





# Credibility-based Model for News Spreading on Online Social Networks

Vincenza Carchiolo<sup>1</sup><sup>a</sup>, Alessandro Longheu<sup>2</sup><sup>b</sup>, Michele Malgeri<sup>2</sup><sup>c</sup>, Giuseppe Mangioni<sup>2</sup><sup>d</sup>  
and Marialaura Previti<sup>2</sup>

<sup>1</sup>*DMI, University of Catania, Italy*

<sup>2</sup>*DIEEI, University of Catania, Italy*

**Keywords:** Credibility, Trust, Social Network, Information Diffusion.

**Abstract:** Trustworthiness in Online Social Networks has become essential to discriminate the goodness of both different information as well as the users it originates. Here a model for news spreading in directed online social networks (OSNs) that takes into account trustworthiness-related issues is introduced. In particular we add a *credibility* network on top of the acquaintance network naturally present in OSNs to model the changing of each node's opinion about his/her neighbors every time a piece of news comes from them over the OSN. We examine three different scenarios of news spreading over OSNs and propose a model suitable for each scenario, evaluating its applicability using a real world weighted directed network.

## 1 INTRODUCTION

Thanks to the rapid growth of Online Social Networks (OSNs) (Persia and D'Auria, 2017) and the enormous amount of information available every day, users of these platforms tend to acquire and disseminate news over them. This process, called *social contagion* (Hodas and Lerman, 2014), can amplify the spread of information in a social network. The decision to propagate or not news can depend on the news contents or the trust in people that publish news.


The goal of the work presented in this paper is to provide a model for information propagation in OSNs that takes into account trust-related issues. In particular, we consider the directed acquaintance network naturally presents in OSNs (e.g., Twitter) as the basis through which news spreads over the network and we introduce an overlay weighted directed network (the *credibility network*) that have edges in the opposite direction respect to edges in the acquaintance network, because for each piece of news spreads from an individual the receivers form or modify their opinion about the spreader's credibility. The credibility values are led by two metrics related to the topology of the


network: the *trust* and the *reliability*. After providing a quantitative definition for each metric, we apply the model with such credibility network in three different simulation scenarios of information spreading exploiting as starting point a real network. This paper follows our previous works on the same topic (Carchiolo et al., 2018a)(Carchiolo et al., 2018b).


The paper is organized as follows: in section 2 an overview of existing related works is presented, while in sec. 3 metrics and credibility network are introduced and the different way in which a piece of news can be propagated over the social networks are detailed through a progressively improved model re-adapted for each kind of propagation. In section 4 the simulations are illustrated and discussed, and finally in section 5 we outline our concluding remarks and future works.


## 2 RELATED WORKS

Several attempts to model the news spreading over OSNs through implicit and explicit use of trust has been performed. The concept of *trust* as a way to assess the quality of information, people, goods, and/or virtual entities spans different research areas, from recommendation systems (Massa and Avesani, 2007) (Carchiolo et al., 2015b) to e-commerce (Fung and Lee, 1999), distributed on-line services (Wang

<sup>a</sup> <https://orcid.org/0000-0002-1671-840X>

<sup>b</sup> <https://orcid.org/0000-0002-9898-8808>

<sup>c</sup> <https://orcid.org/0000-0002-9279-3129>

<sup>d</sup> <https://orcid.org/0000-0001-6910-0112>

and Emurian, 2005), security and privacy (Vasudevan et al., 2012) and many others. In some cases a *trust network* is created for each user and it contains his *friends* as nodes and an associated trust value for each of them as edges weights, provided that usually trust is not for free, rather some effort must be paid to earn trustworthiness from others (Carchiolo et al., 2015a).

Goldbeck (Golbeck et al., 2003) proposed a method for creating a trust network on the semantic web allowing users to express the level of trust for each person they know about a specific topic. This weighted network was used to infer trust values between individuals not directly connected to each other. In another work (Golbeck, 2005) authors proposed TidalTrust to derive the trust relationship based on the premise that neighbors with higher trust ratings are likely to agree with each other about the trustworthiness of a third party, so for a fixed trust rating shorter paths have a lower average difference and higher trust ratings have a lower average difference. This work was extended by Zhang et al. (Zhang et al., 2006) including pairwise trust ratings and reliability factors of the entities in the network and using an edge-weighted network for trust assessment. It calculates the similarity of two raters by comparing their ratings about the same provider and then it is adopted to decide which neighbor recommendation should be followed. Comparing two recommendations, the recommendation from a rater that is more similar to the trustor will be chosen. Dubois et al. (DuBois et al., 2011) presented a method to compute trust and distrust combining an inference algorithm that relies on a probabilistic interpretation of trust based on random graphs with a modified spring-embedding algorithm in order to classify hidden trust edges as positive or negative.

