Role of Trust in Creating Opinions in Social Networks

Jiří Jelínek
Institute of Applied Informatics, Faculty of Science, University of South Bohemia,
Branišovská 1760, 370 01, České Budějovice, Czech Republic

Keywords: Trust, Social Systems, Opinion Dynamics, Multi-Agent Systems.

Abstract: Although we are not always aware of this, our existence and especially communication are based on the principles of trust. The importance of trust is crucial in systems where risk is present e.g. when handling the information we have acquired through communication because it is not always possible to immediately verify the truthfulness of it. The aim of this paper is to link two areas, namely the reality in the human community described above and the available knowledge of social networks and multi-agent systems, and try to simulate real trust concerned scenarios in society by these tools. The multi-agent model will be presented, which simulates the behavior of the heterogeneous group (people-like) entities in the process of creating their opinion about the world on the basis of information acquired through communication with other agents. The focus is placed on the processes influencing trust in communication partners and its dynamics. The results of the experiments are also presented.

1 INTRODUCTION

Although we are not always aware of it, our existence and communication in particular are based on principles based on moral values in society. The key role here is played by the trust between communicating parties, the importance of which is crucial to further handle the sometimes unverified information we have acquired through these communications.

Today we often hear statements made by people in the media that are either unsubstantiated or frankly false. Some individual from society could react to these statements, making it clear that their opinion is somewhat different. However, these false statements frequently go unnoticed in the media, and then it is up to the individual to state the conformity or inconsistency of the statement with his/her opinion of the world. In case of an inconsistency, confidence in the given source of information is reduced.

The consequences of both cases mentioned are very serious and lead to increased caution when communicating and place an emphasis on an individual's own knowledge. These individuals also explore the trustworthiness of the communication partners and are able to better consider whether the communication brought usable information.

We could consider this topic as a purely philosophical one, but it is not. The same problems can be observed in the information systems and multi-agent models and also in the Internet of Things. The time has come when well-known people begin to call for a basic codification of the IoT environment in terms of ethics and accountability (Cerf, 2017).

The aim of this paper is to link these two areas, namely the reality in the human community described above and the available knowledge of social networks and multi-agent systems, and to try to simulate real trust scenarios by these tools.

The next sections of the paper are organized as follows: section 2 focuses on the current state of the knowledge and a discussion on the selection of literature dealing with this field. Section 3 describes the model presented and its configuration and classification. Section 4 then focuses on implementing the model and experiments.

2 STATE OF THE ART

The problem of trust has gone through several periods in the past when it was more emphasized. The last two of these periods took place around 2002-2006 and during 2012-2016. A large number

Jelínek, J.
Role of Trust in Creating Opinions in Social Networks.
DOI: 10.5220/0006592102080215
In *Proceedings of the 10th International Conference on Agents and Artificial Intelligence (ICAART 2018) - Volume 1*, pages 208-215
ISBN: 978-989-758-275-2

of contributions mainly focused on the field of multi-agent systems can be found during these periods and beyond, which were concerned with the question of trustworthiness in communication.

Surveys such as (Ramchurn et al., 2004), (Pinyol and Sabater-Mir, 2013) and (Granatyr et al., 2015) are especially important for examining the issue so as the introductory commentary for the conference section (Falcone and Singh, 2013). The classification of existing models of trust is also proposed in (Granatyr et al., 2015). In section 3.4 we classify our model according to these criteria. Two approaches to working with trust in a partner are presented in (Ramchurn et al., 2004) - individual and systematic one. We use the elements of both of them. Our model is based on an individual approach and the credibility of the environment is guaranteed on a system-wide level.

A well-known but often difficult to describe relationship of trust and risk is mentioned in the paper (Varadharajan, 2009). Also the validity of the partner’s trustworthiness is presented as dependent on the type of service, message content, or field of expertise. However, the frequent service overlap and link to an individual rather than a service is cited in other materials. We think that trust can be shared in areas similar to one another, where one can expect a similar competence of a partner. In our model, we suppose trust is connected to an individual.

The next paper (Yolum and Singh, 2003) focuses on a specific area of service provision. The model described focuses primarily on the system of transmitting references between agents about service providers. The quality of these services is evaluated by agents, but the model does not work with verifying the messages. We considered this verifying mechanism to be important and thus we implemented it in our model.

