Effectiveness of Information Retraction

Cindy Hui*, Malik Magdon-Ismail†, Mark Goldberg† and William A. Wallace*
*Department of Industrial and Systems Engineering
Rensselaer Polytechnic Institute
Troy, New York
Email: huic@rpi.edu, wallaw@rpi.edu
†Department of Computer Science
Rensselaer Polytechnic Institute
Troy, New York
Email: magdon@cs.rpi.edu, goldberg@cs.rpi.edu

***Abstract*—In this work, we study the effectiveness of information retraction in situations where information being spread requires recipients to make a decision or take an action. Consider the scenario where information is introduced into a network, advising recipients to take an action. If at a later time, the information is found to be inaccurate and the action is unnecessary, it becomes a concern to cease the information from spreading any further and stop people from taking the action. The spread of inaccurate information can lead to confusion and mistrust, and therefore it is important to be able to quickly impede or retract inaccurate information, if needed to at a later time. We investigate the idea of introducing counter messages into a network to interfere with an ongoing diffusion and stop the action that was prescribed by the previous messages. These counter messages are diffusive themselves and may spread through the network based on the recipient's evaluation of the information. We present an empirical framework for modeling the spread of actionable information and information retraction. Using the framework, we perform preliminary experiments to investigate strategies for broadcasting the counter message, in particular, how to identify individuals that should receive the counter message directly from the information source. There is a trade off between a fast effective spread of actionable information and the ability to retract the information. Findings also suggest that alternate strategies will have to be explored to incorporate group structures and the distribution of trust in designing a useful abort mechanism.**

***Index Terms*—agent-based simulation, information diffusion, information retraction, social networks**

I. Introduction

Consider the scenario where information is introduced into a network, advising recipients to take an action. If at a later time, the information is found to be inaccurate and the action is unnecessary, it becomes a concern to cease the information from spreading any further and stop people from taking the action. The spread of inaccurate information can lead to confusion and mistrust, and therefore it is important to be able to quickly impede or retract inaccurate information, if needed to at a later time. We investigate the idea of introducing counter messages into a network to interfere with an ongoing diffusion and stop the action that was prescribed by the previous messages. These counter messages are diffusive themselves and may spread through the network based on the recipient's evaluation of the information.

The interest of this study is to compare the spread of the actionable information with the spread of the counter messages. We present an empirical framework for modeling the spread of actionable information and counter messages. The nature in which pieces of information spread and how individuals evaluate the information would depend on the characteristics of the information and the understanding of the context.

II. Related Work

Whether the case is to prevent disease spreads, protect computer networks from viruses, or control the spread of bad gossip or information, a common goal is to achieve the best possible immunization effect with the minimum amount of necessary resources. The assumption is that resources, e.g. vaccination, anti-virus software, advertisement target, can be costly and limited.

Much literature looks at immunization strategies for epidemics on social networks as well as viruses on computer networks. In both contexts, there is a virus or disease is being spread in a network and the immunization strategy is minimize the spread of the virus or disease by immunizing certain nodes in the network. Immunization strategies focus on selecting which nodes to immune, to prevent the spread of disease in various complex network structures. The selection of nodes to vaccinate are often determined from a static network structure and is often done before the virus or disease spread occurs [1], [2], [3] . Some research also considered the case where the immunization and the virus or disease spread through the network concurrently [4], [5].

Related research have also looked at this problem as the spread of competing information in networks, where there is a good campaign (immunization) and a bad campaign (virus). Budak et al. [6] investigated the problem of limiting the spread of misinformation by finding optimal methods for disseminating good information. The authors looked at identifying a subset of individuals in the network that needs to be convinced to adopt a good information campaign so that the number of individuals that adopt the bad information campaign is minimized.

