Combining Computational Social Science and Graph Theory Techniques to Identify Key Coordinating Focal Structures in Social Media Capable of High Information Dissemination

Mustafa Alassad[a,1], Billy Spann[b], Nitin Agarwal[b,1]

[a] *Department of Systems Engineering.*
[b] *Department of Information Science.*
College of Engineering and Information Technology (EIT)
University of Arkansas, Little Rock, AR, USA

Article History

Keywords:

Focal Structure Analysis

Deviant Cyber Flash Mob Detection

Centrality-Modularity

Misinformation

Disinformation

Abstract

Social media has influenced socio-political aspects of many societies around the world. It is an effortless way for people to enhance their communication, connect with like-minded people, and share ideas. Online social networks (OSNs) can be used for noble causes by bringing together communities with common shared interests and to promote awareness of various causes. However, there is a dark side to the use of OSNs. OSNs can also be used as a coordination and amplification platform for attacks. For instance, aggressors can increase the impact of an attack by causing panic in an area by promoting attacks using OSNs. Public data can help aggressors to determine the best timing for attacks, scheduling attacks, and then using OSNs to coordinate attacks on networks or physical locations. This convergence of the cyber and physical worlds is known as cybernetics. In this paper we introduce an integrated method to identify malicious behavior and the actors responsible for propagating this behavior via online social networks. Throughout history we have used surveillance techniques to monitor negative behavior, activities, and information. Quantitative socio-technical methods such as deviant cyber flash mob detection (DCFM) and focal structure analysis (FSA) can provide reconnaissance capabilities that enable cities and governments to look beyond internal data and identify threats based on active events. Groups of powerful hackers can be identified through FSA which is an integrated model that uses a betweenness centrality method at the node-level and spectral modularity at group-level to identify a hidden malicious and powerful focal structure (a subset of the network). Assessment of groups using DCFM methods can help to identify powerful actors and prevent attacks. In this study, we examine multiple data sets integrating the DCFM and FSA models to help cybersecurity experts provide a better picture of the threat which will help to plan a better response.

1 Introduction

Social Media is characterized as one of the powerful engines for online interaction and information exchange (Shu, Sliva, Wang, Tand, & Liu, 2017) that allow access to millions of people on social media platforms (Dale, 2017). People use online social network (OSN) platforms such as Facebook, Twitter, and Instagram to communicate with their relatives, friends, and co-workers aiming to share ideas, information, and daily activities. Also, online social networks are used in large cities as a way to monitor traffic congestion, deliver online training sessions and enhance public services such as reporting broken water lines, hazardous road conditions, and other governmental services

[1] Corresponding authors.
Email addresses: mmalassad@ualr.edu (M. Alassad), bxspann@ualr.edu (B. Spann), nxagarwal@ualr.edu (N. Agarwal).

enhancements (Lorenzi et al., 2013). However, since OSN platforms are easy to use and offer free access to millions of people, this environment has also reshaped the lenses through which these platforms are viewed and given birth to new dark information operations such as fake news, misinformation, disinformation, online anti-government campaigns, anti-corruption campaigns, and political election campaigns.

Today, Facebook, Twitter, Instagram and other social platforms are common tools used for disseminating conspiracy theories, spreading radical ideology, organizing cyber flash mobs, and many other hateful actions that can take place. In addition, many malicious groups and users are misusing these platforms and turning them into tools of influence with many negative societal impacts. The following are examples of the dark side of information operations: using OSNs to influence the public's political decisions, encouraging anti-government protests, performing cyberattacks, spreading fake news, attacking smart infrastructure networks, stopping transportation systems, shutting down education institutions, cyber operations, organizing protests that shut down administration buildings, and encouraging young generations to accept/follow their radical agendas. All of these negative behaviors are part of a shift in how online information is viewed and have the ability to impact millions of honest online users. For example, Facebook was used to motivate millions of online users to participate in the Egyptian revolution in 2009 (Şen, Wigand, Agarwal, Tokdemir, & Kasprzyk, 2016). In another example, a Twitter network was used to spread/manage information about Saudi Women driving activities in 2011(Şen et al., 2016). Further, a YouTube channel was used to spread a conspiracy theory about the South China Sea conflict in 2016 (Alassad, Hussain, & Agarwal, 2019), and a video channel on YouTube was used by malicious commenters to spread radical information about other shared videos (Alassad, Agarwal, & Hussain, 2019). Finally, there are many other recent movements such as the "Yellow Vest Movement", "Hong Kong Protest", and the "Iraqi Protest in October 2019" as more recent campaigns that were managed, directed, and controlled by online social media platforms.

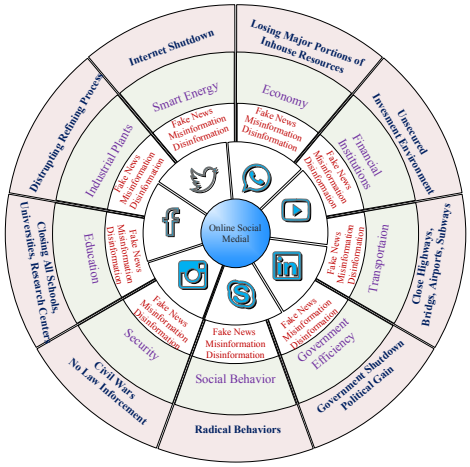


Figure 1: Negative impacts generated by malicious users on social media platforms

In this paper, we discuss several real-world scenarios that focus on the negative impacts generated by the dark side of online information behavior. An interesting approach to viewing the scenarios mentioned in this paper is shown in Figure 1 where the core of this environment begins with online social networks. The next layer considers the tactics, techniques, and procedures used to generate data in different sectors of the environment. Finally, the outer layer is the resulting impact of the information operation. One scenario occurs when malicious hidden online users are coordinating to attacks government infrastructure networks such as transportation systems by closing important highways, bridges, airports, and subways in big cities. A second scenario is when the online malicious users are coordinating to attack educational institutions in different parts of a big city by spreading fake news related to a lack of security or terrorist attacks, aiming to close a maximum number of schools, colleges, universities, and research centers. All these scenarios and many others can be part of the dark side of the online information and can use the well-known social platforms as weaponized information by malicious users to create unstable economics, politics, security, or social well-being. Figure 1 summarizes the negative impacts on infrastructure networks in cities and municipalities generated by malicious users on social media platforms . Malicious users can conduct malicious

activities on different platforms to coordinate multiple attacks on each or all parts of a smart cities' important asset(s) at any time.

The ideas from the above examples are to point out the forgotten and hidden side of activities in social networks, where any malicious groups of attackers can threaten normal life and deceive millions of people. These coordinating groups can influence many others to believe and follow their agendas across the country, guide them to attack targeted locations, and organize higher level of flash mobs that can shut down important administrative buildings, or close schools and transportation systems. In addition, these different influential malicious groups are often without formal leaders, but they have enough resources and followers on social media platforms that enable them to convince others to join their radical agendas.

Identifying hidden malicious groups in complex social networks using traditional clustering methods are not very effective and require extensive research. The challenges with these methods will be discussed further in sections 2 and 3. Currently, there are also no clear solutions and strategies to identify and stop such active malicious groups, where cybersecurity experts may react with random solutions such as suspending the central users or shutting down the entire Internet service in big cities. However, such actions are always followed by negative consequences on thousands of users, and it is impossible to analyze all central users' actions or track their connections in the network. In addition, cutting off the Internet service in big cities could be the worse solution, where this solution would impact millions of lives, harming the communications networks, transportation system, smart grids, losing millions of dollars hourly that will damage the economy, potential impacts to security and law enforcement, and many other smart infrastructure networks connected to the Internet as mentioned in Figure 1.

In recent years many robust quantitative approaches have been applied to analyze user metrics in complex social networks. The most common methods are centrality methods such as degree and betweenness centrality at the individual level. Also, methods such as modularity helps to characterize the community structure at the network or group level (Zafarani, Abbasi, & Liu, 2014). Both of these traditional methods lack a method for identifying active hidden groups within a network as explained below (Şen et al., 2016).

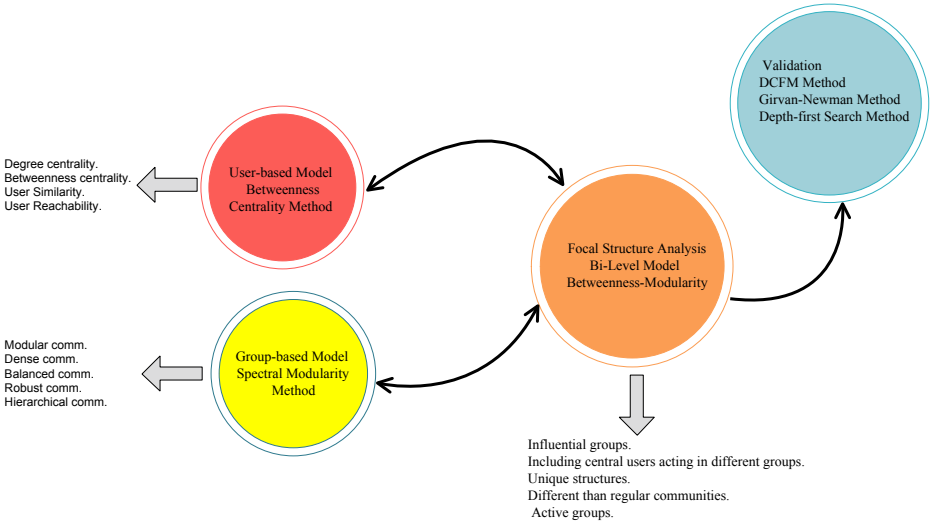


Figure 2: Overall focal structure analysis model structure.

To overcome the limitations in traditional community detection methods, this study proposes a novel approach that considers individual-based community detection algorithms using the betweenness centrality method (Freeman, 1978; Zafarani et al., 2014) together with group-based community detection algorithms using the spectral modularity method (Tsung, Ho, Chou, Lin, & Lee, 2017). However, considering these two community detection categories alone would lacks the depth and insight into finding the most influential malicious sets of users and network connections that would maximize the damage to a network. Therefore, we propose an integrated model, developing the individual-

level measure which considers the user's betweenness centrality value, and the group-level measure utilizing the modularity method which is used to measure the groups' influence in the entire network. Figure 2 shows the proposed model structure and how it would overcome the limitations of both user-based and group-based community detection algorithms. The resulting model is a bi-level centrality-modularity model called Focal Structure Analysis (FSA), where the resultant focal structure's cannot be discovered by the regular community detection algorithms alone. The FSA model identifies sets of users hidden within the network as active groups that can influence the maximum number of users in the network.