Other works that exploit the OSN structure has been proposed by Hang and Singh (Hang and Singh, 2010) that employed a graph-based approach based on similarity between each node's friends trust network for measuring trust with the aim to recommend a node in a social network using the trust network, Kuter et al. (Kuter and Golbeck, 2007) that proposed a Bayesian trust inference model for estimating the confidence on the trust information obtained from specific sources, Caverlee et al. (Caverlee et al., 2008) that proposed a social trust model that exploits both social relationships and feedback by users after each interaction to evaluate trust where users' feedback have a different weight based on their link quality (higher weights belong to users with a lot of links with user having high trust ratings) and Zuo et al. (Zuo et al., 2009) that proposed a model that uses a

trust certificate graph and calculates trust along a trust chain, then, it exploits the composability of trust in the form of fusion of relevant trust chains to form a base trust chain set.

In contrast to most of the previous exposed works that derive data from users feedback, Kim (Kim et al., 2008) built a Web of trust without using explicit user ratings. His approach consists on calculating users expertise in a certain topic, which involves calculating the quality of reviews using the reputation of raters and then the reputation of writers, calculating the users affinity to the category, where the user affinity to the ratings is derived from the average number ratings and reviews provided by them in each category, finally deriving degree of trust from the user's affinity to the topic and another users expertise on the topic.

Another set of OSNs trust models that exists in literature only use interactions among users within the network to calculate trust. Liu et al. (Liu et al., 2008) proposed an approach for predicting trust in online communities using the interaction behaviors of OSNs users. This model considered the *temporal factor*, i.e., the time difference between two connected users respective actions and described a supervised learning approach that automatically predicts trust between a pair of users using the *user factors*, representing evidence derived from actions of individual users, and the *interaction factors*, representing the evidence derived from interactions between pairs of users.

Nepal et al. (Nepal et al., 2010) proposed STrust, a social trust model based only on interactions within the social network. The model consists of two types of trust: the *popularity trust* refers to the acceptance and approval of a member in the community and representing the trustworthiness of the member from the perspective of other members in the community, and the *engagement trust* refers to the involvement of the member in the community and representing the trust the member has towards the community. This model aims to increase the social capital of the community by encouraging positive interactions within the community and, so, increase the social trust in the community.

Adali et al. (Adali et al., 2010) evaluated trust based on communication behaviors of OSNs users. Behavioral trust is calculated based on two types of trust: *conversation trust*, that specifies how long and how frequently two users communicate with each other, and *propagation trust* that is obtained from one user to other users in the network and indicates the degree of trust placed on the information and implicitly on the user that created the information.

In the last decade some hybrid trust models that

use both interactions among OSNs users and OSNs structure has been created, even if the literature on these promising models is limited. Trifunovic et al. (Trifunovic et al., 2010) proposed a social trust model for opportunistic networks. This model uses two complementary approaches for social trust establishment: *explicit social trust* that is based on consciously established social ties and produces a general decrease of trust with the growth of the number of links between pairs of users, and the *implicit social trust* that is based on frequency and duration of contact between two users, but take into account not only the length of interaction, but also the similarity in order to avoid that a set of negative long interactions produces a high trust between pairs of users.

Zinoviev et al. (Zinoviev et al., 2010) proposed a game theoretical model of the information forwarding and feedback mechanisms in a social network that take into account the personalities of the sender and the receiver, including their perceived knowledgeability, reputation, and desire for popularity, and the global characteristics of the network.

Wu et al. (Wu et al., 2017) investigated the dynamics of competitive information diffusion over a connected social network, proposing a modified SIR model for two competitive information, where each individual may turn to either of the two information after interacting with a spreader, while the spreader associated with one information may change into the other information. The population is divided into three subgroups: innovators, ordinary and laggard subgroups, and they observed that innovators and larger network degree can help to increase the coverage of the information among the population but they cannot help one information to compete with the other one. Moreover, innovators cannot always accelerate the convergence speed, which depends more on the network topology.