978-1-4577-1051-3/11/$26.00 ©2011 IEEE

III. Experimental Framework

First, we describe a diffusion framework for simulating the spread of actionable information and counter messages through a network. The purpose of the counter message is to interfere with an ongoing diffusion and to stop the action that was prescribed earlier. To avoid confusion, the message being diffused will be referred to as the $Action$ message. The action associated with the $Action$ message is to spread the information and leave the network after a period of time, i.e. individual may remove themselves from the network. The counter message will be referred to as the $Abort$ message. The action associated with the $Abort$ message is to not leave the network.

A. Diffusion model

The diffusion model defines how information flows through the social network and how individual nodes process the information from incoming messages and determine their behaviors. The messages are introduced through external source nodes. Each message is classified into one of two types: $Action$ or $Abort$ and is characterized by a source-value pair (S, V), which specifies the original source and a corresponding information value.

The messages are propagated when nodes interact and the information value of the message may change as it is pass from node to node. When the message is passed from a sender to a recipient, the information value of the message at the recipient is a function of the social relationship between the sender the recipient. We model this by placing a trust weight on the edge which defines the likelihood that a message will be believed as it is passed from one node to another.

1) Information propagation: If (S, V) is a source-value pair at node a which is propagated to node b then the source-value pair at node b is $(S, \alpha(a, b) * V)$, where $0 \leq \alpha(a, b) < 1$ is the propagation loss from a to b, quantified by the social relationship between nodes a and b.

Each node has an $Action\_set$ and an $Abort\_set$. The $Action\_set$ contains the source-value pairs (S_i, V_i)... for messages relating to message type $Action$ while the $Abort\_set$ stores the messages $(S_i, V_i)'$... relating to $Abort$. At the end of each time step, each node will merge all of the information they received and update their properties based on the fused information value. The process in which information is fused is described by the following steps.

2) Information fusion: The first step is to combine the information values of messages that originated from the same source. For each message type, when the same source appears in multiple messages, the combined information value for that source at the receiver node is at least the maximum of the information values for the source over all the messages and at most the sum of all the information values of the source.

The next step is to combine the fused information value at the node for each type of message, i.e. the Action messages in the $Action\_set$ are fused into one value, $Action\_fused$ and the Abort messages in the $Abort\_set$ are fused into one value, $Abort\_fused$.

For each type of message, we combine the information values from each source by taking a weighted convex combination of the sum and maximum of the values according to a parameter λ, where $\lambda \in [0, 1]$.

Suppose that node k has source-value pairs $(S_1^k, V_1^k), (S_2^k, V_2^k), \ldots$ for message type $Action$ and $(S_1^k, V_1^k)', (S_2^k, V_2^k)', \ldots$ for message type $Abort$ then the fused information value at node k is computed as follows:

$$Action\_fused_k = \lambda * \sum_i V_i^k + (1 - \lambda) * \max_i V_i^k \tag{1}$$

. Similarly,

$$Abort\_fused_k = \lambda' * \sum_i (V_i^k)' + (1 - \lambda') * \max_i (V_i^k)' \tag{2}$$

.

The last step is to merge the fused values of the Action messages with the fused values of the Abort messages to determine a total fused value. For any node k, we compute the information fused value $fused_k$ by taking the difference between its Action message fused value and its Abort fused value.

$$fused_k = Action\_fused_k - Abort\_fused_k, fused_k \in \mathbb{R} \tag{3}$$

3) Node states and behavior: After computing the fused information value, the node will determine its state and behavior based on whether the information value exceeds certain thresholds. Initially, all the nodes are Uninformed. When nodes become exposed to information, they can enter into one of three states: Disbelieved, Undecided, or Believed. Each node has two thresholds, a lower bound LB and an upper bound UB such that

$$0 \leq LB \leq UB \leq 1 \tag{4}$$

Depending on which threshold its fused information value exceeds, the node would undertake a state change:

- If $fused_k > UB$, then the node will enter Believed state.
- If $LB < fused_k < UB$, then node will enter Undecided state.
- If $fused_k < LB$, then node will enter Disbelieved state.

