scheme identifying "elite" sybil users participating in the campaigns. The elite sybil users are highly rated accounts utilized to generate trustworthy and realistic-looking reviews.

Perozzi and Akoglu [53] proposed AMEN, an algorithm for ranking communities by a proposed "normality" measure, based on communities' coherency, that is, internally consistent, and externally separated from their boundaries, based on attributes and topological structure means. Perozzi et al. tested their algorithm on several real-world datasets while introducing labeled anomalous communities by disordering the topological structure of chosen commu-

nities and changing their vertices' attributes assignment. They have achieved AUC scores ranging from 0.18 to 0.60 on the different datasets.

Bansal and Sharma [7] presented ADENMN, which treated attributed networks as multiplex networks by splitting a network into different network layers, where each layer represented the network created by a certain attribute of the original network. By assigning the same latter "normality" score to each community at each layer, and accumulating the "layer activity"-weighted scores to uncover anomalous communities. They achieved MAP scores ranging from 0.22 to 0.51 on real-world datasets injected with anomalous communities created similarly to the latter.

Luan et al. [45] proposed RM-CNN, a convolutional neural network classifying whether a network contains an anomalous community given an expected degrees model. They supplied the model with the residuals produced by subtracting the expected adjacency matrix of a random network generated by a given random network generating algorithm with a certain set of parameters from the actual adjacency matrix. They evaluated their model by utilizing a dataset composed of simulated networks, where the anomaly-containing networks contain a dense community generated by Erdős-Rényi [22] random network generating algorithm embedded in the background network and achieved AUC scores ranging from 0.89 to 1.00.

3 Methods

In this study, we apply concepts from the domains of *Graph Theory*, *Complex-Networks Analysis*, and *Supervised-Learning* as building blocks of CMMAC algorithm, whose purpose is to uncover anomalous communities in complex networks. In the following subsections, we describe, in detail, the phases of our anomalous communities detection algorithm and our anomaly-infused community-structured random network generator.

3.1 Anomalous Communities Detection Algorithm

CMMAC requires two preliminary steps, (1) Community-detection in the examined network, whose results are stored as a *partition map*,³ and (2) Splitting the network into train and test sets that share common structural properties, to allow training on part of the network and detect anomalous communities on the rest of network. We separated the network by splitting the *partition map* into two *partition maps*, such that the two resulting sets do not share common communities but may share common vertices.

According to our hypothesis, the task of detecting anomalous communities in networks requires the following main steps: (a) We begin by utilizing the two input partition maps to construct two bipartite networks, where each is composed of a group of vertices that "represent" communities in the original network, "regular" vertices, and edges denoting a "regular" vertex belongs to a community in the original network (see Sect. 3.1.1), (b) we then extract topological features of the newly created network and utilize the train set topological features to train a link-prediction classifier (see Sect. 3.1.2), and (c) lastly, based on the aggregation of the link-prediction classifier probability results of the test set, we extract meta-features and rank them. As anomalous communities tend to contain an improbable set of vertices, the corresponding anomalous community-representing vertices are more likely

³ A set of key-value pairs, where each key corresponds to a community, and the matching value is a list of the community's vertices.

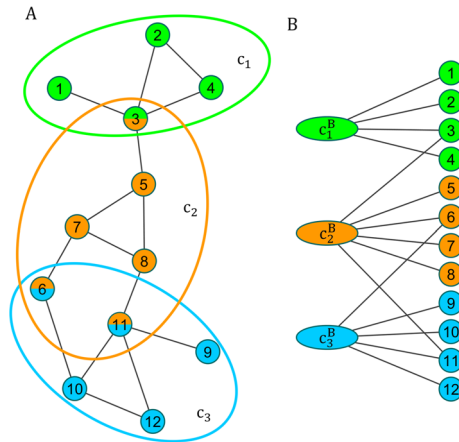


Fig. 1 **A** an example of an overlapping community-structured network G , where the set of vertices is $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\} \in V$, the set of communities is $\{c_1, c_2, c_3\} \in C$, and $c_1 = \{1, 2, 3, 4\}$, $c_2 = \{3, 5, 6, 7, 8, 11\}$, and $c_3 = \{6, 9, 10, 11, 12\}$. **B** The corresponding derived bipartite network BPG with the set of regular vertices V and community-representing vertices $\{c_1^B, c_2^B, c_3^B\} \in C^B$, and the set of edges E^B which state the belonging of a vertex to a community

found at the bottom margin of the ranked meta-features (see Sect. 3.1.3). In the following subsections, we will elaborate on each one of these steps.

3.1.1 Constructing a Bipartite Network

To utilize information on vertices' co-membership between communities, we begin by creating two new bipartite undirected networks based on the given partition maps. Let $G := (V, E)$ be a network, where V is a set of the network's vertices, and E is a set of the network's edges, and let $\{c_i\}_{i=1}^n \in C$ be the set of n communities in G . We define the new bipartite network in the following manner: Using G , we constructed a new bipartite undirected network $BPG := (V \cup C^B, E^B)$, where $C^B := \{c_i^B \in C^B \mid \forall c_i^B \in C^B, \exists c_i \in C\}$, and $E^B := \bigcup_{i=1}^n E_i^B$ where $E_i^B := \{(c_i^B, v_j) \mid v_j \in c_i \text{ and } c_i \in C\}$. Namely, using G , we constructed a new bipartite network in which the one part is composed of all the vertices $v \in V$ of G , and the other part consists of new vertices, where each vertex $c_i^B \in C^B$ in BPG represents a community $c_i \in C$ in G . The undirected edges between a community-representing vertex and a regular vertex in BPG stand for the belonging of the regular vertices to the corresponding communities in network G (see Fig. 1).

3.1.2 Constructing a Link-Prediction Classifier

After generating the communities' bipartite network, the next step of our algorithm is to construct a link-prediction classifier. The classifier's task is to produce a probability of the existence of an edge (v, c^B) in BPG , given two vertices $v \in V$ and $c^B \in C^B$.

3.1.2.1 Feature Extraction The task of link-prediction is addressed by numerous studies. Particularly, techniques based on deep neural networks [10, 18, 41] and stochastic gradient descent [32, 47] were proposed over the last decade and achieved state-of-the-art results. Since

CMMAC is meant to be used in large-scale networks and to suit a variety of networks, we chose to utilize a method that efficiently extracts easy-to-compute features for link-prediction and feeds them into an efficient classification model. Fire et al. [24] presented that just by using computationally efficient features, it is possible to achieve highly accurate link prediction classifier. Similar to Fire et al. [24], we calculate a set of topological features for the edges to construct the link-prediction classifier. We used only features which are meaningful for bipartite networks and modified them to adapt for analyzing bipartite undirected networks. Namely, we define the following features:

- Let be $u_i \in \{V \cup C^B\}$, a *neighborhood* $\Gamma(u_i)$ is defined as the set of vertex u_i 's adjacent vertices:

$$\Gamma(u_i) := \{u_j \mid (u_i, u_j) \in E^B\}$$

The bipartite network reasons the following property—a *neighborhood* of a vertex $v \in V$ only contains community-representing vertices $c^B \in C^B$ and vice versa.

- The *degree* of $u_i \in \{V \cup C^B\}$ is defined as:

$$d(u_i) := |\Gamma(u_i)|$$

- For two vertices $v \in V$ and $c^B \in C^B$, the *Total Friends* of u and v is defined as the number of distinct friends that v and c^B have together:

$$TF(v, c^B) := |\Gamma(v) \cup \Gamma(c^B)|$$

- As described in Sect. 3.2, the *Preferential Attachment Score* feature is based on the phenomenon that “rich” vertices increase their connectivity at the expense of the “poor” vertices [8]. We estimate how “rich” the two vertices $v \in V$ and $c^B \in C^B$ are, by multiplying their degrees:

$$PA(v, c^B) := |\Gamma(v)| \cdot |\Gamma(c^B)|$$

- The *Friends Measure* hints two vertices connection “strength” by the number of connections between two vertices $v \in V$ and $c^B \in C^B$ *neighborhoods* and is defined as:

$$FM(v, c^B) := \sum_{x \in \Gamma(v)} \sum_{y \in \Gamma(c^B)} \delta(x, y)$$

Where $\delta(x, y)$ is defined as:

$$\delta(x, y) := \begin{cases} 1 & \text{if } x = y \text{ or } (x, y) \in E^B \\ 0 & \text{otherwise} \end{cases}$$

- The *Shortest Path* was demonstrated as a significant feature in the link-prediction task [35]. For two vertices $v \in V$ and $c^B \in C^B$ we define *Shortest Path* as:

$$SP(v, c^B) := \begin{cases} \text{shortest path length between } c \text{ and } v^B \text{ in } BPG & \text{if a path exists} \\ -1 & \text{otherwise} \end{cases}$$

3.1.2.2 Classifier Construction Similar to Kagan et al. [40], we train a link-prediction classifier on an equivalent number of positive and negative examples, where the edges taken into account are the train set bipartite network *BPG* edges. We define a positive example as an existing edge $(v, c^B) \in E^B$, which stands for $v \in c$, or the belonging of vertex v to community c in the original network G . We define a negative example, as a non-existing edge

$(v, c^B) \notin E^B$, which implies vertex $v \notin c$, namely, vertex v does not belong to community c in the original network G .

We uniformly sample positive and negative examples from the train network, and then calculate the features for each of the positive and negative edges in the train network and each edge in the test network. For each edge we calculate the edge features and the vertex features of both vertices (see Sect. 3.1.2.1). Finally, we utilize the *XGBoost* algorithm [17] to construct the bipartite link-prediction classifier. We chose *XGBoost* since previously conducted studies concluded *XGBoost* performs well in terms of accuracy and efficiency in several cases of link-prediction tasks [49, 56].⁴

3.1.3 Detecting Anomalous Communities

After constructing the link-prediction classifier, we utilized it to create an unsupervised anomaly detection algorithm, which reduces the complexity of searching for anomalies in a large space (see Fig. 2). We utilized the link-prediction classifier to emit the existence probabilities of all edges in the test network. Next, we aggregated the probabilities of the edges of community-representing vertices in several forms to create different meta-features. Then, we ranked the community-representing vertices by each one of the meta-features. Lastly, we manually examined the communities indicated by the community-representing vertices ranked at the bottom margins to find anomalous communities.

