Detection and Analysis of Fake News Users' Communities in Social Media

Abdelouahab Amira, Abdelouahid Derhab, Samir Hadjar, Mustapha Merazka, Md. Golam Rabiul Alam, *Member, IEEE*, and Mohammad Mehedi Hassan, *Senior Member, IEEE*

***Abstract*— The widespread use of social media platforms has led to an increase in the dissemination of fake news with the intention of manipulating public opinion and causing chaos and panic among the population. To address this issue, we focus on detecting the organized groups that participate together in fake news campaigns without prior knowledge of the news content or the profiles of social accounts. To this end, we propose a *spatial–temporal similarity graph*, a novel graph structure that connects social accounts that participate in the early stage of similar fake news campaigns. A community detection algorithm is applied on the similarity graph to cluster the users into communities. We propose a *community labeling algorithm* to label the communities as benign or malicious based on the output of a fake news classifier. Evaluation results show that the community labeling algorithm can correctly label the communities with an accuracy of 99.61%. In addition, we perform a statistical comparison analysis to identify the structural community features that are statistically significant between benign and malicious communities.**

***Index Terms*— Community detection, community labeling, fake news, similarity graph.**

I. Introduction

SOCIAL media are playing an increasingly significant role in today's society. People use these platforms to report events and share news on a large scale. It has become commonplace for news to reach people through social media before being broadcast by traditional media such as TV, radio, and newspapers.

In general, users do not check the accuracy of news and content they share on social media, resulting in the wide dissemination of fake news. Fake news can take many forms, including clickbait, disinformation, misinformation, hoax, parody, satire, rumor, and deceptive news [1], [2], [3]. Fake news can have negative effects on users and society. For instance, fake news can manipulate public opinion and be exploited by states to negatively influence the political decisions of a population and destabilize society.

Different approaches have been proposed in the literature to deal with fake news [1]. The first approach focuses on analyzing the content of news to determine whether it is fake or not. The second approach aims at detecting social bot accounts that are programmed to launch different attacks, including spreading fake content. The third approach focuses on detecting fake news campaigns that aim to manipulate public opinion in an organized way. To this end, the propagation patterns of news are analyzed, as fake and real news propagate differently.

Although detecting fake news campaigns has received attention in the literature [4], [5], [6], it cannot identify the source of the threat, i.e., the human and social bot accounts that intentionally participated in the campaigns. People could participate in the fake news campaign without bad intentions because they simply disseminated every news they received or wanted to express an opinion regarding the news.

To address the above limitation, we focus in this article on identifying the threat actors behind the news campaigns, i.e., groups of social accounts that spread the fake news in an organized manner. To this end, we rely on the assumption that these organized groups actively participate together in many news campaigns. In addition, the organized groups are considered early birds as they usually start the news campaigns or join them in early stages [7].

In this article, we propose a novel approach for detecting organized social groups that participate in fake news campaigns without prior knowledge of the news content or user profiles. We use the assumption that these groups actively participate together in many news campaigns. We cluster these groups using a community detection algorithm based on their spatial–temporal correlated activities in the fake news campaigns. Our main contributions are as follows.

1) We propose a novel graph structure called the *spatial–temporal similarity graph*, which connects social accounts that participate in the early stage of similar fake news campaigns.
2) Based on this similarity graph, we apply a state-of-the-art weighted community detection algorithm, named the label propagation algorithm (LPA), to identify the

Manuscript received 31 December 2022; revised 1 April 2023; accepted 24 May 2023. This work was supported by the Deanship of Scientific Research, King Saud University through the Vice Deanship of Scientific Research Chairs, Chair of Pervasive and Mobile Computing. *(Corresponding author: Abdelouahid Derhab.)*

Abdelouahab Amira, Samir Hadjar, and Mustapha Merazka are with the Research Center for Scientific and Technical Information (CERIST), Algiers 16000, Algeria, and also with the Departement Informatique, Faculte des Sciences Exactes, Universite de Bejaia, Bejaia 06000, Algeria (e-mail: amira@cerist.dz; hadjar@cerist.dz; mmerazka@cerist.dz).

Abdelouahid Derhab is with the Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh 11451, Saudi Arabia (e-mail: abderhab@ksu.edu.sa).

Md. Golam Rabiul Alam is with the Department of Computer Science and Engineering, BRAC University, Dhaka 1212, Bangladesh (e-mail: rabiul.alam@bracu.ac.bd).

Mohammad Mehedi Hassan is with the Department of Information Systems and Research Chair of Pervasive and Mobile Computing, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia (e-mail: mmhassan@ksu.edu.sa).

Digital Object Identifier 10.1109/TCSS.2023.3282572