Using Computational Social Science Techniques to Identify Coordinated Cyber Threats to Smart City Networks

Mustafa Alassad[1], Billy Spann[1], Samer Al-khateeb[2], Nitin Agarwal[1]

[1]University of Arkansas, Little Rock, AR, USA
{mmalassad,bxspann,nxagarwal}@ualr.edu
[2]Creighton University, Omaha, NE, USA
SamerAl-Khateeb1@creighton.edu

Abstract

Smart cities are increasingly facing cyber-attacks due to the endeavors they have made in technological advancements. The challenge for smart cities, that utilize complex digital networks to manage city systems and services, is that any device that relies on internet connectivity to function is a potential cyber-attack victim. Smart cities use smart sensors. Online Social Networks (OSNs) act as human sensors offering significant contributions to the amount of data used in smart cities. 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 smart city infrastructure. This convergence of the cyber and physical worlds is known as cybernetics. Quantitative socio-technical methods such as deviant cyber flash mob detection (DCFM) and focal structure analysis (FSA) can provide reconnaissance capabilities that enable cities to look beyond internal data and identify threats based on active events. Assessment of powerful actors using DCFM detection methods can help to identify and prevent attacks. Groups of powerful hackers can be identified through FSA which is a model that uses a degree centrality method at the *node-level* and spectral modularity at *group-level* to measure the power of a focal structure (a subset of the network). DCFM and FSA models can help cyber-security experts by providing a better picture of the threat which will help to plan a better response.

Keywords

Online Social Networks, Focal Structure Analysis, Flash Mob Detection, Spectral Modularity, Degree Centrality, Network Clustering, Smart Cities, Cyber Security.

1. Introduction

Transformation to smarter cities presents many challenges for researchers and engineers as they face new procedures, data management platforms, and operations. Building new and efficient smart systems open the door for many new issues such as privacy, security, big data coming from various sensors, public and private services, and social systems. Although these systems are being transformed into smart systems by connecting them to the internet A.K.A. the Internet of Things (IoT), it still needs more cybersecurity enhancements.

The critical infrastructure of smart cities should have monitoring capabilities for optimizing security methods, reducing vulnerability, increasing reliability. This will enhance the transportation systems, the security of smart power grids and various energy systems such as: petroleum refineries, health, and food systems. Such monitoring systems require data collection, real-time processing, analysis, and decision-making capabilities.

Today, various industries have services that monitor many malicious activities and threats, such as hackers who try to access crucial department databases to steal information or damage a provided service. In recent years, many malicious cyber activities across the world have been reported to cause enormous damage to various critical smart systems [1].

In this research, we are considering the massive growth of social media platforms in the recent years such as Twitter, Facebook, YouTube, and WeChat, and how many social applications must work with significant amounts of personal and public data. People use these tools to share information, opinions, and activities with their relatives, friends and other cultural organizations. However, in the last few years, the use of these platforms was changed by a few radical organizations. Malicious actors misused social media to amplify and share terrorist activities and malicious threats, information dissemination, propagating radical behaviors, spreading fake news, and conducting cyber-attacks on public and private online smart infrastructure networks [2].

Quantitative methods have been applied to help to analyze the complex social networks in recent years. Some of the most common approaches to quantitative network analysis use measures such centrality and modularity to help define network structure and model the networks. Node-based community detection algorithms using the degree centrality method [3], [4] and group-based community detection algorithms using the modularity method [5], [6], are considered in our research and presented in section 2. However, merely considering these two community detection categories alone, lacks the depth and insight into the most influential aggressors and network links that would maximize the damage to a smart city infrastructure grid. Therefore, we propose a mixed model, developing the node-level measure which considers the individual's centrality value, and then spectral modularity (group-level) is employed to measure the groups' influence at the Network-Level. The resultant model is a Bi-Level centrality-modularity maximization model called Focal Structure Analysis (FSA). These focal structures (sub network or sub graphs) are the hidden intensive groups that can influence maximum number of users in the network.

The contributions from the model in this research considers the shortcomings in the regular community detection algorithms, where the node-based methods cannot identify these groups, and the group-based method cannot cluster intensive small groups. We are proposing a mix of the node and group-based community detection algorithms, whereby we create a model consisting of two major sections: the bi-level optimization section, and the deviant cyber flash mob detection method. Other supplementary sections are also used to help in clustering the network. Finally, the model utilizes small real-world metrics to identify FSA sets and then evaluate them using the deviant cyber flash mob detection (DCFM) method to determine if the aggressors' and sets can influence the entire network.