The model in this research includes different contributions such as overcoming the limitations in traditional community detection algorithms by introducing the betweenness-modularity model shown in Figure 2. Contributions from this bi-level model also include an integration of the traditional betweenness centrality method in the first level individual-based analysis and the traditional modularity method in the group-based analysis in the second level. The model also utilizes small-world metrics to evaluate the identified FSA sets and then evaluate them using the deviant cyber flash mob detection (DCFM) method to determine if the users and groups can influence other groups in the network. The next contribution is to evaluate the proposed model's performance comparing the betweenness-modularity model to the other centrality models such as the centrality-modularity model. The final contribution is to propose an effective optimal mechanism and strategy in finding the intensive groups within a network, then suspending these malicious sets of coordinating users, thereby stopping the spread of misinformation or disinformation disseminating throughout online social networks.

The rest of the paper is organized as follows. Section 2 is about the research motivations and the problem definition. Section 3, discusses the related works. In section 4, we summarize the data sets used in this paper. Section 5, is the research methodology. A toy case study is reviewed in section 6 and a real-world social network case study is implemented in section 7. Section 8 is to validate the results and model performance. Section 9 summarizes the research, findings, and the future works.

2 Research Motivation and Objectives

The main objective in this research is to integrate two traditional community detection algorithms to enhancing the cybersecurity network analysis. This research proposes a way to investigate, identify, and suspend malicious groups hidden in online social networks. These groups are responsible for dissemination of conspiracy theories and negative information spread to the different parts of a network. The identified groups are also able to control information flow to the maximum number of users in social networks. The biggest challenge in the approach is the identification of hidden, active, influential, and malicious sets of users including highly central users in complex social networks. These users are coordinating to spread fake news, propagating radical actions and practicing dark agendas. They can inspire other users to compromise systems such as financial institutions, smart power grids, transportation networks, communication, health, education, or entire cities' smart infrastructure networks.

These hidden influential malicious sets of users (focal structures) have enough resources on social media platforms to coordinate, motivate, and control different campaigns in different locations at the same time. These focal structures can organize their campaigns around a location's population size, natural obstacles in the targeted environment, and other common social dimensions. For example, in big cities, they could motivate their followers to close the main highways, bridges, airports, educational institutions, or other important administration buildings. In border cities, they could advise other followers living in that area to campaign near trading facilities thereby blocking the import/export operations. Similarly, in industrial cities, they can campaign beside the industrial facilities interrupting all-important daily operations, as shown in Figure 1. As a result, these types of coordinated misinformation or disinformation campaigns inflict significant damages on economic, trade, transportation, and other important systems in cities and governments, including smart cities.

Identifying focal structures in complex social networks is a challenging task, especially where they represent the negative behaviors that can exert a profound influence on political, economic, and social well-being. The current methods and theories cannot identify such intensive hidden malicious sets. For example, the group-based and user-based community detection algorithms (Zafarani et al., 2014) lack the ability to cluster such influential hidden sets (Şen et al., 2016). In addition, the current methods are designed to work independently, where the group-based

methods such as modularity are built on measuring the communities' features only (Clauset, Newman, & Moore, 2004; Newman, 2004a, 2004b, 2006), and the user-based methods such as centrality would measure the individual's aspects only (Nygren, 2010; Zafarani et al., 2014).

This research implements system design and focal structure analysis to find and suspend those sets of users spreading negative information and behaviors in complex social networks. Identifying hidden influential sets and suspending them without impacting the overall infrastructure network is the best solution to stem the spread of fake news, misinformation, and disinformation, and will minimize the network's damages caused by such negative information. In this research, we use a network of users who are posting radical messages on Twitter to paralyze the daily life in big cities. These malicious sets could be responsible for organizing multiple cyberattacks to maximize damage to the network, spread fake news and convince their followers to participate in or create their own campaigns in different locations to maximize the infrastructure damages. In this paper, considering that a deviant cyber flash mob occurring on large scale city infrastructure would likely have crippling effects on big cities, we identify these key malicious sets of users, and then suspend them from their locations in the network to stop their negative influence without taking down the remaining network.

3 Literature Review

We classify the related works into two main types, namely, community detection and focal structure analysis. We also provide a cursory review of misinformation, disinformation and online fake news.

3.1 Community Detection Algorithms Review

There are many approaches to examining and detecting central users in social networks such as YouTube, Flicker, Twitter, and Facebook, where most central users are identified by posting interesting content to attract their followers, initiating an interesting conversation or posting about a new topic (Al-Rubaye & Menezes, 2016; Alassad, Agarwal, et al., 2019; Briscoe, Appling, Mappus, & Hayes, 2014; Herzig, Mass, & Roitman, 2014; Jones & O'Neill, 2010).

Other researchers measure central users based on their influence in the network, resources they are consuming, and the information users can spread based on their positions in social network (Agarwal, Liu, Tang, & Yu, 2008, 2012; Borgatti, 2005; Chen & Wang, 2009; Kempe & Kleinberg, 2003; Leskovec, Mcglohon, Faloutsos, Glance, & Hurst, 2007; Leskovec, McGlohon, Faloutsos, Glance, & Hurst, 2007; Li, Wang, Sun, & Xia, 2018; Richardson & Domingos, 2002a). Complex Networks on social platforms have been investigated to show how users' power in social networks (Chua, 2014; Kivran-Swaine, Govindan, & Naaman, 2011) can spread, pass, and block information from other users. Methods such as PageRank (Page, Brin, Motwani, & Winograd, 1998) and HITS (Kleinberg, 1999) are robust methods in measuring such factors. Yet another researcher applied these topics in blogs and marketing (Agarwal et al., 2008, 2012) to find influential users that can spread information to a maximum number of users in the network (Richardson & Domingos, 2002b).

Although it is important to study the similarity of individual connected users' attributes in the network, research in identifying community structure led to the development of optimized community detection algorithms. Spectral modularity used linear algebra methods to calculate the complex networks efficiently (Şen et al., 2016; Von Luxburg, 2007; Zafarani et al., 2014). Similarly an approach was used by (Hagen, Member, & Kahng, 1992), to identify the optimum ratio for clustering complex networks. (Blondel, Guillaume, & Lefebvre, 2008) used an empirical approach to get the optimum modularity values in complex networks. Another research method applied a mixed integer linear programming method (Sato & Izunaga, 2018) to find the optimum highest modularity values, using a novel branch and price framework to linearize the problem. However, given all of the research on optimizing a graph's modularity values, this method is still being studied by many researchers where they all summarized that this problem is an NP-hard problem (Java, Joshi, & Finin, 2008; Newman, 2004a, 2006; Newman & Girvan, 2003; Wang, Shen, & Luan, 2008).

3.2 Misinformation, Disinformation and Online Fake News Review

The popularity of social media platforms has increased exponentially in recent years encouraging many academia, marketing agencies, and cybersecurity firms to research and explore the information, behaviors, and impacts generated by these online platforms (Myers, Sharma, Gupta, & Lin, 2014). Online social networks have experienced a surge in negative behavior campaigns such as fake news, misinformation, and disinformation generated by malicious users to achieve their desires. Spreading this type of real-time misleading information to millions of online users has resulted in many negative consequences to politics, economic issues, social behaviors, and people's daily life (Zhang & Ghorbani, 2019) .

Research has been conducted in network structures, intelligence, and tools to outline, distinguish and compartmentalize fake news, misinformation, and disinformation campaigns (Søe, 2018). However, the authors concluded that current algorithms are insufficient and need additional capabilities to handle such topics. There are many fact-checking resources available in terms of news related to politics, technology, business, civic life, social media, and emails (Zhang & Ghorbani, 2019). For example, Hoaxy.iuni.iu.edu (Shao, Ciampaglia, Flammini, & Menczer, 2016) is a framework to check misinformation related to various sources of information on social media, websites, and emails. This website relies on other known reputable websites to check the content, tweets, and any claims about those topics (Zhang & Ghorbani, 2019). Resources such as Factmata.com, Hoax-slayer.com, PolitiFact.com, and Snopes.com are designed to fight online fake news topics, but fighting online fake news, misinformation and disinformation is still a difficult task (Shao et al., 2016; Søe, 2018).

Many efforts have been made to identify and prevent users that participate in misinformation or disinformation campaigns and spread fake news, where suspending these users early, would minimize the negative effects generated by such malicious users. However Shu et al. (2017) (Shu et al., 2017), suggested ways to minimize online fake news by suspending or removing suspicious online accounts and maximizing online true news.

3.3 Focal Structure Analysis Review

The first research published by (Şen et al., 2016) introduced focal structure analysis in social networks. The authors suggested a greedy algorithm to identify focal structures responsible for spreading fake news in social networks. They also found small sets of influential sets of users responsible for influencing thousands of users on Facebook. (Alassad, Agarwal, et al., 2019) presented a bi-level centrality-modularity model to examine intensive groups of co-commenters spreading fake news in a YouTube channel, where the authors explored hidden intensive groups and ranked them for further investigations. (Alassad, Hussain, et al., 2019) found key information spreaders in a complex social network by using a bi-level decomposition optimization method in a YouTube channel spreading fake news about the South China Sea conflict where the authors monitored the impacts of suspending these key sets of spreaders from the network. In an extended study, Alassad et al. (Alassad, Hussain, et al., 2019) used computational social science techniques to identify coordinated cyber threats to smart cities networks. In this research, the authors identified intensive sets of aggressors, measured their power utilizing the deviant cyber flash mob detection method, and then analyzed the network's changes when a focal structure was suspended from the network.

4 Proposed Dataset

In this research, we are proposing two datasets to explain our discoveries and implement the complex analysis as follows:

4.1 Les Misérables Social Network

This dataset contains a coappearance network of characters in the Les Misérables Novel (Hugo, 1887) shown in Figure 3, where this network is considered to explain the bi-level betweenness-modularity model's steps and the complexity analysis. The network's statistics are in Table 4.

4.2 ISIS Network

A Twitter network consisted on 1,453 users and 1,487 links is considered as real-world data set. An initial set of Twitter usernames were provided in a report published by the International Centre for the Study of Radicalization and Political Violence (ICSR) in which they provided a list of individuals who help ISIS disseminate their propaganda on Twitter and other social media platforms (Al-Khateeb & Agarwal, 2014) as presented in Figure 4.