3.1.3.1 Meta-Feature Extraction Inspired by Kagan et al. [40], we utilized the classifier to emit existence probabilities edges and aggregated them into meta-features. Based on the link-prediction classifier, we first provide formal definitions for the terms we use to describe the meta-features:

- Let $p(v, c^B)$ be the probability of the existence of an edge (v, c^B) in *BPG* as emitted by the link-prediction classifier, where $v \in V$ and $c^B \in C^B$.
- Let $EdgeProbabilities(c^B) := \{p(v, c^B) \mid v \in \Gamma(c^B) \text{ and } c^B \in C^B\}$ be the set of vertex c^B edges' existence probabilities.
- Let $EdgeLabels(c^B) := \{EdgeLabel(v, c^B) \mid v \in \Gamma(c^B) \text{ and } c^B \in C^B\}$ be the set of vertex c^B edges' labels, that is, the label classifications of the edges with respect to a predefined *threshold*, where $EdgeLabel(v, c^B)$ is defined as:

$$EdgeLabel(v, c^B) := \begin{cases} 1 & \text{if } p(v, c^B) \geq \text{threshold} \\ 0 & \text{otherwise} \end{cases}$$

Based on the above definitions, we define the following four meta-features as:

- *Edges Normality Probability Mean* is defined as the probability of a community-representing vertex c^B to be normal, in other words, is the mean (μ) taken over the existence probabilities of its edges:

$$EdgesNormalityMean(c^B) := \mu(EdgeProbabilities(c^B))$$

⁴ We evaluated *XGBoost*, as well as other known effective link-prediction classifiers, such as *Random Forest* [24, 64] and *Feed-Forward Neural Network* [55]. Our results indicated that the link-prediction classifier constructed using the *XGBoost* algorithm outperformed the other link-prediction classifiers.

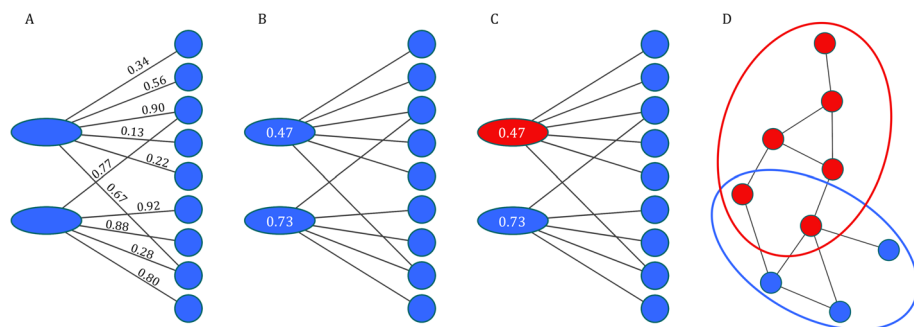


Fig. 2 Algorithm overview. **A** After constructing the bipartite network, we created a link-predictor based on its topological features and predict edges' existence. **B** For each community-representing vertex, we aggregate the predicted probabilities into meta-features, for example, averaging them. **C** We rank them by the meta-features. **D** We fetch the corresponding original communities and manually examine them

- *Edges Normality Probability STDV* is defined as one minus the standard deviation ($1 - \sigma$) of a set of vertex c^B edges' existence probabilities:⁵

$$\text{EdgesNormalitySTDV}(c^B) := 1 - \sigma(\text{EdgeProbabilities}(c^B))$$

- *Predicted Edge Labels Mean* is defined as the mean of the set of predicted labels of vertex c^B 's edges:

$$\text{PredictedEdgeLabelsMean}(c^B) := \mu(\text{EdgeLabels}(c^B))$$

- *Predicted Edge Labels STDV* is defined as the standard deviation of the set of predicted labels of vertex c^B 's edges:

$$\text{PredictedEdgeLabelsSTDV}(c^B) := 1 - \sigma(\text{EdgeLabels}(c^B))$$

3.1.3.2 Meta-Feature Ranking After obtaining the meta-features of all community-representing vertices $c^B \in C^B$ in the test network, we ranked the vertices by each one of the meta-features. We then manually examined the communities indicated by the corresponding k bottom vertices at each ranked meta-feature, where k is a defined threshold.

3.2 Anomaly-Infused Community-Structured Random Network Generator

To evaluate the proposed method, we striven to generate community-structured networks similar to real-world scenarios. A mutual property of many complex networks is that the vertex connectivity follows a power-law distribution [23]; reflecting the fact new vertices attach preferentially to existing high-degree vertices [8]. Furthermore, in real-world networks, the majority of the communities have a certain extent of overlap [1, 46], there exist vertices' co-memberships between them.

Based on the above two statements, we reasoned generating a network where each community follows preferential attachment property and generating connections between these communities, would be a well-suited notion to mimic real-world overlapping community-structured networks. A simple implementation of the described concept would be to generate

⁵ STDV-based meta-features are preceded with $1 -$ (one minus) since they behave the opposite from the rest of the features.

subnetworks using the Barabási–Albert algorithm [8], i.e., creating subnetworks by adding new vertices, each with m edges attached preferentially to existing vertices with high degree, and then connect them by connecting pairs of vertices from different subnetworks with a certain probability p .

We developed an algorithm encapsulating the essence of this concept and generalizing it further. Our algorithm creates subnetworks of two types, normal and anomalous, using two different random network generating algorithms. It then connects them in a “*dual-preferential*” manner, by connecting vertices from “new” subnetworks to existing subnetworks by a probability corresponding to the subnetworks’ sizes, and within the chosen subnetworks to vertices with a probability corresponding to their degrees. The connected subnetworks are considered as overlapping communities in the created network. The two types of random network generating algorithms allow different types of “normal” and “anomalous” communities in the generated network.

The algorithm creates an overlapping community-structured network composed of normal and anomalous communities, given the following four parameters for each of the groups, normal communities and anomalous communities (see Algorithm 1): (1) Random network generating algorithm (denoted *alg*), (2) a list of communities’ sizes to create (denoted *comm_sizes*), (3) arguments needed for random network generating algorithm (denoted *args*), and (4) a fraction of inter-connection to create between communities (denoted *inter_p*). It returns the network, as well as its partition map describing the communities’ belonging vertices. A detailed description of the algorithm is presented in “Appendix A”, and we have published the implementation of the algorithm as an open-source code. An evident example and a comprehensive explanation of how to choose parameters for the algorithm are provided in “Appendix B”.

4 Experimental Setup

4.1 Data Description

We evaluated our algorithm on two labeled datasets and performed two case studies by applying our algorithm on two unlabeled networks. We generated over 10 GB of networks data to be utilized throughout the study. The following subsections describe the creation of the datasets.

4.1.1 Labeled Datasets

To the best of our knowledge, there are no publicly available network datasets with labeled anomalous communities. To evaluate our proposed algorithm we utilized two labeled datasets: (1) Networks created from Reddit subnetworks infused with anomalous communities, and (2) fully simulated networks with anomalous communities created by our network generator.⁶ To avoid cherry-picking and to learn both strengths and weaknesses of *CMMAC*, we created the datasets such that they represent various anomalous communities’ situations, and specifically contain the regions where *CMMAC* changes from underperforming to outperforming the other methods.

⁶ Refers to our Anomaly-Infused Community-Structured Random Network Generator throughout this section.

Algorithm 1**Anomaly-Infused Community-Structured Random Network Generator**

```

1: procedure GENERATERANDOMNETWORK
Require:  $alg_{norm}, comm\_sizes_{norm}, args_{norm}, inter\_p_{norm},$ 
 $alg_{anom}, comm\_sizes_{anom}, args_{anom}, inter\_p_{anom}$ 
2:  $G \leftarrow$  empty undirected network
3:  $Partitions \leftarrow$  empty map
4: for each tuple in
     $[(alg_{norm}, comm\_sizes_{norm}, args_{norm}, inter\_p_{norm}),$ 
 $(alg_{anom}, comm\_sizes_{anom}, args_{anom}, inter\_p_{anom})]$  do
5:    $alg, comm\_sizes, args, inter\_p \leftarrow$  tuple // unpack tuple
6:   for  $c = 1$  to  $|comm\_sizes|$  do
7:      $G^c = \langle V^c, E^c \rangle \leftarrow$  CreateNetwork( $alg(comm\_sizes[c], args)$ )
8:     AddVerticesToNetwork( $G, V^c$ )
9:     AddEdgesToNetwork( $G, E^c$ )
10:    AddVerticesToPartition( $c, V^c$ )
11:   end for
12:   for  $c = 1$  to  $|comm\_sizes|$  do
13:     InterConnect( $V^c, inter\_p$ )
14:   end for
15: end for
16: return  $G, Partitions$ 
17: end procedure

18: procedure INTERCONNECT
Require:  $V^c, inter\_p$ 
19: for  $i = 1$  to  $\lfloor |V^c| \times p \rfloor$  do
20:    $u \leftarrow$  ChooseRandomVertex( $V^c$ )
21:    $otherComm \leftarrow$  ChooseWeighted( $comm\_sizes_{norm}$ )
22:    $v \leftarrow$  ChoosePreferentially( $V^{otherComm}$ )
23:   AddEdgesToNetwork( $G, \{(u, v)\}$ )
24:   AddVerticesToPartition( $otherComm, \{v\}$ )
25: end for
26: end procedure

```

In the following subsections we describe the processes of acquiring real-world data, its perturbation to introduce labeled anomalous communities, and the generation of the fully simulated labeled networks.

4.1.1.1 Real-World Networks Infused with Artificial Anomalies Reddit is a popular collection of forums where people share news, content, or comment on others' posts. Reddit is composed of hundreds of thousands of communities, also called "subreddits." Each subreddit is devoted to a different topic such as sports, sciences, and events [66]. Using Reddit data, Jason Michael Baumgartner constructed a massive dump of Reddit comments, which he published and maintained [38]. This dataset contains the ID and the time each comment was posted, the subreddit it was posted in, the user who posted the comment, and the ID of the parent comment.⁷ In this study we utilized data obtained from the Reddit comments dataset, cleaned, and preprocessed by Fire and Guestrin [23].⁸ The data contains over 2.37 billion posts posted from December 2005 through October 2016, by 19.72 million unique users, in 20,136 subreddits, each with more than 1000 comments.

⁷ The comment ID to which the current comment replied.

⁸ http://dynamics.cs.washington.edu/nobackup/reddit/reddit_last_graphs.tar.gz.

Table 1 Networks created by merging Reddit comments dataset subreddits' networks, each composed of 110 subreddits

Sampled network	$ V $	$ E $	Avg. degree
1	40,526	69,638	3.44
2	38,085	60,754	3.19
3	37,785	57,741	3.06
4	34,213	64,638	3.78
5	35,473	52,091	2.94

To evaluate *CMMAC* on anomaly-infused real networks, we utilized the Reddit comments dataset to create 1000 networks and infused them with generated anomalous communities for creating a dataset with ground truth labels. To create each of the anomaly-infused real networks, we sampled random subreddits from the Reddit comments dataset and constructed their networks. To follow the overlap property of real networks [46] and to preserve a certain degree of co-membership information, which is required for *CMMAC*, we constrained each sampled subreddit to have at least three users in common with at least two other subreddits in the network.

Formally, for each subreddit $s_i, i = 1 \dots k$, we define the subreddit's network to be: $G^i := \langle V^i, E^i \rangle$, where V^i is the set of vertices representing unique users who posted or commented within the subreddit s_i , and E^i is the set of edges representing connections between users in subreddit s_i . Each edge $(u, v) \in E^i$ exists if a user u replied to a comment, or as been replied to, by a user v , within subreddit s_i . For each subreddit $s_i, i = 1 \dots k$, exists at least two subreddits s_m and s_j , where $|V_i \cap V_m| \geq 3$ and $|V_i \cap V_j| \geq 3$. Next, we merged the k networks into a single network, that is, $G := \langle V, E \rangle$, where $V = \bigcup_{i=1}^k V^i$ and $E = \bigcup_{i=1}^k E^i$.

