Minimizing the Spread of Misinformation in Online Social Networks: A Survey

DOI:
10.1016/j.jnca.2021.103094

Document Version
Accepted author manuscript

Citation for published version (APA):
Sakellariou, R., & Zareie, A. (2021). Minimizing the Spread of Misinformation in Online Social Networks: A Survey. *Journal of Network and Computer Applications*, *186*, [103094]. https://doi.org/10.1016/j.jnca.2021.103094

Published in:
Journal of Network and Computer Applications

Minimizing the Spread of Misinformation in Online Social Networks: A Survey

Ahmad Zareie and Rizos Sakellariou

Department of Computer Science, The University of Manchester, UK

Abstract

Online social networks provide an opportunity to spread messages and news fast and widely. One may appreciate the quick spread of legitimate news and messages but misinformation can also be spread quickly and may raise concerns, questioning reliability and trust in such networks. As a result, detecting misinformation and containing its spread has become a hot topic in social network analysis. When misinformation is detected, some actions may be necessary to reduce its propagation and impact on the network. Such actions aim to minimize the number of users influenced by misinformation. This paper reviews approaches for solving this problem of minimizing spread of misinformation in social networks and proposes a taxonomy of different methods.

Keywords: Social Networks, Misinformation Spread Minimization, Influence Minimization, Diffusion Models

Contents

1 Introduction **2**

2 Preliminaries **4**

2.1 Online Social Networks 4

2.2 Diffusion Models 5

2.3 Influence Detection Models 6

3 The Problem of Minimizing the Spread of Misinformation **7**

4 Blocking-Based Methods **10**

4.1 Node Blocking Methods 10

4.1.1 Static Approach 11
4.1.2 Adaptive Approach 14
4.2 Edge Blocking Methods 17
4.2.1 Source-Ignorant Approach 18
4.2.2 Source-Aware Approach 19

5 Clarification-Based Methods 20
5.1 Campaign-Oriented Methods 21
5.1.1 Structural Methods 21
5.1.2 Behaviour-Aware Methods 25
5.2 Protection-Oriented Methods 27

6 Evaluation Strategies and Datasets 28

7 Conclusion and Future Directions 31

1. Introduction

The proliferation of internet technologies has led to an increasing number of online social networks and users. Several indicators suggest that the number of users keeps increasing and a large number of people have accepted online social networks as a major source of news. The potential of social networks has led to significant research in trying to propagate news widely by identifying so-called influential users [1, 2]. This problem, known as Influence Maximization [3, 4], has attracted lots of attention recently. However, spreading news fast gives rise to an adverse effect: misinformation can be spread fast too.

Users may spread misinformation inadvertently or with different financial and social motivations [5]. Misinformation propagation has become a significant threat in social networks and reduces the reliability and confidence of the users towards news and messages. As quoted in [6], a report published by the World Economic Forum regards spreading misinformation as one of the top global economic risks. Spreading misinformation or unsubstantiated rumours may have widely negative impact and may lead to economic damages, significant disruption or even widespread panic; various examples have been mentioned in the literature [7, 8, 9, 10, 11, 12]. Misinformation may take different forms. In this paper, the term misinformation is used as a general term to refer to

any false or inaccurate information which may be spread in online social networks intentionally or unintentionally.

Confronting misinformation in social networks has attracted lots of attention among researchers. To deal with it, there are several aspects that have to be addressed: (i) identification of misinformation among newly produced information, also known as misinformation detection, is important as early detection of misinformation decreases the chances of wide propagation with potentially adverse effects; (ii) detection of the sources of misinformation is important as it helps identify the culprits and potentially malicious users who initiate the propagation of misinformation; (iii) tracking subsequent (re)appearances of already detected misinformation, possibly in a slightly altered form but still misinformation; (iv) minimization of the spread of misinformation is another important aspect which aims to prevent the propagation of misinformation in the network. A plethora of methods have been proposed for each of these aspects in the literature.

Methods to detect misinformation and identify sources are reviewed in [13, 5, 14] and [5, 15], respectively. Methods to detect misinformation are based on mapping a stream of social media posts to a classification system that labels posts as misinformation or non-misinformation. Methods to identify sources are based on the network structure and propagation graph from which users or locations that initiate misinformation are identified. In [16], intervention methods for misinformation detection and mitigation are classified and reviewed. Approaches for the development of data mining tools for misinformation tracking and verification are reviewed in [17]. In [18], methods for detection and controlling rumour in social networks are reviewed from a multidisciplinary (Psychology, Sociology and Epidemiology) viewpoint; [18] also reviews the features that favour wide propagation of misinformation. Yet, the literature lacks a comprehensive review and classification of the methods explicitly proposed to minimize the spread of misinformation, which act as an important deterrent when confronting misinformation. Although [5, 18, 16] shortly pay attention to this topic, they do not focus on minimizing the spread of misinformation. This paper aims to fill this gap by reviewing and classifying all existing methods in the literature for the minimization of the spread of misinformation. In comparison with previous surveys, distinct differences of our work are:

- We focus on approaches that minimize the spread of misinformation in social networks, after misinformation has been detected.

- A new taxonomy and a comprehensive review of state-of-the-art methods is presented that offers extensive coverage of the subject.
- Evaluation strategies that include real-world datasets and random models to generate synthetic datasets for evaluation purposes are also presented.
- Current challenges and potential future directions are thoroughly discussed.

The rest of the paper is organised as follows: Section 2 contains definitions and background information. A formal definition of the problem of Minimizing the Spread of Misinformation (MSM) and key strategies to address it are presented in Section 3. A detailed discussion of the different methods to find solutions to the MSM problem is given in Sections 4 and 5. Section 6 covers evaluation strategies and datasets for the assessment of different methods. Finally, Section 7 concludes the paper and discusses future research directions.

2. Preliminaries

2.1. Online Social Networks

An online social network is an abstraction that captures the interactions between people relying on some internet-based infrastructure. People join online social networks with different goals, such as socializing, keeping in touch with friends, as well as reading and/or sharing news. The ability of every user to spread news is an important benefit of online social networks but it has an adverse effect too. Alongside legitimate information, spreading misinformation may have some disruptive impact, including distrust and unreliability towards news [19].

In the literature, an online social network is modelled as a graph. The nodes and edges indicate users and relationships between them, respectively. In this paper, a social graph is denoted by $G = (V, E)$, where $V = \{v_1, v_2, \ldots, v_{|V|}\}$ and $E \subseteq V \times V$ represent nodes and edges of the graph. If $e_{ij} \in E$, it means there is a relationship between nodes v_i and v_j and these nodes are called neighbours. Γ_i denotes the set of neighbours of node v_i; the cardinality of this set indicates the degree of the node, i.e., $d_i = \mid \Gamma_i \mid$. A weight w_{ij} may be associated to each edge e_{ij} indicating the influence (spreading) probability of node v_i on v_j, that is, how likely (weight values closer to 1) or unlikely (weight values closer to 0) it is that node v_i can influence node v_j. In some research, the network is considered as a directed graph. In a directed graph, $e_{ij} \in E$ denotes v_i is an in-neighbour

of v_j and v_j is an out-neighbour of v_i, which assumes that influence is not bi-directional and if one node influences another the opposite is not necessarily true.

In principle, whether the edges are considered as directed or undirected depends on the nature of relationships in the network. For instance, friendship on Facebook is an undirected relationship while the follow relationship on Twitter is a directed relationship. In addition, in some research the network is considered as unweighted graph, which means that all edges have the same influence. If additional information is available, the influence between each pair of users can be determined; then, distinct weights are assigned to the edges and the network is modelled as a weighted graph.

2.2. Diffusion Models

Different diffusion models have been proposed to simulate the process of spreading information and determine the influence of an initial set of spreader nodes. Modelling the behavior of users in accepting and forwarding information in social networks is a challenging topic [20]. Diffusion models aim to describe the propagation process based on some observations about the network. Thus different diffusion models are applied to model the spreading process. In principle there are three main classes for the commonly used diffusion models: threshold models [21, 22], cascading models [23, 24], and epidemic models [25, 26].

The Linear Threshold (LT) model [4] is the most popular threshold model. In this model, each node v_i has an activation threshold Θ_i and can be in either active or inactive state during propagation. In timestamp $t = 0$, the initial spreader nodes are set to active and all other nodes are set to inactive. In each timestamp $t > 0$, each inactive node v_j changes its state to active if $\sum_{v_i \in AN_j} w_{ij} \geq \Theta_j$, where AN_j is the set of neighbours of node v_j which are active in $t - 1$. The propagation process continues until no node is activated in a timestamp. At the end, the number of active nodes indicates the influence of the initial spreader set.

The Independent Cascade (IC) model [4] is a well-known cascading model. Same as with the LT diffusion model, each node can be in either active or inactive state. Initial spreader nodes are set as active in $t = 0$. In each timestamp $t > 0$, each node v_i activated in $t - 1$ has one chance to activate each of its neighbour v_j with probability α. Regardless of whether v_i activates any of its neighbours or not, it moves to inactive state. This process continues until no node is activated in a timestamp t. The number of nodes activated during the process indicates the influence of the initial spreader nodes. Sometimes, influence in the IC model can be determined using the live-edge technique [4].

In this technique some of the edges are set as live and some are set as blocked, randomly. If, after this process, there is a path between two nodes, this implies influence.

The Susceptible-Infected-Recovered (SIR) model [27] is a widely used epidemic model in the literature. In this model, each node can be in either susceptible (SU), infected (IN), or recovered (RE) state. In timestamp $t = 0$, the initial spreader nodes are set to IN and all other nodes are set to SU. In each timestamp $t > 0$, each infected node v_i moves to recovered state with probability β after its attempt to infect each of its susceptible neighbours with probability α. The infection process continues until no infected nodes remain in the graph. At the end of the process, the number of recovered nodes represents the influence of the initial spreader set. The SIR model can be regarded as a generalization of the IC model, as the latter appears to be a special case of SIR in which $\beta = 1$.

In practice, the diffusion process may be repeated many times and the mean of the obtained results may be used to estimate the influence of initial spreader nodes.

2.3. Influence Detection Models

In this subsection different models to determine the influence of a set containing one or more nodes are described.

- Simulation-based model: This model applies a diffusion model by repeating the simulation of spreading process a number of times and considering the mean of the obtained results as the influence of the set. The time complexity of a simulation-based model to determine an influential k-size set is $\mathcal{O}(kr|V|^2|E|)$, where r is the number of times that diffusion process is repeated.

- Path-based model: Maximum Influence Arborescence (MIA) [28] is the most popular path-based model that is based on the idea that the influence diffusion of a node is restricted to a local region. Two trees, known as Maximum Influence In-Arborscence (MIIA) and Maximum Influence On-Arborscence (MIOA), are generated to indicate influencers and influencees of a node, respectively. The size of these trees can be adjusted by a given parameter θ to meet a trade-off between accuracy and time efficiency. The time complexity of the path-based model to determine an influential k-size set is $\mathcal{O}(|V|t_{i\theta} + kn_{o\theta}n_{i\theta}(n_{i\theta} + log|V|))$; where $t_{i\theta}$, $n_{o\theta}$ and $n_{i\theta}$ are the time complexity of constructing MIIA for each node, maximum size of MIIA and maximum size of MIOA, respectively.

