

# Aborting a Message Flowing Through Social Communities

Cindy Hui, Malik Magdon-Ismail, William A. Wallace and Mark Goldberg  
Rensselaer Polytechnic Institute, Troy, New York.

Email: cindy.hui@alum.rpi.edu, magdon@cs.rpi.edu, wallaw@rpi.edu, goldberg@cs.rpi.edu

**Abstract**—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 necessary to stop the information from spreading and to prevent actors from taking the action. We investigate the concept 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 diffused and may spread through the network based on the recipient’s evaluation of the information. We present a framework for modeling the spread of actionable information and information retraction. Using the framework, we perform 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 that 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

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. Such a need may arise, for example, if an evacuation warning has been issued and it is later deemed that evacuation is not needed, or if malicious information is spreading and we wish to spread a counter rumor. We investigate the aborting of a message that is currently diffusing through a network, with the purpose of stopping the action that was prescribed by the previous message. These abort messages are introduced into the network and may spread through the network based on the recipient’s evaluation of the information.

The objective of this study is to develop a model in which an actionable message and its abort message both diffuse in the network. We motivate this concept using a Warning-Abort scenario in the context of evacuation. The actionable information in this case is the *Warning*, which advises individuals to take a certain action (eg. evacuate) as a protective measure against an incoming threat. The *Warnings* are broadcasted to the network and may diffuse as individuals decide to propagate the information. Suppose at a later time, new findings suggest that there is no longer a threat to the community. As a result there is a need to *Abort*, i.e. withdraw the previously issued warning by sending an abort message. In such a situation, we want to

investigate methods to effectively withdraw or minimize the effect of the warning messages. Successful retraction of the misinformed warning would minimize costs associated with unnecessary evacuations and false alarms.

Although we describe the abort concept using the context of warnings, our work is generally applicable to the spread of any actionable message and a need to negate the already spreading message. The framework has two basic components. The first component is a model of diffusion that describes how information flows through a network. This involves defining how nodes process the various types of information and how this process impacts the information flow. The second component considers how the original message (the warning) and the abort message are modeled to ultimately affect the actions of the node, in particular, how to merge the opposing pieces of information and how that impacts the node’s properties and decision making process. The particular details of the information spread and how individuals evaluate the information would depend on the specific characteristics of the information and the context of the diffusion.

We assume that the network structure changes as the result of the warning message spreading through the network. In other words, nodes may decide to leave the network, i.e. evacuate, as the result of believing the warning message. The abort information is introduced into the network after the warning message, and will propagate through the network that evolves from the warning message. Using the framework, we perform experiments to investigate strategies for broadcasting the abort message, in particular, how to identify a set of seed nodes that should receive the abort message and when to inject the abort information into the network. We also examine the effect of model parameters, such as network structure and trust distribution, on the effectiveness of the abort.

## II. RELATED WORK

In preventing disease spread, protecting computer networks from viruses, or controlling 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, or 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, a virus or disease is being spread in a network and the immunization strategy tries to minimize the

spread of the virus or disease by immunizing certain nodes in the network. Immunization strategies focus on selecting which nodes to immunize, 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], [4], [5], [6], [7]. Some research also considered the case where the immunization and the virus or disease spread through the network concurrently [8], [9].

Related research has looked at this problem as the spread of competing information in networks where there is a good campaign (immunization) and a bad campaign (virus) [10] or as the spread of multiple products or opinions in a competing environment [11]. Budak et al. [10] 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. Broecheler et al. [11] looked at modeling the spread of multiple competing phenomenon, e.g. in situations where individuals may only select one product out of a set of competing products. Their interest was in determining the eventual results from these competing diffusive processes, e.g. how many people in the network would adopt a certain product. While these works are related to ours, none of them effectively accounts for the social processes involved in the diffusion. Ours directly does.

### III. THEORETICAL FRAMEWORK

First, we present a theoretical framework for simulating the spread of actionable information and the abort message. The purpose of the abort message is to interfere with an ongoing diffusion and to stop the action that was prescribed earlier. We describe the model for simulating the spread of actionable information and the abort message. The message being diffused will be referred to as the *Warning* message. The action associated with the *Warning* 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 action associated with the *Abort* message is to not leave the network and spread the abort.

