SOME METHODS FOR RUMOR PREVENTION IN SOCIAL NETWORKS

The thesis submitted in partial fulfilment

for the Award of Degree

DOCTOR OF PHILOSOPHY

by

SHRUTI BAJPAI

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY

(BANARAS HINDU UNIVERSITY)

VARANASI -221005

INDIA

Roll No.: 17071503 **Year: 2024**

Chapter 6

Conclusion and Future Work

In this paper, we explore and present two issues related to rumors and different approaches to dealing with them. We also delved into various challenges that come with these issues and explained how our methods tackle these challenges. This chapter presents the overall conclusion of the thesis in Section 6.1, where we examine the outcomes of the thesis objectives. Furthermore, we present potential areas for future research based on the findings made in this thesis in Section 6.2.

6.1 Conclusions

Rumors are one of the most prominent problems in social networks. They can adversely affect society by creating social unrest, panic, and harming the reputation of people. Prevention of rumors is thus important to maintain peace and safeguard people's rights and well-being. This thesis is an attempt towards providing solutions for two important issues related to rumors, i.e., identifying the source of rumors and preventing the spread of rumors in the social network. To achieve this, we contributed three models as discussed in Chapter 3, 4 and 5 respectively. The conclusion of each contribution is presented in the following paragraphs.

Ontology based model for rumor source identification- In Chapter 3, our aim is to provide a semantic web solution for finding the rumor source initiator on OSNs using ontologies, the semantic web technology. We present a three-layered ontology-driven model for OSNs having a design-time layer that defines a domain-specific upper-level ontology for OSNs that is vendor-independent, an integration layer that populates the ontology with data from OSNs, creating a knowledge base in the form of RDF triples and runtime layer which queries the knowledge base using SPARQL to detect rumor initiators based on temporal data and user activities. Two case scenarios are considered in the model- when rumor veracity is known and when rumor veracity is unknown. In the first scenario, the model backtracks user activities to find the earliest instance of rumor propagation. The second scenario further analyzes user and post features to determine the credibility of the rumor's initiator. The model is tested for a Twitter case study and the OQuaRE framework is used to evaluate the quality of the ontology. The model scored a global average of 4.24, indicating that it is generally acceptable but that there is room for improvement in structural and functional adequacy. A significant feature of the model is its support for interoperability across different OSNs. This is achieved by mapping vendor-specific lower-level ontologies to the generic upper-level ontology, ensuring consistent identification across platforms.

SIRB: Rumor Blocking Model- In chapter 4, we present a user's topic interest-based rumor control approach that blocks rumors at node and edge levels. We consider the interest of users in the topic of the rumor, their influence on the network, and their trust in fellow users. We present the SIRB model for blocking rumors at the node and link levels. This model has the potential to immediately contain a rumor by directly preventing its dissemination through strategic blocking at the node or link level. This approach can be particularly effective in stopping harmful content from reaching a wider audience, thus minimizing potential damage. However, this model raises concerns about censorship, as users may perceive this method as an infringement on free speech, leading to potential backlash and loss of trust in the platform. The risk of false positives, where legitimate content or users are mistakenly blocked, can inadvertently harm innocent parties and disrupt vital communications. In addition, this approach is reactive, that is, it addresses the issue only after the rumor has started to spread, which may not prevent the rumor from gaining initial traction. As networks grow in size and complexity, the scalability of blocking becomes increasingly challenging, making it difficult to monitor and intervene effectively in all cases. These limitations highlight the need for counter-rumor spread methods, which offer a more proactive and scalable solution.

SIRPA: Rumor Prevention Model- Chapter 5 introduces an integrated approach based on MCDM to prevent rumors on social networks. We utilized the AHP-TOPSIS method to identify key nodes in social networks and proposed the SIRPA model for counter-rumor diffusion. This model takes a proactive approach by actively engaging with the network to provide alternative accurate information that can neutralize the impact of the original rumor. This participation helps dilute the false narrative and encourages discussion and critical thinking among the audience, fostering a more informed and discerning community. Also, once the counter-rumor is introduced into the network, it can spread organically, leveraging the network's existing dynamics to reach a broad audience without the need for continuous monitoring or intervention. This makes it particularly effective in large, complex networks where blocking or direct intervention might be impractical. Moreover, by offering an alternative narrative rather than simply suppressing information, counter-rumor methods avoid the pitfalls of censorship, helping to maintain user trust and platform integrity.

6.2 Future Work

In this subsection, we discuss some future possibilities that can further expand and improve the proposed models. There are some aspects that can be investigated, necessitating additional exploration. We list potential avenues for future work as follows:

Ontology based model for rumor source identification- The model introduces the concept of interoperability among different OSNs having semantically equivalent concepts. However, this concept needs to be validated in our proposed work. Regarding future possibilities, we suggest further validation of the model across various OSNs to ensure its robustness and effectiveness in different contexts. Additionally, there is potential for improvement in the structural and functional aspects of the ontology to enhance its accuracy and applicability, particularly by increasing the richness of annotations and properties. We can also expand the ontology model as an overall rumor handler capable of detecting rumors, identifying their sources, analyzing their impact, and suggesting strategies to deal with rumors. This opens another possibility of integrating more advanced AI and machine learning methods for automated extraction and analysis of user and post-features, improving the detection accuracy of rumor initiators. In addition, expanding the model to handle real-time data streams from OSN could enable faster detection and response to emerging rumors.

SIRB: Rumor Blocking Model- For the SIRB model, there are some aspects which need further investigation. First, since users' interests evolve over time, there is potential to incorporate real-time interest tracking into the rumor-blocking model. Second, social networks are inherently dynamic, with nodes and edges continuously added or removed. Therefore, it is essential to develop a rumor blocking model that can adapt to these changing network dynamics.

SIRPA: Rumor Prevention Model- While the proposed SIRPA model shows significant findings, several areas need further investigation. First, the model assumes static social networks, but real-world networks are dynamic, requiring adaptations for continuously evolving structures and updated influential node selection.

Second, the AHP-TOPSIS method's criteria weights are currently based on subjective judgment, and future research could explore other optimization techniques for more objective weight determination. Third, while the focus has been on selecting keynodes, strategic orchestration and placement of these keynodes within the network could further enhance rumor prevention, particularly by considering factors like network density and community structures.