Lastly, we utilized some functionality of our network generator, specifically, only the anomalous parameters tuple, (see Sect. 3.2) to generate a anomalous communities and attach them to the network. We attached them in a "dual-preferential" manner, by connecting vertices from the generated communities to subreddits chosen by a probability corresponding to their sizes, and within them to vertices chosen by a probability that corresponds to their degrees. Since the "new" vertex connected with a high chance to a "central" vertex in the subreddit it attached to, we considered it as part of the subreddit (A detailed description of our network generator and the "dual-preferential" attachment property is presented in "Appendix A").

In this study, we constructed 1000 networks as described above, by creating five networks composed of $k = 110$ subreddits (see Table 1), and attaching each of them 200 distinct sets of ten anomalous communities ($a = 10$), where each generated with a different combination of parameters fed to our network generator. The motivation for choosing the parameters is to get experiment results that avoid cherry-picking, and properly present the regions where *CMMAC* changes from underperforming to outperforming the other methods to learn and report its strengths and weaknesses. (For further details on the selection of network generation parameters, see "Appendix B"). Specifically, we used the following parameters grid: (1) $alg_{anom} = \text{Erdős-Rényi}$ [22], (2) $args_{anom} \in \{0.05, 0.1, 0.2, 0.4, 0.8\}$,⁹

⁹ In *Erdős-Rényi* random network generation algorithm $args_{anom}$ denotes p , the probability of edge existence between each pair of vertices.

(3) $inter_p_{anom} \in \{0.05, 0.1, 0.15, 0.2, 0.25, 0.3, 0.35, 0.4\}$, and (4) $comm_sizes_{anom} \in \{q_0, q_{0.1}, q_{0.25}, q_{0.5}, random\}$.¹⁰

4.1.1.2 Fully Simulated Networks Boshmaf et al. [11] studied the vulnerability of OSNs' to large-scale infiltration by socialbots. They created a Socialbot Network (SbN), that is, a community of fake users that form many connections among each other to generate attraction from regular users. Next, the fake users randomly connect to real users in the targeted OSN. Then, to avoid detection due to anomalous structure, or due to the detection of one fake user who presented anomalous behavior, the SbN decomposes by deleting connections between the fake users. Finally, the SbN performs an attack of choice, usually information harvesting for spreading fake news Boshmaf et al. [11].

Inspired by Boshmaf et al. [11], we utilized our network generator (see Sect. 3.2) to evaluate CMMAC on synthetic networks that simulate different points in the progress of the SbN decomposition and different networks' properties, by generating 1000 anomaly-infused community-structured random networks.

We chose parameters for the network generator so (1) the “normal” part of each network imitates the properties of a real network, in particular, the Reddit's network described in Section 4.1.1.1, and (2) the “anomalous” part will provide experimental results that properly present the regions where CMMAC starts outperforming the other methods. For further details on the selection of network generation parameters see “Appendix B”.

We constructed the 1000 fully simulated networks using the following parameters: (1) $alg_{norm} = \text{Barabási-Albert}$ [8], (2) $args_{norm} = 1$,¹¹ (3) $inter_p_{norm} = 0.075$, (4) $comm_sizes_{norm} \in \{random_sample_i, i = 1..5\}$, where $random_sample$ is a set of 5 distinct lists, each composed of 110 community sizes, sampled from the Reddit comments dataset subreddit's sizes distribution, (5) $alg_{anom} = \text{Erdős-Rényi}$ [22], (6) $args_{anom} \in \{0.01, 0.02, 0.04, 0.08, 0.16\}$ to compensate for the relatively low average degree of the normal communities, (7) $inter_p_{anom} \in \{0.05, 0.1, 0.15, 0.2, 0.25, 0.3, 0.35, 0.4\}$, and (8) $comm_sizes_{anom} \in \{q_0, q_{0.1}, q_{0.25}, q_{0.5}, random\}$ is a list of ten community sizes, sampled from the 110 normal community sizes distribution, where q_x denotes quantile x of the distribution and $random$ denotes uniform random sampling from the distribution.

4.1.2 Unlabeled Real-World Networks

This section describes the process of acquiring, cleaning, and preprocessing real-world unlabeled network datasets, to which we applied our algorithm to discover meaningful insights. We utilized the Reddit comments dataset, specifically data from the “r/Place” project, and the Hebrew Wikipedia revisions data.

4.1.2.1 Reddit's r/Place Network On April 1st, 2017, a collaborative project and social experiment called “r/Place” was initiated by Reddit [19]. The creators created a white 1000×1000 —pixel canvas and posted it online with a call for users to edit it, hinting them for collaboration. Users could only change one pixel color every 5 mins. After 72 h, and more than a million unique users, the canvas colors had been changed more than 16.5 million

¹⁰ $comm_sizes_{anom}$ is a list of 10 community sizes, sampled from the 110 normal community sizes distribution, where q_x denotes quantile x of the distribution and $random$ denotes uniform random sampling from the distribution.

¹¹ In Barabási-Albert random network generation algorithm $args_{norm}$ denotes m , the number of edges that connect a new vertex to existing vertices.

times. The canvas turned into a beautiful skirmish of nations' flags and symbols, ideologies, famous paintings and characters, and much more.

We utilized the Reddit comments dataset [38] by filtering 5.8 million comments from over one million unique users in 12,870 subreddits posted between April 1st through April 4th at midnight, particularly, at the time of the *r/Place* project. We cleaned the data by removing comments that did not include information about the author. We then grouped the comments by subreddit and cleaned the data further by removing subreddits that contained less than 50 comments.

We processed the data further by filtering in only the 610 subreddits that actively participated in the *r/Place* project,¹² and from those we chose 468 subreddits that ranged in size from 50 to 2500. We created a network from the resulting 468 subreddits with the same process described by Fire and Guestrin [23]. The formal definition is similar to the definition described in Section 4.1.1.1, without overlapping constraints. The resulting network consisted of 181,019 vertices and 339,306 edges.

4.1.2.2 Hebrew Wikipedia Revisions Network Wikipedia is a free, open-content collaborative online encyclopedia maintained by volunteering editors, also called *Wikipedians*. Wikipedia is one of the most popular websites [58], containing more than 174 million articles, in more than 300 languages, and which are read monthly by 1.5 billion unique visitors as of November 2020 [26]. In the last 2 years, the articles have been maintained by an average of 45 million edits per month, also called *Revisions*, which are performed by an average of 70 thousand active *Wikipedians* [26].

We utilized Quarry,¹³ an online public interface for running *SQL* queries against the Wikipedia database, to acquire all revisions made to articles in the Hebrew Wikipedia between January 1st, 2016, and July 14th, 2020 (To view the utilized query See "Appendix D"). The data contains almost 7.5 million revisions, performed by 295,263 Wikipedians, in 269,355 articles. The revisions dataset contains the revision ID, as well as information about the Wikipedian who performed the revision, its timestamp, the ID of the parent revision,¹⁴ and the article title that was revised. We inner-joined the data with itself on the *parent_revision_id* attribute to get the network of revising Wikipedians answering to each other, where the articles they revise are considered as communities.

We further preprocessed the data by filtering in only articles with between 20 and 80 distinct revising users and users that revised between 5 and 300 unique articles, to enforce overlap between articles regarding revising users. The resulting data contained 72,633 revisions done in 2123 articles.

Formally, for each article a_i , $i = 1 \dots k$, we define the article network to be: $G^i := \langle V^i, E^i \rangle$, where V^i is the set of vertices representing unique Wikipedians who revised article a_i , and E^i is the set of edges, representing the connections between Wikipedians within article a_i . Each edge $(u, v) \in E^i$ exists if Wikipedian u revised Wikipedian v 's revision or the opposite, within article a^i . We then constructed the whole Hebrew Wikipedia revisions network by merging the article networks; that is, $G := \langle V, E \rangle$, where $V = \bigcup_{i=1}^k V^i$ and $E = \bigcup_{i=1}^k E^i$. The resulting network consisted of 12,736 vertices and 13,765 edges.

¹² <https://draemm.li/various/place-atlas/>.

¹³ <https://quarry.wmflabs.org/>.

¹⁴ The revision modified by the current revision.

4.2 Experiments

To extensively evaluate our algorithm, we utilized the labeled datasets described in Sect. 4.1. We first split the datasets to train and test sets as follows: For each of the labeled networks described in Sect. 4.1.1, we selected 20 communities for the train set to train a suitable link-prediction classifier and 100 communities for the test set. Furthermore, we split the communities, so the train set was composed only of normal communities, while the test set was composed of 90 normal communities and ten anomalous communities (10%), which represents an estimation of anomalies percentage in an average social network [40]. For the *r/Place* dataset described in Sect. 4.1.2.1, we randomly chose 100 communities for the train set and 350 communities for the test set. Finally, for the Hebrew Wikipedia revisions dataset described in Section 4.1.2.2, we randomly selected 100 articles for the train set and 1000 articles for the test set. For further details on our train-test split methodology, see “Appendix C”.

For each of the labeled datasets, we began by analyzing the ranking predictive ability of each of the meta-features, namely, by ranking the communities by each of our algorithm’s meta-features, comparing the resulting rankings, and choosing one meta-feature to use for the comparison to other methods. Then, we compared *CMMAC*’s performance to other methods with respect to the three parameters (*comm_sizes_{anom}*, *args_{anom}*, and *inter_p_{anom}*) we used to create and attach the anomalous communities in our experiments.

The other methods we utilize for the comparison are the following known topology-based measures and methods: (a) *Average degree* [16]—the average degree of all vertices in a community; (b) *Cut ratio* [68]—the fraction of existing cut edges out of all possible edges; (c) *Conductance* [6]—the fraction of total edge volume that points outside the community); (d) *Flake-ODF* [27]—the fraction of community vertices that have fewer edges pointing inside the community than to the outside; (e) *Average-ODF* [27]—the average fraction of the community cut; (f) *AMEN* [53]; and (g) *ADENMN* [7].

To utilize the latter two algorithms in our study,¹⁵ we implemented in Python the *Unattributed-AMEN/ADENMN* algorithm, which is based on *AMEN* [53] and *ADENMN* [7] (both share the same topological-based part), but only considers the topological structure of the network and ignores the vertex attribute-based logic. Namely, it omits the vectors of attributes and corresponding weights, and the weights learning process. To be precise, *Unattributed-AMEN/ADENMN* implements the “normality score” expressed by:

$$N = \sum_{\substack{i \in C, j \in C, \\ i \neq j}} \left(A_{ij} - \frac{k_i \cdot k_j}{2 \cdot |E|} \right) - \sum_{\substack{i \in C, b \in B, \\ (i, b) \in E}} \left(1 - \min \left(1, \frac{k_i \cdot k_b}{2 \cdot |E|} \right) \right),$$

where k_i denotes the degree of vertex i , C denotes a community, A denotes the adjacency matrix of C , B denotes the set of boundary-vertices of C , and E denotes the set of edges in the whole examined network.