The diffusion model defines how information flows through the social network and how individual nodes process the information from incoming messages. Messages are introduced through external source nodes and may propagate when nodes interact. A node determines its behavior based on its state of belief in the *Warning* and *Abort* messages, which is measured by computing the fused value of all the information it has received.

We assume that the *Abort* message will spread on the network that is evolved from the spread of the *Warning* message, since each message type relates to either taking or not taking the same action. Note that when there is no *Abort* message, this is a general model for diffusion of actionable information and reduces to the model in [12].

#### A. Model for Diffusion and Abort

The social network is a directed graph  $G = (V, E, T)$  where  $V$  is a set of nodes,  $E$  is a set of edges, and  $T$  is a set of trust weights on the edges. Each trust weight  $t_{ij} \in T$  represents the likelihood that a message will be believed as it is passed from node  $i$  to node  $j$ .

There are two types of messages that diffuse in the network, *Warning* and *Abort*. Each message is characterized by its original source and a corresponding information value. Let  $w_i^\ell$  be the information value of warning source  $\ell$  at node  $i$ . Similarly, let  $a_i^m$  be the information value of abort source  $m$  at node  $i$ . Each node stores a *Warning* set, containing all the messages relating to message type *Warning*, and an *Abort* set with the messages relating to *Abort* messages. Let  $\{w_i^1, w_i^2, \dots\}$  be the set of *Warning* messages present at node  $i$  and  $\{a_i^1, a_i^2, \dots\}$  be the set of *Abort* messages at node  $i$ . The sources of warnings and aborts are treated as nodes in the network with links to nodes and trust values.

At the end of each time step, every node  $i$  will merge all of the information it received and update its properties based on the fused information value  $F_i$ . The process by which a node's information is fused to obtain  $F_i$  is described next. There are three basic steps: 1) Information propagation; 2) Information fusion; 3) Action.

1) *Information propagation*: If  $w_i^\ell$  is the value of information for source  $\ell$  at node  $i$  and node  $i$  propagates this information to node  $j$ , then the value of information for source  $\ell$  propagated to node  $j$  is  $w_i^\ell t_{ij}$ , where  $0 \leq t_{ij} \leq 1$ . Thus, there is the propagation loss from  $i$  to  $j$ , quantified by the trust between nodes  $i$  and  $j$ . Note that trust may be asymmetric, so in general,  $t_{ij} \neq t_{ji}$ .

2) *Information fusion*: There are three steps for determining the fused information value  $F_i$  for any node  $i$ . The first step is to combine the information values of messages that originate from the same source. The node then combines all values in its warning set to obtain  $W_i$ , a value for warning; similarly, the node obtains  $A_i$ , a value for abort, from the abort set. Lastly, the node computes the fused information value  $F_i$  as a function of  $W_i$  and  $A_i$ .

A node receives messages from its neighbors. Suppose that  $i$  has received information from some subset of its neighbors  $\mathcal{N}_i$ . Then  $i$  first combines all messages relating to the same information source. For example, considering the warning message from source  $\ell$ ,

$$w_i^\ell = f_1(\{w_j^\ell t_{ji}\}_{j \in \mathcal{N}_i}),$$

where  $f_1$  satisfies  $\max_{j \in \mathcal{N}_i} w_j^\ell t_{ji} \leq w_i^\ell \leq \sum_{j \in \mathcal{N}_i} w_j^\ell t_{ji}$ .