Regarding the delivery of the service, ideas are presented in the paper (Sen, 2013). The paper presents some interesting notes about trust in general, such as the relationship of trust and the cost of the service or the communication. This idea is interesting and we would like to implement it in our model.

The problem of anonymity is discussed in (Fredheim et al., 2015), which presents the study of the behavioral changes on a discussion forum before and after the mandatory identification. This area is generally neglected in multi-agent systems. Our model is not an exception, but anonymity will be the subject of further development of it. The current status can be described as identification with the pseudonym.

On the contrary, the article (Huang and Fox, 2006) coincides partially with our approach in focusing on the dissemination of information in social networks. The issue of possible transitivity of trust is also raised. However, from our point of view, it is more appropriate to set the agent’s trust in their partner’s partner as a product of the agent’s trust in their partner and the partner’s trust in their partner. This respects the experience and trust in partners.

A model examining the spreading of information in the social network can be found in (Jelínek, 2014). The experience gained when constructing this model was used in this contribution, especially the rating mechanism of communication partners, defined on the basis of individual communication between agents.

The field of monitoring the developments on the dynamics of individual opinions in conjunction with political or similar influences is focused in (Horio and Shedd, 2016). The authors present their work in the field and the main published models - Deffuant-Weisbuch (DW) (Deffuant et al., 2000) and Hegselmann-Krause (HK) (Hegselmann and Krause, 2002). For our model, the statement based on (Lorenz, 2007) is interesting - when forming opinions (communication for this purpose), individuals prefer partners with similar opinions.

3 DESCRIPTION OF THE MODEL

The area targeted by this contribution is specific due to the focus on disseminating information inside the community and creating a world opinion, especially in relation to mass communication. We focus on situations where verification of truthfulness of transmitted messages is possible only with a delay and sometimes not possible at all.

The specificity of the presented model is also in using an information (knowledge) base of individual agents, which can be presented as a basis on which the opinion of the individual about the world is formed. We suppose expression of trust with a single number in the range (0, 1), where 1 means absolute trust. We also distinguish between two types of trust - the trust in the partner and the trust in the content of the information.

3.1 Model Principles

Three logical levels can be identified in the model. At the highest level, the model focuses on the trustworthiness of communication in the social network while examining the problems of the truth of the information transmitted. The subsequent influence on the development of opinions of the individuals in the community is also taken into account. This topic is related to the issue of trust at a higher level - trust in general. This is also where the influence of information verification is examined.

The middle level is agent's trust setting in the multi-agent environment itself. Here, the model uses the local tools - agents independently evaluate the credibility of their partners with the help of the content of the message. The main processes of communication and setting and working with trust in partners are defined at this level. The model is capable of implementing agents with different settings and behaviors (a heterogeneous community).

The third level of the model is the representation of transmitted information and the specific methods used for calculating the necessary parameters and their relation to higher levels of the model. We use a representation of knowledge with the N3 clauses (subject – link - object) complemented by a continuous sureness parameter within the interval (-1, 1). The sureness is an inseparable part of N3 knowledge representation, so we talk about the extended N3 knowledge representation. The clause is further supplemented with metadata about the source (from whom it was obtained), the origin (who originally created it), the trust in it, its verification state and its activity state (related to the process of forgetting). The last three metadata are continuous values on the interval (0, 1).

Exactly one clause is transferred during one communication between agents, and each agent gradually creates its own knowledge base represented by a set of these clauses. The base can be represented as an oriented graph with subjects and objects in the nodes and links between them. The graph is assumed to preserve the transitivity of the links for calculating some of the values, (if $A \xrightarrow{link} B\ and\ B \xrightarrow{link} C, then\ A \xrightarrow{link} C$).

The agent's trust in the partner (i.e. the hope the partner is able to provide us with the information and also wants to do so) is set purely individually within the inner processes of the agent. The agent is limited to its own experience when setting the trust.

3.1.1 Information Verification

The truthfulness of the message the recipient may or may not be able to be verified. The time factor is also important (verification may not take place immediately when receiving the message but later). The key factor is whether the recipient has access to the resources that allow the information to be verified.