Since our algorithm is a ranking algorithm, we utilize evaluation measures from the field of *information retrieval*. Most of the baselines we compare to are simple, while we consider *AMEN* and *ADENMN* more advanced algorithms. To properly compare *CMMAC* to them, we use the same evaluation measure they used [7, 53], *average precision* obtained from the *AUC of the precision-recall curve* [60]. To compare *CMMAC* meta-features we use the measured *MAP*, obtained by taking the mean of several *average precision* scores.

¹⁵ *AMEN* was implemented in MATLAB, and was published as an open-source. *ADENMN* implementation was never published as an open source.

To uncover anomalous communities in the unlabeled datasets, we first utilized *CMMAC* to rank the communities in each of the networks' test sets. Then, to reduce the problem searching space, we selected only the three communities ranked at the bottom by each meta-feature and intersected them into one set. We also utilized the described baselines to rank the communities and intersected their three bottom-ranked communities as well.

To report reliable results, since the data was unlabeled, we manually examined each of the resulting communities, both by *CMMAC* and by the other methods, to seek anomalies: (1) in the Reddit r/Place project dataset, we comprehensively reviewed posts during and related to the r/Place project, within the examined subreddit, as well as posts that generally review the r/Place project and mentions the examined subreddits, and looked up anomalous behavior, and (2) in Wikipedia, we developed a code that produces a list of differences between each pair of consecutive revisions for a given article throughout a specific period. The output is composed of deletions and additions of content, as well as special actions, such as page protection activation. Finally, we sought anomalous behavior through extensive reviewing of the differences.

5 Results

The following section presents the results obtained from the experiments we conducted. First, we describe the evaluation results of the labeled datasets (see Sect. 5.1). Then, we present the communities that were revealed when applying our method to two unlabeled real-world network use cases (see Sect. 5.2).

5.1 Labeled Datasets

To evaluate our method on labeled datasets, we utilized the 2,000 networks we created in two datasets, as described in Sect. 4.1.1. We first analyze the predictive ranking ability of the meta-features in each of the datasets. Within the Reddit-based networks dataset, among all meta-features, the *EdgesNormalitySTDV* achieved the highest MAP score of 0.526 (see Fig. 3), while within the fully simulated networks dataset, the *PredictedEdgeLabelsMean* and the *PredictedEdgeLabelsSTDV* meta-features achieved the highest MAP score of 0.554 (see Fig. 4). Consequently, we utilized the latter meta-features to compare *CMMAC* to the other methods. Specifically, we utilized the *EdgesNormalitySTDV* meta-feature to report the comparison results in the Reddit-based networks dataset (see Fig. 5), and the *PredictedEdgeLabelsSTDV* meta-feature to report the comparison results in the fully simulated networks dataset (see Fig. 6).

5.2 Unlabeled Real-World Networks

This section presents the findings we discovered in two real-world unlabeled datasets. We utilized our algorithm to rank the communities by each of the meta-features. We then chose only the distinct communities ranked at the three lowest rankings by each of the meta-features (see subreddits list in "Appendix E"), thereby we reduced the searching space drastically. We then manually examined each of the resulting communities described in Sect. 4.2 and encountered interesting case studies. To verify the fidelity of the results obtained by *CMMAC*, we also utilized all the other methods described in Sect. 4.2 and manually examined their results.

Meta-Features Predictive Ranking Ability Procured in Reddit-Based Anomaly-Infused Networks Dataset

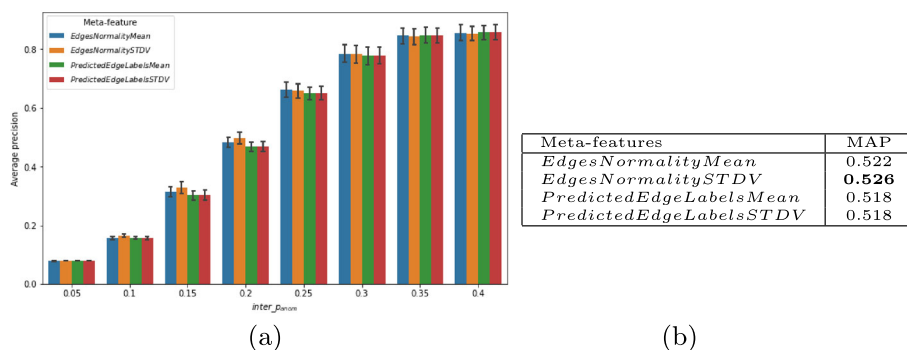


Fig. 3 **a** Average precision achieved by each meta-feature when applied to *Reddit-based anomaly-infused networks*. Each bar color indicates a different meta-feature, and the whiskers indicate the confidence interval obtained by 125 networks' results. **b** MAP score of each meta-feature, calculated by taking the mean average precision scores at all $inter_panom$ values range

Meta-Features Predictive Ranking Ability Procured in Fully Simulated Networks Dataset

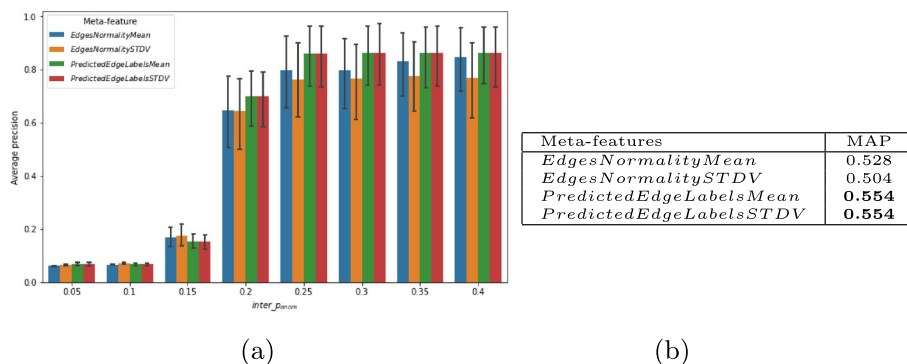


Fig. 4 **a** Average precision achieved by each meta-feature when applied to *fully simulated networks*. Each bar color indicates a different meta-feature, and the whiskers indicate the confidence interval obtained by 125 networks' results. **b** MAP score of each meta-feature, calculated by taking the mean average precision scores at all $inter_panom$ values range

5.2.1 Reddit's r/Place Network

To evaluate *CMMAC* on Reddit's *r/Place* project test set we utilized the network construction method described in Section 4.1.2.1. We utilized *CMMAC* to rank the subreddits by each of the meta-features, as well as utilized the other methods to rank the subreddits. We selected the three bottom-ranked subreddits (see Tables 3 and 4). Intersecting the three bottom-ranked subreddits resulted in ten distinct subreddits returned by *CMMAC*, and nine distinct subreddits returned by the other methods, where there are no common subreddits between our algorithm and the other methods.

We manually examined all the subreddits as described in Sect. 4.2, and exposed the following subreddits which presented abnormal behaviors, which were returned by *CMMAC*:

Reddit-Based Networks Dataset Evaluation and Comparison

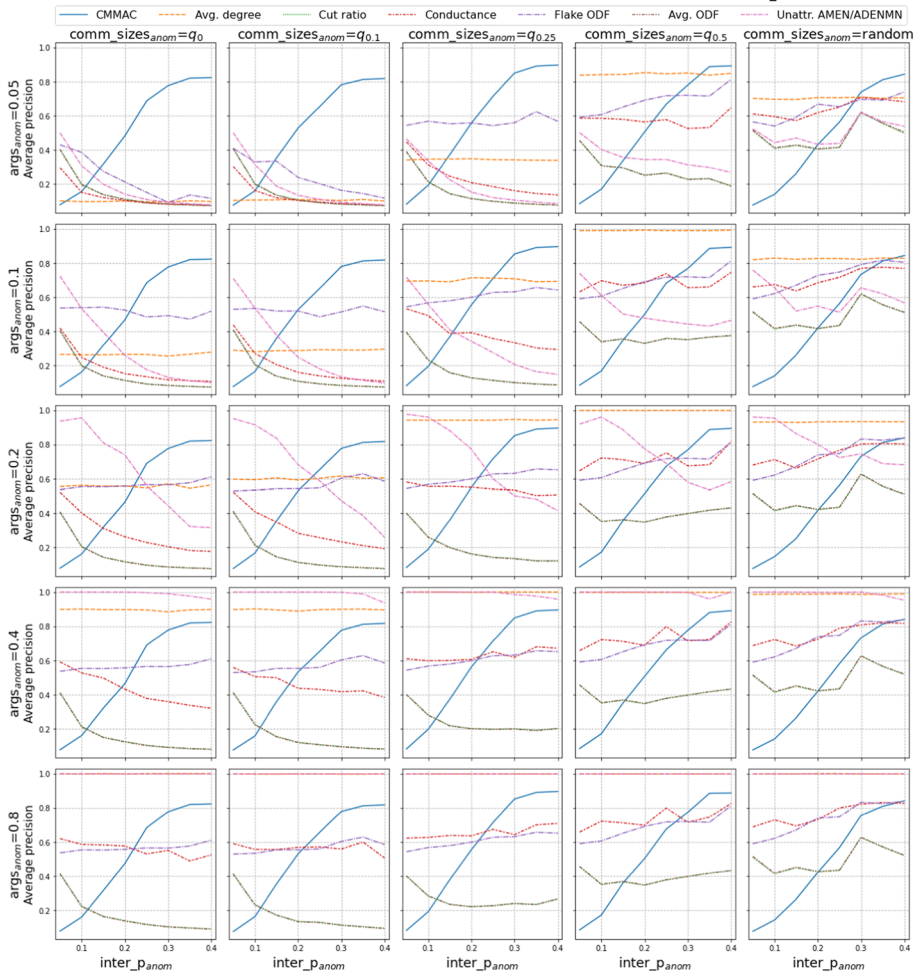


Fig. 5 Evaluation of *CMMAC*'s *EdgesNormalitySTDV* meta-feature and comparison to other methods on *Reddit-based anomaly-infused networks*. Each row of sub-plots describes a different $args_{anom}$ value, namely, the probability of edge existence between each pair of vertices in anomalous communities (density). Each column of subplots describes a different $comm_sizes_{anom}$ value, that is, a quantifier describing the size of the anomalous communities as compared to the normal communities. At each of the subplots the X-axis describes $inter_p_{anom}$ values, namely, the percentage of vertices in the anomalous communities that form "dual-preferential" inter-connections to normal communities. For each of the parameters obtained by this grid, we measured the *average precision* score, obtained from the *AUC of the precision-recall curve*, [60] which the Y-axis describes

- *r/BlueCorner*¹⁶—According to the Redditor *Andrewcshore315* [62] a member of the *r/TheBlueCorner* subreddit, the *r/BlueCorner* began as a violent subreddit that tried to paint the whole canvas with blue pixels, ruining other artifacts on its way. Due to its behavior, it quickly gained enemies, which made its users cease to cooperate and eventually abandon it. Many of the deserting users joined a new subreddit called *r/TheBlueCorner*, which was led by new leadership, this time aiming to maintain the structure of the blue

¹⁶ <https://www.reddit.com/r/BlueCorner/>.