Multiple case studies leveraged the two aforementioned approaches independently, such as Sen et al. [8], utilized a greedy model on a Facebook network and concluded that Facebook was used to mobilize crowds in 2007 during the Egyptian Revolution [9]. The authors in [9] studied a Twitter network, where they identified a small influential set of users who are responsible for the 2011 Saudi Arabia women's right to drive campaign [9]. Alassad et al. [10] studied a network of commenters on YouTube that disseminated disinformation. He used a decomposition optimization model to identify small influential sets of commenters responsible for commenting on various videos.

For our practical implementation of this mixed-mode model that would extend to the smart city domain, we consider an ISIS dataset provided in a study conducted by the International Centre for the Study of Radicalization and Political Violence (ICSR) which shows a group of individuals who helped ISIS recruiters to disseminate their propaganda on Twitter and other social media platforms [7]. This mixed-mode model was also applied on a YouTube channel that was spreading fake news in the South China Sea [11].

1.1 Problem Statement

The aim of this study is to apply a *non-traditional cybersecurity network approach* to cluster and analyze influential sets of social media users. These users are highly central disseminators who can amplify information spread to a maximum number of individuals in the network. One of the big challenges that are facing network scientists is to identify and suspend such hidden coordinating groups of malicious users in complex social network. These focal structures of malicious users in the network can be influential and can disseminate their radical or terrorist propaganda to threaten smart cities' intelligent systems very effectively.

These sets of aggressors (focal structures) can coordinate attacks on various smart city infrastructures by utilizing well-known social media platforms, for example, they can post directions, locations, and other coordination activities on social media informing their followers. Since smart cities rely on internet services, the government would not want to shut down internet service across the entire smart city network and risk financial, economic, or security lose. The success of a deviant cyber flash mob targeting a smart city infrastructure would likely have a crippling effect on the smart city. Identifying hidden influential groups and suspending them without impacting the total infrastructure network is essential. In this research we use a network of commenters who are posting radical directions on Twitter to paralyze infrastructure in smart cities. These FSAs could be responsible for organizing multi-cyber-attacks to maximize the damages to the network,

spread fake news and convince other nodes in the network to participate in or create their own cyber-attacks. In this paper, we identify these malicious set of users, and then suspend them from their locations in the network to stop their influence without taking down the remaining network.

The rest of the paper is organized as follows. Section 2 summarizes the data set and the research methodology. Section 3, we apply the proposed model to the dataset collected and demonstrate the model efficiency. Finally, we conclude with intended future work in section 4.

2 Methodology

The proposed model is designed to (1) overcome the shortcomings in regular community detection methods [4, 10], (2) advance the FSA model proposed by Sen et al. [9, 12], and (3) use the DCFM model developed by Al-khateeb et al. [13] to identify a sets of powerful actors in complex social networks aiming to conduct deviant acts that can damage smart cities' infrastructures.

2.1 Data Set

In this research, we collected data of a Twitter network consisting of 1,453 nodes and 1,487 edges. 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 [16]. We crawled these usernames' friends and followers then cross-intersected them with another dataset collected during three beheading events conducted by ISIS in Egypt, Libya, and Palestine [17]. For the users in the resultant dataset, we calculated control, interest, and power to estimate the power of each node (user) in the network. We built the communication (retweets and mentions) network for these users then ran our model to determine the focal structures within the network. These FSAs are ranked based on the sum of power for all users within that focal structure.

2.2 Node-Level & Group level Measures

The first step in collecting the necessary measurements for the model after identifying the user network is to calculate node-level power, degree centrality (node-level measurements) and the clustering coefficient (group-level measurements). The power of each node is calculated using a collective action-based model developed by Al-khateeb et. al [18,19]. The degree centrality method is utilized to measure a node's sphere of influence [4]. Fig. 1 shows the average degree centrality for all 53 FSA sets. In addition to degree centrality, the model needs to consider the node's neighbors' friendship as well, to determine if the friends-of-friends are also his/her friend. Hence, we used the clustering coefficient as shown in Fig.2 to determine if a node exhibits this behavior or not [3, 4]. The final analysis uses not only the node's degree centrality, but also the network power calculated by the DCFM method.

The result of the two methods combined, i.e., the degree centrality and clustering coefficient, are ranked as sets of active local communities consisting of highly central nodes that have active neighbors (can communicate with each other). The measurements from these two methods will be exported to the Network-Level to measure their ability to maximize the network's sparsity or their communication to other aggressors' groups.