We could also discuss what source the agent would consider being sufficiently objective (trusted) to verify the message. However, this creates a vicious circle because the same aspects are relevant for this source as are for the sender of the message. One possible way is to define an authority that will objectively store truthful information about the world and will be able to verify the message and truthfully inform the questioner. This authority in the model is a special agent called the *world*. The information (clauses) provided by the *world* are generally correct and verified but agents do not have to know that immediately. We call the communication of the agent with the *world* and obtaining information from it as an *observation*.

3.2 Selected Model Details

Due to the limited space of this contribution, some key functionality has been selected from the model, which will be further explored in the following subsections.

3.2.1 Clause Usefulness

The model works with the knowledge base of the agent, over which it quantifies several variables. The first of the key parameters is the usefulness u_c of the given clause from the interval (0, 1).

The clause is useful if it delivers information the agent does not have on his or her base and cannot be derived from it, or has it, but with less sureness or worse metadata. Deriving, in this case, means to find the shortest path in the base graph starting with the subject of the clause and ending in the object where the type of all the links is the same as the link in the clause.

If the new N3 clause has a higher sureness (positive or negative), it is useful for the agent and included in the base.

If this is not the case, the path described above is searched for, and if it exists, the metadata of the clauses contained in the path are investigated. The aim here is determining the value of the metadata for the entire sequence of clauses. According to the principle of the weakest part of the chain, it will be the lowest value of the whole path, so the minimum value of verification v_{min} and trust t_{min} is sought. If $v_c > v_{min}$ and therefore the new clause is better verified, it is useful in $u_c = v_c - v_{min}$. If this does not apply, the confidence is calculated in the same way, i.e. for $t_c > t_{min}$ the usefulness of clause is $u_c = t_c - t_{min}$.

If the path does not exist in the base, the benefit is set according to the N3 clause element information. Usefulness is set as

$$u_c = \max(f_s, f_l, f_o), \tag{1}$$

where f_x are values calculated for three elements of N3 (subject, link, object) as

$$f_x = \frac{1}{(d_x + 1)} \tag{2}$$

The d_x value is the degree of the given node or the frequency of the given link type in the base. This calculation encourages the agent's behavior to expand its knowledge base and, therefore, clauses containing N3 elements not yet included in the base or included with a low degree or low frequency are more useful.

3.2.2 Trust in Clause

Trust in the clause is generally based on its content, but our confidence in the source from which we obtained it is also significant. The weights of these parts are matters of the personality profile of the individual and therefore the model must allow them to be modified. The specific confidence calculation method in the t_c clause is then set according to the formula

$$t_c = k_s(1 - |s_c - s_b|) + (1 - k_s)t_s t_p, \tag{3}$$

where k_s is the personal self-trust factor of the individual in his own knowledge in the range (0, 1), s_c is the sureness of the N3 clause, s_b then the sureness of the N3 derived from the individual's knowledge base as the minimum value of the sureness of the same N3 clauses in the base or the path found by derivation (see 3.2.1.). The t_s parameter is the agent’s trust in the sender and t_p the sender’s trust in that clause. Obviously, for $k_s = 1$ the individuals will rely solely on their knowledge and vice versa.

3.2.3 Trust in Sender

The value of t_s is the subject of a further description of the model. In principle, this trust in the source of information will certainly be based on verifying the information obtained from it. However, it is also necessary to consider a state where verification is not available at a given moment or is not available at all. The t_s value evolves over time and describes the long-term experience with the partner. This dynamics is expressed by a classical mechanism of the gradual modification of the value t_s according to the formula

$$t_s = t_s + k_t(x_c - t_s), \tag{4}$$

where k_t is the adjustment factor with value in the interval (0, 1). The value x_c in the formula is either the value v_c (if verification is available) or the trust value t_c in other cases.

3.3 Model Parameters and Initialization

The model is designed with high flexibility and the user can set it using the five parameters for the entire model:

- The number of individual objects occurring as objects or subjects in clauses.
- The number of link types occurring in clauses.
- The number of clauses forming the knowledge base about the world administered by the *world* agent.
- The initial number of agents in the simulation (which can change).
- The number of simulation steps.