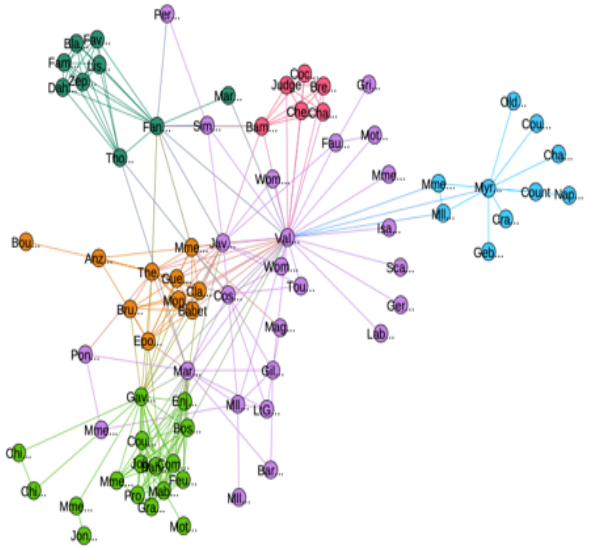


Figure 3: Les Miserabel network, clustered into 6 sets via modularity method.

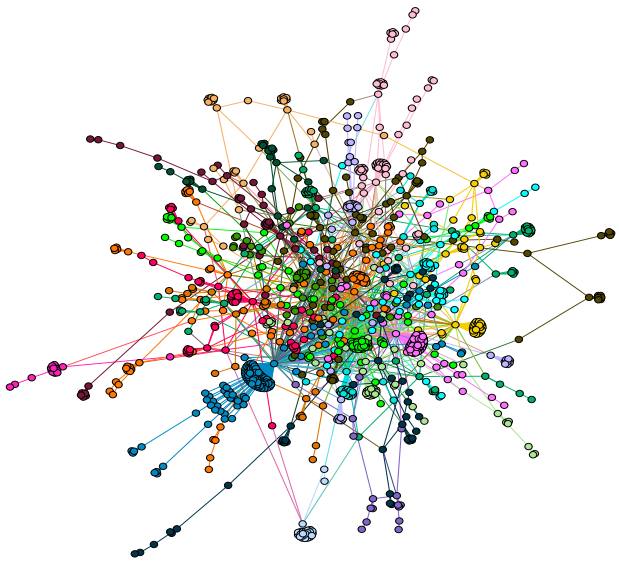


Figure 4: ISIS network, clustered into 40 sets via modularity method.

5 Information Behavior System Design

Users' behavior on online social media is reflected in their activities, interests, and social behaviors. Information using objects such as pictures and video posts that has evidence using facts can be considered truthful and is defined to be accurate (Shu et al., 2017). However, malicious users occupy online platforms to spread negative information such as (fake news, misinformation, disinformation) related to their agendas, political, and marketing gains without true evidence. The essential need is to identify this negative information and how it can be stopped or suspended. This information can harm online users and represents the dark side of online information.

Malicious users can spread negative information across the network individually or as groups of coordinating users working to influence individuals and communities at the same time. For this purpose, we split our analysis into two sections; individual or user-level analysis and group-level analysis. The user-level will investigate the malicious user's behaviors, sources, and power of controlling information flow in the network, and the group-level will investigate the groups' influence on other communities or the entire network.

The problem definition is as follows : given an undirected online social network, $G = (V, E)$, where V is a set of all users in the network, and E represents the links between all users, find κ influential sets of users that can maximize the influence in V, where κ is not given.

5.1 User-Based Level Betweenness Centrality Method

The traditional betweenness centrality method (Freeman, 1977) is the first method employed to study the users' local features. This includes features such as the power to spread information to other users, thereby increasing their ability to influence other followers. This method also identifies the ability to mobilize a crowd in the network, where the more users in the network that depend on this user to communicate, the more power that user has (Faust & Wasserman, 1994) . A high betweenness approach gives the most power to the user in the center of a local star shape network, allowing the user to control other neighbors' links and information. In addition, an overall definition for the betweenness centrality method would be like a real-world network measurement describing a user's influence, resources, and opportunities inside the network (Barrenas, Chavali, Holme, Mobini, & Benson, 2009) (Huang, Sun, Liu, Song, & Weninger, 2011) (Freeman, 1978) (Borgatti & Everett, 2006). By implementing this method, the model will build local communities consisting of a central user and his/her length one neighbors. The betweenness centrality for each user is measured in this research as presented in Eq. (1), and the normalized value $\beta'(v_i)$ is calculated via Eq (2).

$$\beta(v_i) = \sum_{s,t \in V \times V} \frac{V_{s,t}(v_i)}{V_{s,t}} \qquad \forall i \qquad (1)$$

$$\beta'(v_i) = \frac{1}{[(m-1)(m-2)/2]} \sum_{i=1}^{n} b(v_i) \qquad 0 \le \beta'(v_i) \le 1 \qquad (2)$$

The second technique employed in this research is the users' linking behaviors with other users in the networks. The clustering coefficient method (Zafarani et al., 2014) is employed to investigate the relationships generated by the users' length one neighbors. This method will reveal information about the users'' neighbors, identify the users neighbors who are friends of each other and monitor the tight communities a central user can build. Eq (3) is used to measure the clustering coefficient values $\psi(Cv_i)$ for each user's (v_i) local community in this research. The aim of using this method is to include active communities in solution procedure and prevent chain ones.

$$\psi(Cv_i) = \frac{(\#\ of\ Triangles) \times 3}{\#\ of\ Connected\ Triples\ of\ users} \qquad 0 \le \psi(Cv_i) \le 1 \qquad (3)$$

The outputs from this level will be sets of influential users, connected to active neighbors that maximized the betweenness centrality values, as shown in Figure 5. Each of these sets of users will be exported to the next analysis level by a special binary vector parameter called $\underset{k \le n}{\overrightarrow{c\delta}_{\iota n \times k}}$, where this vector is a $n \times k$ binary matrix expanded by local sets $\mathbb{C}(\delta_{v_i})$ after each iteration. In the other words, this vector will transfer the optimal solutions from the user-iteratively to the group-level, passing a new set of influential users joined to the previous solution after many iterations. Likewise, it consists of k sets of users that maximized the betweenness centrality and need to be exported to the group-level to test their global influence.

In the results of this level, we are measuring the betweenness centrality values $\beta'(v_i)$ and the clustering coefficient values $\psi(Cv_i)$ for each user, but the model will map those values to their correspondent communities or their set of users $\mathbb{C}(C\delta_{v_i})$. The community $\mathbb{C}$ is the set of users that is connected to user (v_i) or the set of users that maximized the betweenness centrality value and has active users. $\mathbb{C}(C\delta_{v_i})$ is merged into the binary matrix $\underset{k \le n}{\overrightarrow{c\delta}_{\iota n \times k}}$ as a vector after i^{th} iterations as shown in Eq (4) bellow and Figure 5.

$$\underset{k \le n}{\overrightarrow{c\delta}_{\iota n \times k}} = \underset{k \le n}{\overrightarrow{c\delta}_{\iota n \times k-1}} \bigcup \mathbb{C}(\delta_{Cv_i}) \qquad \forall i \qquad (4)$$

The methods used in this section are essential to study each users' behaviors, resources, actions and their neighbors' activities. By exporting active communities from the user-level to the group-level, model will do all necessary numerical measurements to find the best focal structure candidates that need to maximize the network's sparsity. Next, the user-level will use the binary vector $\underset{k \le n}{\overrightarrow{c\delta}_{\iota n \times k}}$ to integrate with the group-level, which includes the

influential user and his/her active neighbors. Figure 5 shows the information exchange procedure between the user-level and the group-level. The aim and the objective function shown in the user-level is to maximize the betweenness centrality values $\beta'(v_i)$ subject to the user's local community clustering coefficient values $\psi(Cv_i)$. This procedure helps to identify the central influential user connected to active neighbors, and then measure their influences and abilities to spread information to the entire network.

5.2 Group-Based Level, Spectral Modularity Method

This section is designed to find the influential sets of users that, jointly, will maximize the modularity values in the network. The group-based function finds the sets of users that have solid connections to other users in the network that are able to influence many others in different parts of the network. These central sets of users, because of their location, they can control information flow to maximize spread in the network. This level of the model is designed to import the local set of users' vector $\overrightarrow{\overline{c\delta}}_{\substack{\iota n\times k\\ k\leq n}}$ identified in the user-level and then search for the best set of users that will jointly maximize the modularity value in the network.

For this purpose, the spectral modularity method (Newman, 2006; Tsung et al., 2017) is employed to simplify the numerical complexity analysis, help generalize the impacts caused by each malicious sets on the entire network, and identify sets that can influence the maximum number of users in different sets (communities) as shown in Figure 5.

The purpose of the group-level objective function is to maximize the spectral modularity values ϱ_j as presented in Figure 5, subject to the sets of users that maximized the betweenness centrality imported from the user-level $\overrightarrow{\overline{c\delta}}_{\substack{\iota n\times k\\ k\leq n}}$ as shown in Eq (6). Then, the model will perform a search of all possible solutions to find the sets of users that will maximize the group-level objective function as shown in Eq (5), where this constraint calculates the spectral modularity ϱ_{jx} at the group-level for x number of iterations and for a given number of sub-graphs that has $\xi_{jx} \in R^{n\times k}, k = \{1,2,\ldots, n\}$ partitions.