### 3 THE CREDIBILITY-BASED MODEL

As discussed previously, the simple acquaintance network naturally presents in each OSNs is not sufficient to model the propagation of news because such networks do not take into account several factors that come into play when someone decides to propagate the news. To this purpose we introduce a duplex network composed by a directed acquaintance network  $A = \langle N, E \rangle$  and a directed weighted credibility network  $C = \langle N, E', c \rangle$  with edges in opposite direction respect to those in the acquaintance network because if a node spreads a piece of news the receiving node

forms an opinion about the spreader modeled through the weight  $c \in [-1, 1]$  (-1 indicates the highest credibility whereas 1 indicates the lowest).

In directed OSNs the basic assumption is that between pairs of individuals there is not necessarily a mutual interest in published posts, so incoming and outgoing edges of acquaintance network hold different roles: outgoing edges represent the link with people interested in what we publish, while the incoming ones are a source of inspiration for arguments of our interest and that in some cases we want to repost. According to this reason we introduce two amounts in the credibility network structure: *trust* and *reliability*.

The **trust** ( $T$ ) in an individual indicates how much he/she is considered trustworthy by its neighbors; high trust values indicate that who is in contact with him/her appreciates the contents he/she posted and considers him/her a person who verifies the news before reposting it (it is related to incoming edges of credibility network);

The **reliability** ( $R$ ) of an individual shows its ability to select which neighbors he/she will accept news from to repost, hence this parameter indirectly influences his/her ability to post true news, i.e. it is related to outgoing edges of credibility network.

In OSNs, many users tend to link with others who share the same news, while malicious users create multiple accounts to repost the news. The members of these two groups of accounts increase each other's trust so the network remainder that is in contact with them can assign a low level of reliability to offset the high level of trust; this is performed in order to re-size their weight in the credibility network and therefore to attenuate the *echo chambers* phenomenon (Baumann et al., 2019).

#### 3.1 Trust and Reliability Metrics

The trust and reliability parameters described above are closely linked each other and influence the credibility of an individual in his neighborhood. In particular, trust of  $v \in N$  is defined as:

$$T_{t+1}(v) = \frac{1}{|v|_{in}} \sum_{u \in U_{in}(v)} R_t(u) c(u, v) \quad (1)$$

$U_{in}(v)$  is the set of neighbors pointing the node  $v$  and  $R_t(u)$  is the reliability at time  $t$ . We define reliability of  $v \in N$ :

$$R_{t+1}(v) = 1 - \frac{1}{|v|_{out}} \sum_{u \in U_{out}(v)} \frac{|T_{t+1}(u) - c(v, u)|}{2} \quad (2)$$

$U_{out}(v)$  is the set of neighbors who are pointed by node  $v$  and  $T_{t+1}(u)$  is the trust calculated with the

eq. 1.

Since credibility  $c \in [-1, 1]$ ,  $T \in [-1, 1]$  as well, where -1 indicates full distrust and 1 indicates full trust; each neighbor has actually a different weight in determining trust depending on his reliability.

To establish the reliability of a node, the closer this value to the values of other users that contributed to generate credibility (i.e. the smaller the difference  $|T_{t+1}(u) - c(v, u)|$ ), the higher its reliability. The value 2 in the denominator is used as normalization factor to balance the discrepancy between  $c(v, u)$  and  $T(u)$  that can be at most 2. From equation 2  $R \in [0, 1]$ , where 0 indicates that he/she emphasizes news of little interest to his neighborhood and conversely 1 indicates that he/she agrees with his neighbors opinion.

In OSNs the state when observation starts cannot be usually considered as *neutral* in which nobody knows others neither opinions exist, so it is likely to set initial values of  $c(u, v) \forall u, v \in N$ . To set in particular values for  $T$  and  $R$  we use the equations (1) and (2) by setting  $R = 1$  and iterating the two equations recursively until convergence occurs, i.e. until  $|T_{t+1}(v) - T_t(v)| < \epsilon$  and  $|R_{t+1}(v) - R_t(v)| < \epsilon$  with proper values for  $\epsilon$ .

