

## Chapter 4

# A Rumor Control Model for Social Networks based on Users' Topic Interest

This chapter focuses on the second contribution of this thesis, i.e., suggesting a model for rumor blocking in social networks. We provide an introduction and motivation for the proposed approach in Section 4.1. Section 4.2 shows the proposed approach. This section lists the factors we have considered for rumor blocking in Subsection 4.2.1, strategies for rumor blocking in Subsection 4.2.2 and the proposed rumor blocking model in Subsection 4.2.3. Section 4.3 discusses the results and findings, and Section 4.4 concludes this chapter with a few future possibilities. Detailed related work is provided in Section 2.2.2.

### 4.1 Introduction

To mitigate rumor propagation within social networks, researchers typically employ one of two strategies. The first approach involves controlling rumors by inhibiting their spread throughout the network, either by blocking them at the node

level [16–18] or at the link level [19]. The second approach triggers a counter-rumor diffusion process as soon as a rumor is detected within the system. Although these methods focus on the structural aspects of the network, they overlook the interests of the users.

Some researchers have attempted to incorporate user interests into rumor-blocking strategies [33, 34], considering factors such as age, location, and gender. Although these factors are important for controlling the spread of rumors, they overlook a crucial element, i.e., the topic of the rumors. Rumors are essentially narratives connected to specific events, happenings, or individuals, which are often associated with particular topics or a combination of multiple topics. In social networks, users are typically drawn to certain topics based on their personal preferences. For example, someone might be a sports enthusiast who avoids political news, or they might have varying degrees of interest in multiple topics. This assumption aligns closely with real-world behavior and is essential to consider when addressing rumor propagation.

It is highly likely that a user will choose not to spread a rumor circulating on a social network if the topic does not align with their interests. Users are typically more connected to others who share similar likes and dislikes. Therefore, when a user decides not to pass on a rumor, they can effectively help contain its spread. People's responses to rumors vary based on their interests, which are influenced by factors such as age, location, and occupation. Twitter, for instance, categorizes tweets into 16 topics, as illustrated in figure 4.1. These topics are further classified as suggested, followed, or not interested, reflecting users' preferences. In addition, users often have multiple overlapping interests. The core idea of this chapter is to leverage a user's topic interests to block the spread of rumors.

## 4.2 Proposed Approach for Rumor Blocking

We consider a social network  $G(N, E)$  where  $N$  is the number of nodes and  $E$  is the number of edges in the social network.  $U$  is the set of users  $u_1, u_2, \dots, u_N$

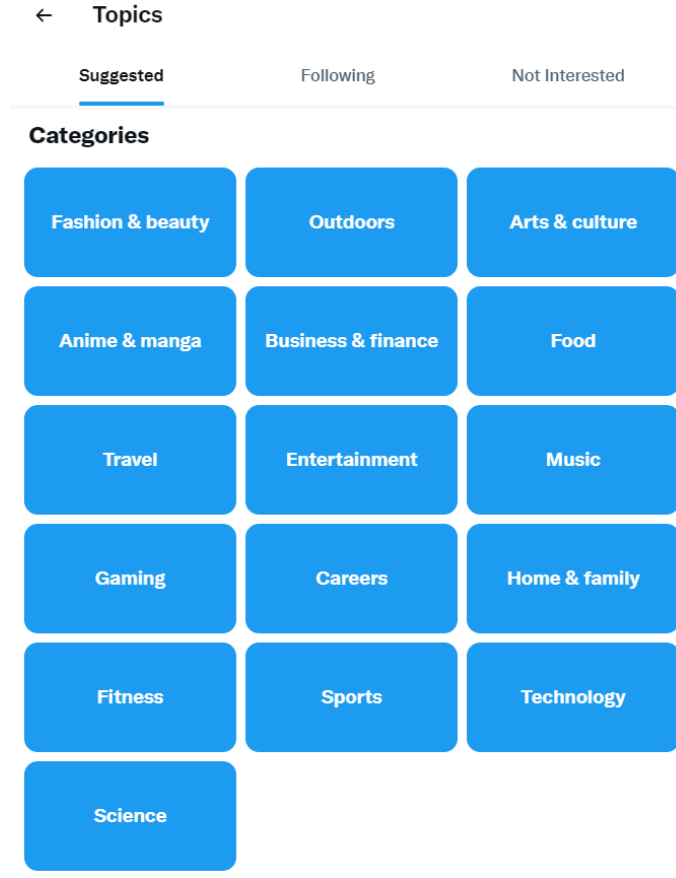


FIGURE 4.1: Categories of Topics suggested by Twitter

connected with each other via links  $e_{ij}$ , when there exists an edge between the nodes  $i$  and  $j$ . Let  $P$  be the set of posts  $p_1, p_2, \dots, p_k$  that circulate on the social network, where  $k$  is the number of posts that circulate on social networks at time  $t$  and  $R$  be a rumor post in circulation such that  $R \in P$ . We assume that each post  $p_i$  belongs to one of the topics  $T_1, T_2, \dots, T_l$  where  $l$  is the number of topics that span multiple domains such as business, politics, entertainment, sport, or others.

### 4.2.1 Factors considered for rumor blocking

To block the rumor in the social network, we consider three factors- user's interest in the topic of the rumor, their influence in the social network, and their trust in the neighboring nodes. These three factors are described as follows.

#### 4.2.1.1 User's topic interest

When a user is interested in a rumor, they will likely consume it and propagate it further. One way to know the user's interest in a post is to find the topic interest of the user. For example, if a user actively follows politics on social networks and consumes related posts, they will likely consume a rumor belonging to the same topic-interest category. Another way to this assumption is that when a user is not interested in the topic of rumor, they will not likely consume it and spread it further. For each topic, social network users have a certain level of interest that is subjective and differs from user to user according to their choice.

We represent a user's topic interest as a vector  $I_m = [i_1, i_2, \dots, i_l]$  where  $I_m$  is the interest vector for  $m^{th}$  user such that  $1 \leq m \leq N$  and  $l$  is number of topics. Each  $I_m$  contains the interest vector of a user for  $l$  number of topics such the  $i_l$  is the user's interest in  $l^{th}$  topic.

#### 4.2.1.2 Influence of the node

Another factor that contributes to rumor blocking on social networks is the influence of the user. We assume that influential users having a high interest in a topic are more useful for blocking rumors than less influential ones. For example, a highly popular user interested in politics is more useful in blocking politics-related rumors. However, if people are not well informed about rumors, they can also be mass spreaders. So, finding and keeping such users well informed about the domain news is necessary.