Then, the model should find the best sets of users to join $\overrightarrow{\overline{c\delta}}_{\substack{\iota n\times k\\ k\leq n}}$ from the user-level that have the best set of users that can sparse the network as indicated in Eq (6), where ξ_{jx} is the join between the sets of users imported from the user-level $\overrightarrow{\overline{c\delta}}_{\substack{\iota n\times k\\ k\leq n}}$ and the candidate sets of users δ_{jx} that presumably will maximize the sparsity when they will join the matrix. Constraint (7) is to get the maximum modularity value $\overline{\mu_{jx}^{Q}}$ from the group-level and $\mathbb{C}\varrho_{jx}$ will export the set of users $\delta_{jx}(\overline{\mu_{jx}^{Q}})$ as the best solution that maximized the network's spectral modularity value. The group-level use a binary vector parameter $\mathbb{C}\varrho_{jx}^{M}$ to interact with user-level, where $\mathbb{C}\varrho_{jx}^{M}$ is the set of users that maximized the modularity values when they joined the network as shown in Eq (8). The selected $\mathbb{C}\varrho_{jx}^{M}$ is the focal structure candidate that met all criteria from both levels.

$$\varrho_{jx} = \frac{1}{2m}\, Tr\left(\xi_{jx} B \xi_{jx}^{T}\right) \qquad \forall j, x \qquad (5)$$

$$\xi_{jx} = \{\, \overrightarrow{\overline{c\delta}}_{\substack{\iota n\times k\\ k\leq n}} \cup\ \delta_{jx} |\ \overrightarrow{\overline{c\delta}}_{\substack{\iota n\times k,\\ k\leq n}} \neq\ \delta_{jx}\} \qquad \forall j, x \qquad (6)$$

$$\overline{\mu_{jx}^{Q}} = \max\{\varrho_{1x}, \varrho_{2x}, \ldots, \varrho_{jx}\} \qquad \forall j, x \qquad (7)$$

$$\mathbb{C}\varrho_{jx} = \delta_{jx}(\overline{\mu_{jx}^{Q}}) \qquad \forall j, x \qquad (8)$$

Figure 5 shows the integration procedure between the traditional community detection methods decomposed into two levels of analysis as explained earlier. The export/import binary vector parameters are employed to handle the information exchange between the two separated levels and provide a method to optimize the best sets selections in both levels. In addition, this procedure will simplify the numerical computations' complexity, linearize the problem

in both levels, and will help to avoid the modularity method's complexities in finding the number of required communities and exploring small active sets of users (Wang et al., 2008). Also, the model terminates the calculation when the modularity values decrease or the model exhausts all possible solutions.

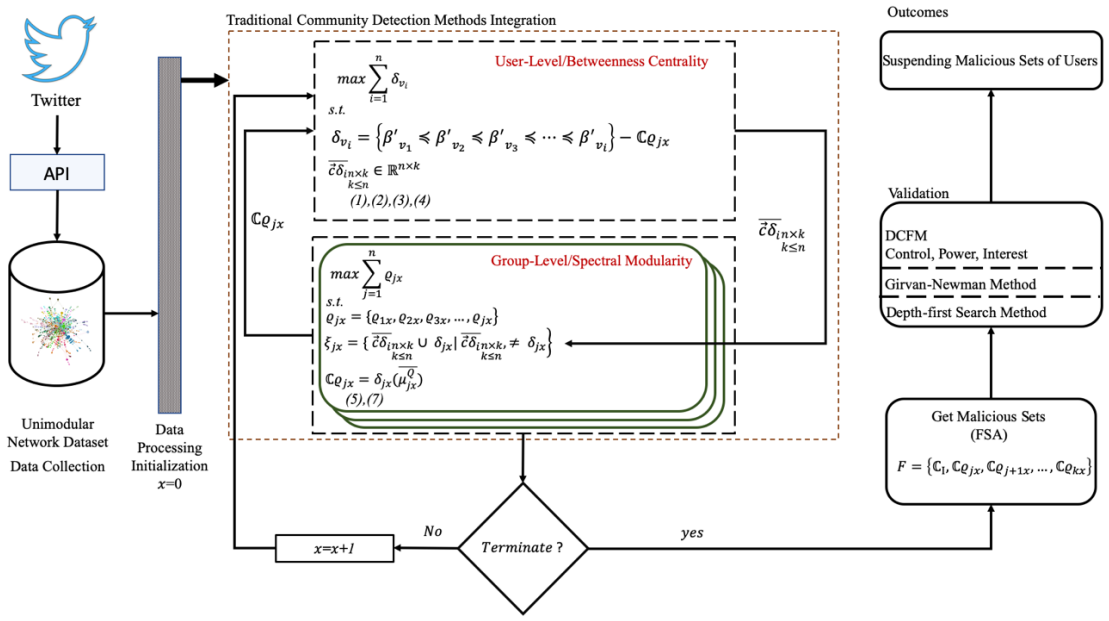


Figure 5: Focal Structure Analysis Model, integration of the traditional Betweenness-Centrality and Modularity Methods.

5.3 DCFM

The Deviant Cyber Flash Mob (DCFM) phenomenon can be considered a form of a cyber-collective action that is defined as an action aiming to improve a group's conditions (such as, status or power). If we can identify those strong influential groups within a network that are organizing a DCFM, we can design counter measures to stop the aggressors from attacking networks, such as smart city infrastructure. Previous work by Al-khateeb and Agarwal (Al-Khateeb & Agarwal, 2014) developed a collective action based theoretical model which identified factors to predict success or failure of a DCFM.

$$\text{Control (C)} \qquad \text{In} - \text{degree Centrality} \qquad (9)$$

$$\text{Interest (I)} \qquad (\text{Number of retweets} + \text{mentions}) \Big/ (\text{Total number of tweets}) \qquad (10)$$

$$\text{Power(P)} \qquad \text{Control (C)} \times \text{Interest (I)} \qquad (11)$$

In their model, the identified factors are – Utility (U) (the benefits an individual gains if the DCFM succeeds or fails), Interest (I) (how much interest an aggressor has based on the utility gained), Control (C) (how much control the aggressor has on the outcome of the DCFM), and Power (P) (how powerful an aggressor is in the group). In this study, we calculate the structural characteristics of our sample DCFM network and assess the impact of these collective action measurements (i.e., I, C, and P) using our Focal Structure Analysis (FSA) model.

6 Model's Strategies and Techniques, Applied to a Small Real Social Network

In this section, we employed a small social network explaining the complexity analysis, utilizing the Les Miserable novel dataset described in section 4.1.

6.1 User-Level Analysis:

In this section, the user's local features are measured, and the model will begin collecting the necessary measurements from the network based on the criteria mentioned in the user-level. The model will identify the influential users that have high betweenness centrality value based on the user's position to deliver the maximum amount of information to other users (Zafarani et al., 2014). Figure 6 shows the number of neighbors belonging to each user in the network, where one user is able to spread information to more than 35 users in the network as influential user.

In addition to the betweenness centrality, the model considers the in-between neighbors' friendships and collected information about each user's neighbors. The clustering coefficient method is able to measure if the user's friends-of-friends are also his/her friends. Figure 7 shows the results from the clustering coefficient method. For example, user # 11 can spread information to more than 35 other users, but his surrounding users are barely connected or hardly worked together in the Les Miserable novel as shown in Figures 6 and 7 (Hugo, 1887).

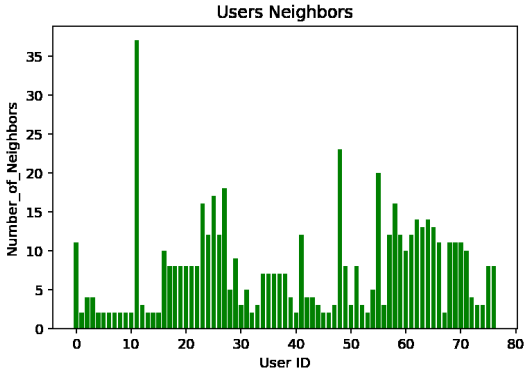


Figure 6: User's neighbors.

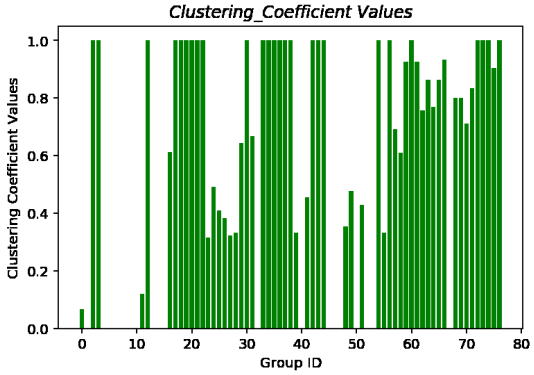


Figure 7: Local sets' clustering coefficient values.

Also, Figure 7 shows the other local communities' status, where many of the users are fully connected and others have zero values. Utilizing this step will help to filter out some users, where any local community that has a zero clustering coefficient value (such as a chain network) is not a social network and the model will exclude these users from the solution procedure. For example, users # 1, 3,4,5,6,7,8,9, and 10, were excluded from the solution, and they will not affect the final outcomes (Zafarani et al., 2014).

In the next step, the model will introduce the highest central user as an initialization to the group-level analysis to find the best joint sets of users that can return the highest spectral modularity value. This step can be implemented by using the binary vector $\overrightarrow{\overline{c\delta}_0}_{77\times 1} = \mathbb{C}(\delta_{Cv_{11}})$ as show in Figure 5, representing user # 11 and his neighbors, where this user has the highest betweenness centrality value $\beta'(v_{11}) = 0.569$ and his connected neighbors return $\psi(Cv_{11}) = 0.715$ clustering coefficient value as shown above.

6.2 Group-Level Analysis

The spectral modularity method proposed by (Freeman, 1977), is used to measure the network modularity value in an integrated process with the user-level. The objective in this section is to evaluate the sets' abilities to maximize the network's modularity value (Wang et al., 2008), where it is the process of searching for key sets that can spread

information to the maximum number of other users in the network (Hagen et al., 1992; Newman, 2004a; Tsung et al., 2017; Von Luxburg, 2007).

In the beginning the model is getting the binary vector $\overrightarrow{\overline{c\delta}}_{\iota_{77\times k}}$ from the user-level as show in Figure 5, and then will iteratively search for all possible solutions to find the best set of users δ_{jx} that will join vector $\overrightarrow{\overline{c\delta}}_{\iota_{77\times k}}$, and will maximize the spectral modularity values ϱ_{jx} as shown in Eq (5) and Figure 5.

In next step, the model will get the optimum spectral modularity value $\overline{\mu_{jx}^{Q}}$ from this level by using Eq (7). The best joint set of users $\delta_{jx}(\overline{\mu_{jx}^{Q}})$ are introduced by Eq (8) as FSA # 1, and the model will export this set of users to the user-level using the binary vector $\mathbb{C}\varrho_{jx}$ as shown in Eq (8). The model will continue the information exchange between these two levels until the model exhausts all possible solutions or the modularity values decreases.

In this section, the model explored twelve focal structures from the network that can maximize the network's sparsity. The Bi-level betweenness-modularity model interactions concluded that these twelve powerful sets are unique structures and include important members acting in many parts throughout the novel and can influence other users in this social network. Table 1 shows the identified focal structures and their associated users.

Table 1: Focal sturcture sets memebers.

