PREFACE

Humans spend a substantial amount of time in social processes, with networking and communication being important aspects of their lives. Earlier, social networking was limited within tribes and communities, having local reach and a limited audience. With the popularity of online social networks (OSNs) in the early 21st century, networking and communication reached a different level with global reach and mass audience. OSNs made the whole world *one global village*. OSN platforms like Facebook, X (formerly Twitter), etc., have facilitated the sharing of ideas, opinions, and news at a massive scale in less time than traditional media. The widespread popularity of OSNs resulted in their extended usages like content sharing, online gaming, support communities, marketing and advertising, social activism and campaigning, etc. This ever-increasing popularity has also turned OSNs into breeding grounds for harmful content like rumors, misinformation, disinformation, hate posts, etc. While it is very important to harness the power of social media, it is very important to safeguard it from harmful content. In this thesis, we have chosen a few important issues related to rumors prevention in OSNs.

Rumors are the unverified piece of information whose veracity status is unknown at the time of circulation. They are often related to some emerging news or controversy and usually disseminate at a faster rate than non-rumors. There is no official responsibility for a rumor, so often, the source of the rumor remains undetected. Rumors may spread due to lack of complete information when the information is released in pieces, lack of evidence to prove the authenticity of the information, or maybe fabricated deliberately in such a way that attracts people to believe them. Rumors are highly undesirable as they create panic, damage reputation, cause financial losses, etc. Based on the above characteristics of rumors, there are many issues to deal with rumors. These issues are detecting whether news is a rumor, finding the initiator of a rumor, determining the veracity status of a rumor,

preventing and controlling the spread of rumors in social networks, assessing the impact of rumors, and many more. In this thesis, we address two issues related to rumors- finding the initiator of a rumor and ways to curtail the rumor spread in a social network.

Often, rumor initiators are left unidentified and face no legal consequence, which promotes rumor-mongering behavior even more. Finding the rumor initiator is one of the most important issues in handling rumors. Many researchers have addressed this problem and proposed solutions from network observation perspectives, centrality and propagation-based approaches, and others. However, there are many existing challenges. Firstly, the solutions proposed are based on network structure-based approaches without considering network semantics. Secondly, the proposed solutions are for networks with limited scope in terms of cycles, directions, and degrees. Thirdly, there is a lack of a common solution that is applicable to all social media platforms. In Chapter 3, we have addressed these issues and tried to provide an ontology-based solution to find rumor initiators in OSNs. Ontologies have been widely used in the social network domain to solve problems associated with social tagging mechanisms, social network access control, rumor detection, rumor modeling, etc. They are considered as excellent tools for providing semantics and interoperability. They are capable of dealing with any network structural constraint and can be queried to extract desirable information.

In Chapter 3, we propose an ontology-based model for OSNs that is intended to find rumor initiators in OSNs. This model comprises three layers- design time, integration, and runtime. The model maps interoperable concepts of different OSNs in the upper-level ontology, which is further used to obtain vendor-specific lower-level ontology. The model is populated and queried using the property path expressions of SPARQL to find rumor initiators for two scenarios, viz., when the veracity of the rumor is known and when the veracity of the rumor is unknown. Further, the proposed model is assessed for its acceptability using the Ontology Quality Requirements and Evaluation (OQuaRE) framework, where the obtained

global average score for the proposed ontology falls into an acceptable scale, making the proposed ontology suitable for rumor source detection.

Another issue that we address in this thesis is the containment of rumors in social networks. Detecting a rumor and identifying its source takes a considerable amount of time. By this time, the rumor has already started to spread in the network and infect nodes. Preventing them at an early stage helps to mitigate the consequential loss and reduces the cost of recovering the nodes affected by rumors in the social network. Rumors can be prevented by disseminating the correct information in the network or by blocking the propagation of rumors. We explored many solutions to prevent and control the spread of rumors in a social network and broadly classified them into three categories- self-media perspective-based approaches, counter-rumor diffusion mechanisms, and rumor-blocking methods. In self-media perspective-based approaches, correct information is disseminated by the authorities or government, by improving literacy and strengthening the public's ability to comprehend the authenticity of the information or by crowdsourcing the user's reaction to rumors etc. However, the credibility and trustworthiness of self-media sources takes time to establish. The perspectives are often limited by the subjective judgment of self-media, and lack of information or ignorance may lead to the inaccurate debunking of rumors. Also, self-media may suffer from the echo chamber effect and confirmation bias.

In rumor-blocking based methods, rumor propagation is blocked at either the node or link levels based on certain assumptions. One such assumption is considering the individual user's interest in a particular topic of the rumor. Users have different interests in different topics, so they consume the rumors related to their interested topic and ignore others. Based on this assumption, in Chapter 4, we propose a rumor-blocking approach that considers the users' topic interest. We consider three factors, i.e., topic interest of users, their influence in the network, and trust in neighbors, and propose two strategies for rumor blocking. The first strategy is node-level rumor blocking, where we consider the node's interest in the

topic and its influence on the network and obtain node-level threshold values for blocking rumors in the network. In the second strategy, i.e., link-level blocking, we consider the similarity in topic interest between two users and trust between them to find the link-level threshold values for blocking rumors. We propose an extended variant of the classical epidemic model Susceptible-Infected-Recovered (SIR) as Susceptible-Infected-Recovered-Blocked (SIRB) to implement these two rumor-blocking strategies in the social network.

Another way to prevent rumors in social networks is using a counter-rumor diffusion mechanism. Counter-rumor messages have to be introduced in the system as soon as a rumor is detected to reduce the time lag between rumor diffusion and counter-rumor diffusion. For counter-rumor diffusion, we need to select a few key nodes and start the counter-rumor diffusion mechanism. These key nodes can be chosen randomly or using a method that maximizes their influence on other nodes. In Chapter 5, we propose an integrated approach for rumor prevention, which selects key nodes for targeted immunization and then runs a counter-rumor diffusion model. For selecting key nodes, we suggest the Analytic Hierarchy Process - Technique for Order of Preference by Similarity to Ideal Solution (AHP-TOPSIS) method, a Multi-Criteria Decision Making (MCDM) based approach that considers multiple criteria for making a decision. Using these key nodes, we propose a counter-rumor diffusion model, Susceptible-Infected-Recovered-Prevented Agent (SIRPA), an improved variant of the SIR model.

In conclusion, this thesis addresses two main issues and their related challenges while dealing with rumors in social networks. The main contributions are exploring and harnessing the advantages of using ontology for rumor source detection and proposing the improved and extended variants of the SIR model that are helpful in rumor prevention. We study the role of MCDM algorithms in finding the key nodes in a social network and their effective use in preventing rumors.