2.3 Network-Level Analysis

The spectral modularity method [6], is used to measure the graph's sparsity inheriting the nodes' sets from the Node-Level. The objective function as shown in the Network-Level in Fig 3, is to import sets from the previous level and then find sets that can maximize the graph's modularity value [10, 11]. The model is searching for sets of groups that can produce the maximum number of aggressors in the network [5, 10, 11, 14].

These focal structures include the maximum number of influential nodes in the network who have the power to convince other nodes in the network to participate in deviant actions, such as multi-cyber-attacks. Also, these nodes can be part of other groups (other focal structures, and can supervise other nodes, control information dissemination, and amplify their radical actions to other parts of the network.

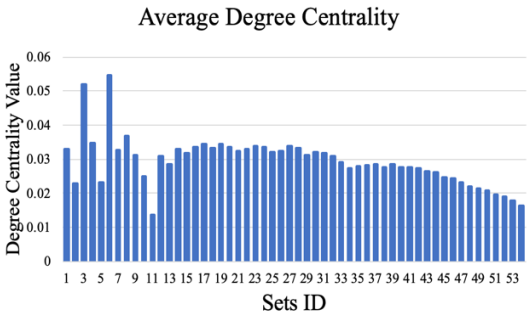

Fig. 1: FSA Sets' average degree centrality values.

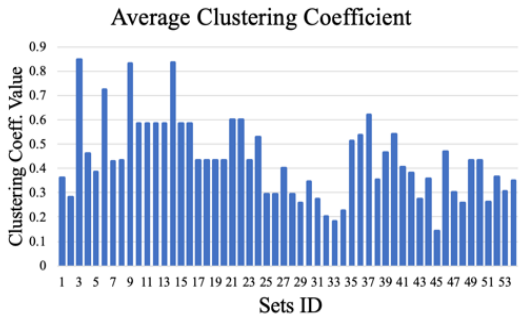

Fig. 2: FSA Sets' average clustering coefficient values.

2.4 FSA Evaluation and DCFM

Decomposition of the identified focal structures help to measure the sets characteristics from different points of views as follows:

2.4.1 Small Real-World Network Metrics

Our model used two measures, namely degree centrality and clustering coefficient to determine its output. The goal of the model is to find subsets in the network (called focal structures) that can maximize the average degree centrality of each node and the average clustering coefficient of these central nodes (to measure the members' connectivity within the sets). Fig 1 shows the identified focal structures (influential sets) average degree centrality values while Fig 2 shows the interaction between these subsets nodes by utilizing the clustering coefficient of the group.

2.4.2 DCFM Metrics

The 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 organizing DCFM, we can design counter measures to stop the aggressors from attacking smart city infrastructure. Previous work by Al-khateeb and Agarwal [13] developed a collective action based theoretical model which identified factors to predict success or failure of a Deviant Cyber Flash Mob (DCFM).

In their model, the identified factors are – Utility (U) (the benefits an individual gain if the DCFM success or fail), 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.

3 Experimental Results

We applied our model to the ISIS Twitter network shown in Fig 4. The model identified the highly influential sets of aggressors in the dataset that maximizes the graph sparsity, influences maximum number of individuals, and includes members acting in different group as shown in Fig 5. Also, the interconnection between pairwise focal structure reveals a spoke and hub communication structure, where a set conveys information to other groups who then carry out operations as shown in Fig 5. The DCFM method calculated the sets' power (influence), whereby the more power they have the darker the sets' color as shown in Fig 5.