Each node state has a corresponding behavior as described in Table I. Since Abort information is also diffusive, it is possible for a Disbelieved node to take the action of propagating Abort information. We introduce a σ threshold, where $\sigma <= LB$, that determines whether the Disbelieved node will perform such an action. If $Action\_fused - Abort\_fused <= \sigma$, then the node will spread Abort information. Otherwise, the node will exhibit no action. If $\sigma = 0$, then the node would require that its Abort fused value to be at least as large as the Action fused value, in order to spread the Abort information. If $\sigma < 0$, then the node will need more Abort information than Action information before it is willing to propagate the information. If $0 < \sigma <= LB$, then the node is more eager to spread the Abort information.

In addition to spreading information, nodes may also seek information. A node in Undecided state will query its neighbors in the network for additional information. Since there

State	Description	Behavior
Uninformed	Node has not received any messages	No action
Disbelieved	Node has received an Action message but does not believe the message	No action
Disbelieved	Node has received an Abort message and possibly an Action message	If $fused_k < \sigma$ then spread Abort message to its neighbors, else no action
Undecided	Node has received an Action message, or received both Action and Abort messages, and is uncertain of what to do	Query neighbors in the network
Believed	Node has received an Action message, or received both Action and Abort messages, and believes the value of the Action message	Spread the Action message to its neighbors and is removed from the network after x time steps
Removed	Node is no longer in the network	No action

TABLE I
DESCRIPTION OF NODE STATES AND CORRESPONDING BEHAVIORS

are two types of messages, it is necessary to define what information is requested when a node queries their neighbors and what information their neighbors will share. When the Undecided node queries for information, they will request for any piece of information that is available from their neighbors, regardless of their own message sets. When the queried node receives a request for information, they will determine what messages to share based on their node state and send the message set with some probability p. If the queried node is

- Uninformed, then nothing is sent or received
- Disbelieved, then only $Abort\_set$ is sent
- Undecided, then both $Action\_set$ and $Abort\_set$ are sent
- Believed, then only the $Action\_set$
- Removed, then nothing is sent or received.

B. Preliminary experiments

The following experiments looks at the the effect of the following parameters on the effectiveness of the abort diffusion.

1) Seed selection for broadcasting Abort information, and
2) Distribution of trust values on the edges in the network.

In these set of experiments, there are two sources of Action information and two sources of Abort information. The following assumptions are made. The initial broadcast of Action messages reaches $s = 20,000$ seed nodes. The subsequent broadcast of Abort messages also reaches $s = 20,000$ seed nodes. The seeds are divided equally among the sources. The Action and Abort messages from the sources will reach all their recipients with probability = 1.0.The nodes in the network have the same trust in the sources for both Action information and Abort information and the information value of Action information is the same as Abort information, i.e. same importance. Unless otherwise specified, the node parameters are listed below.

- Information fusion parameters for $Action\_set$ and $Abort\_set$: $\lambda_1 = 0.0$ and $\lambda_2 = 0.5$
- Nodes threshold ($LB = 0.4$, $UB = 0.7$)
- Edge probability (p=0.75)
- Threshold for spreading Abort information: $sigma = 0.0$
- Time steps between entering $Believed$ state and $Removed$ state (5)
- Time steps for spreading Abort (10)

When a node enters Believed state, it will contact their neighboring nodes and try to spread the Action information for 5 time steps. If they remain in Believed state for the entire duration, they will then be removed from the network and enter Removed state. When the node is removed, all the incoming and outgoing edges from the node are removed as well. Note that it is possible for a Believed node to receive Abort information and change to an Undecided or Disbelieved state. If this occurs and the node enters Believed state at a future time step, the node will once again spread Action information for 5 time steps.

The experiments simulate the diffusion process of Action and Abort information on a random group model network with 100,000 nodes and density 0.00004. The random group model consists of two groups of equal sizes, where the edge probability between nodes from different groups is p_d and the edge probability between nodes from the same group is $p_s = 2 * p_d$.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

In analyzing the experimental results, we compare the following the following two cases. First, we simulate the spread of the Action messages and record the proportion of nodes that, enter Removed state, i.e. depart the network, for each network structure and model configurations. Next, we simulate the spread of Action messages followed by Abort messages and record the proportion of nodes that depart the network. We compare the two proportions to evaluate the effectiveness of the spread of Abort information.