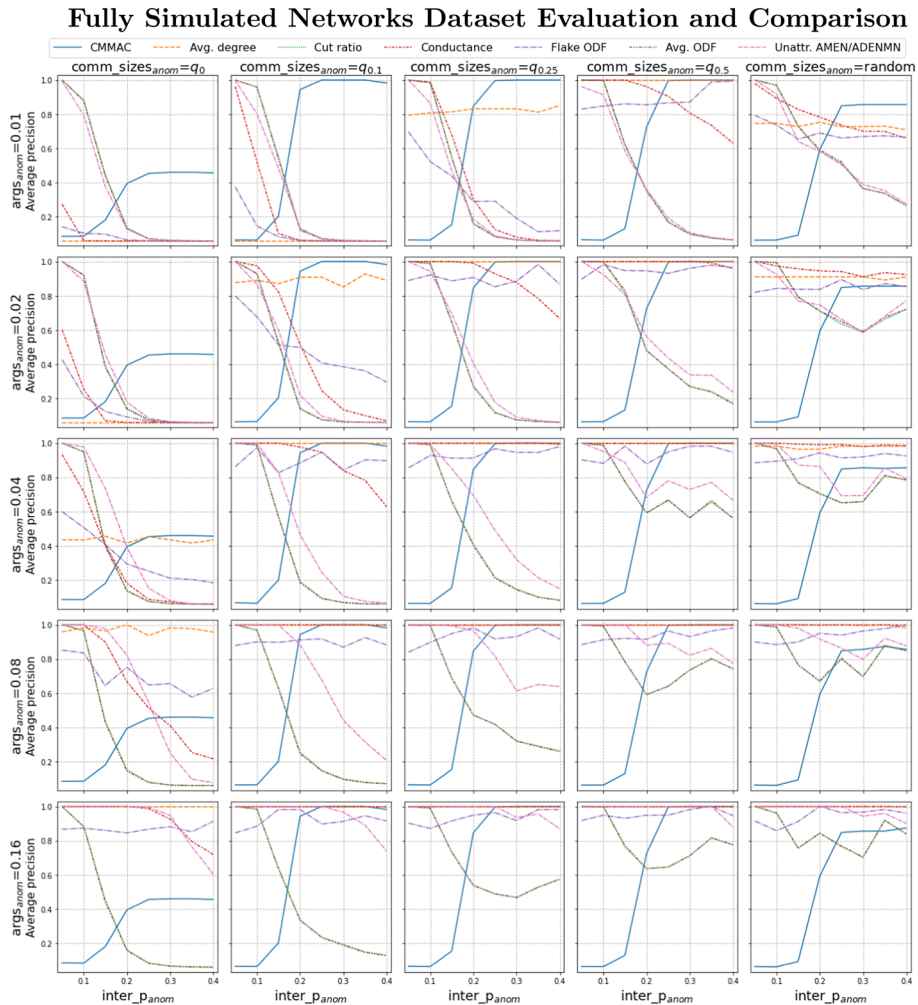


Fig. 6 Evaluation of CMMAC's *PredictedEdgeLabelsSTDV* meta-feature and comparison to other methods on *fully simulated networks*. Each row of subplots describes a different $args_{anom}$ value, particularly the probability of edge existence between each pair of vertices in anomalous communities (density). Each column of subplots describes a different $comm_sizes_{anom}$ value, that is, a quantifier describing the size of the anomalous communities as compared to the normal communities. At each of the subplots, the X-axis describes $inter_p_{anom}$ values, namely, the percentage of vertices in the anomalous communities that form “dual-preferential” inter-connections to normal communities. For each of the parameters obtained by this grid, we measured the *average precision* score, obtained from the *AUC of the precision-recall curve*, [60] which the Y-axis describes

corner while respecting and protecting other arts. The subreddit *r/BlueCorner* was ranked 349 out of 350, that is, 2nd from the bottom by CMMAC's *PredictedEdgeLabelsSTDV* meta-feature. For the rankings achieved by the other meta-features and by the other methods see Table 2.

- *r/COMPLETEANARCHY*¹⁷—A comprehensive inspection involving a systematic investigation through its posts during and related to the *r/Place* project, as well as questioning

¹⁷ <https://www.reddit.com/r/COMPLETEANARCHY/>.

some of the participants brought up that subreddit *r/COMPLETEANARCHY* presented an anomalous behavior—a complete failure of collaboration. Namely, there were many attempts to propose ideas, tactics, and courses of action, which were hardly commented upon and were never executed. Today there are no traces of their participation in the *r/Place* project. The subreddit *r/COMPLETEANARCHY* was ranked 348 out of 350, that is, 3rd from the bottom by *CMMAC*'s *PredictedEdgeLabelsSTDV* meta-feature. For the rankings achieved by the other meta-features and by the other methods see Table 2.

We could not detect any anomalous subreddits among the subreddits returned by the other methods.

5.2.2 Hebrew Wikipedia Revisions Network

To evaluate *CMMAC* on the Wikipedia revisions network test set, we utilized the network construction method described in Sect. 4.1.2.2. We utilized *CMMAC* to rank the article-representing communities by each of the meta-features, as well as utilized the other methods to rank the communities. We selected the three bottom-ranked articles (see Tables 5 and 6). Intersecting the three bottom-ranked articles resulted in six distinct articles returned by *CMMAC* and 12 distinct articles returned by the other methods. *CMMAC*'s results and the other methods' results shared one common article.

We manually examined all the articles as described in Sect. 4.2, and detected the following article, which presented anomalous behavior within its revisions history according to *CMMAC* results:

- *COVID-19 effects on the (Israeli) education system*¹⁸ [67] - The article *COVID-19 effects on the education system* [67] was created in April 2020 and was dedicated to the effect of COVID-19 on the Israeli education system. In the two and a half months it existed within our dataset, many of its revisions were in regard to the gaps between the different Israeli society sectors, and government criticism. This article was used as a fertile ground for a political scuffle, due to its fast popularity gaining on account of COVID-19 related news article. The article *COVID-19 effects on the education system* was ranked 998 out of 1000 articles, that is, 3rd from the bottom by *CMMAC*'s *EdgesNormalitySTDV* meta-feature. For the rankings achieved by the other meta-features and by the other methods see Table 2.

We could not detect any anomalous articles among the articles returned by the other methods.

6 Discussion

By analyzing the results presented in Sect. 5, the following can be noted:

First, by analyzing the behavior of *CMMAC* along the X-axis, namely the *inter_panom* values, at each of the subplots in Figs. 5 and 6, we can conclude that *CMMAC* performance is correlated to the fraction of inter-connections between anomalous communities and other communities. Specifically, it performs better as the fraction of inter-connections arises. Namely, when more cross-boundary edges exist between anomalous and other communities. As the percentage of inter-connections increases, more vertices communities' co-membership information is available to *CMMAC*, thereby enhancing its performance. However, the inferior results achieved by setting lower inter-connections fraction values indicate a limitation of

¹⁸ Refers to the Hebrew Wikipedia page “השפעת מגפת הקורונה על מערכת החינוך”.

Table 2 The ranking of the anomalous communities we ranked by each of *CMMAC*'s meta-features and other methods

	Reddit's r/Place (350 Subreddits)		Wikipedia revisions (1000 Articles)
	r/BlueCorner	r/COMPLETEANARCHY	COVID-19 effects on the education system
<i>CMMAC</i>			
EdgesNormalityMean	321	297	989
EdgesNormalitySTDV	222	197	998
PredictedEdgeLabelsMean	336	334	994
PredictedEdgeLabelsSTDV	349	348	994
<i>Other methods</i>			
Average degree	106	195	952
Cut ratio	80	166	663
Conductance	79	151	639
Flake-ODF	16	27	373
Average-ODF	80	166	661
Unattributed-AMEN/ADENMN	77	165	688

The bold numbers denote *CMMAC*'s meta-feature which ranked the corresponding community with the lowest ranking among all the meta-features

CMMAC. Namely, *CMMAC* depends on a somewhat degree of overlap between communities in the examined network. Networks without overlapping communities lack essential information for *CMMAC* to work properly. Nonetheless, most of the communities in real-world networks tend to overlap [1, 46].

Second, *CMMAC* requires inputs in form of partition maps that indicate each community's contained vertices. The creation of the partitions maps relies on a preliminary step of detecting overlapping communities in the observed network. The latter is a hard task, especially when utilizing only structural properties [63]. The combination of the dependency on detecting the overlapping communities, and the fact overlapping between communities is essential for *CMMAC*, presents a limitation of our approach. When we utilize non-network data and model it as a network in which we create communities according to the definition of the problem, we skip the need of detecting overlapping communities. For example, the creation of the Wikipedia revisions network is described in Sect. 4.1.2.2.

Third, by analyzing the subplots along the rows in Figs. 5 and 6, namely, the densities of the anomalous communities, we can conclude *CMMAC* is not affected by the density of a community, while all the other *internal-consistency*-based¹⁹ methods are, videlicet, *Average degree*, *Conductance*, *Flake-ODF*, and *Unattributed-AMEN/ADENMN*. Specifically, all the *internal-consistency*-based methods' performances degraded as the anomalous communities get sparser.

Fourth, by examining the evaluation results concerning the size of anomalous communities', i.e., along the columns in Figs. 5 and 6, we infer *CMMAC* is not affected by the size of a community, whereas all the other methods are affected by the size. In particular, the other methods achieve poorer scores as the anomalous communities become smaller.

¹⁹ The degree of how community's vertices are internally well connected.

Fifth, according to the overall evaluation results in Figs. 5 and 6, we can conclude that *CMMAC* outperforms other methods in the cases where the properties of the anomalous communities become similar to the rest of the communities, and when there are many cross-boundary edges between the anomalous communities and the other communities. Simply put, in the scenarios where the anomalous communities are small, sparse, and hard to separate from the other communities. It is important to keep in mind the latter finding was achieved and holds for a network whose structure follows a power-law distribution. To the best of our knowledge, no other method utilizes co-membership information. Particularly, the methods we utilized as baselines are founded upon either *internal-consistency*, *external-separability*,²⁰ or both. The mutual property of all these methods (apart from *Average degree*) is that they all degrade when the boundaries fade, that is, when the fraction of inter-connections arises.

Sixth, we showed that *CMMAC* is a suitable solution for identifying malicious communities in an OSN, such as Socialbot Networks. Their fake users connect randomly to other normal users and then detach their internal edges [11]. However, we presume *CMMAC* would be less effective in cases where the malicious communities present a “more specific” strategy of connecting to other communities, other than the “dual-preferential” attachment, such as connecting to vertices with similar attributes. We believe the described case will result in fewer “unexpected” edges, which in their turn, will contribute more “false” data for *CMMAC*’s link-predictor. In the future, we intend to improve our Anomaly-Infused Community-Structured Random Network Generator by adding an “attribute-oriented” attachment functionality, to simulate such cases. To enable *CMMAC* to handle such cases, we plan to reinforce its link-predictor with features that are based on attributes of vertices.

