Key player identification in terrorism-related social media networks using centrality measures

Ilias Gialampoukidis, George Kalpakis, Theodora Tsikrika, Stefanos Vrochidis and Ioannis Kompatsiaris
Information Technologies Institute
Centre for Research and Technology Hellas
Thermi-Thessaloniki, Greece
Emails: {heliasgj, kalpakis, theodora.tsikrika, stefanos, ikom}@iti.gr

***Abstract*—Monitoring terrorist groups and their suspicious activities in social media is a challenging task, given the large amounts of data involved and the need to identify the most influential users in a smart way. To this end, many efforts have focused on using centrality measures for the identification of the key players in terrorism-related social media networks, so that their suspension/removal leads to severe disruption in the connectivity of the network. This work proposes a novel centrality measure, Mapping Entropy Betweenness (MEB), and assesses its effectiveness for key player identification on a dataset of terrorism-related Twitter user accounts by simulating targeted attacks that remove the most central nodes of the network. The results indicate that the MEB affects the robustness of this terrorist network more than well-established centrality measures, in the largest part of the attack process.**

I. Introduction

Social media networks, e.g. Twitter (http://twitter.com) and Facebook (http://facebook.com), have globalized the communication among people of different nationality, religion, culture or residence. On the other hand, though, due to their great power and reach, they have proven to be a very useful tool for terrorist organizations in their effort to recruit and radicalize new members, raise new funds, organize strategic operations and exchange information that can be exploited for subversive use [1], [2], [3]. Law Enforcement Agencies (LEAs) are thus interested in monitoring terrorist-related activity in social media networks, where the problem is to identify the most influential user accounts, known also as "key player" discovery [4]. Special attention has been paid to Twitter that has attracted several terrorist communities [5], [6], [7], due to its nature that permits the inexpensive communication of multimedia messages (tweets) to users worldwide.

Many complex technical and real-world networks, ranging from computer science to molecular biology [8], including social media networks such as Twitter [9], exhibit a scale-free topology [8], [10] characterized by a highly heterogeneous degree distribution, which follows a power-law. These so-called *scale-free networks* are very robust on random attacks and they are very vulnerable when targeted attacks are performed [11] at their most central nodes (key players), in an attempt to destroy their internal connectivity and turn them into a set of isolated smaller networks. An attack on a scale-free network may be triggered not only by malicious intentions (e.g. to breakdown the connectivity of a computer network), but also by incentives beneficial to the society (e.g. to prevent disease propagation). Hence, the scale-free topology, can be exploited so as to perform attacks on the most central users playing a vital role in the information exchange with the goal to spread their propaganda. Such an attack could remove or suspend user accounts considered as potential sources for disseminating terrorist-related information, and can be executed by the collaboration of LEAs with social media organizations.

Several approaches proposed for detecting key players in a complex network mainly focus on utilizing different centrality measures. *Degree centrality* is based on the size of the neighborhood, *betweenness centrality* on the percentage of shortest paths crossing a given node, and *closeness centrality* on the average distance of a given node to all others [12]. The *eigenvector centrality* takes into account the centrality of all nodes in the neighborhood of a given node [13] and is closely related to the *PageRank* centrality [14], where the centrality of a node is a function of the weighted centralities of the node's neighborhood. *Mapping Entropy* [15] weights the degree centrality of a node, using the entropy of the degree distribution on a local level. Moreover, the k-core of a network (i.e. a linked set of nodes with degree at least k) has also been used to locate influential nodes in a network [16]. Given though that its computation is degree-based and does not consider the shortest paths that cross a given node, it is not appropriate for the case of terrorist-related networks where the key players show high betweenness centrality [4].

Over the past two decades, many works have examined the network structure of terrorist organizations. One of the early efforts examined the social connections of the 9/11 hijackers and their accomplices and detected the ring leaders of the terrorist attacks based on their network structure [17]. Later work emphasized the use of social network analysis for understanding the core characteristics of terrorist groups [18]. More recent research has focused on explaining the survival mechanisms of the Global Salafi Jihad (GSJ) terrorist network, and concluded that its scale-free topology constitutes a major factor for its ability to remain active, even after being severely damaged by the authorities [19]. Furthermore, several research efforts have studied the use of social media, and especially Twitter, by terrorist organizations. These include a study

This is the accepted manuscript.
2016 European Intelligence and Security Informatics Conference
978-1-5090-2857-3/16 $31.00 © 2016 IEEE
pages: 112-115, DOI 10.1109/EISIC.2016.38

on Twitter's role in facilitating (i) the Mumbai (November 2008) terrorists to execute their attack by monitoring and utilizing situational information broadcast through Twitter [5], (ii) the Islamic State's (IS) strategy for communicating their propaganda for radicalizing and recruiting Twitter users [6], and (iii) feeder accounts of terrorist organizations from the Syria insurgency zone for exchanging information [7].