A. Seed selection for broadcasting Abort information

One strategy is to perform a retraction where the Abort messages are delivered to the same set of nodes that initially received the Action messages. In this case, the Abort information tries to catch up to the Action information to stop the spread. Another strategy is to select a different set of nodes to propagate the Abort information, either randomly or targeted, e.g. highest degree nodes. In these experiments, the same number of nodes are selected for broadcasting Action messages as well as Abort messages.

Figure 1 shows the simulation results using various seeding strategies for Action and Abort information on the group

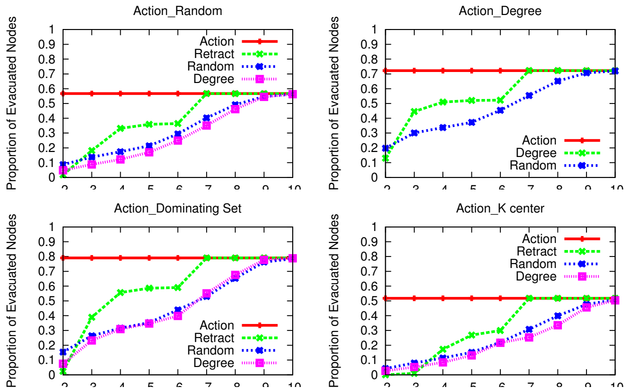

Fig. 1. Simulation results Group model network. Average trust of the network is 0.70. Trust in source is 0.80 and the information value of the messages is 0.95.

model network. The red line displays the proportion of evacuated nodes as the result of the diffusion of the Action information and serves as the benchmark for comparison for the presented seed selection strategies.

The results show that under these configurations, a retraction is only effective if the Abort messages are broadcast soon after the Action information. The trust in the information source is relatively high and the information value of Action messages is also high. Along with the predefined node thresholds, the fused value of the information at the seed node will easily exceed the upper bound threshold and the selected seeds nodes would enter Believed state upon receiving the Action message broadcast directly from the source and immediately propagate the Action information. The Abort message becomes ineffective if it is delivered at time step 7 or later. The more effective the Action diffusion is the more difficult it is to retract the spread. In most of the cases, broadcasting the Abort information after 2 time steps is most effective in minimizing the number of evacuated nodes when the messages are sent to the set of nodes with highest degrees. However, when the Action information spreads from highest degree nodes, sending Abort information is randomly selected nodes is more effective in immunizing the Action messages.

B. Distribution of trust and Effects of Groups

The following experiments looks at the effects of the distribution of trust and groups in the model for the various seeding strategies. The trust values between nodes are assigned depending on the sender and receiver's social group membership and the average trust of the network t_{avg} is kept constant. High trust is defined with the value $t_{high} = t_{avg} + \epsilon$ and low trust with value $t_{low} = t_{avg} - \epsilon$, where ϵ is the trust differential from the average trust t_{avg}. Here, ϵ is equal to 0.05. The following two scenarios are compared. In the first scenario, nodes have equal trust in each other. There are essentially no groups and no differences in trust between nodes, i.e. $\epsilon = 0$ and $t_{high} = t_{low} = t_{avg}$. In the second scenario, edges connecting nodes who belong to the same group have with a higher trust value of t_{high} and edges between nodes from different groups have a lower trust value of t_{low}.