If a node does not have incoming or outgoing edges, it is not possible to calculate the trust or reliability values respectively using previous equations hence we suppose that nodes without incoming edges are hypothetically pointed by all the other  $N - 1$  nodes of the network and similarly nodes without outgoing edges are supposed to point at each other node in the network. For all these edges we set weight to 1, meaning that maximum credibility is assigned; the approach resembles that used in defining the teleportation in PageRank algorithm (Gleich, 2014).

Equations 1 and 2 in this scenario become:

$$T_{t+1}(v) = \frac{1}{N-1} \sum_{\substack{u \in N \\ u \neq v}} R_t(u) c(u, v) = \frac{1}{N-1} \sum_{\substack{u \in N \\ u \neq v}} R_t(u) \quad (3)$$

$$\begin{aligned} R_{t+1}(v) &= 1 - \frac{1}{N-1} \sum_{\substack{u \in N \\ u \neq v}} \frac{|T_{t+1}(u) - c(v, u)|}{2} \\ &= 1 - \frac{1}{2(N-1)} \sum_{\substack{u \in N \\ u \neq v}} |T_{t+1}(u) - 1| \end{aligned} \quad (4)$$

### 3.2 News Spreading Models

The process of news diffusion can occur in different ways: sometimes the news propagates over the network without opposition, while in other cases conflicting opinions arise. To address this, we consider three kinds of news spreading models:

- **No-competitive news spreading model** when news can propagate over the network without opposition
- **Competitive news spreading model** in which there are two different thought factions about the same topic that propagate the news at the same time and a group of target OSN users reached by both factions is called to decide which side they are on
- **Competitive news spreading model with delay** same as previous but one line of thought is disseminated after the other and a group of target OSN users is called to decide if publish the retraction after the propagation of first news

In the following we describe these models in a further refinement.

#### 3.2.1 No-competitive Model

After the setting of the initial values on credibility network, to consider OSN users previous activities we suppose that a set of nodes  $S$  becomes spreader, activating themselves to propagate a piece of news. The ignorant neighbors  $I$  exposed to that piece of news must decide whether to repost it or not therefore the sum of the credibility of the edges linking with spreader nodes must exceed the activation threshold of the inactive nodes.

The activation threshold  $g_t(v)$  of a node  $v$  must take into account the contribution of incoming and outgoing edges that in the previous interactions contributed to help that node to create an opinion about its neighborhood. This two contributions are embedded in trust and reliability values calculated before the node is requested to evaluate a new piece of news posted by a spreader, hence the threshold value will be:

$$g_t(v) = R_{t-1}(v) T_{t-1}(v) \quad (5)$$

Therefore, an inactive node  $v$  will become active if:

$$\frac{1}{|U_{out}^S(v)|} \sum_{u \in U_{out}^S(v)} c(v, u) > g_t(v) \quad (6)$$

$U_{out}^S(v) = U_{out}(v) \cap S$  is the set of neighbors spreading the news. If there are new spreaders at time  $t$ , the procedure is repeated for their inactive neighbors otherwise the propagation ends.

#### 3.2.2 Competitive Model

As described above in this scenario two conflicting piece of news are spread simultaneously, hence at a given instant  $t_0$  two groups of spreader  $S_1$  and  $S_2$  are activated. For each subsequent instant for both

pieces of news the activation of the neighboring inactive nodes is attempted according to the following equations:

$$\frac{1}{|U_{out}^{S_1}(v)|} \sum_{u \in U_{out}^{S_1}(v)} c(v,u) > g_t(v) \quad (7)$$

$$\frac{1}{|U_{out}^{S_2}(v)|} \sum_{u \in U_{out}^{S_2}(v)} c(v,u) > g_t(v) \quad (8)$$

If a node is exposed to both ideas at the same time and both sums of credibilities exceed the threshold  $g_t(v)$  a further comparison is necessary to evaluate which group of nodes mostly influences the inactive node:

$$\frac{1}{|U_{out}^{S_1}(v)|} \sum_{u \in U_{out}^{S_1}(v)} c(v,u) > \frac{1}{|U_{out}^{S_2}(v)|} \sum_{u \in U_{out}^{S_2}(v)} c(v,u) \quad (9)$$

If the first term is higher than the second the disputed node is activated for the first piece of news, for the second one elsewhere. At the end of each step if there are new spreaders the attempts of propagation are carried out on the nodes directly reached by the new spreader, otherwise they end.