FSA ID	Members
FSA 1	Woman2, Cosette, Toussaint, Valjean, Javert
FSA 2	MmeMagloire, Myriel, Valjean, MlleBaptistine
FSA 3	Valjean, Marguerite, Fantine
FSA 4	Tholomyes, Fantine, Dahlia, Zephine, Blacheville, Favourite, Fameuil, Listolier
FSA 5	Perpetue, Simplice, Fantine
FSA 6	Chenildieu, Brevet, Judge, Valjean, Cochepaille, Bamatabois, Champmathieu
FSA 7	MmeThenardier, Thenardier, Anzelma, Eponine
FSA 8	Valjean, MotherInnocent, Fauchelevent
FSA 9	BaronessT, Marius, Gillenormand
FSA 10	Prouvaire, Feuilly, Grantaire, Gavroche, Combeferre, Courfeyrac, Bahorel, Joly, Bossuet, Enjolras
FSA 11	Child2, Gavroche, Child1
FSA 12	Montparnasse, Gavroche, Eponine, Claquesous, Thenardier, Gueulemer, Babet, Brujon

6.3 Validation

To validate the above focal structure analysis and quantitatively measure their impacts in the network, we used two methods to calculate the sets' influence and power when each focal structure set is suspended from the network. This procedure exposes information about each focal structures' activities such as the number of locally influenced users and the number of groups influenced by each focal structure. It also reveals information to the researcher about where and what focal structures are more active than others in the network.

In addition, the size of a focal structure is an important factor. If the suspended focal structure is a small set but can maximize the network's sparsity value, then such set is considered a powerful focal structure consisting of influential users. These small focal structures have the ability to control the information flow to many other users in the network more efficiently than larger size focal structures with low influence.

The model utilizes the Newman-Girvan modularity method (Clauset et al., 2004; Newman, 2004a) to measure the general impacts that each focal structure has on the network and to monitor the changes in the communities after suspending each focal structure in the network. Suspending the influential focal structures will change the network's structure, disconnect many other users, and cause other groups to disappear altogether from the network. As shown in Table 2, suspending each focal structure will change the network's structure incredibly, creating new sets of communities as measured modularity method, and disconnect many users from the network.

The second method used to validate the model's outcomes is to measure the local impacts generated by suspending each focal structure. The model can measure the number of users that will lose their connection to other users in the network if any focal structure is suspended from the network. For this purpose, a depth-first search and linear graph algorithm (Tarjan, 1972) is employed to measure the number of weakly connected users before and after suspending a focal structure from the network as show in Table 2.

From Table 2 above, the analysis identified that FSA #1 consisted of five users maximized the network's modularity value into (0.615), which is (14%) higher than the original modularity value (0.538). Also, FSA # 2 consisted of only four nodes maximized the number of disconnected characters (13 weakly connected) from the network when its members were suspended from the network. FSA #2 can also sparse the network into 19 other communities which is (72%) higher than the original number of communities (11). likewise, (Tarjan, 1972) found that FSA # 2 will maximize the number of weakly connected users, and this set will increase the weakly connected users from 1 to 13 users.

Table 2: Focal structures impacts on the network.

FSA #	Number of nodes	Modularity Value	Number of Communities	Weakly Connected Nodes
1	5	0.615	17	9
2	4	0.566	19	13
3	3	0.592	14	7
4	8	0.492	11	1
5	3	0.545	11	1
6	6	0.557	12	7
7	4	0.556	6	2
8	3	0.592	13	8
9	3	0.576	8	1
10	10	0.534	9	4
11	3	0.572	8	2
12	8	0.579	9	4

7 Real-World Scenario - Resolving the Negative Influence in ISIS Network

To measure the model's effectiveness in real-world scenarios, we applied the above steps to different social media networks as shown in Figure 4 and Table 4. The analysis conducted on the focal structures impacts both the user and network level. For this section, we analyze the ISIS network shown in section 4.2 and Figure 4. We will also use the Deviant Cyber Flash Mob (DCFM) model developed by Al-khateeb and Agarwal (Al-Khateeb & Agarwal, 2014) to calculate the power, interest, and control for each of the focal structures. The integration of the DCFM model into the analysis will be used as an additional support measure to validate the betweenness-modularity results from the real-world networks such as ISIS network shown in section 4.2 and Figure 4.

7.1 User-Level Analysis- ISIS Network

The model will begin by analyzing the network and identifying the users. The next step is to calculate the user's power, betweenness centrality and the clustering coefficient for each user and his/her neighbors. The power of each user is measured by employing the collective action-based DCFM model developed by Al-khateeb et al. (Al-khateeb & Agarwal, 2019; Al-Khateeb & Agarwal, 2014) and the betweenness centrality method measures a user's ability to spread information to other users (Zafarani et al., 2014). Figure 8 shows the number of users' neighbors in the network, where one user is shown to be have 150 neighbors, and thus the ability to spread information to more than 150 other users.

In addition to the neighbors' friendship measurement, the information about each user's local community is considered by calculating the clustering coefficient as shown in Figure 9. For example, user # 0 can spread information to more than 150 other users, however his local community has 0.5 clustering coefficient value, which means that some users who are friends to user # 0 are also friends of each other and can exchange information between them (Tarjan, 1972; Zafarani et al., 2014). The final analysis from this level of our model uses not only the betweenness

centrality and clustering coefficient methods, but also the interest and power of malicious actors as calculated by the DCFM method as explained in section 8.1. Figure 10 shows the top twenty powerful sets of users measured by the DCFM method, where these users have the ability and mutual interest to spread conspiracy theories, perform cyberattacks, deceive other users, or disseminate misinformation or disinformation throughout the network.

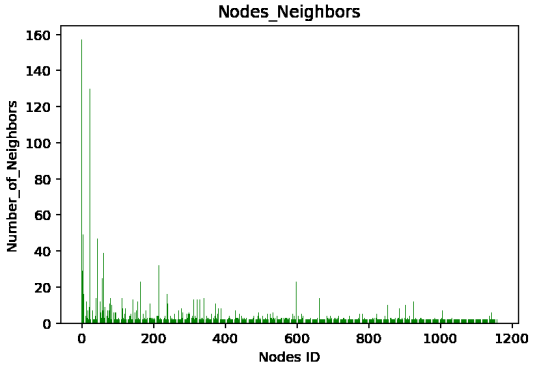


Figure 8: Users' neighbors.

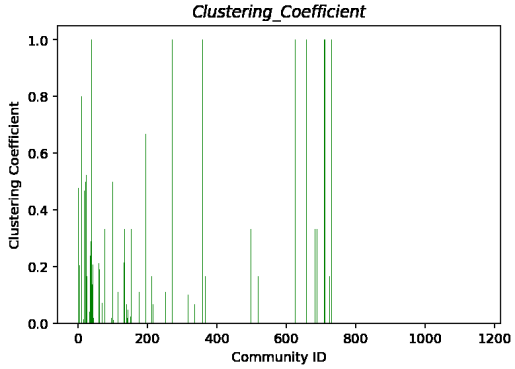


Figure 9: local sets' clustering coefficient values.

The result of using these two methods, i.e., the betweenness centrality with clustering coefficient, and DCFM power calculations, identifies small communities. These small communities are classified as sets of active local malicious groups consisting of highly influential users that have active neighbors (i.e., can communicate with each other). The measurements from these two methods will be exported to the group-level analysis to measure the sets ability to maximize the network's sparsity and their ability to communicate to other users in different groups.

7.2 Group-Level Analysis- ISIS Network

The spectral modularity method is used to measure the graph's sparsity which inherits the active users' groups from the previous, user-level. The objective of this is to maximize the network's modularity value and find key malicious sets of users that can spread information to the maximum number of users in the network. In other words, the second level objective is designed to complete the procedure of stopping negative information dissemination to the entire network by finding the sets of key sets of radical spreaders in the network. These malicious sets of users are often hidden in the network, and can control information flow to the maximum number of users in a network. Removing or early suspending them from the network would show the ability to stop the dissemination of misinformation or disinformation in a social media network.

This level of the model identified sixty-one focal structures hidden in the network that met the criteria mentioned in section 5. These intensive malicious sets include highly central users that have the power to control the information flow to many other users in the network and have enough resources to enable them to gain access, structurally, to different parts of the network. Their resources are enough to influence other users to participate in malicious activities such as anti-social behaviors, radical actions, cyberattacks, and other actions as explained in Figure 1.

In addition, this level of the analysis is about the sets' power to control information flow to other users in the network. Figure 11 presents the malicious sets' average betweenness centrality values. These values provide evidence on active focal structures in the network. These focal structures are active sets that have high betweenness centrality values and can influence the maximum number of users in the network by using their active members to coordinate and access different parts of the network. Therefore, these sets are not only intra-set active users, but they can control information flow to many other inter-set users in different parts of the network.

In summary, the network-level identifies the influential sets of users that have the highest ability to disseminate information through social networks such as Twitter. These sets consist of influential users that can control the information flow to other users in the network and have enough resources to participate in different groups in the network. Since these sets have different abilities and structural statistics, we measured their power and validated their abilities to disperse the network if they were suspended from the network as explained in the following sections.

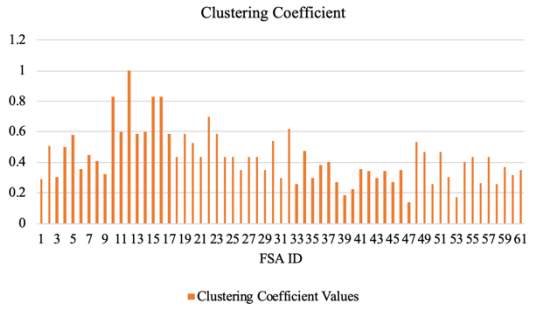


Figure 10: FSA sets' Avg. clustering coefficient values.

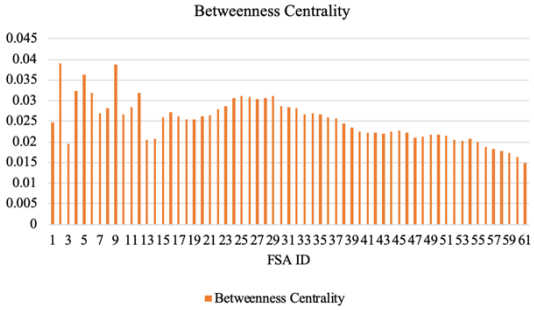


Figure 11: FSA sets' betweenness centrality values.

8 Validation- ISIS Network

The validation procedure includes the results from three different methods. The first method is related to the sets' power, interest and control measured by DCFM method. The second and third validation procedures are the modularity method and Depth-First Search method respectively.