To find the influential nodes in a social network, we calculate an influence score  $IS$ , for each node. The influence score of each node is calculated based on their position in the network. So, we use the structural properties of the social network topology. To calculate the influence score of the nodes, we have used a multi-criteria decision making (MCDM) method called Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) [59]. TOPSIS is a popular method to

find the influential nodes using the values of the centrality measures of the nodes on social networks [60, 62–64, 120]. We have used degree centrality (*DC*), eigenvector centrality (*EC*), betweenness centrality (*BC*), and closeness centrality (*CC*) as centrality-based criteria. The reason to choose TOPSIS is to find the influence scores of the nodes from multiple perspectives such as popularity, accessibility, and diffusion speed.

To calculate the influence score, we provide a decision matrix  $A_{n*c}$  where  $n$  is the number of nodes, and  $c$  is the number of criteria, which is four in our case. Each element of the decision matrix  $a_{ij}$  represents the  $j^{th}$  criteria value of  $i^{th}$  node. We have a weight matrix  $W$  to store the criteria weight for each criterion. We provide equal weight to all the four criteria. The TOPSIS score for each node is calculated using the method in algorithm.1. The TOPSIS score of each node is the influence score of the node.

---

**Algorithm 1:** Influence Score Calculation using TOPSIS

---

**Input** Decision Matrix ( $A_{n*c}$ )

**Output** Influence-score values (IS)

- 1: Normalize the decision matrix:  $\bar{A}_{ij} = \frac{A_{ij}}{\sqrt{\sum_{j=1}^n A_{ij}^2}}$
  - 2: Calculate the weighted normalized matrix:  $B_{ij} = \bar{A}_{ij} * W_j$
  - 3: Calculate positive ideal:  $P = \max(B_{ij})$
  - 4: Calculate negative ideal:  $N = \min(B_{ij})$
  - 5: Calculate positive separation measure:  $SM_P = \sum_{i=1}^n \sqrt{(B_{ij} - P)^2}$
  - 6: Calculate negative separation measure:  $SM_N = \sum_{i=1}^n \sqrt{(B_{ij} - N)^2}$
  - 7: Calculate influence score:  $IS = \frac{SM_N}{SM_P + SM_N}$
- 

### 4.2.1.3 Trust among the nodes

Trust among nodes also determines to what extent a user will consume a rumor and propagate it further. A user will likely believe a rumor if it is coming from a trusted source rather than a non-trusted source. So, if a rumor comes from a non-trusted source, the user must be less interested in it and block it. Trust can be calculated using the common neighbors approach. It is based on the idea that users

who share many common neighbors are more likely to trust each other. Trust can be calculated using the Jaccard Index [121] as-

$$t_{ij} = \frac{|\Gamma(i) \cap \Gamma(j)|}{|\Gamma(i) \cup \Gamma(j)|} \quad (4.1)$$

Here,  $t_{ij}$  is the trust value between nodes  $i$  and  $j$ ,  $\Gamma(i)$  and  $\Gamma(j)$  are the sets of neighbors of nodes  $i$  and  $j$ , respectively. The fraction numerator represents the number of common neighbors shared by the nodes  $i$  and  $j$ , and the denominator represents the total number of neighbors of the nodes  $i$  and  $j$ . The resulting quotient measures the similarity between the neighborhoods of nodes  $i$  and  $j$ , which can be used to estimate their trust level.

## 4.2.2 Rumor blocking strategy

In this subsection, we propose strategies to block the rumor. Rumor blocking can occur at the node-level or at the link-level. We explain these rumor-blocking level strategies as follows.

### 4.2.2.1 Node-level blocking

In node-level rumor-blocking strategy, we calculate a weighted node interest (WNI) that provides a user's likelihood of engaging with a rumor by combining both their topical interest and influence within the network. The intuitive idea behind using WNI is that users are more likely to consume and propagate a rumor if they are both interested in its topic and in a position of influence. If a user is highly interested in the topic and is also influential, they are more likely to consume and share a rumor. Even if a user is influential, if they have no interest in the topic, they are likely to ignore the rumor. Conversely, if they're interested but not influential, their role in propagation is limited. This approach mirrors empirical behavior where influential users tend to amplify the content they find relevant. So, if the user's WNI in the topic of the rumor is less than a threshold, then they will not

likely consume the rumor and neither forward it. Each  $k^{th}$  node or user has a topic interest vector  $I_k = (i_1^k, i_2^k, \dots, i_l^k)$  where  $l$  is the number of topics and an influence score  $IS(k)$  associated with it. So, we find a weighted node's interest  $WNI$  for node  $k$  as follows-

$$WNI(k) = IS(k) * I_k \quad (4.2)$$

A rumor  $R$  belongs to some topic of interest. Let  $\theta = (\theta_1, \theta_2, \dots, \theta_l)$  be the node-level threshold for each topic to which rumor belongs. Then,

$$\begin{cases} \text{if } WNI(n) < \theta_m : \text{Rumor belonging to topic } m \text{ is blocked for node } n \\ \text{if } WNI(n) \geq \theta_m : \text{Rumor is consumed by node } n \end{cases} \quad (4.3)$$

So, if the user's interest in the rumor topic exceeds the threshold interest, they consume and diffuse the post further; else, block the rumor.

#### 4.2.2.2 Link-level blocking

In the link-level rumor blocking strategy, propagation of rumors through links is blocked if the weight assigned to the link is less than the threshold value for the link. Each link  $e(i, j)$  has a weight  $w_{ij}$  that represents the similarity of topic interests between two nodes. If the topic of interest between two nodes is similar, then the rumor is more likely to propagate between them. The topic similarity between two nodes is calculated using the JS divergence [122]. The JS divergence method is used to calculate the similarity between two probability distributions based on the KL divergence [123]. JS divergence is symmetric in nature and so can be used for directed and undirected networks. The lower the value of JS divergence, the higher the similarity of topic interest between two users. Given  $I_u$  and  $I_v$  be the topic interest vectors for the two users  $u$  and  $v$  and  $I_m$  be the mean of  $I_u$  and  $I_v$ . The similarity score is calculated as follows.

$$KLD(I_u, I_m) = I_u * \log \frac{I_u}{I_m} \quad (4.4)$$

$$KLD(I_v, I_m) = I_v * \log \frac{I_v}{I_m} \quad (4.5)$$

$$w_{ij} = JSD(I_u, I_v) = \frac{KLD(I_u, I_m) + KLD(I_v, I_m)}{2} \quad (4.6)$$

After a user consumes the rumor and propagates it further, the links are checked if there is a scope for rumor blocking. Each link contains a trust between the nodes based upon their common neighbors and a similarity score based on similarity or dissimilarity of node's topic interest. We consider that if a rumor reaches a node, then the node has to consume it. So, here a blocking mechanism for the links is proposed. When a node receives a rumor, it first checks if it is coming from a trusted source or not. If it is coming from a trusted source and the user is interested in topic of rumor, he/she further diffuses the rumor to his/her neighbor if the similarity score is greater than the threshold value otherwise block it.