When selecting the agent parameters, the aim was to eliminate some of the limits of the existing models identified in section 2. E.g. it means implementing the self-trust factor (see 3.2.2) and the probability of choosing a random partner (reflecting the random communication in the community). The next seven parameters determine the agent’s behavior:

- The probability of observation, i.e. acceptance of a new clause from the world agent.
- The probability of accepting a new clause from a partner in communication.
- Agent forgetting factor affects (decreases) the activity of the given clause or orders its deletion when the activity is very low.
- The probability of choosing a random partner which takes into account random communications.
- The probability of selecting a random clause in communication. Otherwise, it is preferred to choose a partner’s clause that contains the same N3 elements as the one obtained last.
- The rate of increasing trust. It is the speed at which trust in the partner providing useful information grows.
- Self-trust rate. The higher, the more the agents rely on themselves and their knowledge.

It is clear that model setting is a multidimensional problem and the model is able to simulate various scenarios according to specific requirements. On the other hand, the number of degrees of freedom represented by the number of model parameters complicates validating the model.

Already during the first experiments with the model, it turned out that the model is very sensitive to the initial settings, especially in terms of whom the agents prefer to communicate with. The model provides three initialization options.

The first option is to choose a scale-free model with random communication partners (*random initialization - RI*). The agent has complete freedom to choose a partner.

The second option is orientation on the preferred sources of information (*preferred initialization - PI*). Network dynamics should respond faster to world changes.

The third option is the second approach alternative but now preferred the locality (*local initialization - LI*). Agents use the closest simple agents (in terms of their numbering).

3.4 Model Classification

Classification of the model was performed in order to fit it into the overall issue of research on trustworthiness. The criteria presented in (Granatyr et al., 2015) were used in the following text in the form of a dimension-value-description.

Paradigm type - cognitive, numerical. The model imitates the behavior of human individuals but also takes into account the numerical procedures based on the processing of historical data and the content and structure of the information transmitted.

Information sources - direct interaction (DI), partly witness information (WI), partially certified reputation (CR). Data collection from direct interaction between agents (DI) is the key to establishing trust but the information about trust or origin transmitted from previous sources and recorded on the transmitted message are also used (WI). In the part of the model (agent *world*) the general validity and full trust (CR) is assumed.

Cheating assumptions - cheating (L2). The model has no assumptions in the area of false information and cheating is allowed. However, the mechanism for verifying a message that is able to reveal the liars is used, even if this does not necessarily become immediately.

Trust semantics - partially. Trust is represented in the model as the only number but it covers several areas with different weights and clear semantic significance.

Trust preferences - partially. The model works with the weights of components from which trust is calculated. These weights characterize the personality of the agent and his preferences and are given as agent parameters. The agent can change them (but this is not being used now).

Delegation trust - no. The delegation concept is not used in our model.

Risk measure - partially. The risk of choosing a trustworthy communication partner can be determined but not necessarily. The key here is if it is possible to verify the quality of the selected risk value by verifying the content of the message.

Incentive feedback - no. Our model assumes that agents truthfully inform on the metadata of messages and communications.

Initial trust - no. Our model does not provide a special initial trust setting for newcomers, but it does not penalize them. The initial trust of a new agent is set to a neutral value 0.5.

Open environment - partly. The model is open and it does not address possible fraud (change of agent identity).

Hard security - no. The possibility of a security breach in communication is not assumed.

4 IMPLEMENTATION AND EXPERIMENTS

The presented model was implemented to verify its ability to simulate the dynamics of communication and creating individual knowledge bases in the community of individuals. Each agent communicates with the others on the basis of a random formula. On the basis of this communication, individuals formulate the opinion about the world in which they live.

The model has been implemented in Java and one of its undisputed benefits is very detailed logs of all significant parameters of each agent and the overall model (millions of values for experiments presented).

The description of the world is generated by the *world* agent. Its knowledge base characterizes the objective state of the world without any distortion caused by the sensors or due to the trust setting. The clauses can then be disseminated to other agents through the communication.

4.1 Experiments

The purpose of the experiments was to simulate and then to analyze the behavior of individuals in an environment with the limited possibility of verifying the information or knowledge. The performed experiments focus on specific scenarios formulated with the aim to match the real world situations very closely. Only the selection of results demonstrating a given tasks has been included in this article.