8.1 Focal Structure Interest and Power

To demonstrate the significance of focal structure sets, we applied the DCFM model to our ISIS Twitter network shown in Figure 4. We crawled all the usernames' friends and followers in the network then cross-referenced them with another dataset collected during three beheading events conducted by ISIS in Egypt, Libya, and Palestine (Al-Khateeb & Agarwal, 2014). For the users in the resultant network, we calculated control, interest, and power using equations (9,10, and 11) to estimate the power of each individual in the network. We built the communication network for these users based on each user's control in the network, then ran our model to evaluate the focal structures within the network. These focal structures are ranked based on the sum of power for all users within that focal structure as shown in Figure 13. The model identified the highly influential malicious sets of users in the dataset that can maximize misinformation spread, influence a maximum number of users (e.g., with radical agendas), and includes powerful users acting in different groups as shown in Figure 14.

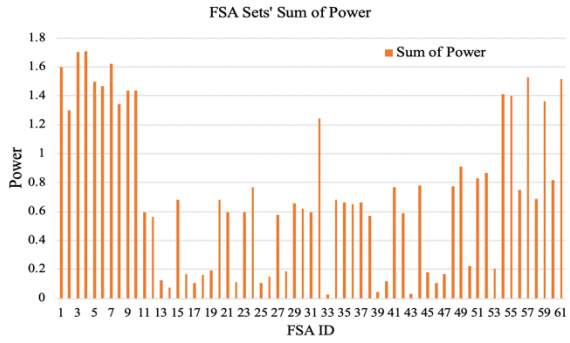


Figure 12: FSA sets' sum of power by DCFM method.

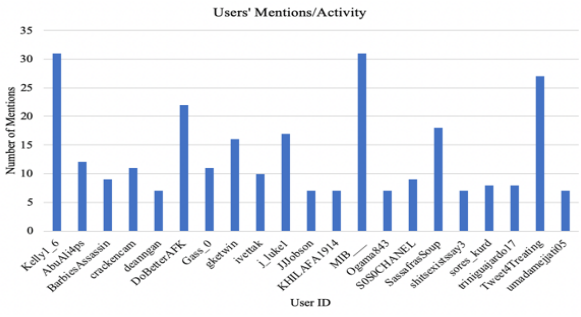


Figure 13: Top 20 malicious influential users by DCFM method.

This part of the procedure provides robust support to the model's findings from both the user-level and network-level, where the user-level only investigates the users' aspects as shown in Figure 13, and the network-level investigates the group of users in the network as shown in Figure 12. From this step we can measure the abilities of malicious sets of users to disseminate misinformation or disinformation in a Twitter network. In addition, this

procedure provides a good path and strong explanation to narrow down the number of sets for further investigations. For example, in Figure 12, the reader can see sets that have low power relative to the rest of the other sets in network, such as FSA sets #29 and #25. These sets are less likely to produce large influences in the network due to their lower power measures. However, other sets with high power such as FSA # 4, and FSA # 3 are essential for further in-depth studies.

The interconnection between pairwise focal structures reveals a spoke and hub communication structure, where a focal structure can convey information to other groups who then could carry out operations to other focal structures as shown in Figure 14. The DCFM method calculated the focal structure's power (influence), whereby the more power they have the darker the sets' color. This part of the analysis could identify how easy it is for a focal structure to direct other members of the network to direct malicious activities or host different kinds of campaigns in different parts of the network.

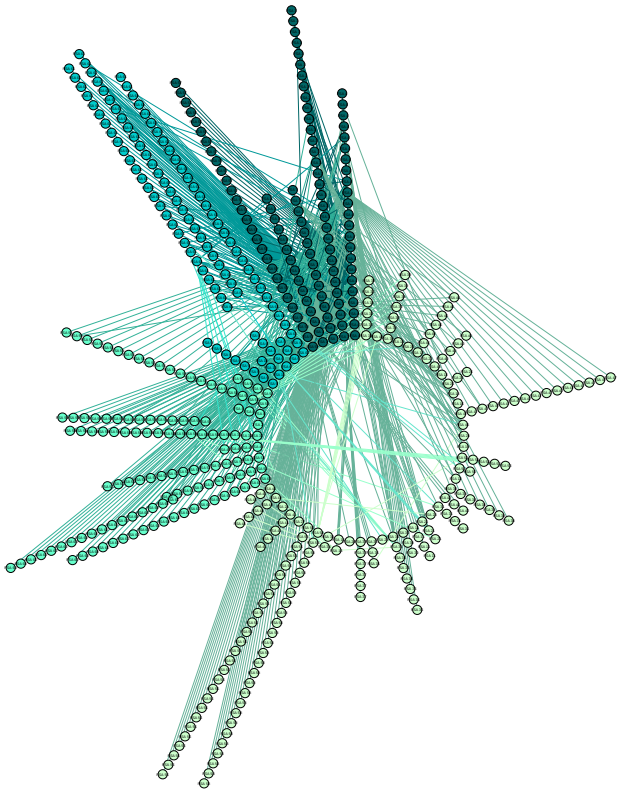


Figure 14: Focal structure power measured by DCFM method.

8.2 Network Sparsity-ISIS Network

This section measures the negative impacts caused by each malicious focal structure at the network level, where it identifies a malicious set of coordinating users' activities. For example, this method could expose information about locations of activities, the number of influenced followers, the number of other groups each malicious set can influence, and where and what malicious sets are more active than others.

For this step, the modularity method proposed by (Girvan & Newman, 2002a) is employed to quantitatively measure the network changes when each focal structure is excluded from the network and compare the results to the original network. The modularity method (Girvan & Newman, 2002a) returns a value of (0.5866) and identified 40 different groups in the network originally as shown in Table 4.

In the next step, we suspended one focal structure at a time and measured the change in the original modularity value and the number of groups as shown in Table 3. For example, FSA # 4, is the most powerful set measured by DCFM was suspended from the network, where this set incredibly sparse the network into (380) other communities which is (89%) increase in the network's sparsity. This set maximized the modularity valued into (0.83) which is (54%) higher than the original value as shown in Figure 15. Suspending such important focal structure has only 24 users is way feasible than shutting down the entire network.

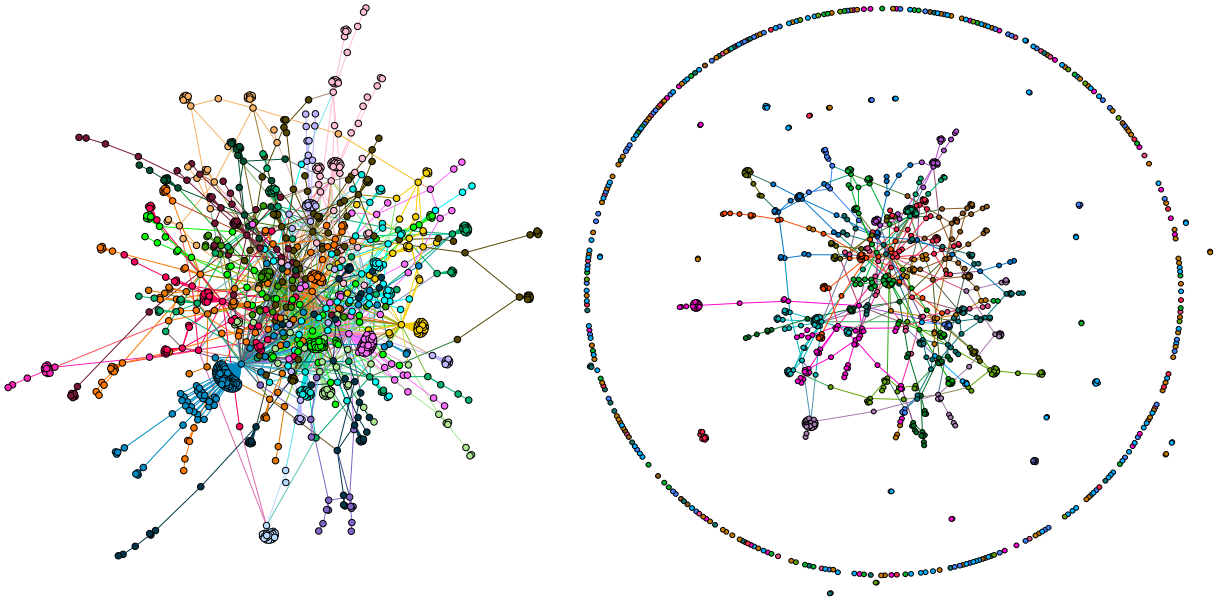


Figure 15: ISIS network before and after suspending FSA # 4.

Table 3 shows the rest of the analysis to other focal structures, where these malicious sets were able to maximize the modularity values in the interval of [0.719-0.83] and increased the network sparsity into (414) groups. Other advantages to suspending these users are related to stopping the spread of misinformation or disinformation by malicious actors using online social media platforms as tools to influence many other users. This method identified the malicious sets' activity locations, and helped to expose their focus, movements, and how many other groups are influenced by their position in the network as shown in Table 3. For example, FSA # 4 is a small group but points to 24 influential users in different parts of the network that can influence 13 other groups in the network.

8.3 Weakly Connected Users- ISIS Network

In this section, we are calculating the local changes caused by malicious sets, and measure the number of other users in the network could be influenced. Similarly, we are investigating the affected users will lose their connection to the network when a malicious set is suspended. These steps will evaluate the impacts generated from each malicious set on other users from other different parts using the online social media platform.

For this purpose, we used the Depth-First Search method proposed by Tarjan et al. (Tarjan, 1972). Local users will be separated from the network if any malicious set is suspended from the network. For example, FSA # 4 is influencing 357 users in the network as shown in Table 3, and if this FSA set was suspended, it would impact information flow to other 357 users. This would obviously help to stop fake news spreading to these users if we stopped this malicious set. In addition, this set increased the number of weakly connected users from 1 in the original network to 357 weakly connected users after suspending FSA # 4. Table 3 shows the rest of the analysis when the model suspends other focal structures from the network.

Table 3: Focal structures impact inside the network.