After computing  $w_i^\ell$  and  $a_i^m$  at node  $i$  (the warning and abort values for each source), the next step is to combine  $w_i^\ell$  into a single warning value  $W_i$  and similarly to combine  $a_i^m$  into a single abort value  $A_i$ .

$$W_k = \lambda_w \sum_m w_k^m + (1 - \lambda_w) \max_m w_k^m; \quad (1)$$

$$A_k = \lambda_a \sum_n (a_k^n) + (1 - \lambda_a) \max_n (a_k^n). \quad (2)$$

These summary information values are a combination of the information values of each source; the actual value is between the maximum and the sum, determined by the parameters  $\lambda_w, \lambda_a \in [0, 1]$ . The range for  $\lambda$  means that more information cannot hurt and the combined information value will be at least the maximum of the information values and at most the sum. The appropriate value of  $\lambda$  to use would depend on the nature of the diffusion. For example, to model fast spreading gossip, we may choose  $\lambda$  closer to 1. Note that the value of  $\lambda$  can be different for *Warning* information and *Abort* information.

The last step is to merge  $W_i$  and  $A_i$  into a single information value  $F_i$ . The values of the *Warning* messages increase the node's likeliness to transition from the Uninformed state to Believed state. On the other hand, the values of the *Abort* message would have the opposite effect. In general, the relationship between the two types of messages can be modeled in various ways by modifying how the information is merged. Our choice is perhaps the simplest:

$$F_i = W_i - A_i. \quad (3)$$

Note that, if node  $i$  only received *Warning* messages but no *Abort* messages, then  $F_i = W_i$ . Similarly, if node  $i$  only received *Abort* messages but no *Warning* messages, then  $F_i = -A_i$ .

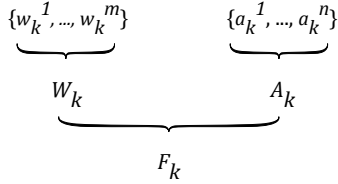


Fig. 1. Information fusion process at node  $k$

3) *Action*: As information spreads and nodes receive messages, each node computes a combined information value, which depends on their perception of the information value of each piece of information and their trust in the information sources and propagators. Given node  $i$ 's information value  $F_i$ , the node may change its state and act. Each node has two defined threshold levels, a lower bound which lies between the Disbelieved and Uninformed states, and an upper bound, which lies between the Undecided and Believed states. The thresholds determine the boundaries for when the node will acknowledge the message and/or take an action. If the nodes combined information value exceeds one of the thresholds, the node will enter a new state.

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  $L_i$  and an upper bound  $U_i$  such that

$$0 \leq L_i \leq U_i \leq 1. \quad (4)$$

In our experiments we used uniform thresholds, so  $U_i = U$  and  $L_i = L$ . Depending on which threshold its fused information value exceeds, the node changes state as follows:

- If  $F_i > U$ , then the node will enter Believed state for the *Warning* message.
- If  $L < F_i \leq U$ , then node will enter Undecided state for the *Warning* message.
- If  $F_i \leq L$ , then node will enter Disbelieved state for the *Warning* message.

Each node state has a corresponding behavior as described in Table I. A Believed node believes the value of the *Warning* information and will attempt to propagate the actionable information to its neighbors for a predetermined number of time steps. Since abort information is also diffusive, it is possible for a Disbelieved node to take the action of propagating *Abort* information. We introduce a  $\sigma$  threshold, where  $\sigma \leq L$ , that determines whether the Disbelieved node will perform such an action. If  $F_i \leq \sigma$ , 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 *Warning* fused value, in order to spread the *Abort* information. If  $\sigma < 0$ , then the node will need more *Abort* information than *Warning* information before it is willing to propagate the *abort* information. If  $0 < \sigma \leq L$ , then the node is more eager to spread the *Abort* information.

In spreading information, the edge probability  $p$  determines the probability that a message is propagated when a node attempts to send a message to another node. Note that the edge probability only determines whether the message is passed or not, and does not affect the information value of the message being passed. The trust weight  $t_{ij}$ , on the other hand, influences the information value of the message being propagated.

In addition to spreading information, nodes may also seek information. A node in the Undecided state will query its neighbors in the network for additional information. Since there are two types of messages (*warning* and *abort*), 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 edge probability  $p$ . If the queried node is

- Uninformed, then nothing is sent or received
- Disbelieved, then only the *Abort* message set is sent
- Undecided, then both *Warning* and *Abort* message sets are sent
- Believed, then only the *Warning* message set
- Removed, then nothing is sent or received.