Given  $t_{ij}$  be the trust between two users  $i$  and  $j$ ,  $\tau$  be the trust value below which the information is not allowed to pass and  $w_{ij}$  be the similarity score between these nodes. Let  $\eta = (\eta_1, \eta_2, \dots, \eta_l)$  be the link-level threshold for each topic to which rumor belongs. Then

$$\left\{ \begin{array}{l} \text{if } t_{ij} < \tau : \text{Rumor belonging to topic } m \text{ is blocked between nodes } i \text{ and } j \\ \text{if } t_{ij} \geq \tau : \text{then} \\ \left\{ \begin{array}{l} \text{if } w_{ij} \geq \eta_m : \text{Rumor belonging to topic } m \text{ is blocked between nodes } i \text{ and } j \\ \text{if } w_{ij} < \eta_m : \text{Rumor is propagated from node } i \text{ to node } j \end{array} \right. \end{array} \right. \quad (4.7)$$

When the user's trust on the neighbor is less than  $\tau$ , they will not consume the rumor. When trust exceeds  $\tau$ , we further check the similarity score. Since a lower value of  $w_{ij}$  represents greater similarity, when the value of the similarity score between two users is higher (which means that their topic of interest is different) than the link-level threshold, rumor is blocked and otherwise propagated.

### 4.2.3 Rumor diffusion blocking model

We propose an extended variant of the classical Susceptible-Infected-Recovered (SIR) model [124] as the Susceptible-Infected-Recovered-Blocked (SIRB) model. SIR model is a compartmental model which is mainly used to model the propagation behavior of epidemics. Since rumor propagation is similar to epidemic propagation, this model is widely used for rumor control in social networks.

The SIR model consists of three compartments of nodes- susceptible, infected and recovered. Susceptible nodes are those that have not received rumor yet but are prone to become infected after receiving it. Infected nodes are those that have received the rumor and further diffused it in the network. Recovered nodes are the infected nodes that know the veracity of rumor and are no longer infected. The state transition diagram for the SIR model is shown in Figure 4.2. We propose a new compartment of blocked nodes over the existing compartments of SIR model. The susceptible nodes that are not interested in a topic become blocked nodes according to the interest distribution. They receive rumors from their neighboring infected nodes and use the node-level or link-level blocking strategy to determine whether to become blocked nodes or infected nodes. The blocked nodes do not further propagate the rumor. Figure 4.2 shows the state transitions for the SIRB model. The SIRB model makes the following assumptions.

1. At any time instance  $t$ , the total number of nodes in the network is constant. The sum of number of susceptible, infected, recovered and blocked nodes is always equal to the total number of nodes in the network.

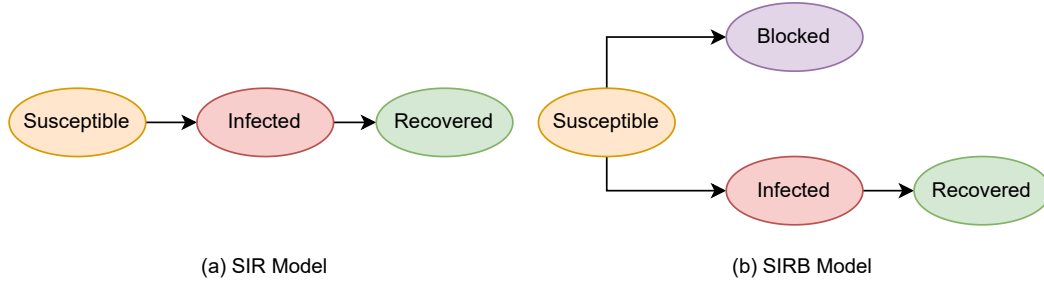


FIGURE 4.2: State transition diagram for SIR and SIRB model

$$n_t(S) + n_t(I) + n_t(R) + n_t(B) = N \quad (4.8)$$

2. During rumor propagation, after applying the blocking strategy, if a susceptible node accepts the rumor, it becomes infected. After knowing the veracity of the rumor, the infected node becomes a recovered node.

*Susceptible*  $\longrightarrow$  *Infected*

*Infected*  $\longrightarrow$  *Recovered*

3. During rumor propagation, after applying the blocking strategy, the susceptible node becomes blocked node.

*Susceptible*  $\longrightarrow$  *Blocked*

Consider a social network  $G(N, E)$  consisting of  $N$  users with  $E$  links among them. At any time instance, each user can be in exactly one of the four states, i.e. susceptible, infected, recovered, or blocked. So, the total number of nodes is  $N$  (equation 4.8). A rumor propagates with infection probability  $\beta$ . During propagation, it uses the blocking strategy and blocks nodes with a blocking probability  $\alpha$ . Infected nodes are later recovered by a recovery probability  $\gamma$ . The rate of change in

susceptible, infected, recovered and blocked nodes is calculated using the following mean-field equations.

$$\frac{dS}{dt} = -\beta \frac{SI}{N} - \alpha \frac{SB}{N} \quad (4.9)$$

$$\frac{dI}{dt} = \beta \frac{SI}{N} - \gamma I \quad (4.10)$$

$$\frac{dR}{dt} = \gamma I \quad (4.11)$$

$$\frac{dB}{dt} = \alpha \frac{SB}{N} \quad (4.12)$$

### 4.3 Results and Discussion

We implemented our proposed rumor control model on a synthetic social network generated using the Barabási-Albert (BA) model [91], as well as on four real datasets from the Twitch network [93] (as discussed in Section 2.3). We conducted various experiments on these datasets to evaluate the effectiveness of the proposed model in blocking rumors within social networks. The experiments were designed to address the following research questions.

- **RQ1:** What should be the value of the node-level threshold  $\theta$  and the link-level threshold  $\eta$  such that rumor is blocked in the network using the node and link-level blocking strategies? (Answered in subsections 4.3.1, 4.3.3, 4.3.4)
- **RQ2:** What is the effect of influence of the node and trust factors on node-level threshold  $\theta$  and edge-level threshold  $\eta$  respectively? (Answered in subsection 4.3.2, 4.3.3)
- **RQ 3:** What is the effect on number of infected nodes and blocked nodes with varying rumor diffusion and rumor blocking probability? (Answered in subsection 4.3.5)

- **RQ 4:** How SIRB model is effective than other rumor control models in containing rumors? (Answered in Subsection 4.3.6)

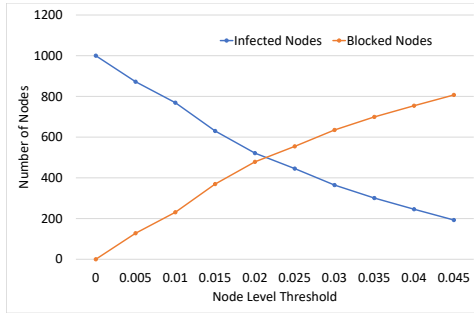
To overcome the randomness in the results, we performed each experiment 1000 times and averaged the results. The following subsections describe the experiments that we performed.