FSA ID	Sum of power	Count of users	# of Weakly conn. users	Count of comm.	Max modularity value	FSA allocation
4	1.7091	23	357	380	0.83	13
3	1.7015	42	394	414	0.825	12
7	1.6221	25	326	348	0.789	7
1	1.5966	24	280	304	0.78	5
57	1.5288	47	256	280	0.811	7
61	1.5177	130	278	300	0.825	9
5	1.4974	16	284	313	0.776	2
6	1.4679	17	247	276	0.775	2
10	1.4391	20	245	269	0.768	1
9	1.4368	13	239	266	0.775	2
54	1.4149	15	240	267	0.756	2
55	1.4009	49	261	282	0.784	3
59	1.3625	54	233	259	0.797	4
8	1.3327	16	219	246	0.735	2
2	1.301	9	171	202	0.719	1
32	1.2455	13	145	166	0.725	1
49	0.909	13	161	181	0.751	1
52	0.8689	32	73	95	0.729	2
51	0.8288	25	161	184	0.734	1
60	0.819	76	115	137	0.767	5

8.4 Comparison Analysis

The last section in this analysis is used to present the different experiments employed to verify the model's behaviors and validate the outcomes based on different types of networks. Table 4 shows the results from different small well known social networks such as the Karate club network (Newman, 2004a, 2004b), Dolphins social network (Newman, 2004a, 2004b), and Les Misérables network (Hugo, 1887). In addition, complex social networks are included in experiments, where a Co-commenter YouTube network (Alassad, Agarwal, et al., 2019), Saudi Arabia Women activities network (Şen et al., 2016), a YouTube Channel spreading fake news about South China conflicts (Alassad, Hussain, et al., 2019; Hussain, Tokdemir, Agarwal, & Al-Khateeb, 2018), and an ISIS network are used to test the betweenness-modularity model's performance.

Table 4 presents the network statistics such as the number of nodes, edges, and focal structures that were found by the proposed model in each network. In the second part of the table, we compared the original networks' modularity values, the number of communities and number of weakly connected users to the results from the betweenness-modularity model. For example, in the Saudi Arabia Women activities network, the betweenness-modularity model was able to maximize the network's modularity value from 0.685 to 0.841 and increase the network's groups from 5

to 325 groups and disconnect up to 325 local users from the network. We have tested other social networks with different sizes as shown in Table 4.

Table 4: Focal structure analysis experimental results on different social networks.

Network	Nodes	Edges	# FSA	Modularity Value		community		Users	
				original	FSA	original	FSA	Original	FSA
Karate Club	34	78	8	0.401	0.538	5	8	1	6
Dolphins	62	159	15	0.519	0.564	5	15	1	7
Les Misérables	77	254	12	0.538	0.615	11	19	1	13
Saudi Arabia	407	457	13	0.685	0.841	14	325	1	325
YouTube co-commenter	9,661	4.4 M	34	0.274	0.577	4	700	1	690
South China Fake News Channel	8,477	47,265	30	0.27	0.656	5	1870	1	1880
ISIS Network	1,453	1,487	61	0. 538	0.86	40	497	1	478

In the next step, we wanted to test the model's performance using a different centrality method such as degree centrality (Zafarani et al., 2014). We compared the results from the model presented in this paper to centrality-modularity, closeness-modularity, eigenvector-modularity results. We also considered the same networks presented in Table 4 above to investigate the model's performance to help to decide which centrality method works better. We applied the centrality methods analysis and then compared the results to the betweenness-modularity results in terms of maximum modularity value (network's sparsity), local users changes, and groups analysis. Finally, we compared the top 20 powerful malicious sets in ISIS network's as shown in Figure 16.

- **Users Analysis:** in this part of the analysis, all models showed similar behaviors at the individual level, where the models returned similar/equal influence on the same number of users. However, the degree centrality model returned low number at ISIS network and closeness centrality outcomes was better at Saudi Arabia, YouTube and ISIS network. The rest networks are showing close results as shown in Figure 16-a.

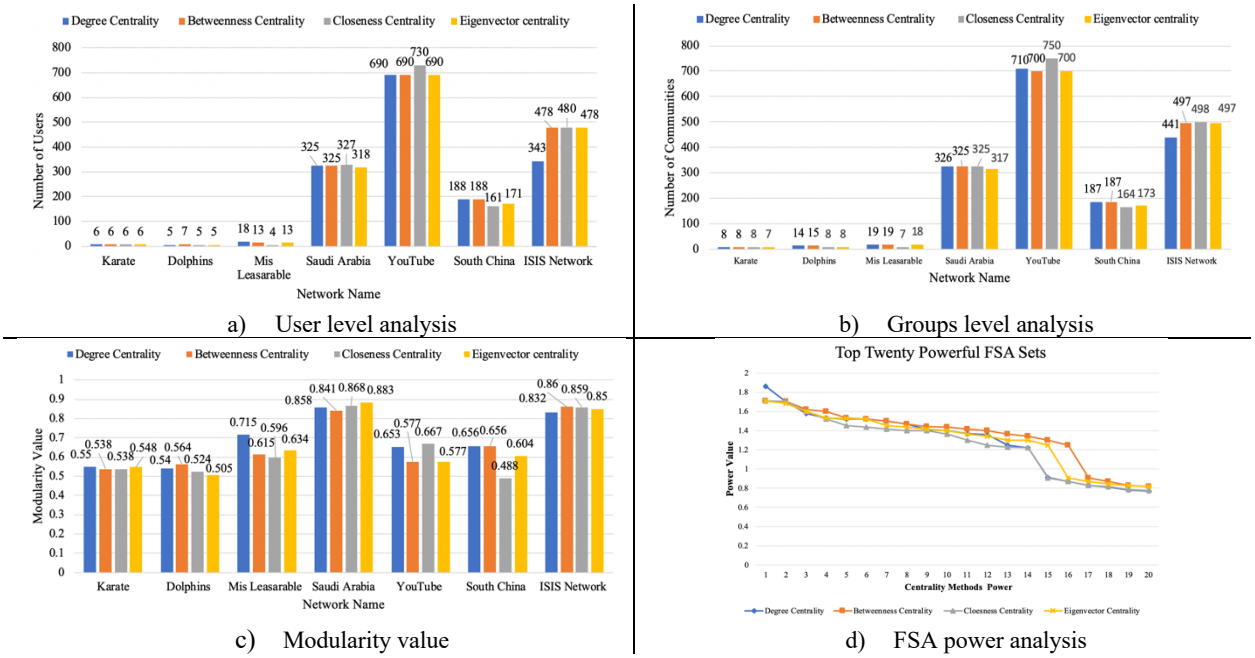
- **Group analysis:** in the community influence, all models showed similar behaviors, where the models where able to find FSA sets have similar/equal influence on number of groups in the network. However, the degree centrality model returned low number of groups at the ISIS network and closeness centrality model was better at YouTube and ISIS network. The rest networks are showing close results as shown in Figure 16-b.

- **Networks' modularity:** in this level of evaluation the degree-modularity maximized the modularity values at "Karate", and Les Misérables network. Equal/similar performance at the rest of the network, except at South China network the Closeness centrality returned low level value as shown in Figure 16-c.

- **Power, Interest, Control:** in this level the top twenty malicious sets' power from the ISIS network measured and compared based on different centrality methods. In this analysis all method showed very similar performances except the top powerful set from degree-modularity model, degree centrality at the first level dominated the all other models' power and then we see a similar behaviors from all other models as shown in Figure 16-d. However, the power dropped at level 14-17 from all methods and meet at level 20th.

-

In the summary of Figure 16, the analysis showed relatively small differences between all four models in all networks or we see produced equal behaviors in in few results. This would allow the analyzer a degree of freedom in using either one of the centrality methods would returned similar influences and powers as explained above and presented in Figure 16. This provides an extra level of trust to the proposed model, the focal structure behaviors, and the influence measured by our procedure, where the bi-level model is able to select the hidden malicious influential sets of users regardless of the occupied centrality method. The model will find influential sets that can maximize the network's sparsity, and at the same time include central active users.



a) User level analysis

b) Groups level analysis

c) Modularity value

d) FSA power analysis

Figure 16: Focal structure analysis performance utilizing different centrality methods.

9 Conclusion

In this paper, we explained the integrated Bi-level max-max model consisting of the user-level analysis (betweenness centrality) and the group-level analysis (spectral modularity) to identify malicious sets of users in a Twitter ISIS network. In addition, different well-known methods were employed to validate the results and the influence generated by each of the identified set, where for the resulted sets we measured their influence on the entire network and the other local users from different parts of the network. Also, we implemented the DCFM method to study the sets' power, interest, control to monitor their overall pictures of malicious strategies in the network.

The model in this paper identified malicious sets of coordinated users able to convince their followers to adopt malicious agendas and participate in radical behaviors, cyberattacks, and possibly demonstrations in different locations in big cities or even smart cities.

This model proposed integrated two traditional well-known community detection methods to stop negative information dissemination in online complex social networks, where suspending these malicious sets of users would not harm other users in network, would prevent malicious multiple cyberattacks, and can decrease the infrastructure networks vulnerability. Also, in this paper we investigated other centrality methods such as degree centrality, closeness centrality and eigenvector centrality methods and compared the results.

Future works will investigate the focal structures strength during a protest campaigns' lifecycle and be considered a supplementary step to validate the model's results.

Acknowledgment

This research is funded in part by the U.S. National Science Foundation (OIA-1920920, IIS-1636933, ACI-1429160,and IIS-1110868), U.S. Office of Naval Research (N00014-10-1-0091, N00014-14-1-0489,N00014-15-P-1187, N00014-16-1-2016, N00014-16-1-2412, N00014-17-1-2605, N00014-17-1-2675,N00014-19-1-2336), U.S. Air Force Research Lab, U.S. Army Research Office (W911NF-16-1-0189), U.S.Defense Advanced Research Projects Agency (W31P4Q-17-C-0059), Arkansas Research Alliance, and the Jerry L. Maulden/Entergy Endowment at the University of Arkansas at Little Rock. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding organizations. The researchers gratefully acknowledge the support.

Reference

Agarwal, N., Liu, H., Tang, L., & Yu, P. S. (2008). Identifying the Influential Bloggers in a Community. *In Proceedings of the 2008 International Conference on Web Search and Data Mining*, 207–218.

Agarwal, N., Liu, H., Tang, L., & Yu, P. S. (2012). Modeling blogger influence in a community. *Social Network Analysis and Mining*, *2*(2), 139–162. https://doi.org/10.1007/s13278-011-0039-3

Al-khateeb, S., & Agarwal, N. (2019). *Deviance in Social Media and Social Cyber Forensics Uncovering Hidden Relations Using Open Source Information (OSINF)*. Springer.

Al-Khateeb, S., & Agarwal, N. (2014). Modeling flash mobs in cybernetic space: Evaluating threats of emerging socio-technical behaviors to human security. *Proceedings - 2014 IEEE Joint Intelligence and Security Informatics Conference, JISIC 2014*, *7*(1), 328. https://doi.org/10.1109/JISIC.2014.73

Al-Rubaye, A., & Menezes, R. (2016). Extracting Social Structures from Conversations in Twitter. *A Case Study on Health-Related Posts." In Proceedings of the 27th ACM Conference on Hypertext and Social Media*, 5–13. https://doi.org/10.1145/2914586.2914599

Alassad, M., Agarwal, N., & Hussain, M. N. (2019). Examining Intensive Groups in YouTube Commenter Networks. *In Proceedings of 12th International Confeerence, SBP-BRiMS 2019*, (12), 224–233.