In summary, the information value of messages may change as it is propagated from one node to another. When the message is passed from a sender to a recipient, the information

State	Description	Behavior
Uninformed	Node has not received any messages	No action
Disbelieved	Node has received a <i>Warning</i> message but does not believe the message	No action
Disbelieved	Node has received an <i>Abort</i> message and possibly a <i>Warning</i> message	If $F_k \leq \sigma$ then spread <i>Abort</i> message to its neighbors, else no action
Undecided	Node has received a <i>Warning</i> message, or received both <i>Warning</i> and <i>Abort</i> messages, and is uncertain of what to do	Query neighbors in the network
Believed	Node has received an <i>Warning</i> message, or received both <i>Warning</i> and <i>Abort</i> messages, and believes the value of the <i>Warning</i> message	Spread the <i>Warning</i> message to its neighbors and leave 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

value of the message at the recipient is a function of the trust between the sender and the recipient as denoted by the weight on the edge. At the end of each time step, each node will merge all of the information it received, as illustrated in Fig. 1. For each type of message (warning and abort), the values of the messages are fused into a single value by taking a weighted convex combination of the sum and maximum of the values over all sources. Next, the total fused information value  $F_i$  is computed by taking the difference of the combined value of the *Warning* messages and the combined value of the *Abort* messages. Each node will then update its properties and determine its state for the next time step by comparing  $F_i$  with its threshold levels.

#### IV. EXPERIMENTAL DESIGN

The assumption is that the *Abort* message will be broadcasted at a later time step after the faulty *Warning* message. The nodes that receive the *Warning* message and enter the *Believed* state will take the action, i.e. evacuate, within a specified time period; but, it is possible for them to receive an *Abort* message before leaving the network and alter their action in response to the abort. On the other hand, it is also possible that *Believed* nodes will have already left the network, i.e. entered the *Removed* state, in which case the *Abort* message would have no effect on those nodes.

In our experiments, we study the effect of the following parameters on the effectiveness of the abort:

- 1) Seed selection for broadcasting *Abort* information;
- 2) Time between the broadcasts of *Warning* messages and *Abort* messages;
- 3) Community structure and the distribution of trust values on the edges in the network.

##### A. Model parameters

Each simulation starts with the initial broadcast of  $S$  *Warning* messages from  $L$  sources. These messages will reach a certain proportion of the nodes in the network, advising these nodes to evacuate. These selected seeds will then attempt to propagate the *Warning* message to the rest of the population. At a later time step, a second set of  $S$  messages will be introduced into the network, but with *Abort* information, i.e. do not evacuate.

We simulate the diffusion process of *Warning* and *Abort* information on a scale-free network and a random group model network, in all cases with 100,000 nodes and average node-degree 4. The scale-free network was formed using the Barabasi-Albert model for generating random scale-free networks using preferential attachment and has a power law degree distribution of the form  $P(k) \sim k^{-3}$ . 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  $p_s = 2 * p_d$ .

In these experiments, there are two sources of *Warning* information and two sources of *Abort* information. The following assumptions are made. The information sources are external to the network. The initial broadcast of *Warning* messages reaches a selected  $S = 20,000$  seed nodes. The subsequent broadcast of *Abort* messages also reaches another  $S = 20,000$  seed nodes. The seeds are divided equally among the sources, i.e. each source connects to 10,000 nodes. The *Warning* and *Abort* messages from the sources will reach all their recipients with probability  $p = 1$ . The nodes in the network have the same trust in the sources,  $t_s$ , for both *Warning* information and *Abort* information and the information value of *Warning* information is the same as *Abort* information, i.e. same importance. We consider two trust values  $t_s = 0.70$  and  $t_s = 0.75$ . Unless otherwise specified, the node parameters are listed below.