### 3.2.3 Competitive Model with Delay

In this type of propagation a piece of news coming from untrustworthy nodes is spread and after a certain number of iterations the retraction comes by trustworthy nodes; the viceversa can also occur, i.e. after the spread of a true piece of news a group of malicious spreaders propagate a piece of news with conflicting content.

In this case the diffusion of the *malicious piece of news* and the further diffusion of the retraction at the end of the propagation must be measured, also allowing nodes that posted the malicious news to publish the retraction if the influence of benevolent nodes is greater than the one of malicious nodes. Therefore, the equations are the same of previous case but the execution times are different.

## 4 EXPERIMENTS

### 4.1 Dataset

In this work we used the **Wikipedia edit war network** topology to carry out our simulations (e.g. (Sumi et al., 2011)). It is composed by 116,836 nodes and 2,027,871 directed edges related to the changes performed by users on pages previously modified by

others. Each edge weight falls into the range  $[-9,12]$  that depends on the number of words modified in favor (if it is an attempt to expand the information) or against another user (if it is an attempt to reverse previous changes).

We considered only the first contact between each pair of nodes, filtering the edge list and normalizing the values so that they fall within the range  $[-1,1]$  in order to use them as  $c(u,v)$ . This is important because it avoids that simulations begin from random trust and reliability values that would not be representative of the previous interaction history between pairs of nodes.

### 4.2 Simulator Workflow

To evaluate the model we implemented a simulator that carries out the following steps in order to emulate the spreading processes on OSN:

- It reads the edgelist and generates the corresponding weighted directed network
- exploiting weights, it calculates trust, reliability and the threshold value (respectively with eqs. 1, 2 and 5) for each node
- It creates the trust ranking and selects the percentage of seeds, i.e. the initial spreaders of a piece news (0.1%, 0.2%, 0.5%, 1%, 2% and 5% of total network nodes) from the top or the bottom of ranking and activates them depending on which category of nodes it wants to use as seeds of news propagation, **high trust seeds (HTS)** or **low trust seeds (LTS)**
- For each inactive node that has at least a spreader as neighbors it checks the eqs. 6 or 7 and 8 (in competitive cases also 9 if the threshold is overcome by both factions) and activates the inactive nodes whose threshold are exceeded
- At the end of each loop, checks the list of new spreaders and if it is not empty restarts the loop;
- When the list of new spreaders does not contain new nodes, it saves relevant information about propagation.

### 4.3 Simulations

In the case of a **no-competitive model** we have two cases of initial spreader nodes: trustworthy (HTS) and not trustworthy (LTS) and simulator calculates how many nodes decide to propagate the piece of news from each group of initial spreader nodes.

In the case of a **competitive model** it calculates how many nodes decide to propagate the piece of

news from two conflicting factions, high and low trust nodes. In the case of disputed nodes, i.e. nodes that come into contact with both groups of spreaders, it is interesting to see how many people follow each of the two sides.

In the case of a **competitive model with delay** in addition to the number of nodes that decide to propagate the piece of news of each faction, it calculates the number of nodes changing their opinion after the propagation of retraction.

Therefore, the following five variants of the aforementioned evolution of the model will be examined:

- High trust seeds in no-competitive model
- Low trust seeds in no-competitive model
- High trust seeds vs low trust seeds in competitive model
- High trust seeds vs low trust seeds in delayed competitive model
- Low trust seeds vs high trust seeds in delayed competitive model

#### 4.4 Results

The distribution of  $c$ ,  $T$ ,  $R$  and  $g$  calculated in the second step of simulator workflow on the Wikipedia edit war network are shown in figs. 1, 2, 3 and 4 respectively.

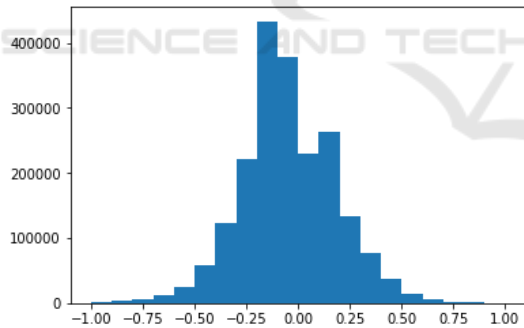


Figure 1: Distributions of credibility initial values for Wikipedia edit war dataset.