Seventh, regardless of the latter specific case we described, we firmly believe that utilizing attributes of vertices will enhance the performance of *CMMAC*. The advantage of the generality of *CMMAC* will not decrease since attributes of vertices could be utilized generically without needing specific domain knowledge or understanding. For this reason, we also aim to equip *CMMAC* with the functionality of utilizing vertices’ attributes generically and feeding them into the link-predictor, which will result in more accurate results of *CMMAC*. Determining the attributes of vertices is straightforward. Notwithstanding, determination and exploitation of community-representing vertices’ attributes require certain manipulation of attributes’ information, which should be further researched and developed.

Eighth, an approach of classifying anomalous communities rather than reducing the manual searching space by ranking is undoubtedly preferable. However, uncovering anomalous communities is a challenging task, particularly since, to the best of our knowledge, there are no existing labeled datasets and because different networks present different anomalous behaviors. We intend to enhance *CMMAC* further by developing the ability to receive a semi-labeled dataset and train a classifier that utilizes the meta-features and possibly additional features and the labeled communities and to classify the rest of the communities.

Finally, according to the real-world non-labeled networks results (see Sect. 5.2), we demonstrate *CMMAC* can be applied to detect anomalous communities “in the wild” in different domains by ranking communities that presented abnormal behavior at the bottom (see Table 2). The two non-labeled datasets we tested are a relatively small sample to test, hence, we intend to test *CMMAC* on more real-world non-labeled datasets. While uncovering anomalous communities in “native-network”²¹ data, such as Reddit’s *r/Place* project network, is a trivial task, the Wikipedia revisions network is an example of structuring non-trivial data into a network and utilizing *CMMAC* to detect anomalies within it. We depicted articles

²⁰ The degree of how community’s vertices are well separated from boundary vertices.

²¹ Data that can intuitively be represented by a network.

as communities and the Wikipedians who edited them as vertices, and by utilizing *CMMAC*, we uncovered articles containing anomalous revisions history. By generalizing this example, we believe *CMMAC* can be utilized to detect anomalies in a variety of domains, in which there exists data that can be modeled as a community-structured network and the resulting network contains a certain extent of overlap between communities.

7 Conclusion and Future Work

The detection of anomalous communities in complex networks is becoming progressively prominent in our networked world. We present a novel generic method for detecting abnormal communities based solely on the co-membership of vertices to communities. Our approach is composed of graph theory notions and straightforward yet accurate machine-learning-based link-prediction techniques. In addition, we developed an algorithm that generates an overlapping community-structured random network to empower further research in the field.

We evaluated our method on 1000 networks generated by us and on 1000 networks sampled from Reddit's comments dataset, where each contained tens of thousands of vertices and edges. We demonstrated our method succeeds in the scenarios where other known methods fail, specifically, when the anomalous communities are well disguised in the background, namely, they are sparse and heavily connected to other communities. We further demonstrated our method could detect anomalous communities in real-world networks by uncovering a violent subreddit and a collaboration-failing subreddit in the Reddit comments network and a Wikipedia article filled with inciting revisions.

Our open framework can be instantly utilized to gain insights into any data modeled as a community-structured network while providing a cost-effective practice that reduces a massive space of potential anomalies to a relatively small, threshold-dependent number of options to explore.

Future directions could be to add more structural features, such as edge weights, and to add vertex attributes to be used as features to enhance the community membership prediction ability in specific domains. Additionally, we aim to examine the use of more advanced techniques based on deep neural networks to construct the link-prediction classifier, to overcome the possible sub-optimal results achieved by the hand-crafted features. Moreover, we intend to transform *CMMAC* into a classifying algorithm rather than a ranking algorithm, in cases where it is applicable, that is, when the dataset is partially labeled.

Acknowledgements We would like to thank Sarah Ruddle for editing and proofreading this article to completion.

Author Contributions All the authors conceived the concept of this study, developed the methodology, and contributed to the manuscript's writing. Shay Lapid collected and created the data and developed the code utilized in this study. Dima Kagan and Michael Fire supervised the research and reviewed, edited, and approved the manuscript.

Funding No funding was received for conducting this study.

Data availability The labeled networks datasets we created (see Sect. 4.1.1) are open and can be found on the project's shared directory.

Code availability The code that implements our Anomaly-Infused Community-Structured Random Network Generator (see Sect. 3.2) and the framework that implements *CMMAC*, including the evaluation process used for the study can be found on the project's GitHub Page

Declarations

Conflict of interest The authors have no competing interests to declare that are relevant to the content of this article.

Ethical approval Not applicable.

Consent to participate Not applicable.

Consent for publication Not applicable.

Appendix A: Anomaly-Infused Community-Structured Random Network Generator

The following section describes in detail our Anomaly-Infused Community-Structured Random Network Generator algorithm. The algorithm pseudo-code is given in Algorithm 2.

The algorithm receives as input eight parameters, which can be divided into two groups of parameters:

- Normal communities parameters: (1) Normal community random network generating algorithm (denoted alg_{norm}), (2) a map of normal communities and their desired sizes to be created (denoted $comm_sizes_{norm}$), (3) arguments needed for the network generating algorithm (denoted $args_{norm}$), and (4) the ratio of vertices of each normal community to be connected to other communities (denoted $inter_p_{norm}$).
- Anomalous communities' parameters: Same types of parameters as the normal communities parameters, but for anomalous communities; denoted (5) alg_{anom} , (6) $comm_sizes_{anom}$, (7) $args_{anom}$, and (8) $inter_p_{anom}$ respectively. We emphasize that $inter_p_{anom}$ indicates the inter-connections fraction between anomalous communities and normal communities.

The algorithm starts by creating an empty network (line 2) and an empty map to be populated by the network partitions (communities) (line 3). Then, for each of the tuples (alg_{norm} , $comm_sizes_{norm}$, $args_{norm}$, $inter_p_{norm}$) and (alg_{anom} , $comm_sizes_{anom}$, $args_{anom}$, $inter_p_{anom}$), the algorithm passes twice through the list of communities sizes $comm_sizes$:

- At the first pass it generates random subnetworks utilizing the network-generating algorithm alg , the arguments $args$ and the sizes are given by $comm_sizes$ (line 7), merges the subnetworks to the main network G , that is, adding the newly created vertices and edges to the main network (lines 8–9), and updates the partition map of each subnetwork (community) to contain its vertices (line 10).
- At the second pass, it uses the *InterConnect* procedure to connect each community to other normal communities (line 12).

Procedure *InterConnect* receives as input two parameters: A set of vertices of the current community V^c , and a fraction that determines the number of inter-connections to create $inter_p$. The procedure connects each newly created normal or anomalous community to other normal communities, using the following routine:

- It first calculates the number of vertices in the given community that should be connected to other communities and randomly selects them (lines 15–16).
- For each of the selected vertices, preferentially chooses another community to connect to (line 17).

- Preferentially chooses a vertex to connect to in the chosen community, adds the created edge to the main network, and the connected vertex from the current community to the other community's partition (lines 18–20), following the intuition that it was likely connected to a “central” vertex in the other community, thus, becoming a part of its community.

The functions of choosing a community to connect to, *ChooseWeighted*, and the vertices to connect to, *ChoosePreferentially*, are named differently to avoid ambiguity; however, they follow the same preferential concept, that is, choose randomly by a probability that correlates to communities' sizes or a vertices' degrees, respectively.

Algorithm 2

Anomaly-Infused Community-Structured Random Network Generator

```

1: procedure GENERATERANDOMNETWORK
Require:  $alg_{norm}, comm\_sizes_{norm}, args_{norm}, inter\_p_{norm},$ 
 $alg_{anom}, comm\_sizes_{anom}, args_{anom}, inter\_p_{anom}$ 
2:  $G \leftarrow$  empty undirected network
3:  $Partitions \leftarrow$  empty map
4: for each tuple in
     $[(alg_{norm}, comm\_sizes_{norm}, args_{norm}, inter\_p_{norm}),$ 
 $(alg_{anom}, comm\_sizes_{anom}, args_{anom}, inter\_p_{anom})]$  do
5:    $alg, comm\_sizes, args, inter\_p \leftarrow$  tuple // unpack tuple
6:   for  $c = 1$  to  $|comm\_sizes|$  do
7:      $G^c \leftarrow V^c, E^c > \leftarrow$  CreateNetwork( $alg(comm\_sizes[c], args)$ )
8:     AddVerticesToNetwork( $G, V^c$ )
9:     AddEdgesToNetwork( $G, E^c$ )
10:    AddVerticesToPartition( $c, V^c$ )
11:   end for
12:   for  $c = 1$  to  $|comm\_sizes|$  do
13:     InterConnect( $V^c, inter\_p$ )
14:   end for
15: end for
16: return  $G, Partitions$ 
17: end procedure

18: procedure INTERCONNECT
Require:  $V^c, inter\_p$ 
19: for  $i = 1$  to  $\lfloor |V^c| \times p \rfloor$  do
20:    $u \leftarrow$  ChooseRandomVertex( $V^c$ )
21:    $otherComm \leftarrow$  ChooseWeighted( $comm\_sizes_{norm}$ )
22:    $v \leftarrow$  ChoosePreferentially( $V^{otherComm}$ )
23:   AddEdgesToNetwork( $G, \{(u, v)\}$ )
24:   AddVerticesToPartition( $otherComm, \{v\}$ )
25: end for
26: end procedure

```

Appendix B: Selection of Network Generation Parameters

To create the fully simulated networks (see Sect. 4.1.1.2) we utilized our Anomaly-Infused Community-Structured Random Network Generator (see “Appendix 3.2”), which receives as input the parameters $alg_{norm}, comm_sizes_{norm}, args_{norm}, inter_p_{norm}, alg_{anom},$

$comm_sizes_{anom}$, $args_{anom}$, and $inter_p_{anom}$. To create the “anomalous” part of the anomaly-infused Reddit-based networks (see Sect. 4.1.1.1) we used a partial functionality of our network generator, which requires only the input of the parameters alg_{anom} , $comm_sizes_{anom}$, $args_{anom}$, and $inter_p_{anom}$. This section describes the selection of the parameters.

The average degree distribution of the communities in Reddit’s network follows a power-law distribution. In particular, the mean average degree of the communities we sampled to create the networks equals 3.28. To imitate properties such as in Reddit’s network, we chose the following parameters to create the “normal” part of the fully simulated network: (1) alg_{norm} = Barabási–Albert [8] since it encapsulates both growth and preferential attachment, which are significant properties in real networks; (2) $comm_sizes_{norm}$ were chosen by sampling communities’ sizes from the Reddit’s network; (3) $args_{norm} = 1$, in this algorithm’s case $m = 1$,²² to produce a degree distribution similar to Reddit’s network; and (4) $inter_p_{norm} = 0.075$, which we derived from the average percent of vertices that are part of cut-edges, in each of Reddit’s network’s communities.