- Sampling-based model: Reverse Influence Sampling (RIS) [29, 30] is the most popular sampling model to approximate the influence of a set. The idea is to randomly generate θ samples of the graph. In each sample a node is randomly selected and a set of nodes that can reach this node are determined as the reverse reachable set of the node. The more the number of samples that are covered by a set, the more influential the set is. The time complexity of the sampling-based model to determine an influential k-size set is $\mathcal{O}(\frac{k(|V|+|E|)log^2|V|}{\epsilon^2})$; where ϵ denotes the error of sampling.

- Centrality-based model: This model applies centrality measures [31] which use the graph structure to determine influence and vitality of each node or edge. Some popular centrality measures are betweenness, closeness, degree or weighted degree. This model is highly efficient with linear time complexity but suffers from low accuracy.

Depending on the influence detection model used, we can approximately determine the time complexity of each method in the rest of paper. In general, in terms of time complexity, these models can be ranked from high to low in the order: simulation-based, path-based, sampling-based and centrality-based.

3. The Problem of Minimizing the Spread of Misinformation

Different approaches have been utilized to detect misinformation [13]. Independent of these approaches, once misinformation is detected, a containment strategy should be adopted to minimize the spread of misinformation. In brief, the problem of *Minimizing the Spread of Misinformation* (MSM) can be defined as follows. A set of Malicious Nodes (MN) intends to propagate misinformation in a social network. A solution to the MSM problem aims to minimize the number of nodes that accept (or are influenced by) this misinformation.

The solution can be broadly based on one of two strategies [32, 33, 34]:

- A blocking strategy (network disruption): a set of nodes or edges are blocked (or removed) to minimize the flow of misinformation in the network.

- A clarification strategy (anti-rumour or counterbalance): true information is propagated in order to increase users' awareness and reduce acceptance or spread of misinformation.

Formally, given a graph $G = (V, E)$, a diffusion model μ, a set MN with size $|MN| \geq 1$, solving MSM aims to find and apply a strategy S to minimize the influence of misinformation. Influence of misinformation is determined by the number of users who accept the misinformation during the spreading process following diffusion model μ. This aim is generally defined using Eq. (1).

$$\begin{aligned} S^* = \arg\min \quad & \varphi_\mu^S(G, MN) \\ s.t. \quad & \text{some constraints} \end{aligned} \tag{1}$$

The MSM problem can be also defined as a maximization problem:

$$\begin{aligned} S^* = \arg\max \quad & \varphi_\mu(G, MN) - \varphi_\mu^S(G, MN) \\ s.t. \quad & \text{some constraints,} \end{aligned} \tag{2}$$

where $\varphi_\mu(G, MN)$ and $\varphi_\mu^S(G, MN)$ represent the influence of the set MN (essentially, this influence is the total number of users accepting the misinformation initiated by the users in the set MN) when no containment strategy is applied and when a strategy S is applied to contain spreading, respectively. That is to say, MSM aims to find a strategy S to maximize the number of users who are protected from misinformation.

Selecting a set of nodes or edges to maximize S^* is an NP-complete problem [4]. In some occasions, the problem, as defined in Eqs. (1) and (2), may be monotone and submodular, in which case greedy heuristics may find a solution within a factor of the optimal solution [4]. In function $f(S) = \varphi_\mu(G, MN) - \varphi_\mu^S(G, MN)$, monotonocity implies that, if an element is added to the set by strategy S, it does not cause a decrease of the value of f. If f is a monotone and submodular function, then for each element a, $f(S \cup a) \geq f(S)$.

As mentioned, the strategies to solve the MSM problem can be divided into two main categories: *blocking-based* and *clarification-based*. Blocking-based strategies degrade the topology of the graph and may be further subdivided into *node blocking* and *edge blocking*. Depending on the strategy, the problem, as defined in Eq. (2), can be further elaborated as follows.

Node blocking strategies aim to find a set of nodes, i.e., $NS \subset V$, whose removal minimizes the spread ability of MN in $G(V', E')$; $V' = V - NS$ and $E' = E - \{e_{ij} \mid v_i \in NS \text{ or } v_j \in NS\}$. The problem is then formally defined as in Eq. (3).

$$\begin{aligned} S^* = \arg\max_{NS \subset V} \quad & \varphi_\mu(G(V, E), MN) - \varphi_\mu(G(V', E'), MN) \\ s.t. \quad & \text{some constraints} \end{aligned} \tag{3}$$

If a node is blocked this implies that all edges connected to the node are removed. This may lead to an excessive removal of edges, which may be undesirable. Blocking edges may be regarded as a more delicate strategy than blocking nodes.

Edge blocking strategies aim to find a set of edges, i.e., $ES \subset E$, whose removal minimizes the spread of misinformation in $G(V, E')$, where $E' = E - ES$. The problem is formally defined as in Eq. (4).

$$S^* = \underset{ES \subset E}{\arg\max} \quad \varphi_\mu(G(V, E), MN) - \varphi_\mu(G(V, E'), MN) \\ s.t. \quad \text{some constraints} \tag{4}$$

In practice, blocking strategies may impact users' experience, who may complain or quit a network [35], while they may also be viewed as a violation of freedom expression [36]. This gives more ground to clarification-based strategies where a set of nodes, TN, is selected to carry out a truth campaign and propagate true (illustrative) information. In clarification-based strategies, the MSM problem is formally defined as in Eq. (5).

$$S^* = \underset{TN \subset V}{\arg\max} \quad \varphi_\mu(G, MN) - \varphi_\mu(G, \{MN, TN\}) \\ s.t. \quad \text{some constraints,} \tag{5}$$

where $\varphi_\mu(G, \{MN, TN\})$ represents the spread ability of MN when both sets MN and TN spread two opposite messages. Users receiving true information will not accept misinformation and will not forward it further in the network, thereby reducing spread of misinformation. In other words, rising the awareness of users prevents the adoption of misinformation in this strategy without degrading the graph as it is the case with blocking strategies. Yet, clarification-based strategies may be less efficient in reducing misinformation spread, as also noted in [36]. In fact, an assessment of the advantages and disadvantages of both blocking and clarification strategies in [32] has led to a compound method that is trying to combine the best of the two worlds.

When some users become victims of misinformation, they may resist to change their beliefs even if they later receive correct information. Because of this, blocking-based strategies may be superior to clarification-based strategies as they typically prevent the receipt of misinformation. On the other hand, blocking edges or even nodes for a long period of time may have a negative impact on user experience and may lead to the withdrawal of users from the network. In comparison to edge blocking, node blocking strategies may lead to higher disruption as all edges connected to the blocked nodes are removed.

Overall, the methods that have been developed to solve the problem of minimizing the spread of misinformation, in line with the key strategies discussed, can be broadly classified according to the hierarchy in Figure 1. This classification is used in the following sections to review all relevant methods.

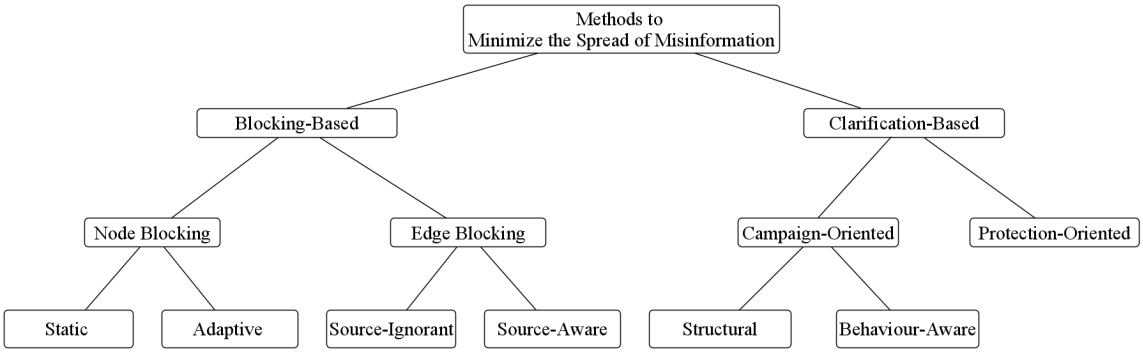

Figure 1: Classification of methods for MSM

4. Blocking-Based Methods

This section covers methods relying on blocking nodes or edges. As discussed, in a blocking strategy a set of nodes or edges are removed to minimize the spread of misinformation in the network.

4.1. Node Blocking Methods

In these methods a set of critical nodes (NS) is identified and these nodes are removed from the social graph; all edges associated with these nodes are accordingly removed. Node blocking methods are also known as node immunization methods in the literature [37, 38, 9]. In principle, there are two different approaches for node blocking: (i) in a *static approach*, NS is selected and nodes are blocked at the beginning of the propagation process; (ii) in an *adaptive approach*, NS is selected and the nodes are blocked selectively during the process to take flow of misinformation into account, thus improving the performance of blocking.

The key properties of both static and adaptive node blocking methods are summarized in Table 1. For each method, the table lists information about the type of graph used to represent the network

and the diffusion model. When there is no indication of the diffusion model used this is because the relevant work deviates from the three common choices. In order to approximately show the time complexity of each method, the model applied for influence detection in each method is also shown in the table.

Table 1: Properties of node blocking methods including class, graph type, diffusion model for propagation (Linear Threshold (LT), Independent Cascade (IC), Susceptible-Infected-Recovered (SIR)) and influence detection model (Influence Model)

Paper (year)	Class	Graph		Diffusion Model			Influence Model
		Directed	Weighted	LT	IC	SIR	
[39] (2002)	Static	No	No				Centrality-based
[40] (2011)	Static	No	No			✓	Centrality-based
[41] (2017)	Static	No	No				Centrality-based
[42] (2013)	Static	Yes	No		✓		Simulation-based
[43] (2019)	Static	Yes	Yes	✓			Sampling-based
[44] (2015)	Static	Yes	Yes		✓		Centrality-based
[45] (2018)	Static	Yes	Yes	✓			Path-based
[9] (2017)	Static	No	Yes			✓	Simulation-based
[46] (2017)	Static	Yes	Yes	✓			Centrality-based
[47] (2018)	Static	Yes	Yes	✓			Simulation-based
[48] (2019)	Static	Yes	Yes	✓	✓		Sampling-based
[49] (2018)	Static	Yes	Yes		✓		Simulation-based
[37] (2018)	Adaptive	Yes	Yes		✓		Path-based
[50] (2019)	Adaptive	Yes	Yes	✓			Sampling-based
[51] (2015)	Adaptive	Yes	Yes				Simulation-based
[35] (2017)	Adaptive	Yes	Yes		✓		Centrality-based
[52] (2019)	Adaptive	No	Yes			✓	Centrality-based

4.1.1. Static Approach

In [39, 40, 41], the impact of removing nodes with high centrality is assessed to determine which centrality measure is the most effective criterion to minimize the spread of misinformation. In [39], the goal is to identify a set of nodes whose removal increases the average distance between each pair of nodes in the graph as this can delay the spread of information (and, consequently, misinformation too). The effect of removing nodes with high-degree and high-betweenness is assessed. The authors show that removal (or immunization) of the high betweenness nodes is a more efficient way to

contain the spread of misinformation in the network. In [40], information spread is regarded as a function of the sum of the sizes of the largest connected clusters. A high-betweenness removal strategy is used iteratively to identify nodes that are immunized. In [41], a random walk algorithm is applied to measure the impact of blocking nodes with high centrality on the spread of information; degree distribution, betweenness and closeness centrality are considered for high centrality. The results show better performance when nodes with high closeness centrality are blocked. In all these methods, the source of misinformation (i.e., the MN set) is ignored, so they can be considered as source-ignorant node blocking methods.