Most interactions in this network are to reverse text changes hence most  $c$  have a small negative value. Accordingly to assign negative credibility values to their neighbors, the reliability values are very high in the initial phase while the  $g$  threshold histogram have the same form of the trust histogram, it just appears more contracted along the X axis due to the reliability resizing. The simulator outputs are shown in tables 1, 2 and 3.

In no-competitive model (table 1) we note that using the same number of seeds HTS can always propagate a piece of news more effectively than LTS. When

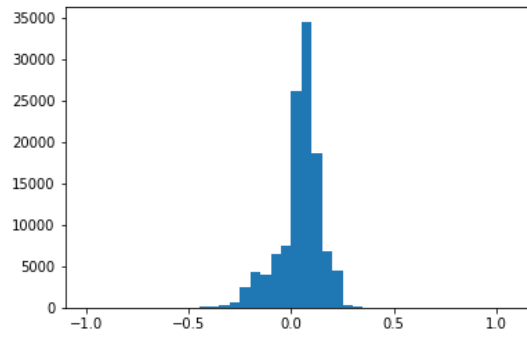


Figure 2: Distributions of trust initial values for Wikipedia edit war dataset.

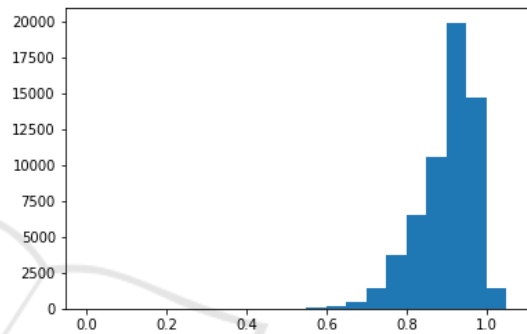


Figure 3: Distributions of reliability initial values for Wikipedia edit war dataset.

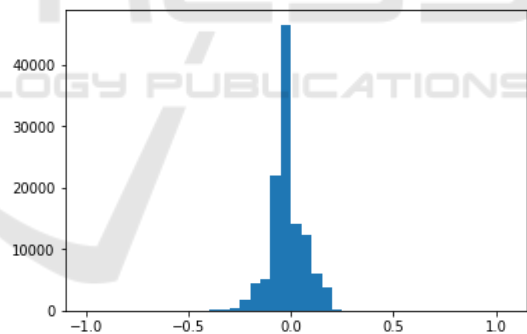


Figure 4: Distributions of  $g$  threshold initial values for Wikipedia edit war dataset.

the seeds are few (0.1%) compared to the total size of the network, LTS cannot convince anyone to repost the piece of news while in the last case (5%) the propagation of the LTS is equal to 1/4 of HTS one, probably thanks to the large number of promoters.

In competitive model (table 2) it can be observed that for the same number of seeds the propagations of both factions are smaller than in no-competitive case. Particularly interesting is the cases of the propagation of LTS with few seeds (0.1%, 0.2% and 0.5%) in which only nodes with few or no contacts with the opposite faction are convinced to propagate the piece of news while almost all nodes reached by HTS has

Table 1: No-Competitive model. Number of nodes that decide to propagate the piece of news deriving from LTS and HTS respectively.

% of seeds	LTS	HTS
0.1	116	13681
0.2	234	14904
0.5	591	16551
1	7657	17763
2	4696	20655
5	6253	24830

Table 2: Competitive model. Number of nodes that decide to propagate a piece of news and, in this set, number nodes in touch with opposite faction for news deriving from LTS and HTS respectively.

% of seeds	LTS	LTS (HTS)	HTS	HTS (LTS)
0.1	116	0	13662	10905
0.2	234	1	14863	11989
0.5	590	6	16443	13218
1	1215	47	17512	15042
2	2564	128	20019	15042
5	6153	312	23245	14763

Table 3: Competitive model with delay. Number of nodes that decide to propagate the piece of news at the end of each propagation and number of *reversed nodes* that change their mind after the second propagation for news deriving from LTS and HTS respectively and vice versa.

