A monitoring tool for terrorism-related key-players and key-communities in social media networks

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

***Abstract*—Terrorists communicate and disseminate their activities using social media, such as Twitter, where complex networks of user accounts are formed and need to be effectively analysed by Law Enforcement Agencies (LEAs). To this end, we propose a novel visualisation tool that assists intelligence analysts and investigators through the presentation of the network formation, components, key-players, key-communities and through support of keyword search in the terrorism domain, highlighting also suspended users and offering navigation in the user network.**

Law Enforcement Agencies (LEAs) are interested in tracking and flagging terrorist-related activities in social media networks; however, they face big challenges in monitoring complex relationships and communication activities taking place over such networks, e.g. exchanges during member recruitment and radicalisation, organisation of strategic operations and information exchange for subversive use [1].

The proposed visualisation tool offers two novel functionalities, based on the key-player identification method of [2] and the key-community detection of [3]. Both are exposed as a combined web service and are performed on data from Twitter using as input a set of five Arabic keywords related to terrorist propaganda. Our collection is based on a crawl that started on February 9, 2017, and currently consists of 27,913 tweets by 15,023 users, among which 3,018 have already been suspended by Twitter and 688 correspond to non-existent accounts.

The presented data can be distinguished into statistics, key-players and key-communities, as demonstrated in Figure 1. The network constitutes a straightforward visual representation of how Twitter accounts mention each other and the communities they formulate. Every node in the graph represents a user (profile picture is shown on the node), while every edge is a connection between two users. Communities are indicated by different colored borders around the nodes, which is a plain way to assign a community to a user account. However, if an account is inactive, the respective node is colored red and labeled as "Suspended!" or is colored black and labeled as "Does not exist!" depending on the case. By clicking on a node, a window pops up to provide more information about the selected user. The pop-up window contains a profile picture on the top left and some account details on the top right, followed by a list of all tweets posted by the featured user. The account details include a name, a username, a description written by the user, a link to the original Twitter page, and a label to inform whether the user is suspended or non-existent. Regarding the list of tweets, each item has external links, if any, they are sorted by date and linked to the original tweet.

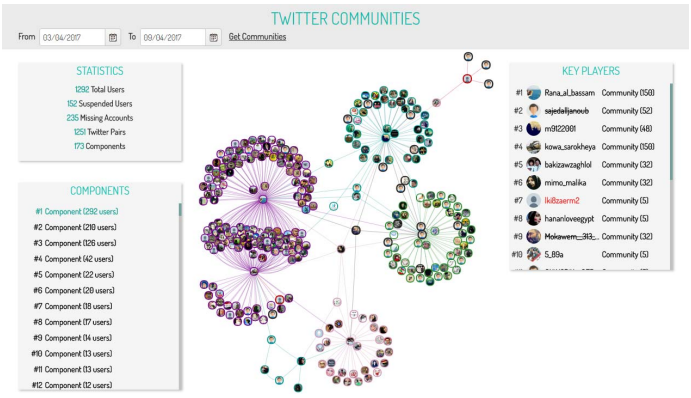

Fig. 1. Screenshot of the system interface

The implementation is based entirely on open-source tools. Data is stored in MongoDB and the web service has been built on Java, but invokes an R script that uses the igraph[1] library to run the key-player identification and the community detection methods. The front-end application was developed using standard Web technologies, including HTML5, CSS, JavaScript, and PHP to communicate with the database. Additional libraries for developing the front-end include jQuery, Kendo UI Core[2], and vis.js[3] for network visualisation.

The proposed tool is not specific to Twitter, and we plan to adapted it to instant messaging and other platforms.

ACKNOWLEDGMENT

This work was supported by TENSOR H2020-700024.

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. Gialampoukidis, G. Kalpakis, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, "Key player identification in terrorism-related social media networks using centrality measures," in *European Intelligence and Security Informatics Conference (EISIC 2016), August*, 2016, pp. 17–19.

[3] I. Gialampoukidis, G. Kalpakis, T. Tsikrika, S. Papadopoulos, S. Vrochidis, and I. Kompatsiaris, "Detection of terrorism-related twitter communities using centrality scores," in *Proceedings of the 2nd International Workshop on Multimedia Forensics and Security*. ACM, 2017, pp. 21–25.

[1] http://igraph.org/r/
[2] https://github.com/telerik/kendo-ui-core
[3] http://visjs.org/