Contrary to the aforementioned studies that simply perform a statistical analysis of the topology and connectivity of the network structure, we examine the scale-free properties of a terrorism-related social media networks in order to detect the most operationally critical accounts, i.e. the key players. Our main contribution is that we propose a novel centrality measure for key player identification, namely Mapping Entropy Betweenness (MEB), aiming at the efficient identification of central nodes (Section II), and assess its effectiveness by simulating targeted attacks, using several centrality measures and the random attack scenario on a dataset of terrorism-related Twitter user accounts (Section III).

II. Identifying Key Players

This section presents the necessary background in identifying the central nodes in a complex network and introduces the MEB centrality measure.

A. Background and Notation

Given an undirected network $G(N, L)$ with N nodes and L links, the degree of a node n_k, $deg(n_k)$, is the number of its adjacent links. The adjacency matrix A has values $a_{ij} = 1$ if node n_i and node n_j are connected and $a_{ij} = 0$ otherwise. The node n_k can at most be adjacent to $N-1$ other nodes and the *degree centrality* (DC) is defined as [12]:

$$DC_k = \frac{deg(n_k)}{N-1} \tag{1}$$

The *betweenness centrality* (BC) [12] of node n_k is based on the number of paths $g_{ij}(n_k)$ from node n_i to node n_j that pass through node n_k to the number of all paths g_{ij} from node n_i to node n_j, summed over all pairs of nodes (n_i, n_j) and normalized by its maximum value $(N^2 - 3N + 2)/2$:

$$BC_k = \frac{2\sum_{i<j}^{N} \frac{g_{ij}(n_k)}{g_{ij}}}{N^2 - 3N + 2} \tag{2}$$

The distance $d(n_i, n_k)$ between any two nodes n_i, n_k in a network is the number of links between the two nodes. *Closeness centrality* (CC) [12] of node n_k is defined as the inverse of the average distance to all other nodes $n_i, i \neq k$:

$$CC_k = \frac{N-1}{\sum_{i=1}^{N} d(n_i, n_k)} \tag{3}$$

The *eigenvector centrality* (EC) [13] of node n_k quantifies the influence of node n_k by taking into account the eigenvector centrality of the neighbors of n_k. Eigenvector centrality is provided by the eigenvector which corresponds to the greatest eigenvalue of the adjacency matrix A.

Google's PageRank (PR) [14], introduced to measure the importance of a Web page, is defined for node n_k as:

$$PR_k = \frac{1-d}{N} + d \sum_{n_i \in \mathcal{N}(n_k)} \frac{PR_i}{L(n_i)} \tag{4}$$

where d is the damping factor (typically set to 0.85), $L(n_i)$ is the number of links to node n_i and $N(n_k)$ is the set of nodes connected to node n_k, referred to as the neighborhood of n_k.

The neighborhood $\mathcal{N}(n_k)$ of n_k has been also used to define the *Mapping Entropy* (ME) centrality, which has recently been proposed [15] as a function of the degree centrality:

$$ME_k = -DC_k \sum_{n_i \in \mathcal{N}(n_k)} \log DC_i \tag{5}$$

Mapping Entropy is in fact the degree centrality DC_k weighted by the average Shannon information in the neighborhood of node n_k [15]. Based on this notion, we propose a centrality measure that weights the betweenness centrality BC_k instead of the degree centrality DC_k.