% of seeds	LTS	HTS	Reversed	HTS	LTS	Reversed
0.1	116	13681	19	13681	116	0
0.2	234	14903	40	14904	234	1
0.5	591	16551	110	16551	588	0
1	7657	17681	5421	17763	5738	3721
2	4696	20582	2413	20655	3458	852
5	6253	24778	1720	24830	6117	83

contacts with the opposite faction and decided anyway to propagate the HTS piece of news. This means that when there are many seeds with low trust (i.e. the piece of news is perceived as false) it is not the content of the news that plays a fundamental role in its propagation rather the influence of the numerous neighbors that propagate it.

In the competitive model with delay (table 3) the HTS propagate the news more effectively than the LTS as in the previous case but when the denial comes from the HTS for all the percentage of seeds there are some nodes that change idea for a small number of seeds (0.1%, 0.2% and 0.5%) there are no publications of the retraction. In each case the number of retractions is higher for HTS respect to LTS.

## 5 CONCLUSIONS AND FUTURE WORK

In this work, we proposed a model that exploits trust and reliability with 3 variations in order to describe the different way a piece of news can be propagated through OSNs: in the no-competitive model each piece of news is free to propagate over the network without opposition, in competitive model two different factions propagate two pieces of news with opposite contents at the same time in order to convince the undecided social network users to align with their own thought group and finally in competitive model with delay the second piece of news propagation happens after the propagation of the first one in order to convince other user to change their minds and publish a retraction.

We implemented a simulator and used a real weighted directed network as starting point for the simulation. This simulator exploits different number

of seeds belonging to two different groups of users, high trust seeds and low trust seeds. The purpose is twofold, we evaluated the influence in news propagation of large groups of seeds respect to smaller ones and the importance of a high trust respect to a low one.

We discovered that as in real OSNs occurs, if a piece of news is propagated by a small group of user with low trust it does not propagate, indeed in such cases only the initial seeds remain involved in news spreading while if the group of seeds has a high number of members it propagates news over the network but with a minor impact respect to the case of the same number of seeds with high trust. This means that trust is an important metric in this scenarios but also the influence of neighborhood plays a key role in the decision to further spread or not.

Currently we are working to an improved model where dynamics is introduced by inserting a credibility update mechanism to check whether and to what extent the changing of user behaviors (e.g. a HTS suddenly start to spread fake news or viceversa) affects the credibility and the related spread.