In other methods, selecting nodes for blocking is done by taking into account the MN set. These methods can be regarded as source-aware node blocking methods. In some of these methods a budget constraint, like the number of blocking nodes or the maximum cost of blocking is considered, while some methods aim to minimize the overall cost of blocking assuming that blocking each node has a cost.

In [42, 43, 44], a set of k nodes, NS, is selected, using the constraints $\mid NS \mid \leq k$ and $NS \subseteq V - MN$ (cf. Eq. (3)); removing these nodes (and their associated edges) the aim is to minimize the influence of MN. In [42], NS is initially empty and its members are selected iteratively. In each iteration, t, the node with the maximum marginal gain is added to NS_{t-1}. The marginal gain obtained from blocking node v_i in iteration t is calculated using Eq. (6) as follows:

$$MG(v_i) = \varphi(G'', MN) - \varphi(G', MN). \tag{6}$$

In the equation, G' is obtained by removing nodes NS_{t-1} and the edges connected to them; G'' is also obtained by removing $NS_{t-1} \cup \{v_i\}$ and the edges connected to them. The function $\varphi(G, MN)$ indicates the influence of MN in graph G. In [42], influence is calculated using an IC diffusion model. Stochastic bi-level programming, in the form of leader-follower game, and one Tabu-based search meta-heuristic and one greedy heuristic are proposed to solve the problem in [43]. In [44], a topic-aware method is suggested. In this method, a topic vector $TP = \{tp^{(1)}, \ldots, tp^{(l)}\}$ is taken into account to determine different topics in the social network. A weight vector $W_{ij} = \{w_{ij}^{(1)}, \ldots, w_{ij}^{(l)}\}$ is also associated to each edge e_{ij}, where $w_{ij}^{(z)}$ indicates the strength of influence of user v_i on v_j on topic $tp^{(z)}$. Misinformation, which is propagated in the network, is represented by a vector $\Psi = \{\psi^{(1)}, \ldots, \psi^{(l)}\}$, where $\psi^{(z)}$ indicates the relevance of misinformation to topic $tp^{(z)}$. Given the vectors W_{ij} and Ψ, the probability of spreading misinformation on each edge is calculated. Then,

the top-k central nodes in the neighbourhood of nodes in MN are selected for blocking. In order to define the top-k central nodes, a topic-aware betweenness and a topic-aware degree centrality measure are proposed.

In [45], blocking each node v_i has a cost c_i. The goal is the identification of a set of nodes so that the total cost of blocking the nodes does not exceed a given budget b. It is also assumed that misinformation is not propagated farther than $T \geq 2$ hops from the misinformation source. The authors first consider the problem with only one node as misinformation source. A sub-tree of depth T whose root is the source of misinformation is constructed. The influence of each node v_i on its child nodes is calculated based on a depth-search-first algorithm. A near optimal solution is then found using dynamic programming. To solve the problem in the general case, with more than one node as misinformation source, a greedy algorithm is proposed. The inefficiency of the greedy algorithm motivates the use of a speed-up approach [53] to improve its performance. In the improved algorithm, misinformation sources are merged into a super source node I and the MIA method [28] is applied to determine the influence of each node. Nodes with a maximum ratio of influence per cost are selected iteratively until the budget is exhausted or no node can be selected with the remaining budget.

In [9], it is supposed that there is just one node as the source of misinformation, i.e., $\mid MN \mid = 1$, and misinformation is propagated up to T hops from the source. The goal is to block the nodes with the highest contagious probability, that is nodes that are most likely to get infected by misinformation. To do so, the contagious probability of each node is calculated based on the SIR diffusion model. Nodes whose probability is greater than a given threshold are considered as candidate nodes for blocking. By removing nodes with low spreading ability from the candidate set, the set NS is finally identified. In [46], the LT diffusion model is extended to propose a time-constraint deterministic LT model. A simulation-based greedy algorithm is then proposed to select a set of nodes whose removal minimizes the spread of misinformation. Due to the high time complexity of the simulation-based method, an efficient heuristic algorithm is also proposed.

Finally, in some research, the goal is to select the smallest set of nodes whose blocking causes a reduction to the spread of misinformation greater than a given threshold. The authors in [47, 48] apply a sampling approach to find the smallest set of nodes whose removal ensures that no more than λ users are influenced by misinformation. In [47], nodes with the maximum marginal gain are added to NS with a greedy approach. In order to calculate the marginal gain of nodes the

authors try different mechanisms such as the live-edge method [4], a speed-up approach [53] and a lazy-forward method [54]. The authors in [48] emulate the spreading process using the LT and IC diffusion models. They show that the problem of the reduction of the spread of misinformation greater than a given threshold is not submodular in the IC model. They apply the speed-up approach [53] to merge MN nodes into a super source node and construct an instance $\hat{G}$ of graph G; the live-edge method is then used to obtain different sample graphs. For each sample, a Directed Acyclic Graph (DAG), rooted in super source node, is built using depth-first traversal to calculate the gain from blocking each node. Nodes with maximum gain are iteratively added to NS with the gain of remaining nodes updated in each iteration.

The community structure of the network is taken into account in [49]. It is assumed that misinformation originates from a set of users in community C_r. In addition to reducing the influence of MN to less than a given threshold, the authors try to prevent influencing so-called bridge nodes (nodes which connect C_r to other communities). This prevents spreading of misinformation to the entire network. Based on minimum vertex cover set, a two-step greedy algorithm is proposed to select NS. In the first step, bridge and reachable nodes are identified using breadth-first traversal originating from nodes in MN; then, the minimum number of nodes needed to protect the bridges are blocked. In the second step, while the influence of MN is greater than the threshold, nodes with the maximum marginal gain are iteratively added to NS; the set of reachable nodes is updated in each iteration.

4.1.2. Adaptive Approach

Instead of selecting and blocking nodes at the beginning of the propagation process, critical nodes can be identified and blocked during the propagation process. Take the schematic graph in Figure 2, for example. Suppose that node M is a malicious node, a source of misinformation, and we have the option of blocking two nodes. Using a static approach it is sensible to block nodes A and B (due to the greater number of out-neighbours compared to C) at the beginning of the propagation process (i.e., $t = 0$) as this shields a large part of the graph (see Figure 2(a)). However, suppose that at $t = 1$ propagation from node M flows as indicated by the red edges in Figure 2(b). In this situation, node B appears to be unaffected and, hence, keeping node B blocked brings no benefit. Instead, blocking node D at $t = 2$ can be more important to stop further spread of misinformation from node C. This example highlights that adaptive actions, depending on the flow

of misinformation, may be more efficient in containing the propagation of misinformation. The goal of methods relying on an adaptive approach is to block nodes based on the flow of misinformation during the propagation process.

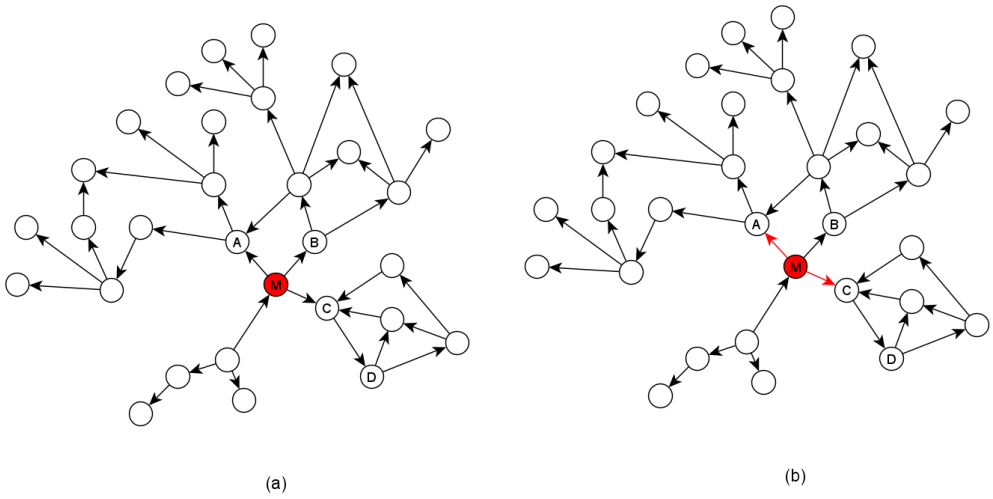

Figure 2: Adaptive approach for node blocking

The connection between the static and the adaptive approach is considered in [38]. To do so, the SIR diffusion model is extended to model their relationship and then applied to assess the impact of the adaptive approach on the propagation process. The effect of the size of MN and propagation probability on these approaches is also studied. The findings suggest that, in essence, the static and the adaptive approach may overall perform similarly, yet an adaptive approach may achieve this result with fewer nodes blocked.

In [37, 50, 51], at each timestamp t during the propagation process, some nodes are dynamically identified and blocked. The goal is to minimize the number of nodes influenced by misinformation at the end of the propagation process. In [37], a heuristic is proposed to calculate the gain from blocking each node based on the propagation probability between a node and all other nodes in the network. At each timestamp t, the node with the maximum gain, BG^t_{max}, is determined and blocked if the expectation of maximum gain at $t+1$ is less than BG^t_{max}. This algorithm is repeated at each timestamp t until k nodes are blocked. The authors in [50] propose two different policies for blocking nodes during the propagation process. In the k-R policy, nodes are blocked in T rounds

and in each round an equal number of nodes, i.e., k/T, with maximum marginal gain, are selected and blocked; a live-edge technique is applied to determine the marginal gain of nodes. In the α-T policy, in each round, a decision on blocking some nodes is made based on the the number of nodes that are reachable from infected nodes. The Reverse Influence Sampling method [29, 30] is also applied to propose a scalable implementation of these policies. In [51], it is supposed that apart from being influenced by neighbours in online social networks, users may be influenced by external sources during the propagation process. In this situation, the importance of using an adaptive approach to block nodes during the propagation process increases. A simulation-based method is proposed to estimate the number of nodes blocked in each timestamp t, say k_t. A heuristic is then proposed to compute the immunization ability (equivalent to gain from blocking) of each node. In each timestamp t, k_t nodes with the highest immunization ability are determined and blocked; the immunization ability of remained nodes is then updated.