### 4.3.1 Applying Node-Level Blocking Strategy for Rumor Control

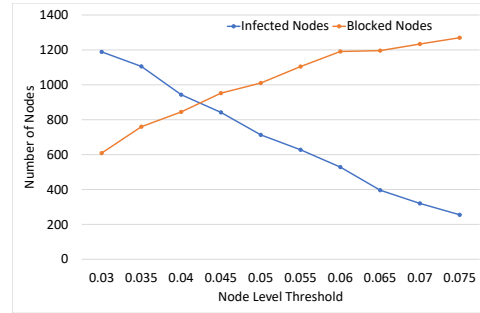
In this experiment, we find the values of the node threshold  $\theta$  for the five datasets we have considered. We calculated the values  $WNI$  for all nodes and used the SIRB model to calculate the infected nodes and blocked nodes using the node-level strategy. The  $WNI$  values of each node are compared against the node-level threshold  $\theta$ , which is initially set to 0 with a step of 0.001. At the initial value of  $\theta$ , the nodes are in the infected state rather than the blocked state. However, as we continue to increase the value of  $\theta$ , blocked nodes are introduced in the system. At a certain threshold value, the blocked nodes outnumber the infected nodes. At this stage, when the number of blocked nodes exceeds the number of infected states, we say that the rumor is blocked on the social network. In table 4.1, we show the threshold values for different datasets obtained by averaging the threshold value over five topics. In Figure 4.3, we show the relationship between infected nodes and blocked nodes with respect to the increase of the threshold value of the node  $\theta$  for the five datasets.

TABLE 4.1: Node threshold  $\theta$  values when Influence Score is considered

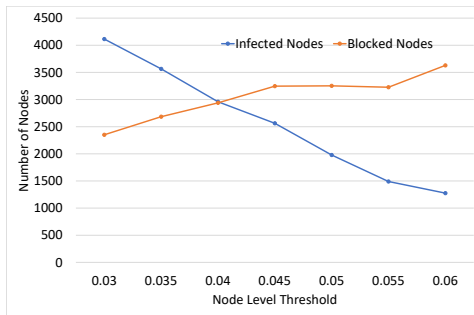
Datasets	BA	EN	ES	PT	RU
Threshold $\theta$	0.0236	0.0420	0.0476	0.0434	0.0412



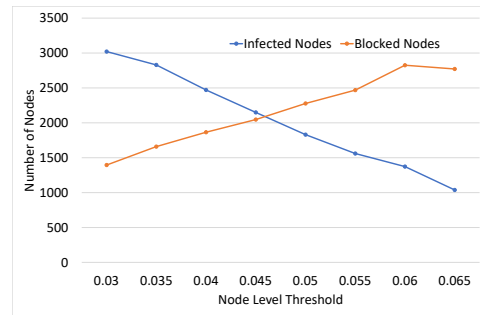
BA Network



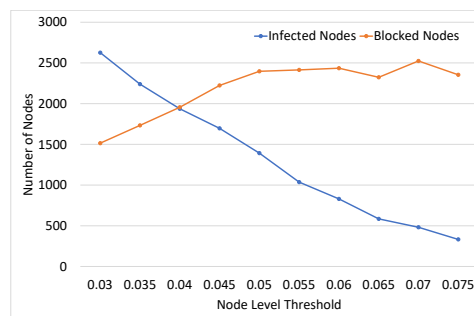
PT Network



EN Network



ES Network



RU Network

FIGURE 4.3: Relation between infected nodes and blocked nodes with the increasing value of  $\theta$

### 4.3.2 Effect of Influence Score on Node-level Threshold

In this experiment, we investigated the effect of excluding the influence score from the node-level blocking strategy in the SIRB model. For the calculation of the Weighted Node Interest (WNI), the influence score of each user is set to 1 which effectively removes the structural impact of network centrality. We computed the WNI values for all nodes in each of the five datasets and applied the SIRB model using the node-level blocking strategy. As before, the WNI values were compared with a threshold at node level  $\theta$ , which is initialized at 0 and increased by 0.001. At the lowest threshold, the majority of nodes entered the infected state, as no blocking conditions were met. As the threshold increased, more nodes began to be blocked based on their topic interest alone. At a certain threshold value, the number of blocked nodes surpassed the number of infected nodes, indicating rumor blocking in the network. Table 4.2 presents the average threshold values for nodes for each dataset, computed over five topics, at which the system transitions to a blocked state. In particular, in the absence of influence scores, the threshold values are higher than in experiments in which influence scores are considered. This suggests that ignoring a user's structural importance in the network reduces the model's ability to block rumors efficiently, as less influential and highly influential users are treated uniformly in the blocking process. An important observation that needs further investigation is that the value of  $\theta$  is almost similar for all data sets (see Figure 4.4).

TABLE 4.2: Node threshold  $\theta$  values when Influence Score is not considered

Datasets	BA	EN	ES	PT	RU
Threshold $\theta$	0.0.201	0.0.2016	0.0.2006	0.1978	0.2008

### 4.3.3 Applying Link-Level Blocking Strategy with Varying Trust Factor

In this experiment, we have implemented the SIRB model using the link-level blocking strategy and calculated the threshold values that drive the system into a rumor-blocking state. To achieve this, we first computed the topic-interest similarity