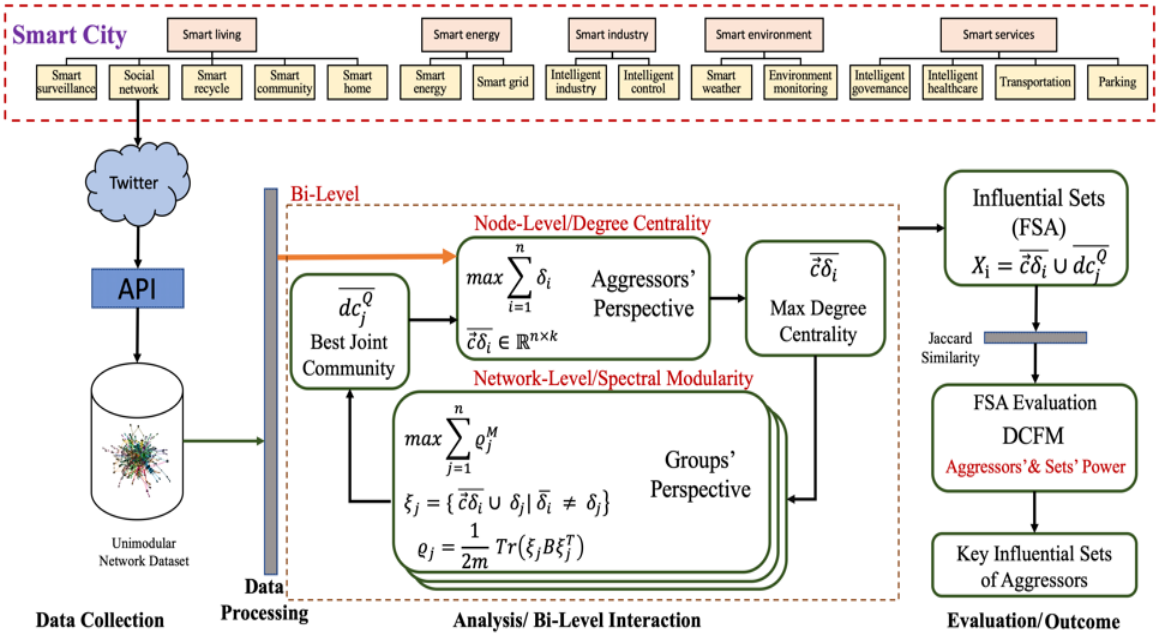

Fig. 3: Focal Structure Analysis (FSA) structure in Smart City, where social media is part of the smart city structure. The model will import the data constructed from the social media platforms such as Twitter.

To understand the focal structures' impact inside the network as shown in Fig 6, we employed two methods as basis to make the evaluation. First, the Girvan-Neman modularity method [15], which returned a modularity value of 0.645 and clustered 40 communities as shown in Fig 4. Second, Trajan et al. [16] found only one weakly connected user in the network. These are the baseline network measurements for this collection of users and their corresponding network structure.

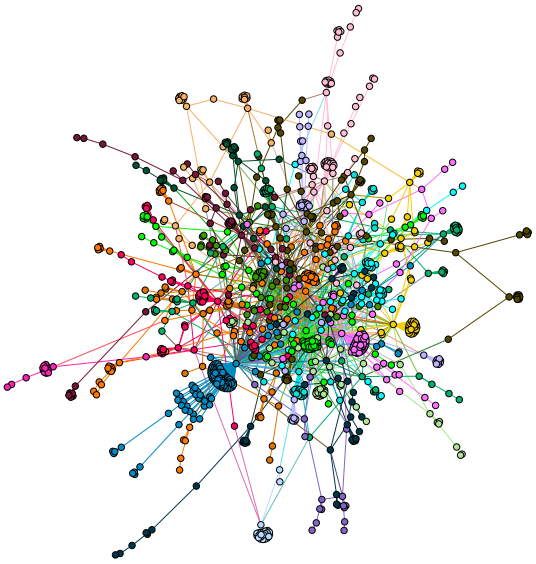

Fig. 4: ISIS Twitter network clustered into 40 groups via modularity method.

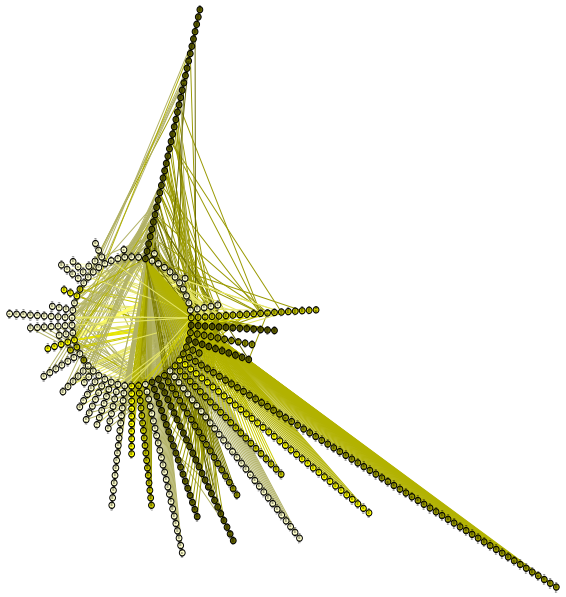

Fig. 5: Commenters are clustered into 54 influential sets. The darker the color, higher the influence.