To report reliable results and to study the strengths and weaknesses of our algorithm, we used a wide range of parameters’ values to create the “anomalous” part of each of the networks: (1) $inter_p_{anom}$ were set to [0.05, 0.1, 0.15, 0.2, 0.25, 0.3, 0.35, 0.4]; and (2) $comm_sizes_{anom}$ were set to [q_0 , $q_{0.1}$, $q_{0.25}$, $q_{0.5}$, random], where the names correspond the quantiles of the normal communities’ sizes distribution. To get exposed to the points where our method changes from underperforming to outperforming the baselines and to enable higher-resolution examination of them, we used two different value ranges for the $args_{anom}$ parameter. Specifically, for the Reddit-based networks we set $args_{anom}$ to be the logarithmic scale [0.05, 0.1, 0.2, 0.4, 0.8] and for the fully simulated networks we set $args_{anom}$ to be on a lower logarithmic scale [0.01, 0.02, 0.04, 0.08, 0.16]. The motivation for choosing the values is described as follows:

The expected average degree of a random community generated by the Barabási–Albert algorithm equals $\mathbb{E}(\bar{k}) = 2 \cdot m$. However, the “dual-preferential” inter-connectivity property of our Anomaly-Infused Community-Structured Random Network Generator, adds extra edges to each community, such that the expected average degree sums up to

$$\mathbb{E}(\bar{k}) = 2 \cdot m + \frac{|V_{norm}^c| \cdot inter_p_{norm}}{|comm_sizes_{norm}|}$$

where $m = 1$, $|V_{norm}^c|$ is the average normal community size, and equals 520, $inter_p_{norm} = 0.075$, and $|comm_sizes_{norm}|$ is the number of normal communities, which equals 110. The mean average degree of the normal communities in the generated networks results in $\bar{k} = 2.35$.

The following concludes the reasons for selecting a lower logarithmic scale of values for the $args_{anom}$ parameter in the fully simulated networks: The mean average degree of the normal communities in the Reddit-based networks is 47% higher than the mean average degree of the normal communities in the fully simulated networks. This facilitates the *internal-consistency*-based baselines to improve faster in the fully simulated networks than in Reddit-based networks. Moreover, we aimed to demonstrate where our method is also superior specifically to the *avg. degree* method, which is the most rapidly affected method by the combination of community size and density.

²² Each new vertex is attached preferentially by one edge to one of the existing vertices.

Appendix C: Train-Test Split Methodology

CMMAC was developed to be a method for real-world uses; thus, we want to avoid consuming too many communities for the training phase at the expense of the extent of communities to test. Following the above utterance, we formulated our datasets such that the test sets contain the majority of the communities, and the train sets only contain enough communities to induce a sufficient number of edges for training.

Specifically, in the labeled network datasets described in Sect. 4.1.1, which we used for the evaluation, we used 20 communities for the train sets, which induced 18,000 positive and negative edges on average, and 100 communities in the test sets, which induced in 45,000 edges on average. In addition, the test sets contained ten anomalous communities out of the 100 communities.

In the real-world network datasets described in Sect. 4.1.2, we had a trade-off between maximizing the potential number of anomalies to detect and filtering a portion of it to constrain overlap between communities, to be applicable for *CMMAC*. We chose a compromise that yields an adequate degree of overlap as well as enough communities to test and then utilized most of the remaining data as follows: (1) 100 subreddit for training and 350 for testing in Reddit's *r/Place* dataset, (2) and 100 articles for training and 1000 for testing in Wikipedia dataset.

Appendix D: Quarry SQL Query for Obtaining Hebrew Wikipedia Revision Data

We utilized Quarry, an online public interface for running SQL queries against the Wikipedia database, to acquire all revisions made to articles in the Hebrew Wikipedia between January 1st, 2016, and July 14th, 2020, using the query in “Algorithm 3”.

Algorithm 3

Quarry SQL query for obtaining Hebrew Wikipedia Revision Data

```
USE hewiki_p;
SELECT
    revision.rev_id, revision.rev_actor, revision.rev_timestamp,
    revision.rev_parent_id, page.page_title, revision.rev_minor_edit,
    revision.rev_deleted
FROM revision
JOIN page ON revision.rev_page=page.page_id
WHERE (
    revision.rev_timestamp BETWEEN 20160101000000
    AND 2020715000000
    AND page.page_namespace = 0
    AND page.page_is_redirect = 0
)
```

Appendix E: Results of Unlabeled Real-World Networks

E.1 Reddit's r/Place Network

The following tables contain all the subreddits that were ranked at the three lowest rankings by each of the meta-features of *CMMAC* (see Table 3) and by each of the other methods we utilized as baselines (see Table 4).

Table 3 Reddit's r/Place project subreddits ranked at the lowest three ranks by each *CMMAC*'s meta-features (the table is split into two)

Ranking	<i>EdgesNormalityMean</i>	<i>EdgesNormalitySTDV</i>
348	starryknights	cavestory
349	placesnek	StrangerThings
350	cavestory	necrodancer
Ranking	<i>PredictedEdgeLabelsMean</i>	<i>PredictedEdgeLabelsSTDV</i>
348	FloydVsVoid	COMPLETEANARCHY
349	GreyBlob	BlueCorner
350	theitalyplace	cavestory

Table 4 Reddit's r/Place project subreddits ranked at the lowest three ranks by each of the methods we compare (the table is split into two)

Ranking	Average degree	Cut ratio	Conductance
348	Philippines	bdsm	India
349	Babymetal	Hamiltonmusical	Philippines
350	Worldpowers	Britishcolumbia	Britishcolumbia
Ranking	Flake-ODF	Average-ODF	Unattributed-AMEN/ADENMN
348	PuzzleAndDragons	bdsm	bdsm
349	Paragon	Hamiltonmusical	Hamiltonmusical
350	bdsm	Britishcolumbia	Britishcolumbia

E.2 Hebrew Wikipedia Revisions Network

The following tables contain all the articles that were ranked at the three lowest rankings by each of the meta-features of *CMMAC* (see Table 5) and by each of the other methods we utilized as baselines (see Table 6).

Table 5 Hebrew Wikipedia revisions network's articles ranked at the lowest three ranks by each *CMMAC*'s meta-features (the table is split into two)

Ranking	<i>EdgesNormalityMean</i>	<i>EdgesNormalitySTDV</i>
998	נועה קירל	השפעת מגפת הקורונה על מערכת החינוך
999	חסידות קרעטשניף	חסידות קרעטשניף
1000	אופוס המגזין למוזיקה קלאסית	אבא ממפלת
Ranking	<i>PredictedEdgeLabelsMean</i>	<i>PredictedEdgeLabelsSTDV</i>
998	אופוס המגזין למוזיקה קלאסית	אופוס המגזין למוזיקה קלאסית
999	חסידות קרעטשניף	חסידות קרעטשניף
1000	רוני אוסליבן	רוני אוסליבן

Table 6 Hebrew Wikipedia revisions network's articles ranked at the lowest three ranks by each of the methods we compare (The table is split into two)

Ranking	Average degree	Cut ratio	Conductance
998	מכבי חיפה כדורגל	עורב	מארק ויליאמס שחקן סנוקר
999	אבנר בירון	דוביים	רוני אוסליבן
1000	ניר קברשי	לשבור את הקרח	מזלף
Ranking	Flake-ODF	Average-ODF	Unattributed-AMEN/ADENMN
998	תפילין	עורב	לשבור את הקרח
999	תרזה מי	דוביים	עורב
1000	חשעה באב	לשבור את הקרח	דוביים

References

- Ahn YY, Bagrow JP, Lehmann S (2010) Link communities reveal multiscale complexity in networks. *Nature* 466(7307):761–764
- Ahn YY, Ahnert SE, Bagrow JP et al (2011) Flavor network and the principles of food pairing. *Sci Rep* 1(1):1–7
- Akoglu L, McGlohon M, Faloutsos C (2010) Oddball: Spotting anomalies in weighted graphs. In: Pacific-Asia conference on knowledge discovery and data mining, pp 410–421
- Akoglu L, Tong H, Koutra D (2015) Graph based anomaly detection and description: a survey. *Data Min Knowl Discov* 29:626–688. <https://doi.org/10.1007/s10618-014-0365-y>
- Altshuler Y, Fire M, Shmueli E et al (2013) Detecting anomalous behaviors using structural properties of social networks. *Soc Comput Behav Cult Model Predict* 7812(April):433–440. https://doi.org/10.1007/978-3-642-37210-0_47
- Andersen R, Fan Chung, Kevin Lang (2006) Local graph partitioning using pagerank vectors. In: 2006 47th annual IEEE symposium on foundations of computer science (FOCS'06). IEEE, Berkeley, CA, USA, pp 475–486. <https://doi.org/10.1109/FOCS.2006.44>
- Bansal M, Sharma D (2020) Ranking and discovering anomalous neighborhoods in attributed multiplex networks. In: Proceedings of the 7th ACM IKDD CoDS and 25th COMAD, pp 46–54
- Barabási AL, Albert R (1999) Emergence of scaling in random networks. *Science* 286(5439):509–512
- Benigni MC, Joseph K, Carley KM (2017) Online extremism and the communities that sustain it: detecting the ISIS supporting community on Twitter. *PLOS ONE* 12(12):1–23. <https://doi.org/10.1371/journal.pone.0181405>
- Berahmand K, Nasiri E, Rostami M et al (2021) A modified deepwalk method for link prediction in attributed social network. *Computing* 103(10):2227–2249