## REFERENCES

- Adali, S., Escriva, R., Goldberg, M. K., Hayvanovych, M., Magdon-Ismael, M., Szymanski, B. K., Wallace, W. A., and Williams, G. (2010). Measuring behavioral trust in social networks. In *2010 IEEE International Conference on Intelligence and Security Informatics*, pages 150–152. IEEE.
- Baumann, F., Lorenz-Spreen, P., Sokolov, I. M., and Starnini, M. (2019). Modeling echo chambers and polarization dynamics in social networks.
- Carchiolo, V., Longheu, A., Malgeri, M., and Mangioni, G. (2015a). The cost of trust in the dynamics of best attachment. *Computing and Informatics*, 34(1):167–184.
- Carchiolo, V., Longheu, A., Malgeri, M., and Mangioni, G. (2015b). Searching for experts in a context-aware recommendation network. *Comput. Hum. Behav.*, 51(PB):1086–1091.
- Carchiolo, V., Longheu, A., Malgeri, M., Mangioni, G., and Previti, M. (2018a). Introducing credibility to model news spreading. In Cherifi, C., Cherifi, H., Karsai, M., and Musolesi, M., editors, *Complex Networks & Their Applications VI*, pages 980–988, Cham. Springer International Publishing.
- Carchiolo, V., Longheu, A., Malgeri, M., Mangioni, G., and Previti, M. (2018b). A trust-based news spreading model. In Cornelius, S., Coronges, K., Gonçalves, B., Sinatra, R., and Vespignani, A., editors, *Complex Networks IX*, pages 303–310, Cham. Springer International Publishing.
- Caverlee, J., Liu, L., and Webb, S. (2008). Socialtrust: tamper-resilient trust establishment in online communities. In *Proceedings of the 8th ACM/IEEE-CS joint conference on Digital libraries*, pages 104–114. ACM.
- DuBois, T., Golbeck, J., and Srinivasan, A. (2011). Predicting trust and distrust in social networks. In *2011 IEEE third international conference on privacy, security, risk and trust and 2011 IEEE third international conference on social computing*, pages 418–424. IEEE.
- Fung, R. and Lee, M. (1999). Ec-trust (trust in electronic commerce): Exploring the antecedent factors. In *Proceedings of the 5th Americas Conference on Information Systems*, pages 517–519.
- Gleich, D. F. (2014). Pagerank beyond the web.
- Golbeck, J. (2005). Personalizing applications through integration of inferred trust values in semantic web-based social networks. In *Semantic Network Analysis Workshop at the 4th International Semantic Web Conference*, volume 16, page 30. Publishing.
- Golbeck, J., Parsia, B., and Hendler, J. (2003). Trust networks on the semantic web. In *International workshop on cooperative information agents*, pages 238–249. Springer.
- Hang, W. and Singh, M. (2010). Trust based recommendation based on graph similarities.
- Hodas, N. O. and Lerman, K. (2014). The simple rules of social contagion. *Scientific reports*, 4:4343.
- Kim, Y. A., Le, M.-T., Lauw, H. W., Lim, E.-P., Liu, H., and Srivastava, J. (2008). Building a web of trust without explicit trust ratings. In *2008 IEEE 24th International Conference on Data Engineering Workshop*, pages 531–536. IEEE.
- Kuter, U. and Golbeck, J. (2007). Sunny: A new algorithm for trust inference in social networks using probabilistic confidence models. In *AAAI*, volume 7, pages 1377–1382.
- Liu, H., Lim, E.-P., Lauw, H. W., Le, M.-T., Sun, A., Srivastava, J., and Kim, Y. (2008). Predicting trusts among users of online communities: an opinions case study. In *Proceedings of the 9th ACM conference on Electronic commerce*, pages 310–319. ACM.
- Massa, P. and Avesani, P. (2007). Trust-aware recommender systems. In *RecSys '07: Proceedings of the 2007 ACM conference on Recommender systems*, pages 17–24, New York, NY, USA. ACM.
- Nepal, S., Sherchan, W., and Bouguettaya, A. (2010). A behaviour-based trust model for service web. In *2010 IEEE International Conference on Service-Oriented Computing and Applications (SOCA)*, pages 1–4. IEEE.
- Persia, F. and D’Auria, D. (2017). A survey of online social networks: Challenges and opportunities. In *2017 IEEE International Conference on Information Reuse and Integration (IRI)*, pages 614–620.
- Sumi, R., Yasseri, T., Rung, A., Kornai, A., and Kertesz, J. (2011). Edit wars in wikipedia. *2011 IEEE Third Intl Conference on Privacy, Security, Risk and Trust and*



*2011 IEEE Third Intl Conference on Social Computing.*

- Trifunovic, S., Legendre, F., and Anastasiades, C. (2010). Social trust in opportunistic networks. In *2010 IN-FOCOM IEEE Conference on Computer Communications Workshops*, pages 1–6. IEEE.
- Vasudevan, A., Owusu, E., Zhou, Z., Newsome, J., and McCune, J. M. (2012). Trustworthy execution on mobile devices: what security properties can my mobile platform give me? In *Proceedings of the 5th international conference on Trust and Trustworthy Computing*, TRUST'12, pages 159–178, Berlin, Heidelberg. Springer-Verlag.
- Wang, Y. D. and Emurian, H. H. (2005). An overview of on-line trust: Concepts, elements, and implications. *Computers in Human Behavior*, 21(1):105 – 125.
- Wu, J., Chiclana, F., Fujita, H., and Herrera-Viedma, E. (2017). A visual interaction consensus model for social network group decision making with trust propagation. *Knowledge-Based Systems*, 122:39–50.
- Zhang, Y., Chen, H., and Wu, Z. (2006). A social network-based trust model for the semantic web. In *International Conference on Autonomic and Trusted Computing*, pages 183–192. Springer.
- Zinoviev, D., Duong, V., and Zhang, H. (2010). A game theoretical approach to modeling information dissemination in social networks. *arXiv preprint arXiv:1006.5493*.
- Zuo, Y., Hu, W.-c., and O’Keefe, T. (2009). Trust computing for social networking. In *2009 Sixth International Conference on Information Technology: New Generations*, pages 1534–1539. IEEE.