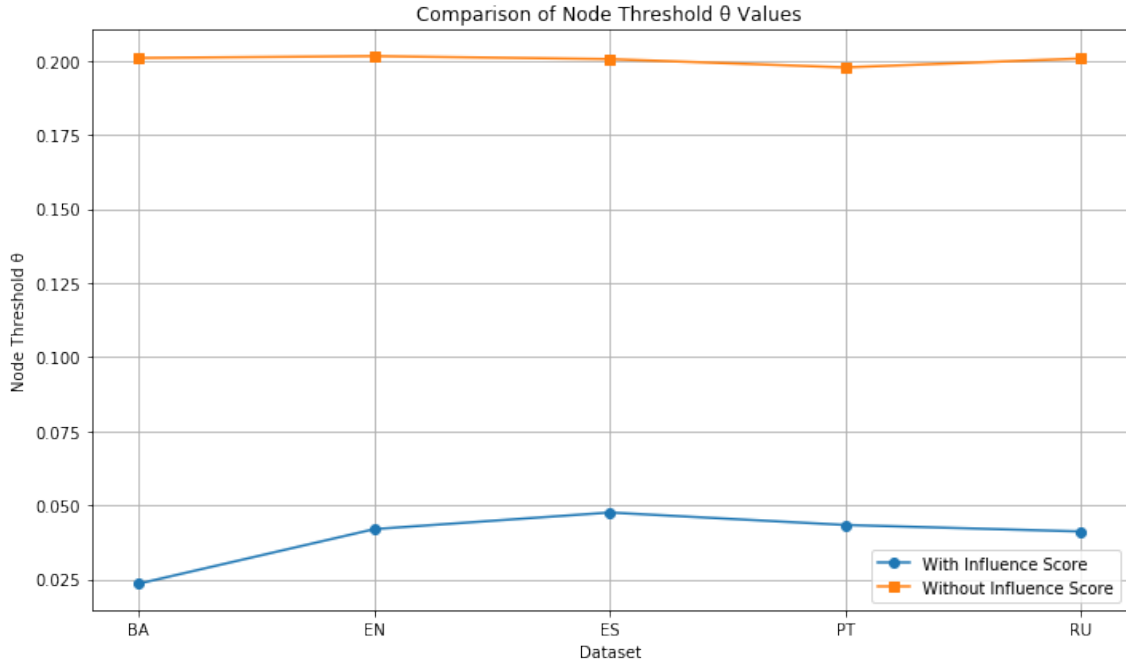


FIGURE 4.4: Node Threshold values with and without considering Influence Scores

between each pair of nodes and measured the trust between them. We then varied the trust threshold  $\tau$  and link-level blocking threshold  $\eta$  to observe their effect on rumor propagation. The initial values of  $\tau$  and  $\eta$  are set to 0 and incremented by 0.01 and 0.001, respectively. To ensure effectiveness, we examined the behavior of the system under different trust levels, reflecting more realistic social scenarios where users have varying degrees of trust in their neighbors. When  $\tau = 0$  (i.e., no trust is there), a majority of nodes are in the blocked state, as minimal interaction is there. However, this scenario is restrictive and does not represent real-world networks, where users generally maintain a baseline level of trust. As the trust threshold  $\tau$  increases, the system becomes more permissive, allowing a greater number of nodes to become infected before blocking takes effect. To bring the system into a blocked state, we calculated the link-level threshold values  $\eta$  for each dataset at varying trust levels. The results are summarized in Table 4.3. Different  $\eta$  values are possible for different values of  $\tau$ . In the BA dataset, with increasing values of  $\tau = 0, 0.005, 0.01, 0.015, 0.02, 0.025$ , the value of  $\eta = 0.071, 0.08, 0.09, 0.1, 0.125, 0.18$

respectively. This pattern demonstrates that blocking effectiveness is sensitive to both trust and topic similarity and that, for each trust level, there exists a critical link-level threshold below which the system successfully suppresses the rumor spread. The result shows that at a particular value of  $\tau$ ,  $\eta$  is the link-level threshold below which the system is in the blocked state, otherwise the infected state. Another observation is that as the value of trust is high, i.e., 0.2, 0.3, etc, even a small value of link-level threshold is sufficient to bring the system into the blocking state.

TABLE 4.3: Link-level threshold  $\eta$  values

Datasets	BA	EN	ES	PT	RU
Trust $\tau$	.01	.001	.01	.01	.001
Threshold $\eta$	0.08	0.34	0.22	0.10	0.13

#### 4.3.4 Comparison of Node-level and Link-level Blocking Strategies

The node-level blocking strategy focuses on the interest of individual users in rumors topics. It blocks the propagation of rumors based on whether a user's interest in a particular topic is within a certain threshold. Thus, it is more user-centric, taking into account how likely a user is to consume and share content. So, node-level blocking is suitable for platforms focused on personalized content delivery, where individual interests dictate user behavior. However, the link-level strategy is more relationship-centric, focusing on the connections between users. It blocks rumors based on the similarity of interests between two users and the level of trust in the relationship. So, with link-level blocking, regardless of a user's interest in a rumor, it may be blocked if the link through which it is spreading is dissimilar in interest.

In node-level blocking, the impact is local to the user. If a user blocks a rumor, it does not propagate from them, but it could still spread through other users via links on the network who have a higher interest in the topic of the rumor. However, in link-level blocking, the impact is more relational and can affect multiple

nodes indirectly. By blocking a rumor on a particular link, we potentially prevent it from spreading to an entire subset of the network connected through that link. Also, node-level blocking is likely to be more scalable as it operates on individual nodes without considering the broader network structure. This makes it easier to implement on large-scale social networks. However, link-level blocking is potentially less scalable because it requires additional evaluation of trust and similarity between links, which increases complexity as the network grows. It may become computationally expensive in very large networks.

Node-level blocking is more effective in networks where users' interests are the primary driver of content consumption and sharing. It is useful in scenarios where personal relevance is a strong determinant of rumor spread. However, it might not account for the influence of highly connected or influential nodes (hubs) that can spread rumors widely, even if their interest is borderline. Link-level blocking is more effective in networks where trust and similarity of interests between users play a critical role in content propagation. This approach is better suited for tightly knit communities or networks where relationship dynamics are crucial. Here, effectiveness heavily depends on accurately measuring trust and similarity between users, which can be challenging. Link-level blocking is ideal for social networks where community-driven content sharing is prevalent and relationships between users significantly influence content spread.

### **4.3.5 Varying rumor diffusion and rumor blocking probability**

This experiment provides an analysis of the effect of varying the probability of spreading rumors  $\beta$  and the probability of blocking rumors  $\alpha$  on rumor control. For this purpose, we have implemented the SIRB model for a 1000 node network for different values of  $\beta$  and  $\alpha$  starting from 0 to 0.5, increasing by a factor of 0.05 each time. We have assumed a recovery probability  $\gamma = 0.001$ , which is negligible. This very low value of gamma helps us to focus on analyzing the relation between  $\beta$  and

$\alpha$ . Also, recovery nodes cannot be more than infected nodes at any time, so we only consider infected nodes for analysis. The simulation results show that when  $\beta > \alpha$ , there is a greater number of infected nodes than blocked nodes. This means that when the probability of infection is greater than the probability of rumor blocking, the system is in an infected state (see Figures 4.5(a) and (b)). When  $\beta = \alpha$ , the system is in the blocking state, that is, the number of blocked nodes exceeds the number of infected nodes (see Figures 4.5(c) and (d)). When  $\beta = \alpha$ , and for very small values of  $\gamma$ , for example  $\gamma = 0, 0.001$ , the number of blocked nodes is equal to the sum of the number of infected nodes and recovered nodes (see Figure 4.6 (a), (b), (c), and (d)). However, for larger values of  $\gamma$ , this may not be the case (see Figures 4.6 (e) and (f)). When  $\beta < \alpha$ , i.e., the probability of rumor diffusion is less than the probability of rumor blocking, the system ends up in a blocked state (see figures 4.5 (e) and (f)). The higher the increase in the probability of rumor blocking, the faster the convergence of the system to the blocked state (see Figure 4.5(g) and (h)).