B. Mapping Entropy Betweenness (MEB) centrality

Degree and betweenness are not identical properties. A node with high degree centrality (hub) has a large number of neighbors, but its spreading capability is reduced if it is located in the periphery of the network [16] and can only influence a local neighborhood and not the whole network. The removal of such a hub, will not necessarily affect the diffusion of information within the rest of the network. In a terrorist-related network, for example, information spread is based on nodes who act as a bridge between any two members, even if their degree centrality is low [20]. When a node acts as a bridge between many pairs of nodes, then its betweenness centrality is relatively high. For that reason, we focus on the betweenness centrality of a node, which we further elaborate, by taking into account the betweenness centrality of its first neighbors. An efficient weighting scheme for the degree centrality is Mapping Entropy [15], which we extend to a novel centrality measure, Mapping Entropy Betweenness (MEB) centrality:

$$MEB_k = -BC_k \sum_{n_i \in \mathcal{N}(n_k)} \log BC_i \tag{6}$$

The weight assigned to BC_k is the sum of all $-\log BC_i$ over the neighborhood of node n_k, as motivated by Eq. (5).

C. Betweenness vs. Mapping Entropy Betweenness

The proposed centrality measure is based on the betweenness centrality and, for each node, takes into account its first neighbors. To assess the potential benefits of introducing these additional nodes in the computation, we compare the effectiveness of MEB over betweenness centrality for key player identification in a network. To this end, we simulate targeted attacks on the network, i.e. the sequential removal of its most central nodes, to test which of the two centrality measures affects most its robustness. First, the k most central nodes are removed and the size of the largest connected component is estimated; then, the centralities are recalculated

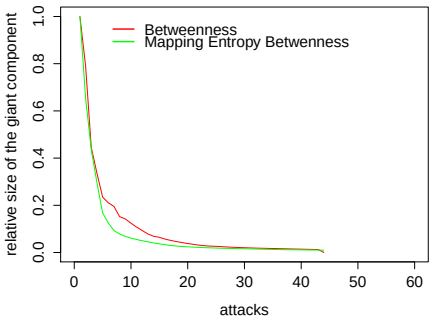


Fig. 1: Decay of the largest connected component in targeted attacks using the betweenness and MEB centrality measures

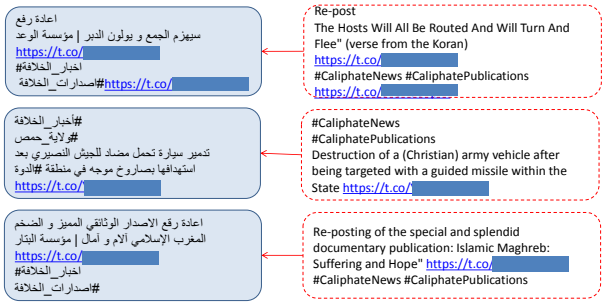


Fig. 2: Tweets in Arabic posted by the most central users, also translated in English. URLs are redacted for security purposes.

before removing again the most central nodes. This process is iterated for a fixed number of attacks and each time the average size decrease of the largest connected component is measured to gauge the impact of these attacks on the network.

Consider, for example, a randomly generated Barabási-Albert network [8] with 3600 nodes and power-law exponent 3.02. The size of the network is selected so as to coincide with the size of the network in our experiments described in Section III. The results of a targeted attack scenario for $k = 1$ are shown in Figure 1 and indicate that the MEB centrality is more effective than the betweenness centrality in the attack scenario where the most central node is sequentially removed, since MEB is able to reduce the size of the largest connected component faster than BC. This indicates that weighting the betweenness centrality of a node with its neighborhood's Mapping Entropy results in a more effective centrality measure.

III. Experiments in a Terrorist Network

In this section, we initially describe the terrorism-related social media dataset used in our experiments and then we simulate several scenarios of targeted attacks on this network, i.e. sequential removal of the most central nodes, to test which centrality measure affects most the robustness of the network.