- When the same source  $\ell$  appears in multiple incoming messages with values  $w_1^\ell, w_2^\ell, \dots$ , then the information from source  $\ell$  at node  $i$  is the max,  $w_i^\ell = \max w_j^\ell t_{ji}$ .
- Information fusion parameters for *Warning* and *Abort* information:  $\lambda_w, \lambda_a = 0.5$
- Edge probability ( $p = 0.75$ )
- Threshold for spreading *Abort* information:  $\sigma = 0.0$
- Time steps between entering *Believed* state and *Removed* state: 5.

When a node enters the *Believed* state, it will contact its neighboring nodes and try to spread the *Warning* information for 5 time steps. If the node remains in the *Believed* state for the entire duration, it will then be removed from the network and enter the *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 the Believed state at a future time step, the node will once again spread Warning information for 5 time steps.

We consider two settings of node thresholds, a lower pair ( $L = 0.3, U = 0.6$ ) and a higher pair ( $L = 0.4, U = 0.7$ ). The node thresholds can be defined in the context of the type of information being diffused and whether the information has high or low utility. A low pair of thresholds would fit the context of contagious information that has low consequences and is likely to be easy propagated between nodes. This would imply that less information is needed for the node to transition to the *Undecided* or the *Believed* state. On the other hand, a relatively higher pair of thresholds would infer that the utility of the information is high and that more information is needed before that node will believe the information and take action.

### B. Community structure and the distribution of trust

Each trust weight  $t_{ij}$  represents the likelihood that a message will be believed as it is passed from node  $i$  to node  $j$ . We observe the effect of community structure by defining on how the trust weights on the edge are distributed through the network. Each edge between pairs of nodes can have a high or low trust value representing their social relationship. We define high trust with the value  $t_h = t_{\bar{n}} + \epsilon$  and low trust with value  $t_l = t_{\bar{n}} - \epsilon$ , where  $\epsilon$  is the trust differential from the average trust  $t_{\bar{n}}$ . Here,  $\epsilon$  is equal to 0.05. The trust values between nodes are assigned depending on the sender and receiver's social group membership and the average trust of the network  $t_{\bar{n}}$  is kept constant. The population of nodes is divided into two groups  $A$  and  $B$ , each with 50,000 nodes. In the scale-free network, each node is randomly assigned to either group  $A$  or group  $B$ . For the group model network, nodes are assigned to groups such that nodes within the same group will have a higher probability of clustering together.

We look at two scenarios. In the first scenario, nodes have equal trust in each other. There is essentially no difference in trust between nodes, i.e.  $\epsilon = 0.0$  and  $t_h = t_l = t_{\bar{n}}$ . In the second scenario, edges connecting nodes who belong to the same group have a higher trust value of  $t_h$  and edges between nodes from different groups have a lower trust value of  $t_l$ . We can then look at how the distribution of trust affect the various seeding strategies for Warning information as well as Abort.

### C. Seed selection strategies

Given a strategy for broadcasting *Warning* information, the purpose is to examine the methods for broadcasting the *Abort* information. For the context of warnings, let's assume that the best strategy for spreading Warning information will be used. Once that strategy is determined, we can observe the effectiveness of *Abort* and determine under what circumstances it would be possible to minimize the number of nodes who take action, i.e. evacuate.

1) *Random Set*: The *Warning* information can be broadcasted to a set of random seeds where the selection is based on no prior knowledge of network characteristics.

Alternatively, the information can be targeted using some knowledge of the network structure. Given a budget of  $s$  nodes as seeds, selecting the  $s$  nodes using targeted strategy may be more efficient in spreading the *Warning* information than a random set of  $s$  nodes. We investigate several targeted strategies for selecting seed nodes to broadcast the *Warning* information.

2) *Degree Set*: We can select the set of nodes with high degrees, since nodes with more neighbors may have higher probability of spreading the information. This strategy can be viewed as targeting information hubs or popular nodes of the network as defined by their degree centrality.

3) *Independent Set*: We select an independent set of seed nodes such that no two nodes in the set are connected by an edge. This strategy attempts to promote information spread by having seed nodes more dispersed throughout the network.