The basic setting of experiments was an environment in which only a limited group of privileged agents has access (two in our experiments). These agents gain objective information by observing the world. One of them does this without a change of information (a good agent), but the other one intentionally manipulates the information and negates the sureness of clauses (a bad agent).

In addition to these privileged agents, there is a set of other simple agents without access to the *world.* They create their knowledge bases only on the basis of communication with other agents, including the privileged ones. With the above-mentioned bad agent exception, it is assumed that this communication takes place without distortion and a change of the information. The factors studied here are the knowledge bases of individuals and their development. The underlying hypothesis here is that an individual can develop his world opinion on the basis of completely erroneous information of a bad agent.

The similarity of the knowledge base of the agent with the knowledge bases of privileged agents was chosen as an output value. This is determined by comparing each simple agent's knowledge clause with a privileged agent base. If the given clause (its N3 parts) can be derived from the base, the clause is considered to be similar according to the difference of sureness between the clause and the base. The resulting summary across all of the simple agent's clauses is then normalized by the size of the agent's knowledge base. It does not apply that the sum of similarities to all privileged agents is 1 - the simple agent more similar to a good one can be partially similar also to bad one.

The second output is the trust (and thus preference) in agents in the social network. It is individually calculated by a particular agent, but its average value can be determined by the formula

$$d_j = \frac{1}{N_j}\sum_{i}^{N_j} d_{ij}, \tag{5}$$

where N_j is the number of agents having among their partners agent j and d_{ij} is the trust of agent i in agent j.

The global model setting was the same for all experiments. There were 20 individual objects and 5 types of links from which 100 clauses were randomly generated. This was sufficient for the selected scenarios, but it would be interesting to examine the influence of the world knowledge base size on the model behavior. The number of simple agents was set to 50; the number of simulation steps (x-axis of all graphs) was usually 500. The experiments also used different settings for individuals (see scenarios).

4.1.1 Scenario 1

The first scenario was a simulation of network dynamics without the possibility of verifying clauses and the process of forgetting. Its goal was to investigate how the initialization method affects the behavior of agents.

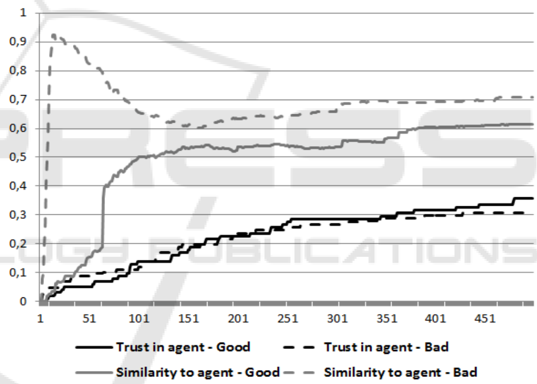

Figure 1: Average similarity of agents to and trust in good or bad one – RI.

Three experiments were performed based on the initialization type. The first was random initialization (RI). Its output normalized by the total number of agents is shown in Figure 1. Because the simple agents can also communicate with each other, we can see at the beginning about 100 steps period, when simple agents create the base without clear orientation to good or bad agent knowledge (the trust in these agents is still evolving). The situation stabilizes after this period of profiling.

It is clear that trust in both privileged agents is essentially the same, as well as the number of clauses from them in the knowledge bases of ordinary agents. However, every simple agent gradually developed into a supporter of one of the privileged (what can be seen from other outputs).

The same scenario for initialization with the preference of direct communication with privileged resources (PI) is shown in Figure 2. We see that trust in privileged agents has slightly increased. However, the greatest change is evident at the beginning of the simulation when agent profiling went very quickly. For this experiment, we can also observe (again from another model outputs) the privileged agents' preference in communication and also the highest values of trust in them from all agents.

A situation very similar to a random initialization occurs in the case of initialization with the closest partner preference (LI). Agent profiling again caused significant fluctuations at the beginning of the simulation.

