Influence Estimation Systems in Social Networks – State of the Art and Credibility Issues

Eleni Koutrouli Antonia Athanasakou Aphrodite Tsalgatidou

Department of Informatics & Telecommunications
National & Kapodistrian University of Athens
Athens Ilisia Greece

{ekou, sdi1400004, atsalga}@di.uoa.gr

ABSTRACT

In the last years, Social Networks have become an integral part of contemporary life. They are being used widely in order to communicate, share opinions on various matters and get informed about the news, while influence in Social Networks has been attracting a lot of attention. This has increased the need for influence estimation systems that can estimate / predict the influence of an entity which motivated us to create a more detailed analysis framework for those systems and use it for analyzing a number of them. The goal of this framework is to differentiate and analyze the different concepts of influence and influence estimation systems, identify malicious behavior that can affect the influence estimation and facilitate the design of a credible influence estimation system.

CCS CONCEPTS

• Information systems- Data management systems

KEYWORDS

Influence, Social Networks, Attacks, Credibility

ACM Reference format:

E.Koutrouli, A. Athanasakou, A. Tsalgatidou. 2021. Influence Estimation Systems in Social Networks – State of the Art and Credibility Issues. In *Proc. of 3rd Summit on Gender Equality in Computing (GEC 2021), Athens, Greece.*

1 Analysis Framework for Influence Estimation Systems for Social Networks

Influence estimation systems (IESs) in social networks (SNs) have attracted a lot of research activity and interest in various fields [1]. The need for efficient IESs has motivated us to study the state-of-the-art of IESs and propose an analysis framework for them by creating a taxonomy that consists of three main components as depicted in Fig 1; influence conceptual model, data acquisition and influence estimation. For the conceptual model, we first consider the goal of the influence calculation which can be the identification of the most influential entities, prediction of influence, discovering of expertise etc. The target of the IES, i.e. users or content, is also taken into account, along with the particular concept of influence. Regarding the data acquisition phase, the kind of information used, particularly social activity and graph data, as well as information regarding the quality and novelty of content are considered. Metadata, such as the number of followers and followees, etc., content analysis-related data (hashtags and keywords) and time-related data are also used. The data collection process is also a parameter used in our analysis. Finally, for the influence estimation component, the metrics used for the aggregation of information, possible machine learning techniques that are used and also the display method of influence are important characteristics that determine the final estimation and presentation of influence.

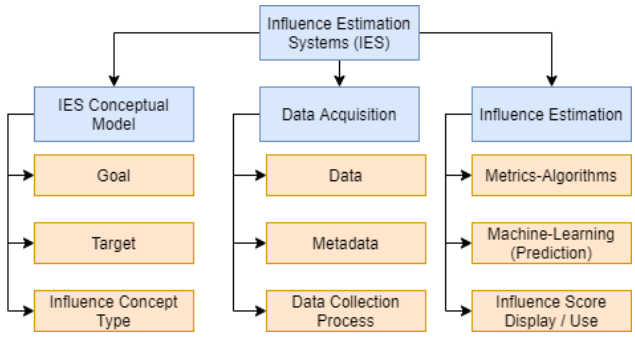

Figure 1: Taxonomy of IESs

2 Attacks and Issues affecting IESs

The analysis of IESs through the created taxonomy, revealed some similarities between them regarding their susceptibility to various attacks. Those attacks can be classified as: (a) Creating fake activity in SNs so as to boost or lower one's influence, (b) Posting and promoting fake content [2]. We also explore other issues that may affect negatively an IES, such as the use of irrelevant data or metrics. Our work can be used for designing credible and efficient IESs for SNs, by facilitating the right design choices and resilience mechanisms.

REFERENCES

[1] . Razis, I. Anagnostopoulos, 2018. Modeling Influence with Semantics in Social Networks: A Survey. ACM Computing Surveys (CSUR), V. 53. https://doi.org/10.1145/3369780

[2] C. S. Atodiresei, A. Tănăselea, A.Iftene, 2018. Identifying Fake News and Fake Users on Twitter. Procedia Computer Science., v. 126, pp. 451-461. 10.1016/j.procs.2018.07.279.