4) *Modified Independent Set*: This strategy is an extension to the Independent Set strategy but takes into consideration the existence of multiple sources. In the modified set, it is possible for two seed nodes to be connected to each other as long as they are connected to different sources.

5) *Dominating Set*: This strategy takes the approach of finding a dominating set of the network. A 1-dominating set for a graph  $G = (V, E)$  is a subset  $D$  of  $V$  such that every node not in  $D$  has at least one neighbor in  $D$ . The procedure for selecting seed nodes starts with finding a dominating set of a graph  $G$  but suspends once the seed limit of  $s$  is reached.

6) *K-center Set*: This strategy takes the approach of finding a set of  $K$ -center nodes, where  $K$  is the number of seeds to select. The goal is to select a set of  $K$  nodes such that for any other node  $\notin K$ , the nearest seed node is as close as possible. The  $K$ -center selection strategy tries to pick seed nodes across the network so that information from the sources can reach across different parts of the network.

Tables II and III show the proportion of Removed nodes for various model configurations, assuming only that Warning messages were diffused. The best seeding strategies for spreading Warning information are presented in bold for each configuration. For the scale-free network, the most effective strategy for spreading the Warning information is by choosing the set of nodes with the highest degree. This strategy produces large proportion of Removed nodes due to the existence of high degree hubs in the scale-free network. For the group model network, choosing the set of nodes with the highest degree does not necessarily result in a large proportion of Removed nodes.

$K$ -center selection appears to be effective only when the thresholds are lowered and information is likely to propagate due to high trust in the network. However, when the thresholds are higher,  $K$ -center selection performs worse than random. This is because the Undecided nodes are unable to query for sufficient amount of information to exhibit a state change when seed nodes are too dispersed through the network. The

Node Thresholds	Scenarios	Trust Values		Seeding strategy for Warning information					
		$t_s$	$t_{\bar{n}}$	Random	Degree	Independent	Modified	Dominating	$K$ -center
$L = 0.3, U = 0.6$	Equal Trust	0.75	0.75	0.9762	<b>0.9999</b>	<b>1.0000</b>	<b>0.9997</b>	<b>1.0000</b>	<b>0.9999</b>
		0.70	0.75	0.8791	<b>0.9875</b>	<b>0.9849</b>	<b>0.9903</b>	<b>0.9826</b>	0.9030
$L = 0.3, U = 0.6$	Higher Trust in Same Group	0.75	0.75	0.9771	<b>0.9993</b>	<b>0.9994</b>	<b>0.9992</b>	<b>0.9992</b>	<b>0.9910</b>
		0.70	0.75	0.9514	<b>0.9976</b>	<b>0.9963</b>	<b>0.9974</b>	<b>0.9973</b>	0.9774
$L = 0.4, U = 0.7$	Equal Trust	0.75	0.75	0.5514	<b>0.9306</b>	0.7219	0.8889	0.8994	0.5562
		0.70	0.75	0.2764	<b>0.4449</b>	0.0000	0.4203	0.3440	0.0000
$L = 0.4, U = 0.7$	Higher Trust in Same Group	0.75	0.75	0.4939	<b>0.7861</b>	0.7032	0.7454	0.7286	0.5186
		0.70	0.75	0.4248	<b>0.6919</b>	0.0000	0.6465	0.6282	0.0000

TABLE II

SCALE-FREE NETWORK. PROPORTION OF REMOVED NODES AS WE VARY TRUST IN SOURCES,  $t_s$ , AND NODE TRUST,  $t_{\bar{n}}$ . THERE ARE TWO INFORMATION SOURCES AND THE INFORMATION VALUE OF EACH ORIGINAL MESSAGE IS 0.95. THE BEST SEEDING STRATEGIES ARE PRESENTED IN BOLD. FOR SOME CONFIGURATIONS, MULTIPLE SEEDING STRATEGIES PRODUCE COMPARABLE RESULTS.