### 4.3.6 Comparison of proposed SIRB model with other existing Rumor Control Models

#### 4.3.6.1 Comparison of proposed SIRB model with SIR model

The proposed SIRB rumor blocking model is an extended variant of the compartmental model SIR obtained by adding a compartment of blocked nodes  $B$  to existing susceptible  $S$ , infected  $I$ , and recovered  $R$  nodes. So, we have used the SIR model as the baseline model for our work. We have shown a comparative analysis of the SIRB model with the SIR model in Figure 4.7. The SIR model considers the probability of rumor diffusion ( $\beta$ ) and the recovery probability ( $\gamma$ ), while the SIRB model also considers the probability of rumor blocking ( $\alpha$ ). We have compared the performance of both models for the initial value 0.00 with a step of 0.05 for each probability. When  $\beta = 0$ , there are no infected nodes in the network. As we continue to increase the value of  $\alpha$  for this value of  $\beta$ , we get blocked nodes using the SIRB

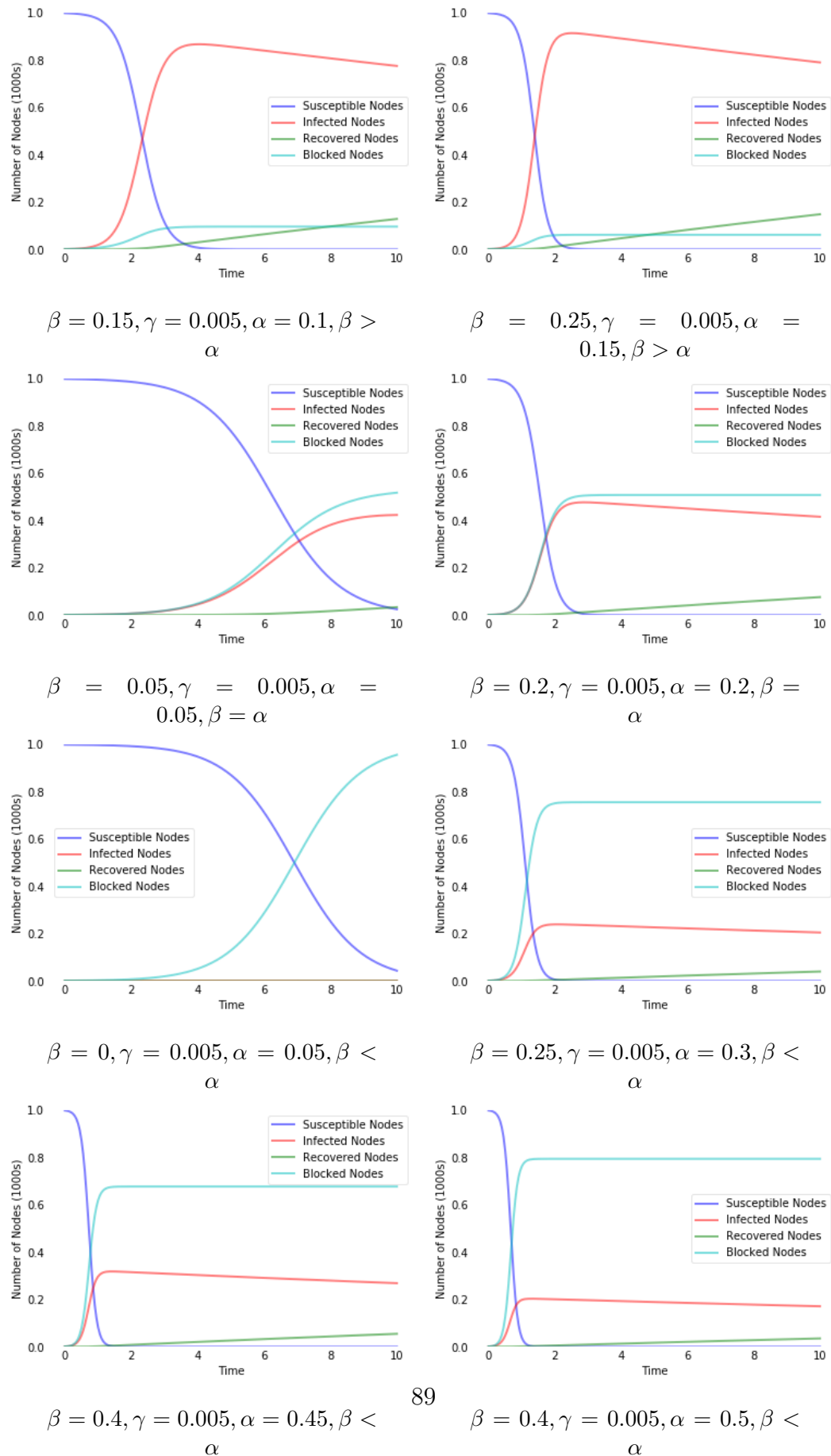


FIGURE 4.5: Implementation results for SIRB model for different  $\beta$ ,  $\gamma$  and  $\alpha$  where  $N=1000$