A dynamic node blocking method based on user experience is considered in [35]. Rumour popularity (indicating the interest of users to the topic of rumour) and the degree of tolerance to the period of time that users can be blocked are taken into account. Global popularity and individual tendency are integrated using the Ising model [55] to model rumour popularity over the time of propagation. User experience is employed to determine the threshold of tolerance to blocking time for users. The goal is to minimize the influence of a rumour by blocking k critical nodes under the constraint of the users' tolerance threshold. A node blocking approach to minimize the spread of misinformation in temporal networks is studied in [52]. It is supposed that nodes and edges are dynamic during the propagation process and nodes are blocked dynamically over this process. The minimum vertex cover is applied to find critical nodes at each timestamp. Due to its time complexity, graph embedding techniques are used to construct a feature-based representation of each node and an approximate solution is determined with the help of refinement learning.

Each of the approaches for node blocking has advantages and disadvantages. Static approaches for node blocking are simple and cheap but may suffer from inaccuracy as they do not deal directly with the propagation pattern. On the other hand, adaptive approaches can improve the effects of blocking by taking into account the pattern of propagation in the network but at the expense of higher computational cost due to the need of monitoring and tracking the propagation pattern.

4.2. Edge Blocking Methods

In node blocking methods the objective is to remove nodes. Edges are blocked when the nodes connecting these edges are blocked. However, as each node may be connected to other nodes through a number of edges, this may remove a large number of edges to such an extent that it may drastically change the network structure. Edge blocking methods aim to address this by identifying a set of critical edges to block, thereby minimizing the spread of misinformation. There are two approaches for edge blocking: (i) a *source-ignorant approach* ignores the source of misinformation and aims to identify a set of edges whose removal minimizes the flow of information in the network; (ii) a *source-aware approach* considers the source(s) of misinformation to identify a set of edges for blocking. In both approaches, the goal is always to minimize the spread of misinformation in the network.

The key properties of the edge blocking methods are summarized in Table 2.

Table 2: Properties of edge blocking methods including source (ignorant or aware), graph type, diffusion model for propagation (Linear Threshold (LT), Independent Cascade (IC), Susceptible-Infected-Recovered (SIR)) and influence detection model (Influence Model)

Paper (year)	Source	Graph		Diffusion Model			Influence Model
		Directed	Weighted	LT	IC	SIR	
[56] (2008)	Ignorant	Yes	Yes	✓			Simulation-based
[57] (2008)	Ignorant	Yes	No		✓		Simulation-based
[58] (2009)	Ignorant	Yes	No		✓		Simulation-based
[59] (2013)	Ignorant	Yes	Yes	✓			Simulation-based
[60] (2012)	Ignorant	Yes	No				Centrality-based
[40] (2011)	Ignorant	No	No			✓	Centrality-based
[41] (2017)	Ignorant	No	No				Centrality-based
[61] (2014)	Aware	Yes	Yes		✓		Simulation-based
[62] (2014)	Aware	Yes	Yes	✓			Simulation-based
[33] (2019)	Aware	Yes	Yes		✓		Path-based
[63] (2013)	Aware	Yes	Yes	✓			Centrality-based
[64] (2018)	Aware	Yes	Yes	✓			Sampling-based
[20] (2014)	Aware	Yes	No				Centrality-based

4.2.1. Source-Ignorant Approach

The problem of minimizing the spread of misinformation is expressed as a contamination degree minimization problem in [56, 57, 58]. The contamination degree of the network is calculated based on the influence of all nodes in the network. In [56], the problem is defined as the identification of a set of k edges, whose removal minimizes the average contamination of all nodes under the LT diffusion model. An iterative greedy algorithm is then proposed to solve the problem; in each iteration an edge whose removal minimizes the average contamination degree of nodes is selected for blocking. Due to the time complexity of the LT diffusion model, a method based on Bond Percolation [65] is proposed to approximate the solution. The contamination degree minimization problem is defined under the IC diffusion model in [57]. A greedy and a bond percolation based method are then proposed to solve the problem. The contamination degree minimization problem is extended in [58] to define the worst contamination degree of nodes in the network. The worst contamination degree refers to the maximum influence of nodes in the graph, while average contamination degree refers to the expected influence of nodes. A greedy algorithm is then proposed to find a set of k edges whose removal minimizes the worst contamination degree of nodes in the graph. Due to the time inefficiency of the greedy algorithm, a bond percolation based method is also proposed to approximately solve the problem.

The authors in [59] aim to block a set of k edges to minimize the spread susceptibility of the network. The spread susceptibility of the network is defined as the summation of influence of all nodes. They prove that the problem is submodular and monotone under the LT diffusion model. A greedy algorithm using the live-edge method is then proposed, which guarantees a solution within $1 - \frac{1}{\epsilon}$ of the optimal solution. In [60], the eigenvalue of the network matrix is considered as a measure for spread susceptibility in the network; the goal is to identify a set of edges whose removal minimizes the eigenvalue of the matrix. Based on eigenvalues a score for each edge is computed. Then, the k edges with the highest score are considered as a solution of the problem. The sum of the sizes of the largest connected clusters of the graph is defined as the spread susceptibility of network in [40]; betweenness centrality of the edges is considered as a measure to select edges whose removal minimizes the spread susceptibility. The problem is defined under a random walk model in [41] and betweenness centrality of the edges is again used to select edges.

4.2.2. Source-Aware Approach

In this approach, it is assumed that a known set of malicious nodes, MN, is the source of the misinformation in the network. The goal is to identify a set of edges whose blocking (removal) minimizes the spread of misinformation that is initiated by nodes MN.

In [61, 62], the aim is to find a set of edges ES, with size k, to minimize the spread of misinformation. An iterative greedy algorithm, under the IC diffusion model, is proposed in [61]; in each iteration, the edge with the maximum marginal gain is added to ES. Due to the high computational time of calculating the influence of a set using diffusion models, the live-edge method is applied to propose an efficient iterative greedy method in [62]. In addition, a descendant-counting tree structure is proposed to update the marginal gain of edges in each iteration of the greedy algorithm efficiently. In [33], the goal is to block k edges of a candidate set to minimize the sum of the activation probability of nodes in the network. The activation probability of a node denotes the probability that the node is influenced by the nodes in MN, in other words, how vulnerable the node is to the misinformation spread by the nodes in MN. Then, a greedy algorithm is proposed that iteratively selects an edge with maximum marginal gain and updates the activation probability of nodes. In [63], it is assumed that blocking each edge has a cost. Problems under a budget constraint are defined and several greedy algorithms are then proposed.

In [64, 20], the problem is considered as a target-based problem. In this problem, the goal is to minimize the spread of misinformation towards a given target set TS. In [64], the problem is solved under two scenarios: (i) unconstrained, where an unlimited number of edges may be blocked to protect TS; (ii) constrained, where at most k edges are blocked to protect TS to the best extent possible. The unconstrained scenario is solved using the minimum cut problem [66]. A sampling-based solution is proposed to select k critical edges in a greedy (and iterative) manner to solve the constrained scenario. The target-based problem is defined under an extension of a cascading diffusion model in [20]; a mathematical programming method is then proposed to identify a set of critical edges.

Compared to source-ignorant edge blocking strategies, source-aware edge blocking strategies may be more effective in terms of blocking misinformation. However, trying to determine the sources accurately and fast is a challenging issue and the effort to achieve this may come at the expense of focusing on actual edge blocking.

5. Clarification-Based Methods

In these methods, once again, the assumption is that misinformation originates from a set of certain malicious nodes, MN. However, the aim is to identify a set of nodes, TN, to initiate a truth campaign, that is, to spread a clarification message that will counter the misinformation originating from MN. The ultimate goal is to minimize the number of users accepting (or influenced by) the misinformation. It is noted that this problem, first modelled by He et al. in [67], is different from the related problem of competitive influence maximization [68], where multiple campaigns are trying to maximize their influence at the same time minimizing the influence of all other competing campaigns. To illustrate this, consider the directed graph shown in Figure 3. Assume that node M is the originator of a misinformation campaign. When the aim is to minimize the spread of misinformation through a clarification message, selecting node B is the best choice as it stops node M from spreading misinformation further. However, in competitive influence maximization where the aim is to maximize the spread of an initiator's own message, selecting node A would look the best choice.

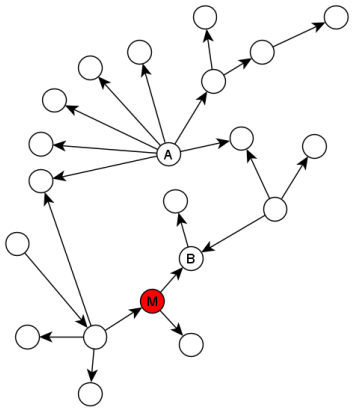

Figure 3: Clarification-based misinformation minimization versus competitive influence maximization.

Clarification-based methods are broadly divided into two categories: (i) *campaign-oriented methods*, where, given a limit for the size of the truth campaign, the aim is to identify appropriate nodes to initiate the truth campaign so that the spread of misinformation is minimized; (ii) *protection-oriented methods*, where the aim is to identify a minimum number of nodes to initiate the truth campaign so that a given proportion of users in the network are protected from misinformation.

The key properties of the clarification-based methods are summarized in Table 3. As noted, in these methods misinformation and truth are spread simultaneously. Thus, besides the type of graph and diffusion model, it is useful to annotate each method with additional information. The column SP (standing for spread probability) shows whether some research assumes that the spread probability of misinformation and truth on each edge is the same or it can differ (same or diff in the table). The column bias shows what happens when a node is activated by both misinformation and truth campaigns at the same time: negative means that the former wins, positive means that the latter wins, whereas unbiased means that some other criterion is used to decide (such as message popularity, users' interest in message, etc).

5.1. Campaign-Oriented Methods

In these methods there is a budget k, which is typically equivalent to the number of nodes that can be used for a truth campaign. The goal is to identify a set TN containing at most k nodes to initiate a truth campaign to minimize the influence of MN, that is, to minimize the number of nodes activated (i.e., users influenced) by misinformation. According to the information considered to select TN, campaign-oriented methods can be divided into two categories: (i) *structural methods* that select TN simply on the basis of structural information of graph; (ii) *behaviour-aware methods* where, in addition to graph structure, individual behaviour of users such as preferences, interests, personal profit or location may also be taken into account to select TN.

5.1.1. Structural Methods

In these methods, a set of nodes is selected to initiate a truth campaign. The selection is based on structural properties of the network graph, something that makes these methods widely applicable as structural information is supposed to be readily available.