A. Dataset Description

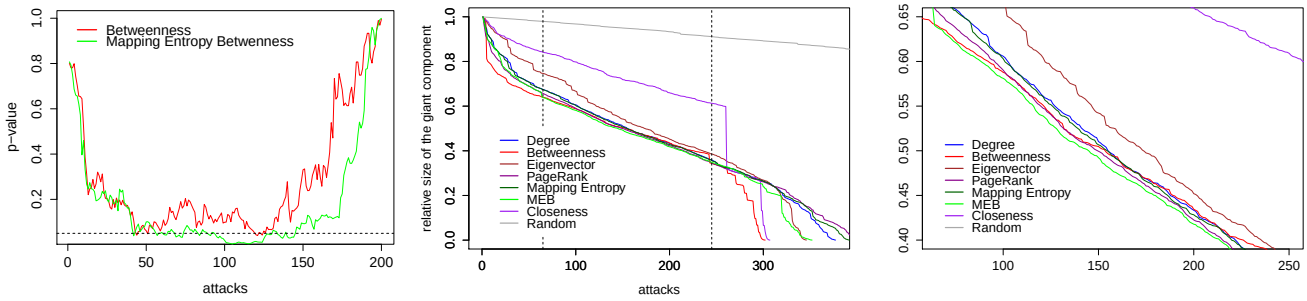
We examine a social media network consisting of terrorism-related Twitter accounts. Our data were collected through a social media discovery tool executing queries on the Twitter API (https://dev.twitter.com/) using a set of Arabic keywords related to terrorists' propaganda. These keywords were provided by law enforcement agents and domain experts in the context of the activities of HOMER EU FP7 project (http://homer-projet.eu) and are related to the Caliphate State, its news, publications, and photos from the Caliphate area.

The dataset consists of 38,766 Twitter posts by 5,461 users. A manual assessment of a sample of 100 posts indicated their relevance to terrorism and, in particular, to the propaganda spread by the Caliphate State; see Figure 2 for some examples. When one user account in mentioned in at least one post of another user, the two user accounts are linked together, thus an undirected network is constructed. In this network, we find the largest connected component (referred also as the "giant component") of 3,600 user accounts (nodes) and 9,203 links. Next, we examine which centrality measure is able to detect the most influential Twitter user(s) and limit the communication effectively within the terrorist network.

B. Results

The power-law behavior of the network's degree distribution is initially tested, in order to check whether the giant component is vulnerable to targeted attacks. The power-law exponent is estimated to be $\gamma = 2.56$ and is statistically significant, as stated by the Kolmogorov-Smirnov hypothesis test with p-value $0.7780 > 0.05$. Therefore, the scale-free character of the network allows for performing targeted attacks on the most central nodes, in order to make the network less operational. The power-law behavior is also tested during the attack process for the degree distribution of the largest connected component. Figure 3(a) indicates that the MEB centrality weakens the power-law behavior more than betweenness centrality in the largest part of the attack process. However, the network does not become less vulnerable to targeted attacks and shows high robustness to random attacks, as shown in Figure 3(b).

The superiority of MEB centrality in the largest part of the attack process is demonstrated in Figure 3, where a random attack scenario is performed ($k = 1$), using each of the centrality measures listed in Section II. Similar results are also observed for $k = 2$ and $k = 3$. For example, in the dashed region (Figure 3(b)), the size of the giant component is reduced only by 5% in random attacks, by 27.10% with closeness centrality, and by 44-49% with the other centrality measures, while using MEB the decrease is up to 50.01%. From the user perspective, after a small number of node removals (approx. 1.5% of the total size) one should replace betweenness with MEB centrality in her attack strategy, in order to further destroy the connectivity in the largest connected component. After 240 attacks, in all targeted attacks scenarios (Figure 3), more than 2/3 of the giant component has been isolated and the remaining nodes do not play a key role in the network's functionality, since the maximum observed degree is less than 9. In addition, MEB achieves the lowest half-life [21], defined as the number of targeted attacks needed to reduce the size of the largest connected component by one half. The half-life for the MEB is 145 attacks, while the half-life is 154 attacks for



(a) Significance p-value at each stage of the attack scenario, testing the fit of the degree distribution to power-law

(b) Decay of the largest connected component

(c) Decay of the largest connected component after a small number of attacks (1.5% of the overall size)

Fig. 3: Targeted attacks using several centrality measures.

the betweenness centrality, 156 for the degree centrality, 150 for the PageRank, 174 for the eigenvector centrality, 261 for the closeness centrality, 1191 for the random attack scenario.

Finally, for each centrality measure, we identified the top-10 nodes (i.e. Twitter accounts). This resulted in a set of 18 unique users who play a key role in the network. An examination that took place 10 days after the dataset contruction showed that 14 accounts had already been suspended by Twitter, while one posted a link that appears to be an (official) ISIS "publications" propaganda page. In most cases (10 out of 14), the suspension had actually taken place within 72 hours of the creation of the account. This indicates the relevance of our dataset to terrorism and also the volatility of these communities given Twitter's efforts to remove accounts that promote such material.