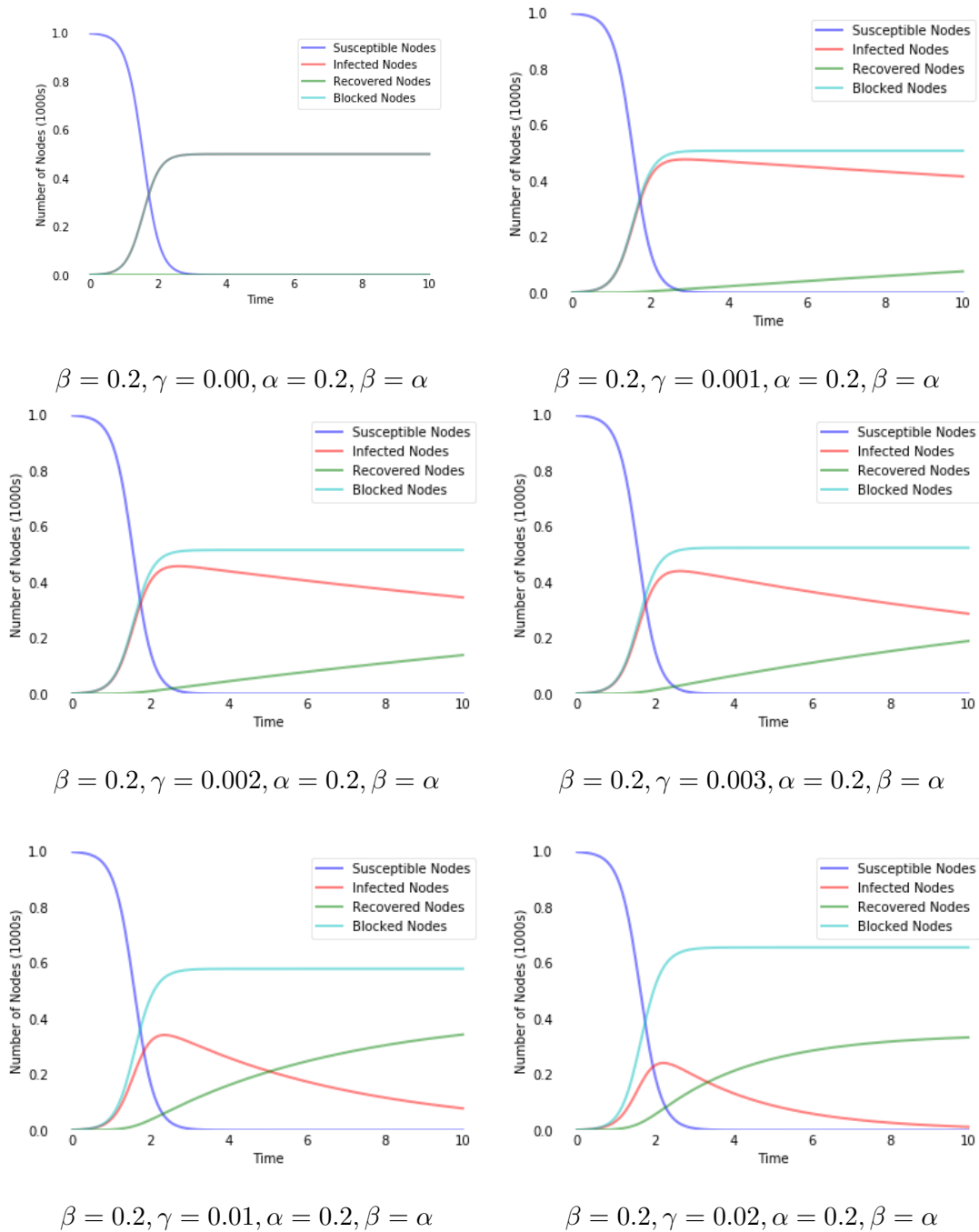


FIGURE 4.6: Implementation results for SIRB model for  $\beta = \alpha$  and different values  $\gamma$  where  $N=1000$

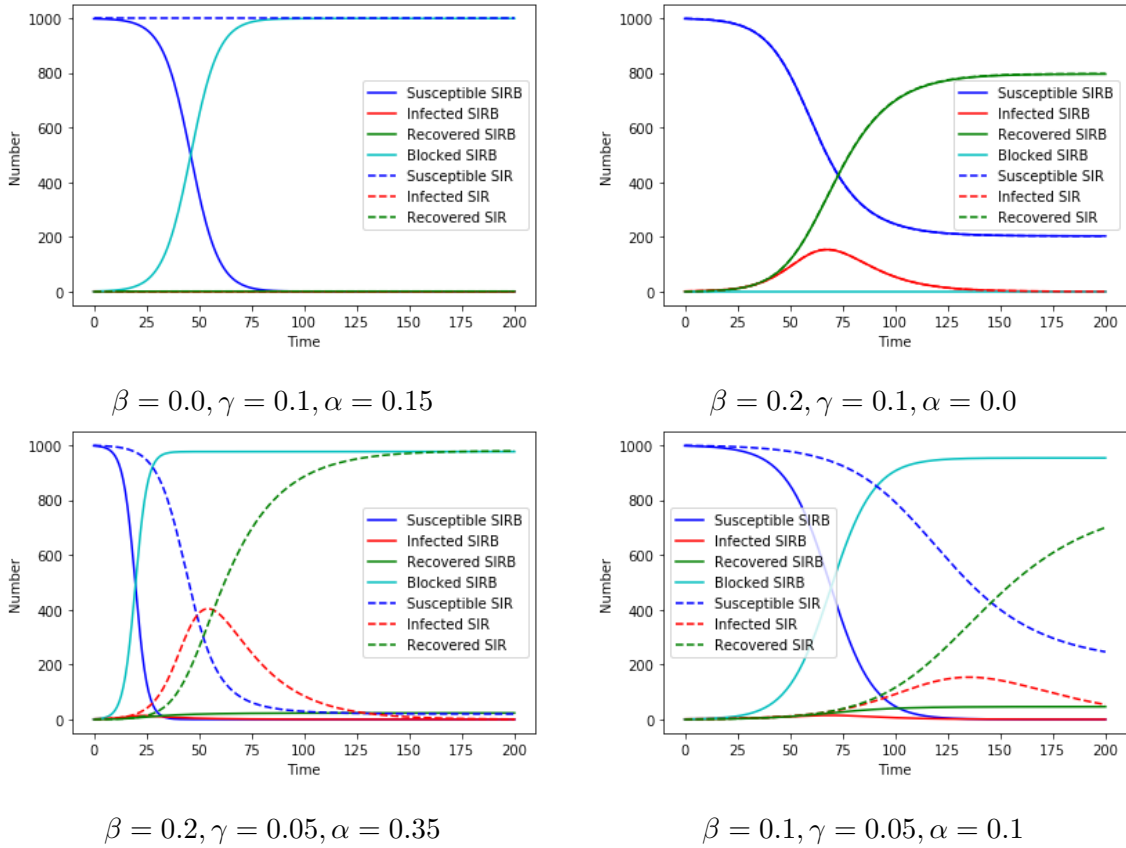


FIGURE 4.7: Comparative Analysis of performance of SIRB and SIR models

model (see Figure 4.7 (a)). The recovery rate does not have any effect in this case as there are no infected nodes. When  $\alpha = 0$ , SIRB model works as SIR model and blocks no node (see figure 4.7(b)). The SIRB model overlaps with the SIR model in this case. When  $\beta = 0.2, \gamma = 0.05$  and  $\alpha = 0.35$ , the SIRB model blocks the node at a faster rate than the SIR model recovers the node from infection (see figure 4.7(c)). Figure 4.7(d) shows one more scenario for  $\beta = 0.1, \gamma = 0.05$  and  $\alpha = 0.1$ . As the value of  $\alpha$  increases, the SIRB model outperforms the SIR model and blocks more nodes from getting infected than the SIR model. Thus, we can say that the proposed SIRB model is better than the SIR model to control rumors on a social network.