Some structural methods consider this problem using an LT diffusion model. In fact, this is the approach considered by the first paper in the topic [67], where a competitive LT diffusion model is proposed to simulate the spreading process of the two opposite campaigns by MN and TN. In this model, each node has two thresholds Θ^- and Θ^+, corresponding to an acceptance threshold for misinformation and truth, respectively. Each edge has two weights w_{ij}^- and w_{ij}^+, corresponding to the spread probability for misinformation and truth, respectively. Each node can be in either inactive, $+$ active or $-$ active state during the process. At timestamp $t = 0$, nodes in MN and TN are set to $-$ active and $+$ active, respectively; all other nodes are set to inactive. At each timestamp $t > 0$,

Table 3: Properties of clarification-based methods including: class (Str standing for structural, Beh standing for behaviour-aware, Pro standing for protection-oriented), graph type, diffusion model (Linear Threshold (LT), Independent Cascade (IC), Susceptible-Infected-Recovered (SIR)), influence detection model (Influence Model), spread probability (SP) and Bias

Paper (year)	class	Graph		Diffusion Model			Influence Model	SP	Bias
		Directed	Weighted	LT	IC	SIR			
[67] (2012)	Str	Yes	Yes	✓			Path-based	Diff	Negative
[69] (2015)	Str	Yes	Yes	✓			Simulation-based	Diff	Unbiased
[70] (2016)	Str	Yes	Yes	✓			Centrality-based	Same	Unbiased
[71] (2019)	Str	Yes	Yes	✓			Centrality/Simulation-based	Same	Unbiased
[34] (2020)	Str	Yes	Yes	✓			Centrality/Simulation-based	Same	Unbiased
[72] (2011)	Str	Yes	Yes		✓		Centrality/Simulation-based	Diff	Positive
[73] (2017)	Str	Yes	Yes		✓		Path-based	Diff	Positive
[74] (2019)	Str	No	No		✓		Centrality-based	Same	Negative
[75] (2019)	Str	Yes	Yes		✓		Centrality/Path-based	Same	Positive
[11] (2017)	Str	Yes	Yes		✓		Sampling-based	Same	Negative
[76] (2019)	Str	Yes	Yes		✓		Sampling-based	Same	Negative
[77] (2013)	Str	Yes	Yes	✓	✓		Centrality-based	Same	Positive
[78] (2018)	Str	Yes	Yes		✓		Sampling-based	Same	Negative
[79] (2017)	Beh	Yes	Yes		✓		Sampling-based	Same	Positive
[10] (2014)	Beh	Yes	Yes	✓	✓		Simulation-based	Same	Negative
[12] (2020)	Beh	Yes	Yes		✓		Sampling-based	Same	Unbiased
[80] (2017)	Beh	Yes	Yes	✓			Simulation-based	Same	Unbiased
[81] (2020)	Beh	Yes	Yes				Centrality-based	Same	Unbiased
[82] (2019)	Beh	Yes	Yes		✓		Sampling-based	Same	Negative
[6] (2018)	Beh	Yes	No		✓		Simulation	Same	Unbiased
[83] (2018)	Beh	Yes	Yes		✓		Path-based	Diff	Unbiased
[84] (2019)	Beh	Yes	Yes		✓		Path-based	Diff	Negative
[85] (2018)	Beh	Yes	Yes			✓	Centrality-based	Same	Unbiased
[86] (2012)	Pro	Yes	Yes	✓	✓		Sampling-based	Same	Positive
[87] (2013)	Pro	Yes	Yes	✓	✓		Sampling-based	Same	Positive
[8] (2013)	Pro	Yes	No		✓		Simulation-based	Same	Positive
[88] (2018)	Pro	Yes	No		✓		Simulation-based	Same	Negative

positive (truth) and negative (misinformation) influence propagate independently following the LT diffusion model. Each newly activated node changes its state to − active or + active based on the campaign that activates the node and no longer changes its state in subsequent timestamps. If at a timestamp $t > 0$ a node is activated by two campaigns, negative influence wins. In order to identify influential users to add to TN, the MIA method [28] is utilized to construct a local directed acyclic graph and determine the influence of each node in containing misinformation spread. Nodes in TN are identified in k iterations; in each iteration, the node with the maximum marginal containment influence is added to TN.

In [69, 70], it is supposed that when a campaign initiates the propagation of some information (regardless of whether the message is true or not), the propagation is limited within T hops and fades after this time. In [69], each node has two different thresholds for accepting misinformation and truth; each edge has two different weights indicating spread probability of misinformation and truth. The LT diffusion model is then extended to simulate the spreading process by misinformation and truth campaigns at the same time. In this model, if a node is activated by two campaigns at the same timestamp, the node decides what message to adopt based on its own preferences. An algorithm is then proposed to find a set of nodes to include in the truth campaign. For this purpose, a set of nodes which may potentially be influenced by the misinformation campaign and have high spread ability (hence, they are influential) are detected as gateway nodes. The nodes for the truth campaign are then selected using a simulation based strategy whose aim is to get the truth campaign to influence gateway nodes before they are influenced by misinformation. An extension of the LT diffusion model is also proposed in [70] to calculate the activation probability of each node by the misinformation campaign. An iterative method is then proposed to select the nodes of the truth campaign; in each iteration the node that minimizes the activation probability of all other nodes by misinformation is added to truth campaign.

In [71, 34], it is assumed that the opinion of users, who are influenced by misinformation, may change after receiving information from the truth campaign. The LT diffusion model is extended to simulate the propagation process under this assumption. Two aspects of the problem are then considered: either every node in the network can be selected as a member of truth campaign, or only a subset of predefined nodes. A greedy simulation based method and a page rank centrality based method are then proposed to solve the problem.

In other structural methods, the problem is defined using the IC diffusion model. A Campaign-

Oblivious IC (COICM) model is proposed in [72]. In this model, each node can be in one of three states: C-state (activated by misinformation), L-state (activated by truth) or inactive state. A misinformation campaign and a truth campaign start spreading at the same time, $t = 0$. At each timestamp t, each node v_i activated in $t-1$ has a chance to activate each of its inactive neighbours. If v_j is activated by v_i, the state of v_j changes to v_i's state and cannot change in subsequent timestamps. This process continues until no more node is activated. If a node is concurrently activated by two campaigns, the truth campaign wins. Applying the COICM model, a greedy algorithm is proposed to identify a near-optimal truth campaign. Due to the time complexity of the greedy algorithm, three heuristic methods based on high degree nodes, early infectees and likeliest infectees are also proposed.

The COICM model is also adopted in [73, 74, 75] to simulate the propagation process. In [73], the problem is considered under two scenarios: (i) CMIA-H, where the spread probability of edges for truth is 1; (ii) CMIA-O, where the spread probability of edges for truth is a value between $[0, 1]$. Applying the MIA method [28], an iterative greedy method is proposed where the node with the maximum containment influence is added to the truth campaign in each iteration. In [74], utilizing degree, betweenness and closeness centrality measures, a centrality-based method is proposed to select nodes for the truth campaign. A community-based method using the COICM model is proposed in [75]. In this method, the COCIM model is first applied to determine the communities and the number of malicious nodes (nodes in misinformation campaign) in each community. Based on the number of malicious nodes in each community, a proportion of nodes for the truth campaign is selected from the community. In [11, 76], two sampling-based methods are proposed using the IC diffusion model. A set of reverse tuples are determined using graph sampling in [11], based on which an approximation algorithm is proposed to select TN. Applying the RIS method [29, 30], a hybrid sampling method is proposed in [76] to inform a greedy method to identify the truth campaign.

The authors in [77] argue that some nodes may get contaminated by misinformation and may spread it (inadvertently becoming members of the misinformation campaign) because they are unaware of the truth. Such nodes would change their mind if they are faced with the truth. In these circumstances, the problem is then to select $\lambda \times k \in MN$ and $(1 - \lambda) \times k \in \{V - MN\}$ nodes to spread the truth and contain misinformation. Applying the LT and IC diffusion models, a greedy simulation-based method is proposed to select nodes with maximum marginal containment influence iteratively. In [78], it is assumed that more than one truth campaign may attempt to

contain the spread of misinformation. To deal with this multi-campaign spreading problem, an extended multi-cascade IC diffusion model is proposed; then, applying game theory, a method is described to select nodes.

5.1.2. Behaviour-Aware Methods

In addition to network structure, user characteristics and behaviour are taken into account by behaviour-aware methods. The motivation is that individual user behaviour may allow more elaborate differentiation of nodes than purely structural methods.

In [79, 10], a time delay is introduced to capture the time that two users may need to exchange information between them; the goal is to minimize the spread of misinformation by a deadline T. In [79], each edge is associated with a login probability to denote how quickly information may be received. Depth-first traversal is first applied to determine the threat level of each node in the graph by MN and build a DAG. Breadth-first traversal is then utilized to construct weighted reverse reachable trees. Then, for each node, a score is calculated based on the threat level and the influence of the node. The node with maximum score is selected for the truth campaign. Then, the score of remaining nodes is updated and the process is repeated iteratively until all required nodes are selected. In [10], in addition to login probability, personal interest in misinformation and truth is taken into account for each user. The problem is then considered under the LT and IC diffusion models. Reachable nodes in $t \leq T$ timestamps are selected as candidate nodes. Utilizing a Monte Carlo method, the nodes of the truth campaign are iteratively selected; a candidate node with maximum containment influence is added to the truth campaign in each iteration.

In [12], personal interest in the information related to the misinformation is also taken into account following a source-ignorant approach. The RIS method [29, 30] is utilized to generate a collection of random reverse sets. A greedy method is then described for maximizing weighted coverage to identify TN that considerably covers the reverse random sets.

In [80], it is considered that when a user accepts an opinion, they may change it after receiving other opinions. A credibility score and a renouncement threshold are considered for each node v_i in [80]; the former represents the trustworthiness of v_i and the latter expresses the how easy (or difficult) it is for v_i to renounce an opinion they had. An extension of the LT diffusion model is proposed to simulate propagation with these features. The nodes of the truth campaign are determined using a simulating annealing algorithm. Users' background knowledge, a hesitating

mechanism and a forgetting-remembering factor are taken into account in [81, 89] to model how a user is influenced by misinformation. A 'Human Individual and Social Behaviors' diffusion model is then proposed to model acceptance and spread of misinformation by users. The truth campaign is identified using a greedy algorithm in k iterations, with a node with maximum marginal containment influence added to the truth campaign in each iteration.

In [82], an activity profit is assigned to each edge. The goal is to identify a set of nodes for the truth campaign so that high profit edges become more protected and less likely to be used to spread misinformation. The authors prove that the problem is not submodular nor monotone, and an approximation algorithm is then proposed. In [6], it is supposed that a misinformation campaign and several truth campaigns happen at the same time. The goal is to identify a truth campaign to minimize the spread of misinformation. A multi-cascade diffusion model is proposed to simulate the propagation process. In this model, each user has a priority for each of the cascades and how a message from each cascade may be perceived. This priority is determined based on the reputation of the source, personal opinion and reliability of message. A greedy algorithm is then proposed to determine upper and lower approximations and obtain a solution.