Moreover, Fig 7, shows the top twenty influential aggressors and the count of FSA sets containing each aggressor. Since we identified that very powerful actors appear in multiple network sets, it enables the

authorities to measure, predict, and allocate the influential aggressors' active strategies, possible spots for information dissemination, and cyber-attacks' locations.

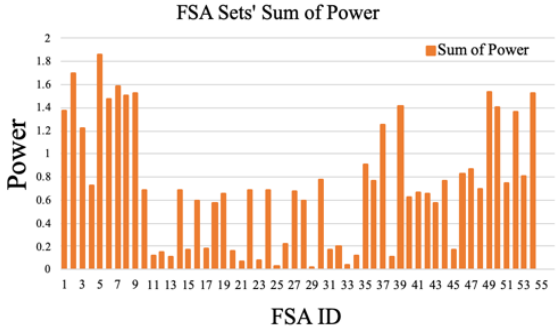

Fig. 6: Sets' power measured by DCFM method.

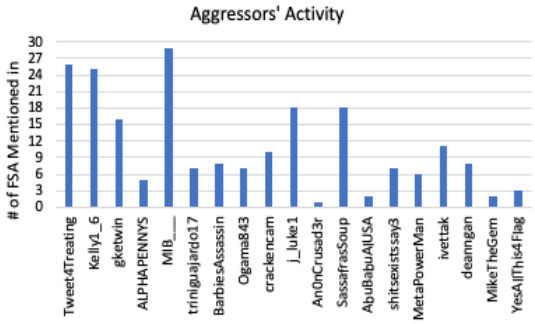

Fig. 7: Top 20 Influential aggressors measured by DCFM.

Table 1 shows the top twenty influential sets of aggressors, where the impact of each set on the modularity and connectivity were measured accordingly. We found that, each of these sets can maximize the graph modularity value into the interval of [0.7-0.83], and they can maximize the graph sparsity from 40 groups into [103-426] groups. This means that by removing the most influential users from the network, the clusters or communities within the network lose their connection to other parts of the network. That is, by removing the aggressors in any given FSA ID in Table 1, the overall network of users becomes isolated to other communities.

Table 1: Top 20 influential sets.

FSA ID	Sum of power	Count of users	# of Weakly conn. users	Count of comm.	Max modularity value	FSA allocation
5	1.86	42	408	426	0.83	19
2	1.7	41	401	423	0.82	13
7	1.58	21	287	313	0.78	9
49	1.53	47	256	280	0.81	15
9	1.52	21	268	290	0.78	9
54	1.52	130	278	300	0.82	20
8	1.5	21	330	352	0.8	13
6	1.47	11	273	298	0.76	9
39	1.41	13	241	268	0.75	12
50	1.4	49	261	286	0.78	15
1	1.37	19	270	292	0.77	7
52	1.36	54	230	254	0.8	19
37	1.25	13	145	175	0.72	5
3	1.22	7	165	189	0.7	5
35	0.91	12	161	187	0.74	8
47	0.87	32	73	103	0.72	10
46	0.83	25	161	190	0.73	8
53	0.81	76	115	142	0.76	20
30	0.78	9	131	191	0.71	4
36	0.77	12	174	198	0.72	5

In addition, based on Trajan et al. [16] the min-max numbers of weakly connected users caused by these sets increase from one to an interval between [73-408] weakly connected users. Most importantly, we were able to identify each FSA set's attack locations by identifying how many FSA sets each aggressor appeared in, (as shown in Fig. 7). proposing that each set of aggressors can attack multiple places at the same time. For example,

FSA (5), the top influential set consisted of 42 aggressors, they can influence 408 individuals, are able to attack 19 different locations in the network and can divide the network into 426 other groups. Therefore, by removing the users within this FSA (5), the network is divided into 426 communities vs 40 communities with FSA (5) included, so aggressors would have to work harder to disseminate information across the network.

4 Conclusion and Discussion

In this research, we have studied social media cybersecurity risks at a network level using computational social science techniques, where aggressors utilize Twitter platforms to perform cyber attacks. Considering the shortcomings of regular community detection algorithms and taking a non-traditional cybersecurity approach, the proposed bi-level model was able to identify hidden influential sets of aggressors in the network. The proposed model was able to identify a spoke and hub communication structure, where a single influential FSA set conveys information to other sets who can carry out deviant behaviors. Such focal structures are more prevalent in terrorist networks.

Throughout this research, we were able to allocate the aggressors' activities, track all their possible cyber-attacks locations, provide an overview of the influential sets, and estimate the aggressors' influence in the network. Using this model could enhance and harden smart cities' strategies against cyber-attacks when they originate from social media platforms by suspending any of those focal aggressors' structures to prevent the massive damages that can be caused to a smart cities critical foundation.