### 4.3.6.2 Comparison of proposed SIRB model with SPNR model

The Susceptible-Positively Infected- Negatively Infected- Recovered (SPNR) model [23] is an extended variant of the SIR model, which divides the infected nodes into positive and negative categories based on the opinions of the users. They suggest a rumor control method guided by opinions, where positively infected nodes that refute the rumor are increased in the network to control the rumor. This model is based on the fact that the maximum users follow the belief of influential users. Thus, they recommend inserting positively infected nodes and connecting them with others for rumor control. Figure 4.8 shows a comparison between our proposed model and the SPNR model. Here, for the SIRB model, infection rate  $\beta = 0.05$ , recovery rate  $\gamma = 0.02$ , and blocking rate  $\alpha = 0.04$ . For the SPNR model, the probability of becoming a positive spreader is 0.6, the recovery rate for positively infected and negatively infected is 0.02. The results show that in the SIRB model, the number of infected nodes remains lower throughout due to early blocking, whereas positive and negative spreaders show more active spread, as the SPNR model allows opinion divergence after infection. Furthermore, in the SIRB model, the number of blocked nodes increases early, indicating early control over rumor spread.

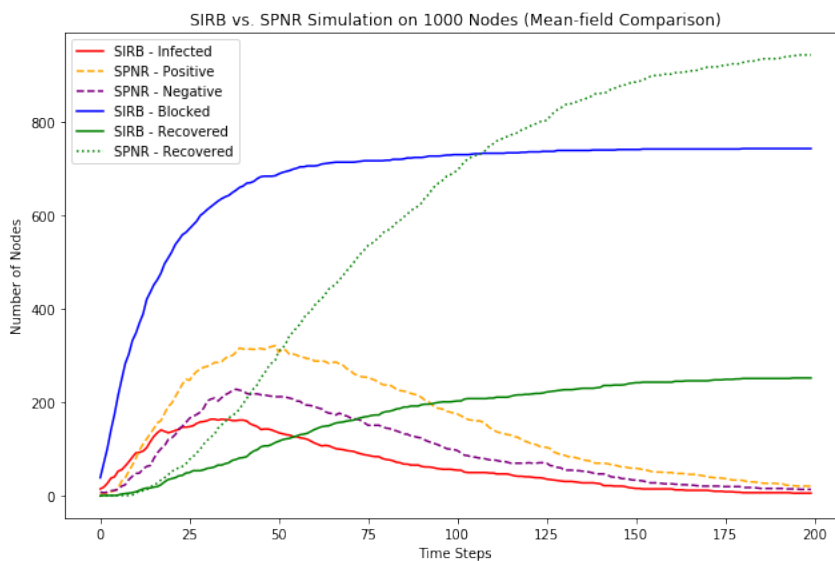


FIGURE 4.8: Comparison between proposed SIRB model and SPNR model

### 4.3.6.3 Comparison of proposed SIRB model with SIRA model

The Susceptible-Infected-Recovered-Anti-spreader (SIRA) model [35] is an extended variant of the SIR model, which accounts for the simultaneous operation of both supporters and deniers of information. This model addresses rumor propagation and control strategies involving anti-spreaders which represent nodes that actively work to counter or suppress the spread of false information. Unlike recovered individuals who no longer participate in the diffusion process, anti-spreaders influence their peers to resist or reject the rumor. Figure 4.9 shows a comparison between our proposed model and the SIRA model. Here, infection rate  $\beta = 0.05$  and recovery rate  $\gamma = 0.02$ . For the SIRB model, blocking rate  $\alpha = 0.04$ . For the SIRA model, the rate of conversion to anti-spreader is 0.03, and anti-spreader deactivation rate is 0.01. The result shows an early and steady rise in the number of blocked nodes in the SIRB model. In addition, the infected population peaks lower and declines faster compared to the SIRA model. In SIRA model, anti-spreaders increase later to correct the spread. So, SIRB is more effective at early stage control by blocking susceptible users before receiving infection.

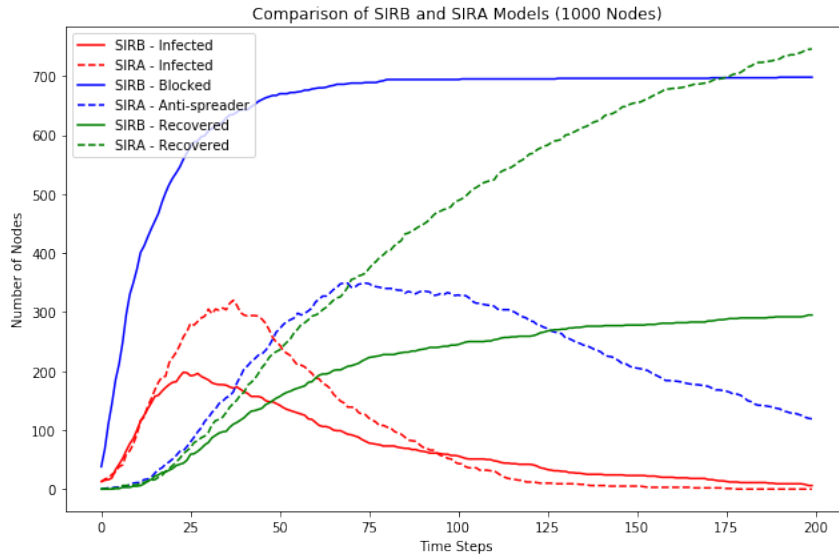


FIGURE 4.9: Comparison between proposed SIRB model and SIRA model

## 4.4 Conclusion

In this chapter, we proposed a rumor control approach based on users' topic interests, which blocks rumors at both the node and link levels. The proposed method was tested on both synthetic and real datasets to evaluate its effectiveness. The results demonstrate the effectiveness of this approach in blocking rumors. The node-level blocking strategy is found to be simpler, more scalable, and particularly effective in environments driven by interest-based rumor propagation, while the link-level blocking strategy, though more complex due to considerations of relationships and trust, is better suited for controlling rumor spread in closely connected networks. Depending on the specific goals and structure of the social network, one strategy might be preferred over the other, or they could be combined for a more robust approach to rumor blocking. However, certain aspects require further investigation. First, since users' interests change over time, there is potential to capture these interests in real time and integrate them into the rumor blocking model. Second, given the dynamic nature of social networks, where nodes and edges are continuously added or removed, there is a need to develop a rumor blocking model that can adapt to these changing network dynamics.

Blocking rumors at the node or link level is adequate for the immediate containment of rumors; however, they have several significant drawbacks. First, it raises censorship concerns, as users may perceive this method as an infringement on free speech, leading to potential backlash and loss of trust in the OSN platform. Also, legitimate content or users may be mistakenly blocked, inadvertently harming innocent parties, and disrupting vital communications. Moreover, this approach is inherently reactive, addressing the issue only after the rumor has started to spread, which may not prevent the rumor from gaining initial traction. As networks grow in size and complexity, the scalability of blocking becomes increasingly challenging, making it difficult to monitor and intervene effectively in all cases. These limitations highlight the need for counter-rumor spread methods, which offer a more proactive and scalable solution. In the next chapter 5, we propose a counter-rumor-based

rumor prevention model that mitigates these challenges and proactively curtails rumors on social networks.