The location of users is taken into account in [83, 84]. In [83], the goal is to minimize the number of users who are located in a region R and are activated (influenced) by a misinformation campaign. A quadtree is constructed based on the location of nodes; traversing this tree determines the nodes in R. Dynamic programming is then proposed to determine the influence of different nodes on the nodes in R using the MIA method [28]. Most influential nodes are greedily identified to contain the spread of misinformation in R. In order to increase the efficiency of the proposed method, pruning nodes with small influence is suggested. In [84], this problem is more constrained as nodes for the truth campaign are selected from the nodes of a specific region; the solution comes through the extension of methods in [83]. User mobility is taken into account in [85] and the SIR diffusion model is extended to simulate rumour propagation in vehicular social networks. In order to contain the spread of misinformation, a set of vehicular nodes are then chosen to spread the truth among other nodes.

In comparison to structural methods, behaviour-aware methods can more effectively minimize the spread of misinformation as they consider user behaviour and preferences. However, such information is not always available in real-world applications, which means that structural methods may be more widely applicable.

5.2. Protection-Oriented Methods

In protection-oriented methods, the problem is the identification of a set TN of minimum size so that a given percentage of users or part of the network are protected from misinformation; these users are not affected by the misinformation campaign.

The problem is modelled as β_T^I-node protector in [86, 87]. In this model, it is assumed that the spread of misinformation is triggered by a set I (source of misinformation), and can be propagated at most T hops from a source. The goal is to identify a set TN of minimum size to protect a fraction of nodes, β, $0 < \beta < 1$. The set I can be known or unknown; T can be unconstrained ($T = \infty$) or constrained by an integer value. Therefore, the problem has four variations. When I is unknown (source-ignorant), the problem changes to influence maximization and it is about the selection of a set TN that influences a fraction of nodes β. An iterative greedy algorithm is proposed to solve the problem with both unconstrained and constrained T; a node with maximum marginal influence is iteratively added to TN for as long as the influence of TN is less than $\beta \times \mid V \mid$. Both the LT and the IC diffusion models can be used by this algorithm to calculate the influence of TN. When I is known (source-aware), with both unconstrained and constrained T, if the number of reachable nodes by I is greater than $(1-\beta) \times \mid V \mid$, an iterative greedy algorithm is applied to protect some of these nodes and achieve the required β protection. Influential nodes are selected and added to TN until the set protects $\beta \times \mid V \mid$. Due to the time complexity of determining the influence of nodes in each iteration, a community-based algorithm is also proposed to protect a fraction of nodes β in each community.

The community structure properties of a network are considered in [8]. It is supposed that the spread of misinformation is triggered by some users in community C_r, i.e., $MN \subset C_r$. The goal is to contain misinformation within the community and prevent its propagation to other communities. For this purpose, so-called bridge nodes, which are nodes located out of C_r and have at least one neighbour in C_r, are first determined. A smallest set of influential nodes is identified to protect a fraction β of the bridge nodes. This problem is solved using greedy algorithms under two different scenarios: (i) opportunistic One-Activate-One where each active node attempts to influence one of its neighbours in the spreading process; (ii) deterministic One-Activate-Many where each active node attempts to influence all of its neighbours. In [88], misinformation spread minimization in multiplex networks is considered; a multiplex network is composed by several social networks which are connected through overlapping users. Overlapping users can spread true information in several

social networks; the goal is to identify the smallest set of nodes that have influence on the overlapping nodes as a way to reduce the influence of misinformation. To solve the problem, a greedy algorithm is proposed that iteratively selects a node with maximum marginal influence using the IC diffusion model.

6. Evaluation Strategies and Datasets

All methods proposed to solve the problem need to be evaluated regarding their performance. In principle, evaluation aims to assess the impact of a method on minimizing the number of nodes of a graph that will be influenced by misinformation. Different graphs are used, which include both synthetic graphs and graphs based on datasets from real-world networks.

In order to evaluate node or edge blocking methods, some nodes are randomly determined as malicious nodes and their spreading ability (that is, how many nodes are influenced by misinformation) is determined. Then, a blocking method is used to block a set of nodes (or, respectively, a set of edges) and the spreading ability of the malicious nodes is re-assessed. The decrease in spreading misinformation indicates the impact of the method.

In clarification-based methods, once again, some nodes are randomly determined as malicious nodes and their spreading ability is determined. Then, a method is used to identify a set of nodes, which will initiate a truth campaign. Both malicious nodes and truth campaign nodes will spread their messages. The number of nodes influenced by misinformation is calculated.

In addition to assessing the impact on minimizing the spread of misinformation, every method is usually assessed with respect to its running time. Typically, a method is ran multiple times and the average running time is reported.

Regarding datasets, random models are used to generate synthetic graphs based on a desired number of nodes, degree distribution, clustering coefficient, etc. A short description of the commonly used models along with the papers that use each of them is given in Table 4.

Table 5 lists some widely used real-world datasets along with a short description and references to papers that use them. Repositories of real-world datasets include: `http://snap.stanford.edu`, `http://konect.cc` and `http://networkrepository.com`.

Table 4: Random models used to generate synthetic graphs

Model	Description	Used by
Barabasi-Albert model [90]	Generates scale free networks which follow a power law distribution degree	[39, 40, 49, 20, 71, 88, 59]
Watts-Strogatz model [91]	Generates small world networks which have a high clustering coefficient and a small average shortest path between pairs of nodes	[39, 43, 20, 71, 88]
Erdos-Reyni model [92]	Generates networks with a small clustering coefficient and a small average shortest path between pairs of nodes	[39, 40, 49, 20]
Dynamic attributed networks with community structure generation model [93]	Generates dynamic networks with a community structure by using micro-operations and macro-operations	[52]
Kronecker model [94]	Generates real life networks with static (power law of degree and eigenvalue distribution, diameter) and temporal (densification of power law, shrinking diameter) properties	[62]

Table 5: Graphs based on real-world datasets

Dataset	Description	Used by
Wikipedia Vote Network [95]	Voting data from the Wikipedia community where directed edges indicate users who voted for other users	[71, 75, 11, 76, 77, 82, 49, 46, 37, 33, 64]
High Energy Physics collaboration network [96]	Scientific collaboration between authors of papers from arXiv	[39, 43, 50, 67, 73, 77, 78, 12, 80, 82, 86, 8, 20]
High-energy physics theory citation network [97]	Citation network from arXiv where a directed edge indicates a paper that cited another paper	[47, 48, 37, 50, 33, 62, 67, 73, 76, 6]
Gnutella peer-to-peer network [96]	Snapshots of the Gnutella peer-to-peer network where directed edges represent connections between hosts	[45, 48, 49, 46, 37, 69, 82]
Epinion Social Network [98]	Consumer reviews from Epinions.com where directed edges indicate a trust relationship	[75, 11, 76, 62, 64, 49]
Slashdot social network [99]	Slashdot user community where edges indicate directed friend/foe links between users	[33, 77, 81]
Youtube social network [100]	Friendships between Youtube users	[11, 76, 81, 88]
Twitter [101, 102, 103]	Relationships between Twitter users	[41, 51, 35, 64, 79, 81, 6, 88]
Meme Tracker [104]	Networks of hyperlinks between news sites where directed edges point to the source	[59, 62, 51]
Oregon Autonomous Systems [97]	A communication network where nodes and edges may be added or deleted over time	[45, 47, 48, 60, 51]
Facebook [101, 103]	Friendships between Facebook users	[44, 9, 35, 61, 63, 69, 74, 78, 81, 83, 84, 86, 88]

7. Conclusion and Future Directions

In this paper, proposed methods for misinformation spread minimization were classified into two categories. In blocking-based methods the idea is to change the network structure; some nodes and/or edges are removed from the network to minimize the spread of misinformation. Blocking nodes and/or edges comes with a cost and may lead to a discredit of the network if it takes a long time to restore connectivity of nodes and edges. In clarification-based methods, the goal is to increase the awareness of users by spreading truth information. This approach does not have the challenges and costs of blocking, but it may be less efficient than a blocking approach.

There are various issues that may drive further research on this topic.

First, the methods proposed have been developed predominantly in the last decade and still need extensive evaluation using different types of networks, diffusion models, and so on. However, as already observed, time complexity is often a key limitation, which may become even more of an issue as there is a need to deal with increasingly larger networks and sophisticated models. This suggests that increased attention on efficiency and scalability of the proposed methods will be necessary to be successful when minimizing the spread of misinformation. In practical terms, it will not be viable for a method to take longer to find a solution that minimizes the spread of misinformation than the time needed for misinformation to propagate, as there is a risk that by the time a solution has been found the situation may have changed completely.

Second, all methods assume that the required data is readily available and correct. However, data availability cannot be always taken for granted. For example, access to complete data about a network and its features or data related to users' behaviour may not be always feasible. Leaving aside issues related to privacy of some of this data, it appears that some methods may have to make decisions under some sort of uncertainty.

Third, most of the proposed methods are designed and evaluated through diffusion models. These models are approximations primarily based on structural information that may fail to generate an accurate diffusion pattern. This means that the performance of different methods may significantly change due to small changes in the diffusion pattern. As reported in [105] the actual propagation pattern of information is likely affected by factors such as human behaviour, common preferences or beliefs and social reinforcement. Diffusion models that take these factors into account can more realistically model the spread of misinformation and help with the evaluation of methods to spread misinformation.

Fourth, as highlighted by this review, the bulk of the methods for minimizing the spread of misinformation are source-aware. When misinformation is detected, one has to pause and detect the sources of misinformation first. Clearly, the success of these methods depends on good methods to detect the sources of misinformation. Proposing methods that can minimize the spread of misinformation even if there is some uncertainty in source detection may also help.

Finally, a key element of the problem is the network structure. Existing research essentially assumes that the network structure is fixed and does not change over time. This may help find solutions but one may easily realize that more dynamic elements in the network structure may make it more realistic to capture the actual interactions in real-world social networks. In fact, multiplex networks (composed of multiple social networks with overlapping users) have already been discussed in some related research in the previous sections. One may think that temporal, dynamic (where the network structure changes over time) as well as multiplex networks may be viewed as a more relevant abstraction of social interactions than fixed networks. Algorithms to minimize the spread of misinformation will need to be developed for such networks.

References

[1] A. Zareie, A. Sheikhahmadi, M. Jalili, Identification of influential users in social networks based on users' interest, Information Sciences 493 (2019) 217–231.

[2] A. Sheikhahmadi, A. Zareie, Identifying influential spreaders using multi-objective artificial bee colony optimization, Applied Soft Computing 94 (2020) 106436.