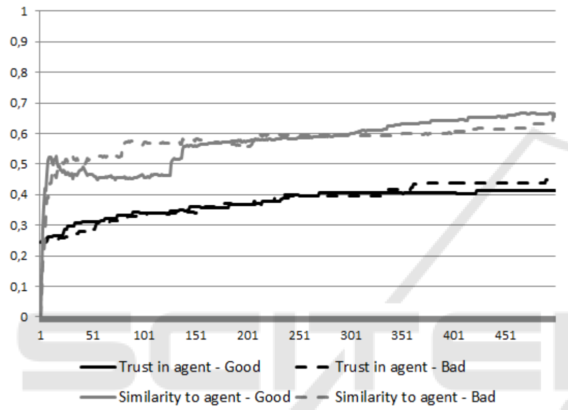

Figure 2: Average similarity of agents to and trust in good or bad one – PI.

4.1.2 Scenario 2

The objective of the second scenario was to verify how dynamics of the network changes when allowing the clauses to be verified. The verification was enabled from step 200, the other settings were the same as in the first experiment from the previous scenario, except the number of simulation steps (here 1000 steps).

Figure 3 shows a change in the behavior of the model and the increase of the average similarity of the agents' bases with a good agent. The agents reoriented themselves to resource that offered information consistent with the real world. However, the opinion of agents originally oriented on a bad agent is changing very slowly. Also, the trust in a bad agent has not fallen to the simulation end but has grown significantly slower than trusting in a good agent.

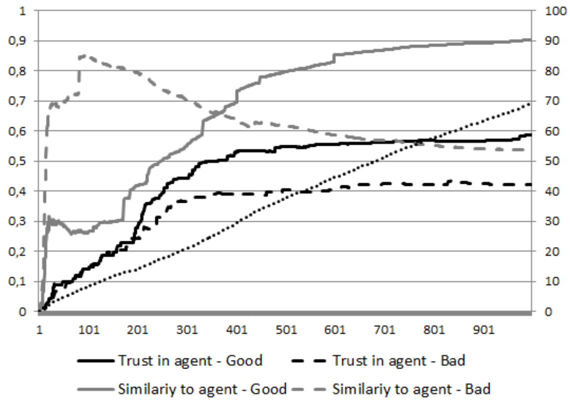

Figure 3: Average similarity of agents to and trust in good or bad one – verification enabled.

The position of the bad agent appears to be quite good but, on other outputs, it can be shown that this is not the case. In a purely binary classification of similarity, the orientation on a good agent is the dominant one from the step about 350.

In Figure 3 (on the right-hand y-axis in percent), is dottted the average size of agents' bases.

4.1.3 Scenario 3

The last simulated scenario was focused on the effect of forgetting on network dynamics. The initial settings were taken from Scenario 2 and modified by enabling forgetting of clauses in agents' bases. The number of simulation steps was also reduced to 500 steps.

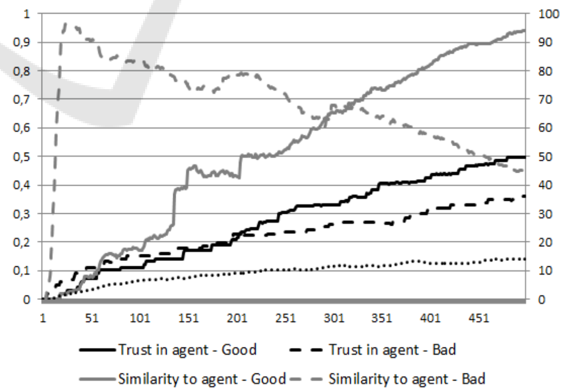

Figure 4: Average similarity of agents to and trust in good or bad one – verification and forgetting enabled.

In Figure 4 the meanings of the lines are the same as in Figure 3. By comparing both Figures, it is obvious that enabling the forgetting of older clauses has greatly accelerated the process of agent orientation to the correct source (good agent). Yet in addition to that, agents' knowledge bases were reduced in size on average of about 2.5 times (measured in step 500). This means that agents have much less knowledge for creating opinions, but the knowledge is of higher quality (clear profiling on the good agent). The smaller knowledge base also significantly contributed to the speed and efficiency of agents' activity.