11. Boshmaf Y, Muslukhov I, Beznosov K, et al (2011) The socialbot network: when bots socialize for fame and money. In: ACM international conference proceeding series, pp 93–102. <https://doi.org/10.1145/2076732.2076746>
12. Boyd DM, Ellison NB (2007) Social network sites: definition, history, and scholarship. *J Comput Mediat Commun* 13(1):210–230. <https://doi.org/10.1111/j.1083-6101.2007.00393.x>
13. Bridges RA, Collins JP, Ferragut EM, et al (2015) Multi-level anomaly detection on time-varying graph data. In: Proceedings of the 2015 IEEE/ACM international conference on advances in social networks analysis and mining, ASONAM 2015, pp 579–583. <https://doi.org/10.1145/2808797.2809406>, [arXiv:1410.4355](https://arxiv.org/abs/1410.4355)
14. Bui XK, Marlim MS, Kang D (2020) Water network partitioning into district metered areas: a state-of-the-art review. *Water* 12(4):1002. <https://doi.org/10.3390/W12041002>
15. Campan A, Cuzzocrea A, Truta TM (2017) Fighting fake news spread in online social networks: actual trends and future research directions. In: Proceedings—2017 IEEE international conference on big data, big data 2017–2018-January (December 2017):4453–4457. <https://doi.org/10.1109/BigData.2017.8258484>
16. Charikar M (2000) Greedy approximation algorithms for finding dense components in a graph. In: Approximation algorithms for combinatorial optimization, third international workshop, APPROX 2000. Springer, Berlin, pp 84–95. https://doi.org/10.1007/3-540-44436-X_10
17. Chen T, Guestrin C (2016) Xgboost: A scalable tree boosting system. In: Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining. Association for Computing Machinery, New York, NY, USA, KDD'16, pp 785–794. <https://doi.org/10.1145/2939672.2939785>
18. Cui G, Zhou J, Yang C, et al (2020) Adaptive graph encoder for attributed graph embedding. In: Proceedings of the 26th ACM SIGKDD international conference on knowledge discovery and data mining. association for computing machinery, New York, NY, USA, KDD'20, pp 976–985. <https://doi.org/10.1145/3394486.3403140>
19. Cuthbertson A (2017) Reddit place: the internet's best experiment yet. *Newsweek* <https://www.newsweek.com/reddit-place-internet-experiment-579049>
20. Di Nardo A, Di Natale M, Santonastaso G et al (2013) Water network sectorization based on graph theory and energy performance indices. *J Water Resour Plan Manag-ASCE* 140:620–629. [https://doi.org/10.1061/\(ASCE\)WR.1943-5452.0000364](https://doi.org/10.1061/(ASCE)WR.1943-5452.0000364)
21. Ding K, Li J, Liu H (2019) Interactive anomaly detection on attributed networks. In: WSDM 2019—Proceedings of the 12th ACM international conference on web search and data mining, pp 357–365. <https://doi.org/10.1145/3289600.3290964>
22. Erdős P, Rényi A (1959) On random graphs I. *Publ Math Debrecen* 6:290–297
23. Fire M, Guestrin C (2020) The rise and fall of network stars: analyzing 2.5 million graphs to reveal how high-degree vertices emerge over time. *Inf Process Manag* 57(2):102041
24. Fire M, Tenenboim L, Lesser O, et al (2011) Link prediction in social networks using computationally efficient topological features. In: 2011 IEEE third international conference on privacy, security, risk and trust and 2011 IEEE third international conference on social computing. IEEE, pp 73–80
25. Fire M, Katz G, Elovici Y (2012) Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies. *HFSP J* 1(1):26–39
26. Foundation W (2020) Wikimedia Statistics. <https://stats.wikimedia.org/#/all-projects>
27. Gary William Flake SL, Giles CL (2000) Efficient identification of web communities. In: Proceedings of the sixth ACM SIGKDD international conference on knowledge discovery and data mining. Association for Computing Machinery, New York, NY, USA, pp 150–160. <https://doi.org/10.1145/347090.347121>
28. Geraghty E (2020) Coronavirus: world connectivity can save lives. <https://www.esri.com/about/newsroom/blog/coronavirus-world-connectivity-can-save-lives/>
29. Girvan M, Newman ME (2002) Community structure in social and biological networks. *Proc Natl Acad Sci USA* 99(12):7821–7826. <https://doi.org/10.1073/pnas.122653799>
30. Gleich D (2006) Hierarchical directed spectral graph partitioning. *Inf Netw* 443
31. Goncalve R (2020) Performing Social Network Analysis to Fight the Spread of COVID-19. <https://www.sisense.com/blog/performing-social-network-analysis-to-fight-the-spread-of-covid-19/>
32. Grover A, Leskovec J (2016) node2vec: Scalable feature learning for networks. In: Proceedings of the 22nd ACM SIGKDD international conference on Knowledge discovery and data mining, pp 855–864
33. Gupta M, Mallia A, Roy S, et al (2014) Local learning for mining outlier subgraphs from network datasets. In: SIAM international conference on data mining 2014, SDM 2014, vol 1, pp 73–81. <https://doi.org/10.1137/1.9781611973440.9>
34. Gutiérrez-Gómez L, Bovet A, Delvenne JC (2020) Multi-scale anomaly detection on attributed networks. In: AAAI conference on artificial intelligence. <https://doi.org/10.1609/aaai.v34i01.5409>, <https://aaai.org/ojs/index.php/AAAI/article/view/5409>

35. Hasan MA, Zaki MJ (2011) A survey of link prediction in social networks. In: Aggarwal C (ed) Social network data analytics. Springer, Boston, pp 243–275. https://doi.org/10.1007/978-1-4419-8462-3_9
36. HC M (2019) BMADSN: Big data multi-community anomaly detection in social networks. *Int J Electric Eng Educ* 0020720919891065
37. Jang-jaccard J (2014) A survey of emerging threats in cybersecurity. *J Comput Syst Sci* 80(5):973–993. <https://doi.org/10.1016/j.jcss.2014.02.005>
38. Jason MB (2022) Reddit Comments Dataset. <http://files.pushshift.io/reddit/comments/>
39. Jimeng S, Huiming Q, Chakrabarti D, et al (2005) Neighborhood formation and anomaly detection in bipartite graphs. In: Proceedings—IEEE international conference on data mining, ICDM pp 418–425. <https://doi.org/10.1109/ICDM.2005.103>
40. Kagan D, Elovichi Y, Fire M (2018) Generic anomalous vertices detection utilizing a link prediction algorithm. *Soc Netw Anal Min* 8(1):1–13
41. Kipf TN, Welling M (2016) Variational graph auto-encoders. [arXiv:1611.07308](https://arxiv.org/abs/1611.07308)
42. Kumar S, Cheng J, Leskovec J, et al (2017) An army of me: Sockpuppets in online discussion communities. In: Proceedings of the 26th international conference on world wide web, pp 857–866
43. Laub Z (2019) Hate speech on social media: global comparisons. <https://www.cfr.org/backgrounder/hate-speech-social-media-global-comparisons>
44. Lim KH, Datta A (2012) Finding twitter communities with common interests using following links of celebrities. In: Proceedings of the 3rd international workshop on modeling social media, pp 25–32
45. Luan M, Wang B, Zhao Y et al (2021) Anomalous subgraph detection in given expected degree networks with deep learning. *IEEE Access* 9:60052–60062. <https://doi.org/10.1109/ACCESS.2021.3073696>
46. McAuley JJ, Leskovec J (2012) Learning to discover social circles in ego networks. In: NIPS. Citeseer, pp 548–56
47. Menon AK, Elkan C (2011) Link prediction via matrix factorization. In: Gunopulos D, Hofmann T, Malerba D et al (eds) Machine learning and knowledge discovery in databases. Springer, Berlin, pp 437–452
48. Miller BA, Beard MS, Wolfe PJ et al (2014) A spectral framework for anomalous subgraph detection. *IEEE Trans Signal Process* 63(16):4191–4206. <https://doi.org/10.1109/TSP.2015.2437841>. [arxiv:1401.7702](https://arxiv.org/abs/1401.7702)
49. Mousa SR, Bakhit PR, Ishak S (2018) An extreme gradient boosting method for identifying the factors contributing to crash events: a naturalistic driving study. *Can J Civ Eng*
50. Noble CC, Cook DJ (2003) Graph-based anomaly detection. In: Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, pp 631–636
51. Papadimitriou P, Dasdan A, Garcia-Molina H (2010) Web graph similarity for anomaly detection. *J Internet Serv Appl* 1(1):19–30
52. Perelman L, Ostfeld A (2011) Topological clustering for water distribution systems analysis. *Environ Model Softw* 26(7):969–972. <https://doi.org/10.1016/j.envsoft.2011.01.006>
53. Perozzi B, Akoglu L (2018) Discovering communities and anomalies in attributed graphs: interactive visual exploration and summarization. *ACM Trans Knowl Discov Data* 12(2):1–40. <https://doi.org/10.1145/3139241>
54. Saey TH (2015) Liberia's Ebola outbreak largely traced to one source. <https://www.sciencenews.org/article/liberias-ebola-outbreak-largely-traced-one-source>
55. Sandhya P, Udayan Ghose UB (2020) Tailored feedforward artificial neural network based link prediction. *Int J Inf Technol* <https://doi.org/10.1007/s41870-019-00362-2>
56. Schlögl M, Stütz R, Laaha G et al (2019) A comparison of statistical learning methods for deriving determining factors of accident occurrence from an imbalanced high resolution dataset. *Accid Anal Prev* 127:134–149. <https://doi.org/10.1016/j.aap.2019.02.008>
57. Seshadhri C, Kolda TG, Pinar A (2012) Community structure and scale-free collections of Erdős–Rényi graphs. *Phys Rev E* 85(5):056109
58. SimilarWeb (2020) Top websites ranking. <https://www.similarweb.com/top-websites/>
59. Singh N, Miller BA, Bliss NT, et al (2011) Anomalous subgraph detection via sparse principal component analysis. In: 2011 IEEE statistical signal processing workshop (SSP), pp 485–488. <https://doi.org/10.1109/SSP.2011.5967738>
60. Su W, Yuan Y, Zhu M (2015) A relationship between the average precision and the area under the roc curve. In: Proceedings of the 2015 international conference on the theory of information retrieval. association for computing machinery, New York, NY, USA, ICTIR '15, pp 349–352. <https://doi.org/10.1145/2808194.2809481>
61. Teng CY, Lin YR, Adamic LA (2012) Recipe recommendation using ingredient networks. In: Proceedings of the 4th annual ACM web science conference. Association for Computing Machinery, New York, NY, USA, WebSci '12, pp 298–307. <https://doi.org/10.1145/2380718.2380757>

62. U/Andrewcshore315 (2017) The blue corner. https://docs.google.com/document/d/1IpQiDkYg94_GeDQ5--lppdBOq8_717MF91vi9ny-q38/edit
63. Vieira VDF, Xavier CR, Evsukoff AG (2020) A comparative study of overlapping community detection methods from the perspective of the structural properties. *Appl Netw Sci* 5(1):1–42. <https://doi.org/10.1007/s41109-020-00289-9>
64. Cukierski W, Hamner B, Yang B (2011) Graph-based features for supervised link prediction. In: The 2011 international joint conference neural networks (IJCNN), pp 1237–1244
65. Wang Y, Zeng D, Cao Z, et al (2011) The impact of community structure of social contact network on epidemic outbreak and effectiveness of non-pharmaceutical interventions. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 6749 LNCS, pp 108–120. https://doi.org/10.1007/978-3-642-22039-5_12
66. Widman J (2020) What is reddit? Digital trends <https://www.digitaltrends.com/web/what-is-reddit/>
67. Wikipedia (2022) Covid-19 effects on israeli education system. https://he.wikipedia.org/wiki/%D7%94%D7%A9%D7%A4%D7%A2%D7%AA_%D7%9E%D7%92%D7%A4%D7%AA_%D7%94%D7%A7%D7%95%D7%A8%D7%95%D7%A0%D7%94_%D7%A2%D7%9C_%D7%9E%D7%A2%D7%A8%D7%9B%D7%AA_%D7%94%D7%97%D7%99%D7%A0%D7%95%D7%9A
68. Yang J, Leskovec J (2012) Defining and evaluating network communities based on ground-truth. In: *MDS '12: Proceedings of the ACM SIGKDD workshop on mining data semantics*. Association for Computing Machinery, New York, NY, USA, pp 1–8, <https://doi.org/10.1145/2350190.2350193>
69. Yu R, He X, Liu Y (2015) Glad: group anomaly detection in social media analysis. *ACM Trans Knowl Discov Data* 10(2):1–22. <https://doi.org/10.1145/2811268>
70. Zhao J, Li J, Zhou B et al (2017) Parallel algorithms for anomalous subgraph detection. *Concurr Comput Pract Exp* 29(3):e3769
71. Zheng H, Xue M, Lu H, et al (2017) Smoke screener or straight shooter: detecting elite sybil attacks in user-review social networks. [arXiv:1709.06916](https://arxiv.org/abs/1709.06916)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.