Alassad, M., Hussain, M. N., & Agarwal, N. (2019). Finding Fake News Key Spreaders in Complex Social Networks by Using Bi-Level Decomposition Optimization Method. *International Conference on Modelling and Simulation of Social-Behavioural Phenomena in Creative Societies*, 41–54. https://doi.org/10.1007/978-3-030-29862-3_4

Barrenas, F., Chavali, S., Holme, P., Mobini, R., & Benson, M. (2009). *Network measures*. 1–4. https://doi.org/https://doi.org/10.1371/journal.pone.0008090

Blondel, V. D., Guillaume, J., & Lefebvre, E. (2008). Fast unfolding of communities in large networks. *Journal of Statistical Mechanics: Theory and Experiment*, *10*, 10008.

Borgatti, S. P. (2005). Centrality and network flow. *Social Networks*, *27*(1), 55–71. https://doi.org/10.1016/j.socnet.2004.11.008

Borgatti, S. P., & Everett, M. G. (2006). A Graph-theoretic perspective on centrality. *Social Networks*, *28*(4), 466–484. https://doi.org/10.1016/j.socnet.2005.11.005

Briscoe, E. J., Appling, D. S., Mappus, R. L., & Hayes, H. (2014). Determining credibility from social network structure. *In Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 1418–1424. https://doi.org/10.1145/2492517.2492574

Chen, W., & Wang, Y. (2009). Efficient Influence Maximization in Social Networks Categories and Subject Descriptors. *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 199–207. https://doi.org/10.1145/1557019.1557047

Chua, T.-S. (2014). The Multimedia Challenges in Social Media Analytics. *Proceedings of the 3rd International Workshop on Socially-Aware Multimedia*, 17–18. https://doi.org/10.1145/2661126.2661131

Clauset, A., Newman, M. E. J., & Moore, C. (2004). Finding community structure in very large networks. *Cond-Mat/0408187*, *70*, 066111. https://doi.org/doi:10.1103/PhysRevE.70.066111

Dale, R. (2017). NLP in a post-truth world. *Natural Language Engineering*, *23*(2), 319–324. https://doi.org/10.1017/S1351324917000018

Faust, K., & Wasserman, S. (1994). SOCIAL NETWORK ANALYSIS. In *Cambridge University Press*.

Freeman, L. C. (1977). A Set of Measures of Centrality Based on Betweenness. *Sociometry*, Vol. 40, p. 35. https://doi.org/10.2307/3033543

Freeman, L. C. (1978). Centrality in Social Networks. *Social Networks*, *1*, 215–239. https://doi.org/10.1016/0378-8733(78)90021-7

Girvan, M., & Newman, M. (2002a). Community structure in social and biological networks. *Pnas*, *99*(12), 7821–7826. https://doi.org/10.1073/pnas.122653799

Girvan, M., & Newman, M. E. J. (2002b). Community structure in social and biological networks. *Proceedings of the National Academy of Sciences*, *99*(12), 7821–7826. https://doi.org/10.1073/pnas.122653799

Hagen, L., Member, S., & Kahng, A. B. (1992). New Spectral Methods for Ratio Cut Partitioning and Clustering. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *11*(9).

Herzig, J., Mass, Y., & Roitman, H. (2014). An author-reader influence model for detecting topic-based influencers in social media. *In Proceedings of the 25th ACM Conference on Hypertext and Social Media*, 46–55.

https://doi.org/10.1145/2631775.2631804

Huang, J., Sun, H., Liu, Y., Song, Q., & Weninger, T. (2011). Towards online multiresolution community detection in large-scale networks. *PLoS ONE*, *6*(8). https://doi.org/10.1371/journal.pone.0023829

Hugo, V. (1887). *Les misérables*. TY Crowell & Company.

Hussain, M. N., Tokdemir, S., Agarwal, N., & Al-Khateeb, S. (2018). Analyzing Disinformation and Crowd Manipulation Tactics on YouTube. *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 1092–1095. https://doi.org/10.1109/ASONAM.2018.8508766

Java, A., Joshi, A., & Finin, T. (2008). Detecting commmunities via simultaneous clustering of graphs and folksonomies. *Proceedings of the Tenth Workshop on Web Mining Ad Web Usage Analysis (WebKDD)*. https://doi.org/10.1002/bbb

Jones, S., & O'Neill, E. (2010). Feasibility of structural network clustering for group-based privacy control in social networks. *In Proceedings of the Sixth Symposium on Usable Privacy and Security*, 9. https://doi.org/10.1145/1837110.1837122

Kempe, D., & Kleinberg, J. (2003). Maximizing the Spread of Influence through a Social Network. *Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 137–146.

Kivran-Swaine, F., Govindan, P., & Naaman, M. (2011). The impact of network structure on breaking ties in online social networks. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 1101–1104. https://doi.org/10.1145/1978942.1979105

Kleinberg, J. O. N. M. (1999). Authoritative Sources in a Hyperlinked Environment. *In Proceedings of the ACM-SIAM Symposium on Discrete Algorithms.*, *46*(5), 604–632.

Leskovec, J., Mcglohon, M., Faloutsos, C., Glance, N., & Hurst, M. (2007). Patterns of Cascading Behavior in Large Blog Graphs. *In Proceedings of the 2007 SIAM International Conference on Data Mining*, 551–556.

Leskovec, J., McGlohon, M., Faloutsos, C., Glance, N., & Hurst, M. (2007). Cascading Behavior in Large Blog Graphs. *In Proceedings of the 2007 SIAM International Conference on Data Mining*, 551–556. https://doi.org/10.1137/1.9781611972771.60

Li, C., Wang, L., Sun, S., & Xia, C. (2018). Identification of influential spreaders based on classified neighbors in real-world complex networks. *Applied Mathematics and Computation*, *320*(11), 512–523. https://doi.org/10.1016/j.amc.2017.10.001

Lorenzi, D., Vaidya, J., Chun, S., Shafiq, B., Naik, V., Atluri, V., & Adam, N. (2013). Community based emergency response. *In Proceedings of the 14th Annual International Conference on Digital Government Research*, 82–91. https://doi.org/10.1145/2479724.2479739

Myers, S. A., Sharma, A., Gupta, P., & Lin, J. (2014). Information Network or Social Network? The Structure of the Twitter Follow Graph. *Proceedings of the 23rd International Conference on World Wide Web*, 493–498. https://doi.org/10.1145/2567948.2576939

Newman, M. E. J. (2004a). Detecting community structure in networks. *The European Physical Journal B - Condensed Matter*, *38*(2), 321–330. https://doi.org/10.1140/epjb/e2004-00124-y

Newman, M. E. J. (2004b). Fast algorithm for detecting community structure in networks. *Physical Review E - Statistical Physics, Plasmas, Fluids, and Related Interdisciplinary Topics*, *69*(6), 5. https://doi.org/10.1103/PhysRevE.69.066133

Newman, M. E. J. (2006). Modularity and community structure in networks. *Proceedings of the National Academy of Sciences*, *103*(23), 8577–8582. https://doi.org/10.1073/pnas.0601602103

Newman, M. E. J., & Girvan, M. (2003). *Finding and evaluating community structure in networks*. 1–16. https://doi.org/10.1103/PhysRevE.69.026113

Nygren, E. (2010). Modeling the social dynamics of online discussion sites. *In Proceedings of the International Workshop on Modeling Social Media*, 2. https://doi.org/10.1145/1835980.1835982

Page, L., Brin, S., Motwani, R., & Winograd, T. (1998). The PageRank Citation Ranking: Bringing Order to the Web. *World Wide Web Internet And Web Information Systems*, *54*(1999–66), 1–17. https://doi.org/10.1.1.31.1768

Richardson, M., & Domingos, P. (2002a). Mining Knowledge-Sharing Sites for Viral Marketing. *Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 61–70.

Richardson, M., & Domingos, P. (2002b). Mining Knowledge-Sharing Sites for Viral Marketing. *In Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 61–70.

Sato, K., & Izunaga, Y. (2018). An enhanced MILP-based branch-and-price approach to modularity density maximization on graphs. *Computers and Operations Research*, 1–25. https://doi.org/10.1016/j.cor.2018.01.012

Şen, F., Wigand, R., Agarwal, N., Tokdemir, S., & Kasprzyk, R. (2016). Focal structures analysis: identifying influential sets of individuals in a social network. *Social Network Analysis and Mining*, *6*(1). https://doi.org/10.1007/s13278-016-0319-z

Shao, C., Ciampaglia, G. L., Flammini, A., & Menczer, F. (2016). *Hoaxy: A Platform for Tracking Online Misinformation*. 745–750. https://doi.org/10.1145/2872518.2890098

Shu, K., Sliva, A., Wang, S., Tand, J., & Liu, H. (2017). Fake news detection: Network data from social media used to predict fakes. *ACM SIGKDD Explorations Newsletter*, *19*(1), 22–36.

Søe, S. O. (2018). Algorithmic detection of misinformation and disinformation: Gricean perspectives. *Journal of Documentation*, *74*(2), 309–332.

Tarjan, R. (1972). Depth-first search and linear graph algorithms. *SIAM Journal on Computing*, *1*(2), 146–160.

Tsung, C. K., Ho, H., Chou, S., Lin, J., & Lee, S. (2017). A Spectral Clustering Approach Based on Modularity Maximization for Community Detection Problem. *Proceedings - 2016 International Computer Symposium, ICS 2016*, 12–17. https://doi.org/10.1109/ICS.2016.0012

Von Luxburg, U. (2007). A tutorial on spectral clustering. *Statistics and Computing*, *17*(4), 395–416. https://doi.org/10.1007/s11222-007-9033-z

Wang, G., Shen, Y., & Luan, E. (2008). Measure of centrality based on modularity matrix. *Progress in Natural Science*, *18*(8), 1043–1047. https://doi.org/10.1016/j.pnsc.2008.03.015

Zafarani, R., Abbasi, M. A., & Liu, H. (2014). Social Media Mining: An Introduction. In *Cambridge University Press*. Retrieved from https://books.google.com/books?id=fVhzAwAAQBAJ

Zhang, X., & Ghorbani, A. A. (2019). An overview of online fake news: Characterization, detection, and discussion. *Information Processing and Management*, (August 2018), 102025. https://doi.org/10.1016/j.ipm.2019.03.004