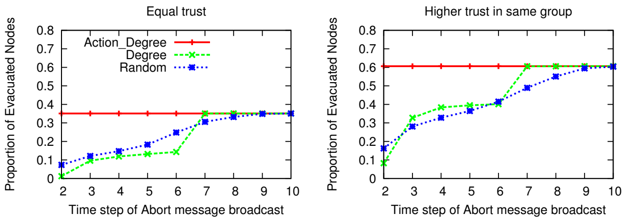

Fig. 2. Simulation results for the Group model network where the Action messages are broadcast to highest degree nodes. Average trust of the network was 0.70. Trust in source is 0.75 and the information values of the Action and Abort messages are 0.95

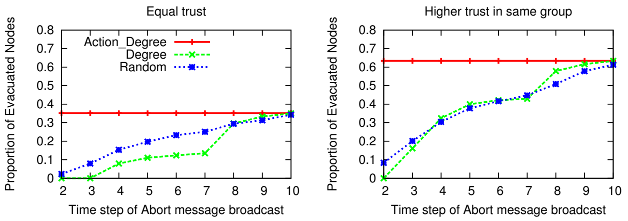

Fig. 3. Simulation results for the Group model network where the Action messages are broadcast to highest degree nodes. Average trust of the network was 0.75. Trust in source is 0.70 and the information values of the Action and Abort messages are 0.95.

We look at the effects of the distribution of trust and groups in the model for two contexts. In the first context, when the Action message is propagated from the information source, the fused value of the information just about exceeds the node's upper bound threshold. The seed nodes will enter Believed state upon receiving the Action information directly from the information source. In the second context, seed nodes will entered Undecided state upon receiving the Action information directly from the information sources. Simulation results for the two contexts are shown in Figures 2 and 3. The Action information is broadcast to the set of nodes with highest degrees. The green line displays the results of the retraction, where Abort messages are broadcast to the same highest degree nodes. The blue line displays the case where Abort messages are broadcast to a random set of nodes. An interesting observation is that in these settings, the retraction strategy for spreading Abort information is effective in the equal trust scenario but not as effective in the higher trust in same group scenario.

V. Conclusion and Future Work

The preliminary experiments presented some interesting observations. The Abort message should be sent out as soon as possible after the Action message in order for the Abort information to have any effect in the network. In addition, the Abort message must have characteristics so that it will diffuse more rapidly than the Action message, e.g. high information value. However, this implies that there is a tradeoff between a rapid spread of the Action message and the possible need to Abort because of new information. If the Action information spreads so effectively through the network and changes the structure of the network, i.e. large proportions of nodes are removed from the network, it would make an Abort situation very difficult and possibly ineffective.

The experiments also showed that for the case of spreading high valued information from high trusted sources, retraction is only effective if Abort messages are broadcast soon after the Action information. Afterwards, an alternative strategy is needed for sending Abort information. Under other circumstances, when the fused value of the information only slightly exceeds the node's threshold to act, retraction is still a possible strategy in a network with homogeneous trust. However, when we introduce trust differentials and groups, retraction is no longer a useful mechanism. This suggests that alternate strategies will have to be explored to incorporate trust variants and the distribution of trust in designing a useful mechanism for spreading Abort messages.

ACKNOWLEDGMENT

This material is based upon work sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-09-2-0053. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on.

REFERENCES

[1] R. Cohen, S. Havlin, and D. ben Avraham, "Efficient immuniation strategies for computer networks and populations," *Physical Review Letters*, vol. 91, no. 24, 2003.

[2] Z. Dezső and A.-L. Barabási, "Halting viruses in scale-free networks," *Phys. Rev. E*, vol. 65, no. 5, p. 055103, May 2002.

[3] R. Pastor-Satorras and A. Vespignani, "Immunization of complex networks," *Phys. Rev. E*, vol. 65, no. 3, p. 036104, Feb 2002.

[4] L. Chen and K. Carley, "The impact of countermeasure propagation on the prevalence of computer viruses," *IEEE Trans. on Systems, Man, and Cybernetics - Part B: Cybernetics*, vol. 34, no. 2, pp. 823–833, 2004.

[5] H.-H. Jo, H.-T. Moon, and S. K. Baek, "Immunization dynamics on a 2-layer network model," *Physica A: Statistical Mechanics and its Applications*, vol. 361, no. 2, pp. 534–542, March 2006.

[6] C. Budak, D. Agrawal, and A. E. Abbadi, "Limiting the spread of misinformation in social networks," Department of Computer. Science, UCSB, Tech. Rep., 2010.