5 CONCLUSIONS

This paper presents a multi-agent model simulating the behavior of the heterogeneous group of (people-like) entities in the process of creating their opinion about the world on the basis of information acquired through communication with other agents. The reason for the constructing the model is to investigate the dynamics of trust in an environment with limited possibilities to verify the transmitted information. Local metadata from previous contacts with the partner are used for establishing trust as well as the knowledge base of the agent. Presenting techniques to evaluate this information and use it in trust settings were presented as well. The model is highly adjustable with global and agent-specific parameters.

The performed experiments were focused on scenarios where the limited possibilities to verify the information caused that the agent's knowledge base could be built on completely incorrect information. The results also showed that the later availability of verified information changes the knowledge base and hence the attitudes of the individuals very slowly. It was also shown that forgetting older clauses from the knowledge base leads to quicker trust profiling of simple agents, and to accepting knowledge primarily from the verified source.

The created model will be further developed and tested especially on the basis of ideas from papers cited in section 2. Future work should be concentrated on analyzing the problem of dynamics of the community structure. Special attention will be laid on model validation, where it will be necessary (due to specific model parameters) to collect real-world data for deeper model validation.

This model could be increasingly used in the future, depending on how individuals and companies gradually discover the possibility of manipulating information. Typical examples of applications can be social systems where individuals can spread unverified or false information and systems with limited ability to verify information.

REFERENCES

Cerf, V. (2017). A brittle and fragile future. *Communications of the ACM*, 60(7), pp.7-7.

Deffuant, G., Neau, D., Amblard, F., & Weisbuch, G. (2000). Mixing beliefs among interacting agents. *Advances in Complex Systems*, *3*(01n04), pp. 87-98.

Falcone, R., & Singh, M. P. (2013). Introduction to special section on trust in multiagent systems. *ACM Trans. on Intelligent Systems and Technology (TIST)*, *4*(2), p. 23.

Fredheim, R., Moore, A., & Naughton, J. (2015). Anonymity and Online Commenting: The Broken Windows Effect and the End of Drive-by Commenting. *Proceedings of the ACM Web Science Conference* (p. 11). ACM.

Granatyr, J., Botelho, V., Lessing, O. R., Scalabrin, E. E., Barthès, J. P., & Enembreck, F. (2015). Trust and reputation models for multiagent systems. *ACM Computing Surveys (CSUR)*, *48*(2), 27.

Hegselmann, R., & Krause, U. (2002). Opinion dynamics and bounded confidence models, analysis, and simulation. *Journal of artificial societies and social simulation*, *5*(3).

Horio, B. M., & Shedd, J. R. (2016). Agent-based exploration of the political influence of community leaders on population opinion dynamics. In *Proceedings of the 2016 Winter Simulation Conference* (pp. 3488-3499). IEEE Press.

Huang, J., & Fox, M. S. (2006). An ontology of trust: formal semantics and transitivity. In *Proceedings of the 8th int. conference on Electronic commerce* (pp. 259-270). ACM.

Jelínek, J. (2014). Information Dissemination in Social Networks. In *Proceedings of the 6th Int. Conference on Agents and Artificial Intelligence-Volume 2* (pp. 267-271). SCITEPRESS.

Lorenz, J. (2007). Continuous opinion dynamics under bounded confidence: A survey. *International Journal of Modern Physics C*, *18*(12), pp. 1819-1838.

Pinyol, I., & Sabater-Mir, J. (2013). Computational trust and reputation models for open multi-agent systems: a review. *Artificial Intelligence Review*, *40*(1), pp. 1-25.

Ramchurn, S. D., Huynh, D., & Jennings, N. R. (2004). Trust in multi-agent systems. *The Knowledge Engineering Review*, *19*(1), 1-25.

Sen, S. (2013). A comprehensive approach to trust management. In *Proceedings of the 2013 int. conference on Autonomous agents and multi-agent systems* (pp. 797-800). International Foundation for Autonomous Agents and Multiagent Systems.

Varadharajan, V. (2009). Evolution and challenges in trust and security in information system infrastructures. In *Proceedings of the 2nd int. conference on Security of information and networks* (pp. 1-2). ACM.

Yolum, P., & Singh, M. P. (2003). Ladders of success: an empirical approach to trust. In *Proceedings of the second int. joint conference on Autonomous agents and multiagent systems* (pp. 1168-1169). ACM.