[3] P. Domingos, M. Richardson, Mining the network value of customers, in: Proceedings of the 7th International Conference on Knowledge Discovery and Data Mining, ACM, 2001, pp. 57–66.

[4] D. Kempe, J. Kleinberg, É. Tardos, Maximizing the spread of influence through a social network, in: Proceedings of the 9th SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM, 2003, pp. 137–146.

[5] P. Meel, D. K. Vishwakarma, Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities, Expert Systems with Applications 153 (2019) 112986.

[6] G. A. Tong, W. Wu, D.-Z. Du, On misinformation containment in online social networks, in: Proceedings of the 32nd International Conference on Neural Information Processing Systems, Curran Associates Inc., 2018, pp. 339–349.

[7] S. Wen, M. S. Haghighi, C. Chen, Y. Xiang, W. Zhou, W. Jia, A sword with two edges: Propagation studies on both positive and negative information in online social networks, IEEE Transactions on Computers 64 (3) (2015) 640–653.

[8] L. Fan, Z. Lu, W. Wu, B. Thuraisingham, H. Ma, Y. Bi, Least cost rumor blocking in social networks, in: 2013 IEEE 33rd International Conference on Distributed Computing Systems, IEEE, 2013, pp. 540–549.

[9] Q. Wu, T. Wang, Y. Cai, H. Tian, Y. Chen, Rumor restraining based on propagation prediction with limited observations in large-scale social networks, in: Proceedings of the Australasian Computer Science Week Multiconference, ACM, 2017, pp. 1–8.

[10] L. Fan, W. Wu, X. Zhai, K. Xing, W. Lee, D.-Z. Du, Maximizing rumor containment in social networks with constrained time, Social Network Analysis and Mining 4 (1) (2014) 214–224.

[11] G. Tong, W. Wu, L. Guo, D. Li, C. Liu, B. Liu, D.-Z. Du, An efficient randomized algorithm for rumor blocking in online social networks, IEEE Transactions on Network Science and Engineering 7 (2) (2020) 845–854.

[12] Q. Fang, X. Chen, Q. Nong, Z. Zhang, Y. Cao, Y. Feng, T. Sun, S. Gong, D. Du, General rumor blocking: An efficient random algorithm with martingale approach, Theoretical Computer Science 803 (2020) 82–93.

[13] A. Bondielli, F. Marcelloni, A survey on fake news and rumour detection techniques, Information Sciences 497 (2019) 38–55.

[14] S. M. Alzanin, A. M. Azmi, Detecting rumors in social media: A survey, Procedia computer science 142 (2018) 294–300.

[15] S. Shelke, V. Attar, Source detection of rumor in social network–a review, Online Social Networks and Media 9 (2019) 30–42.

[16] K. Sharma, F. Qian, H. Jiang, N. Ruchansky, M. Zhang, Y. Liu, Combating fake news: A survey on identification and mitigation techniques, ACM Transactions on Intelligent Systems and Technology 10 (3) (2019) 1–42.

[17] A. Zubiaga, A. Aker, K. Bontcheva, M. Liakata, R. Procter, Detection and resolution of rumours in social media: A survey, ACM Computing Surveys 51 (2) (2018) 1–36.

[18] M. Ahsan, M. Kumari, T. P. Sharma, Rumors detection, verification and controlling mechanisms in online social networks: A survey, Online Social Networks Media 14 (2019) 100050.

[19] K. Shu, A. Sliva, S. Wang, J. Tang, H. Liu, Fake news detection on social media: A data mining perspective, SIGKDD Explorations 19 (1) (2017) 22–36.

[20] Y. Song, T. N. Dinh, Optimal containment of misinformation in social media: A scenario-based approach, in: International Conference on Combinatorial Optimization and Applications, Springer, 2014, pp. 547–556.

[21] A. Borodin, Y. Filmus, J. Oren, Threshold models for competitive influence in social networks, in: International Workshop on Internet and Network Economics, Springer, 2010, pp. 539–550.

[22] M. Granovetter, Threshold models of collective behavior, American Journal of Sociology 83 (6) (1978) 1420–1443.

[23] T. Carnes, C. Nagarajan, S. M. Wild, A. Van Zuylen, Maximizing influence in a competitive social network: a follower's perspective, in: Proceedings of the 9th International Conference on Electronic Commerce, ACM, 2007, pp. 351–360.

[24] J. Goldenberg, B. Libai, E. Muller, Using complex systems analysis to advance marketing theory development: Modeling heterogeneity effects on new product growth through stochastic cellular automata, Academy of Marketing Science Review 9 (3) (2001) 1–18.

[25] A. Buscarino, L. Fortuna, M. Frasca, V. Latora, Disease spreading in populations of moving agents, EPL (Europhysics Letters) 82 (3) (2008) 38002.

[26] J. Zhou, N. N. Chung, L. Y. Chew, C. H. Lai, Epidemic spreading induced by diversity of agents' mobility, Physical Review E 86 (2) (2012) 026115.

[27] R. Pastor-Satorras, C. Castellano, P. Van Mieghem, A. Vespignani, Epidemic processes in complex networks, Reviews of Modern Physics 87 (3) (2015) 925.

[28] W. Chen, C. Wang, Y. Wang, Scalable influence maximization for prevalent viral marketing in large-scale social networks, in: Proceedings of the 16th International Conference on Knowledge Discovery and Data Mining, ACM, 2010, pp. 1029–1038.

[29] C. Borgs, M. Brautbar, J. Chayes, B. Lucier, Maximizing social influence in nearly optimal time, in: Proceedings of the 25th Annual Symposium on Discrete Algorithms, SIAM, 2014, pp. 946–957.

[30] Y. Tang, X. Xiao, Y. Shi, Influence maximization: Near-optimal time complexity meets practical efficiency, in: Proceedings of the 2014 International Conference on Management of Data, ACM, 2014, pp. 75–86.

[31] L. Lü, D. Chen, X.-L. Ren, Q.-M. Zhang, Y.-C. Zhang, T. Zhou, Vital nodes identification in complex networks, Physics Reports 650 (2016) 1–63.

[32] S. Wen, J. J. Jiang, Y. Xiang, S. Yu, W. Zhou, W. Jia, To shut them up or to clarify: Restraining the spread of rumors in online social networks, IEEE Transactions on Parallel and Distributed Systems 25 (12) (2014) 3306–3316.

[33] R. Yan, Y. Li, W. Wu, D. Li, Y. Wang, Rumor blocking through online link deletion on social networks, ACM Transactions on Knowledge Discovery from Data 13 (2) (2019) 1–26.

[34] L. Yang, Z. Li, A. Giua, Containment of rumor spread in complex social networks, Information Sciences 506 (2020) 113–130.

[35] B. Wang, G. Chen, L. Fu, L. Song, X. Wang, Drimux: Dynamic rumor influence minimization with user experience in social networks, IEEE Transactions on Knowledge and Data Engineering 29 (10) (2017) 2168–2181.

[36] A. I. E. Hosni, K. Li, S. Ahmad, Darim: Dynamic approach for rumor influence minimization in online social networks, in: International Conference on Neural Information Processing, Springer, 2019, pp. 619–630.

[37] D. Yang, X. Liao, H. Shen, X. Cheng, G. Chen, Dynamic node immunization for restraint of harmful information diffusion in social networks, Physica A: Statistical Mechanics and its Applications 503 (2018) 640–649.

[38] Q. Wu, X. Fu, Z. Jin, M. Small, Influence of dynamic immunization on epidemic spreading in networks, Physica A: Statistical Mechanics and its Applications 419 (2015) 566–574.

[39] P. Holme, B. J. Kim, C. N. Yoon, S. K. Han, Attack vulnerability of complex networks, Physical Review E 65 (5) (2002) 056109.

[40] C. M. Schneider, T. Mihaljev, S. Havlin, H. J. Herrmann, Suppressing epidemics with a limited amount of immunization units, Physical Review E 84 (6) (2011) 061911.

[41] P. Dey, S. Roy, Centrality based information blocking and influence minimization in online social network, in: 2017 International Conference on Advanced Networks and Telecommunications Systems, IEEE, 2017, pp. 1–6.

[42] S. Wang, X. Zhao, Y. Chen, Z. Li, K. Zhang, J. Xia, Negative influence minimizing by blocking nodes in social networks, in: Proceedings of the 17th Conference on Late-Breaking Developments in the Field of Artificial Intelligence, AAAI Press, 2013, pp. 134–136.

[43] K. Tanınmış, N. Aras, İ. K. Altınel, E. Güney, Minimizing the misinformation spread in social networks, IISE Transactions 52 (8) (2020) 850–863.

[44] Q. Yao, R. Shi, C. Zhou, P. Wang, L. Guo, Topic-aware social influence minimization, in: Proceedings of the 24th International Conference on World Wide Web, ACM, 2015, pp. 139–140.

[45] C. V. Pham, M. T. Thai, H. V. Duong, B. Q. Bui, H. X. Hoang, Maximizing misinformation restriction within time and budget constraints, Journal of Combinatorial Optimization 35 (4) (2018) 1202–1240.

[46] C. V. Pham, H. M. Dinh, H. D. Nguyen, H. T. Dang, H. X. Hoang, Limiting the spread of epidemics within time constraint on online social networks, in: Proceedings of the 8th International Symposium on Information and Communication Technology, ACM, 2017, pp. 262–269.

[47] C. V. Pham, Q. V. Phu, H. X. Hoang, Targeted misinformation blocking on online social networks, in: Asian Conference on Intelligent Information and Database Systems, Springer, 2018, pp. 107–116.

[48] C. V. Pham, Q. V. Phu, H. X. Hoang, J. Pei, M. T. Thai, Minimum budget for misinformation blocking in online social networks, Journal of Combinatorial Optimization 38 (4) (2019) 1101–1127.

[49] J. Zheng, L. Pan, Least cost rumor community blocking optimization in social networks, in: 3rd International Conference on Security of Smart Cities, Industrial Control System and Communications, IEEE, 2018, pp. 1–5.

[50] Q. Shi, C. Wang, D. Ye, J. Chen, Y. Feng, C. Chen, Adaptive influence blocking: Minimizing the negative spread by observation-based policies, in: 35th International Conference on Data Engineering, IEEE, 2019, pp. 1502–1513.

[51] C. Song, W. Hsu, M. L. Lee, Node immunization over infectious period, in: Proceedings of the 24th International Conference on Information and Knowledge Management, ACM, 2015, pp. 831–840.

[52] A. W. Wijayanto, T. Murata, Effective and scalable methods for graph protection strategies against epidemics on dynamic networks, Applied Network Science 4 (18) (2019) 1–32.

[53] Y. Zhang, A. Adiga, S. Saha, A. Vullikanti, B. A. Prakash, Near-optimal algorithms for controlling propagation at group scale on networks, IEEE Transactions on Knowledge and Data Engineering 28 (12) (2016) 3339–3352.