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.

References

[1] R. E. Hall, J. Braverman, J. Taylor, and H. Todosow, "The Vision of A Smart City," Ins, Fr. Sept. 28, Paris, *Fr. 2nd Int. Present. Life Ext. Technol. Work. Paris*, pp. 1–6, 2000.

[2] N. Abouzakhar, "Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations," 2013.

[3] L. C. Freeman, "Centrality in Social Networks," *Soc. Networks*, vol. 1, pp. 215–239, 1978.

[4] R. Zafarani, M. A. Abbasi, and H. Liu, *Social Media Mining: An Introduction*. Cambridge University Press, 2014.

[5] M. Girvan and M. E. J. Newman, "Community structure in social and biological networks," *Proc. Natl. Acad. Sci.*, vol. 99, no. 12, pp. 7821–7826, 2002.

[6] C. K. Tsung, H. Ho, S. Chou, J. Lin, and S. Lee, "A Spectral Clustering Approach Based on Modularity Maximization for Community Detection Problem," *Proc. - 2016 Int. Comput. Symp. ICS 2016*, pp. 12–17, 2017.

[7] N. A. Mohammad Yasin, "Impact of ISIS ' Online Campaign in Southeast Asia," *Int. Cent. Polit. Violence Terror. Res.*, vol. 7, no. 4, pp. 26–32, 2015.

[8] V. Romano, J. Duboscq, C. Sarabian, E. Thomas, C. Sueur, and A. J. J. MacIntosh, "Modeling infection transmission in primate networks to predict centrality-based risk," *Am. J. Primatol.*, vol. 78, no. 7, pp. 767–779, 2016.

[9] F. Şen, R. Wigand, N. Agarwal, S. Tokdemir, and R. Kasprzyk, "Focal structures analysis: identifying influential sets of individuals in a social network," *Soc. Netw. Anal. Min.*, vol. 6, no. 1, p. 17, 2016.

[10] M. Alassad, N. Agarwal, and M. N. Hussain, "Examining Intensive Groups in YouTube Commenter Networks," *Proc. 12th Int. Confeerence, SBP-BRiMS 2019*, no. 12, pp. 224–233, 2019.

[11] M. Alassad, M. N. Hussain, and N. Agarwal, "Finding Fake News Key Spreaders in Complex Social

Networks by Using Bi-Level Decomposition Optimization Method," in *International Conference on Modelling and Simulation of Social-Behavioural Phenomena in Creative Societies*, 2019, pp. 41–54.

[12] F. Sen, R. T. Wigand, N. Agarwal, D. Mahata, and H. Bisgin, "Identifying focal patterns in social networks," *Proc. 2012 4th Int. Conf. Comput. Asp. Soc. Networks, CASoN 2012*, no. November 2012, pp. 105–108, 2012.

[13] S. Al-Khateeb and N. Agarwal, "Modeling flash mobs in cybernetic space: Evaluating threats of emerging socio-technical behaviors to human security," *Proc. - 2014 IEEE Jt. Intell. Secur. Informatics Conf. JISIC 2014*, vol. 7, no. 1, p. 328, 2014.

[14] M. E. J. Newman, "Modularity and community structure in networks," *Proc. Natl. Acad. Sci.*, vol. 103, no. 23, pp. 8577–8582, 2006.

[15] M. Girvan and M. Newman, "Community structure in social and biological networks," *Pnas*, vol. 99, no. 12, pp. 7821–7826, 2002.

[16] R. Tarjan, "Depth-first search and linear graph algorithms," *SIAM J. Comput.*, vol. 1, no. 2, pp. 146–160, 1972.

[17] Al-khateeb, Samer, and Nitin Agarwal. "Examining botnet behaviors for propaganda dissemination: A case study of isil's beheading videos-based propaganda." 2015 ieee international conference on data mining workshop (icdmw). IEEE, pp. 51-57, 2015.

[18] Al-khateeb, Samer, and Nitin Agarwal. "Developing a conceptual framework for modeling deviant cyber flash mob: A socio-computational approach leveraging hypergraph constructs." Journal of Digital Forensics, Security and Law 9.2 (2014): 10.

[19] Al-khateeb, Samer, and Nitin Agarwal. "Analyzing deviant cyber flash mobs of isil on twitter." International conference on social computing, behavioral-cultural modeling, and prediction. Springer, Cham, pp. 251-257, 2015.