IV. Conclusion

This work addressed the key player identification task in terrorist social media networks. Using terrorism-related keywords, we created a social network of Twitter users, aiming at the efficient identification of the most influential accounts in the Caliphate State propaganda. A novel centrality measure was proposed, Mapping Entropy Betweenness (MEB), which is able to destroy the connectivity faster than other centrality measures in the largest part of the targeted attacks. We plan to assess the combination of MEB centrality with other prominent centralities in other terrorism-related networks, so as to efficiently and quickly determine influential accounts.

Acknowledgments

This work was partially supported by the EC projects HOMER (FP7-312883) and MULTISENSOR (FP7-610411).

References

[1] R. L. Thompson, "Radicalization and the use of social media," *Journal of strategic security*, vol. 4, no. 4, p. 167, 2011.

[2] I. Von Behr, A. Reding, C. Edwards, and L. Gribbon, "Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism," *Brussels: RAND*, 2013.

[3] R. Torok, "make a bomb in your mums kitchen: Cyber recruiting and socialisation of white moors and home grown jihadists," 2010.

[4] A. Berzinji, L. Kaati, and A. Rezine, "Detecting key players in terrorist networks," in *Intelligence and Security Informatics Conference (EISIC), 2012 European*. IEEE, 2012, pp. 297–302.

[5] O. Oh, M. Agrawal, and H. R. Rao, "Information control and terrorism: Tracking the mumbai terrorist attack through twitter," *Information Systems Frontiers*, vol. 13, no. 1, pp. 33–43, 2011.

[6] A. T. Chatfield, C. G. Reddick, and U. Brajawidagda, "Tweeting propaganda, radicalization and recruitment: Islamic state supporters multi-sided twitter networks," in *Proceedings of the 16th Annual International Conference on Digital Government Research*, 2015, pp. 239–249.

[7] J. Klausen, "Tweeting the jihad: Social media networks of western foreign fighters in syria and iraq," *Studies in Conflict & Terrorism*, vol. 38, no. 1, pp. 1–22, 2015.

[8] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[9] S. Aparicio, J. Villazón-Terrazas, and G. Álvarez, "A model for scale-free networks: Application to twitter," *Entropy*, vol. 17, no. 8, pp. 5848–5867, 2015.

[10] L. Li, D. Alderson, J. C. Doyle, and W. Willinger, "Towards a theory of scale-free graphs: Definition, properties, and implications," *Internet Mathematics*, vol. 2, no. 4, pp. 431–523, 2005.

[11] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, "Breakdown of the internet under intentional attack," *Physical review letters*, vol. 86, no. 16, p. 3682, 2001.

[12] L. C. Freeman, "Centrality in social networks conceptual clarification," *Social networks*, vol. 1, no. 3, pp. 215–239, 1978.

[13] P. Bonacich and P. Lloyd, "Eigenvector-like measures of centrality for asymmetric relations," *Social networks*, vol. 23, no. 3, p. 191, 2001.

[14] S. Brin and L. Page, "Reprint of: The anatomy of a large-scale hypertextual web search engine," *Computer networks*, vol. 56, no. 18, pp. 3825–3833, 2012.

[15] T. Nie, Z. Guo, K. Zhao, and Z.-M. Lu, "Using mapping entropy to identify node centrality in complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 453, pp. 290–297, 2016.

[16] F. D. Malliaros, M.-E. G. Rossi, and M. Vazirgiannis, "Locating influential nodes in complex networks," *Scientific reports*, vol. 6, p. 19307, 2016.

[17] V. Krebs, "Uncloaking terrorist networks," *First Monday*, vol. 7, no. 4, 2002.

[18] S. Saxena, K. Santhanam, and A. Basu, "Application of social network analysis (sna) to terrorist networks in jammu & kashmir," *Strategic Analysis*, vol. 28, no. 1, pp. 84–101, 2004.

[19] J. Xu, D. Hu, and H. Chen, "The dynamics of terrorist networks: Understanding the survival mechanisms of global salafi jihad," *Journal of Homeland Security and Emergency Management*, vol. 6, no. 1, 2009.

[20] J. Qin, J. J. Xu, D. Hu, M. Sageman, and H. Chen, "Analyzing terrorist networks: A case study of the global salafi jihad network," in *Intelligence and security informatics*. Springer, 2005, pp. 287–304.

[21] B. Furht, *Handbook of social network technologies and applications*. Springer Science & Business Media, 2010.