[54] J. Leskovec, A. Krause, C. Guestrin, C. Faloutsos, J. VanBriesen, N. Glance, Cost-effective outbreak detection in networks, in: Proceedings of the 13th International Conference on Knowledge Discovery and Data Mining, ACM, 2007, pp. 420–429.

[55] D. Chelkak, S. Smirnov, Universality in the 2D Ising model and conformal invariance of fermionic observables, Inventiones Mathematicae 189 (3) (2012) 515–580.

[56] M. Kimura, K. Saito, H. Motoda, Solving the contamination minimization problem on networks for the linear threshold model, in: Pacific Rim International Conference on Artificial Intelligence, Springer, 2008, pp. 977–984.

[57] M. Kimura, K. Saito, H. Motoda, Minimizing the spread of contamination by blocking links in a network, in: Proceedings of the 23rd National Conference on Artificial Intelligence, Vol. 2, AAAI Press, 2008, pp. 1175–1180.

[58] M. Kimura, K. Saito, H. Motoda, Blocking links to minimize contamination spread in a social network, ACM Transactions on Knowledge Discovery from Data 3 (2) (2009) 1–23.

[59] E. Khalil, B. Dilkina, L. Song, Cuttingedge: influence minimization in networks, in: Proceedings of the Workshop on Frontiers of Network Analysis: Methods, Models, and Applications at NIPS, 2013.

[60] H. Tong, B. A. Prakash, T. Eliassi-Rad, M. Faloutsos, C. Faloutsos, Gelling, and melting, large graphs by edge manipulation, in: Proceedings of the 21st International Conference on Information and Knowledge Management, ACM, 2012, pp. 245–254.

[61] Q. Yao, C. Zhou, L. Xiang, Y. Cao, L. Guo, Minimizing the negative influence by blocking links in social networks, in: International Conference on Trustworthy Computing and Services, Springer, 2014, pp. 65–73.

[62] E. B. Khalil, B. Dilkina, L. Song, Scalable diffusion-aware optimization of network topology, in: Proceedings of the 20th International Conference on Knowledge Discovery and Data Mining, ACM, 2014, pp. 1226–1235.

[63] C. J. Kuhlman, G. Tuli, S. Swarup, M. V. Marathe, S. Ravi, Blocking simple and complex contagion by edge removal, in: 13th International Conference on Data Mining, IEEE, 2013, pp. 399–408.

[64] X. Wang, K. Deng, J. Li, J. X. Yu, C. S. Jensen, X. Yang, Targeted influence minimization in social networks, in: Pacific-Asia Conference on Knowledge Discovery and Data Mining, Springer, 2018, pp. 689–700.

[65] M. Kimura, K. Saito, R. Nakano, Extracting influential nodes for information diffusion on a social network, in: Proceedings of the 22nd National Conference on Artificial Intelligence, Vol. 2, AAAI Press, 2007, pp. 1371–1376.

[66] C. H. Papadimitriou, K. Steiglitz, Combinatorial optimization: algorithms and complexity, Prentice-Hall, 1982.

[67] X. He, G. Song, W. Chen, Q. Jiang, Influence blocking maximization in social networks under the competitive linear threshold model, in: Proceedings of the International Conference on Data Mining, SIAM, 2012, pp. 463–474.

[68] S. Bharathi, D. Kempe, M. Salek, Competitive influence maximization in social networks, in: Proceedings of the 3rd International Conference on Internet and Network Economics, Springer-Verlag, 2007, pp. 306–311.

[69] H. Zhang, H. Zhang, X. Li, M. T. Thai, Limiting the spread of misinformation while effectively raising awareness in social networks, in: International Conference on Computational Social Networks, Springer, 2015, pp. 35–47.

[70] W. Liu, K. Yue, H. Wu, J. Li, D. Liu, D. Tang, Containment of competitive influence spread in social networks, Knowledge-Based Systems 109 (2016) 266–275.

[71] L. Yang, Z. Li, A. Giua, Rumor containment by spreading correct information in social networks, in: American Control Conference, IEEE, 2019, pp. 5608–5613.

[72] C. Budak, D. Agrawal, A. El Abbadi, Limiting the spread of misinformation in social networks, in: Proceedings of the 20th International Conference on World Wide Web, ACM, 2011, pp. 665–674.

[73] P. Wu, L. Pan, Scalable influence blocking maximization in social networks under competitive independent cascade models, Computer Networks 123 (2017) 38–50.

[74] N. Arazkhani, M. R. Meybodi, A. Rezvanian, Influence blocking maximization in social network using centrality measures, in: 5th Conference on Knowledge Based Engineering and Innovation, IEEE, 2019, pp. 492–497.

[75] J. Lv, B. Yang, Z. Yang, W. Zhang, A community-based algorithm for influence blocking maximization in social networks, Cluster Computing 22 (3) (2019) 5587–5602.

[76] G. A. Tong, D.-Z. Du, Beyond uniform reverse sampling: A hybrid sampling technique for misinformation prevention, in: Conference on Computer Communications, IEEE, 2019, pp. 1711–1719.

[77] S. Li, Y. Zhu, D. Li, D. Kim, H. Huang, Rumor restriction in online social networks, in: 32nd International Performance Computing and Communications Conference, IEEE, 2013, pp. 1–10.

[78] G. Tong, W. Wu, D.-Z. Du, Distributed rumor blocking with multiple positive cascades, IEEE Transactions on Computational Social Systems 5 (2) (2018) 468–480.

[79] C. Song, W. Hsu, M. L. Lee, Temporal influence blocking: minimizing the effect of misinformation in social networks, in: 33rd International Conference on Data Engineering, IEEE, 2017, pp. 847–858.

[80] I. Litou, V. Kalogeraki, I. Katakis, D. Gunopulos, Efficient and timely misinformation blocking under varying cost constraints, Online Social Networks and Media 2 (2017) 19–31.

[81] A. I. E. Hosni, K. Li, S. Ahmad, Minimizing rumor influence in multiplex online social networks based on human individual and social behaviors, Information Sciences 512 (2020) 1458–1480.

[82] T. Chen, W. Liu, Q. Fang, J. Guo, D.-Z. Du, Minimizing misinformation profit in social networks, IEEE Transactions on Computational Social Systems 6 (6) (2019) 1206–1218.

[83] W. Zhu, W. Yang, S. Xuan, D. Man, W. Wang, X. Du, Location-aware influence blocking maximization in social networks, IEEE Access 6 (2018) 61462–61477.

[84] W. Zhu, W. Yang, S. Xuan, D. Man, W. Wang, X. Du, M. Guizani, Location-based seeds selection for influence blocking maximization in social networks, IEEE Access 7 (2019) 27272–27287.

[85] Y. Wu, H. Huang, J. Zhao, C. Wang, T. Wang, Using mobile nodes to control rumors in big data based on a new rumor propagation model in vehicular social networks, IEEE Access 6 (2018) 62612–62621.

[86] N. P. Nguyen, G. Yan, M. T. Thai, S. Eidenbenz, Containment of misinformation spread in online social networks, in: Proceedings of the 4th Annual Web Science Conference, ACM, 2012, pp. 213–222.

[87] N. P. Nguyen, G. Yan, M. T. Thai, Analysis of misinformation containment in online social networks, Computer Networks 57 (10) (2013) 2133–2146.

[88] A. I. E. Hosni, K. Li, C. Ding, S. Ahmed, Least cost rumor influence minimization in multiplex social networks, in: International Conference on Neural Information Processing, Springer, 2018, pp. 93–105.

[89] A. I. E. Hosni, K. Li, S. Ahmed, Hisbmodel: a rumor diffusion model based on human individual and social behaviors in online social networks, in: International Conference on Neural Information Processing, Springer, 2018, pp. 14–27.

[90] A.-L. Barabási, R. Albert, Emergence of scaling in random networks, Science 286 (5439) (1999) 509–512.

[91] D. J. Watts, S. H. Strogatz, Collective dynamics of 'small-world'networks, Nature 393 (6684) (1998) 440–442.

[92] P. Erdos, A. Rényi, On the evolution of random graphs, Publications of the Mathematical Institute of the Hungarian Academy of Sciences 5 (1) (1960) 17–60.

[93] C. Largeron, P.-N. Mougel, O. Benyahia, O. R. Zaïane, Dancer: dynamic attributed networks with community structure generation, Knowledge and Information Systems 53 (1) (2017) 109–151.

[94] J. Leskovec, D. Chakrabarti, J. Kleinberg, C. Faloutsos, Z. Ghahramani, Kronecker graphs: an approach to modeling networks, Journal of Machine Learning Research 11 (2) (2010) 985–1042.

[95] J. Leskovec, D. Huttenlocher, J. Kleinberg, Signed networks in social media, in: Proceedings of the Conference on Human Factors in Computing Systems, ACM, 2010, pp. 1361–1370.

[96] J. Leskovec, J. Kleinberg, C. Faloutsos, Graph evolution: Densification and shrinking diameters, ACM Transactions on Knowledge Discovery from Data 1 (1) (2007) 2.

[97] J. Leskovec, J. Kleinberg, C. Faloutsos, Graphs over time: Densification laws, shrinking diameters and possible explanations, in: Proceedings of the 11th International Conference on Knowledge Discovery in Data Mining, ACM, 2005, pp. 177–187.

[98] M. Richardson, R. Agrawal, P. Domingos, Trust management for the semantic web, in: International Semantic Web Conference, Springer, 2003, pp. 351–368.

[99] J. Leskovec, K. J. Lang, A. Dasgupta, M. W. Mahoney, Community structure in large networks: Natural cluster sizes and the absence of large well-defined clusters, Internet Mathematics 6 (1) (2009) 29–123.

[100] J. Yang, J. Leskovec, Defining and evaluating network communities based on ground-truth, Knowledge and Information Systems 42 (1) (2015) 181–213.

[101] J. Leskovec, J. Mcauley, Learning to discover social circles in ego networks, in: F. Pereira, C. J. C. Burges, L. Bottou, K. Q. Weinberger (Eds.), Advances in Neural Information Processing Systems, Vol. 25, Curran Associates Inc., 2012, pp. 548–56.

[102] M. De Domenico, A. Lima, P. Mougel, M. Musolesi, The anatomy of a scientific rumor, Scientific reports 3 (1) (2013) 1–9.

[103] M. Magnani, L. Rossi, The ml-model for multi-layer social networks, in: International Conference on Advances in Social Networks Analysis and Mining, IEEE, 2011, pp. 5–12.

[104] J. Leskovec, L. Backstrom, J. Kleinberg, Meme-tracking and the dynamics of the news cycle, in: Proceedings of the 15th International Conference on Knowledge Discovery and Data Mining, ACM, 2009, pp. 497–506.

[105] S. Pei, L. Muchnik, S. Tang, Z. Zheng, H. A. Makse, Exploring the complex pattern of information spreading in online blog communities, PloS One 10 (5) (2015) 1–18.