Node Thresholds	Scenarios	Trust Values		Seeding strategy for Warning information					
		$t_s$	$t_{\bar{n}}$	Random	Degree	Independent	Modified	Dominating	$K$ -center
$L = 0.3, U = 0.6$	Equal Trust	0.75	0.75	0.9402	0.9561	0.9709	0.9601	0.9678	<b>0.9809</b>
		0.70	0.75	0.8155	0.8725	<b>0.9163</b>	0.8947	<b>0.9105</b>	0.8373
$L = 0.3, U = 0.6$	Higher Trust in Same Group	0.75	0.75	0.9554	0.9607	<b>0.9703</b>	0.9638	<b>0.9694</b>	<b>0.9760</b>
		0.70	0.75	0.9243	0.9455	<b>0.9597</b>	0.9522	<b>0.9624</b>	<b>0.9644</b>
$L = 0.4, U = 0.7$	Equal Trust	0.75	0.75	0.5670	0.7225	0.7157	0.7594	<b>0.7906</b>	0.5175
		0.70	0.75	0.2766	0.3513	0.0000	<b>0.3914</b>	0.2859	0.0000
$L = 0.4, U = 0.7$	Higher Trust in Same Group	0.75	0.75	0.5780	0.6903	<b>0.7714</b>	0.7132	0.7537	0.5686
		0.70	0.75	0.5067	0.6341	0.0000	<b>0.6562</b>	<b>0.6556</b>	0.0000

TABLE III

GROUP MODEL NETWORK. PROPORTION OF REMOVED NODES AS WE VARY TRUST IN SOURCES,  $t_s$ , AND NODE TRUST,  $t_{\bar{n}}$ . THERE ARE TWO INFORMATION SOURCES AND THE INFORMATION VALUE OF EACH ORIGINAL MESSAGE IS 0.95. THE BEST SEEDING STRATEGIES ARE PRESENTED IN BOLD. FOR SOME CONFIGURATIONS, MULTIPLE SEEDING STRATEGIES PRODUCE COMPARABLE RESULTS.

Dominating set of nodes is most effective when the node thresholds are lowered.

When the node thresholds are high, the independent set and modified independent set strategies are more useful for spreading the Warning information. The independent set of nodes is effective when the trust in the source is higher (0.75), but when the trust in source is lowered (0.70), the independent set is not useful. Although the seed nodes receive the messages directly from the source, because of their trust in the source and their thresholds, they will enter *Undecided* state. When the *Undecided* nodes try to query their neighbors, they are unable to receive any additional information since all their neighbors are be *Uninformed* by definition of the heuristic. In those cases, the modified independent set is preferred.

Depending on the structure of the network, e.g. scale-free or group model, the node characteristics, e.g. threshold levels, and the distribution of trust, we can decide on an effective strategy for spreading Warning information. Once that strategy is determined, we can observe the spreading of Abort and determine under what circumstances it would be possible to minimize the number of nodes who take action, i.e. evacuate.

## V. EXPERIMENTAL RESULTS AND DISCUSSION

In analyzing the experimental results, we compare the following two cases. First, we record the proportion of nodes that, enter the Removed state, i.e. depart the network, for each network structure and model configurations when only Warning messages are present in the network. We consider the situations where the Warning diffusion produces the largest

diffusion using the seeding strategies described. Next, we simulate the spread of Warning 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.

The Abort information is introduced into the network at a later time step in an attempt to immunize or eliminate the Warning information. One strategy is to perform a retraction where the Abort messages are delivered to the same set of nodes that initially received the Warning messages. In this case, the Abort information tries to catch up to the Warning 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 Warning messages as well as Abort messages.

Fig. 2 and Fig. 3 shows selected simulation results using various seeding strategies for Warning and Abort information on the scale-free network and group model network, respectively. The x-axis shows the time step at which the Abort message is broadcast. Recall that the Warning information is broadcast at time step 1. The red line displays the proportion of evacuated nodes as a result of the diffusion of the Warning information and serves as the benchmark for comparison to the different seed selection strategies. The green line displays the results of the retraction, where Abort messages are broadcast to the same nodes as the Warning. The blue line displays the case where Abort messages are broadcast to a random set of nodes. The pink line displays the case where the Abort messages are

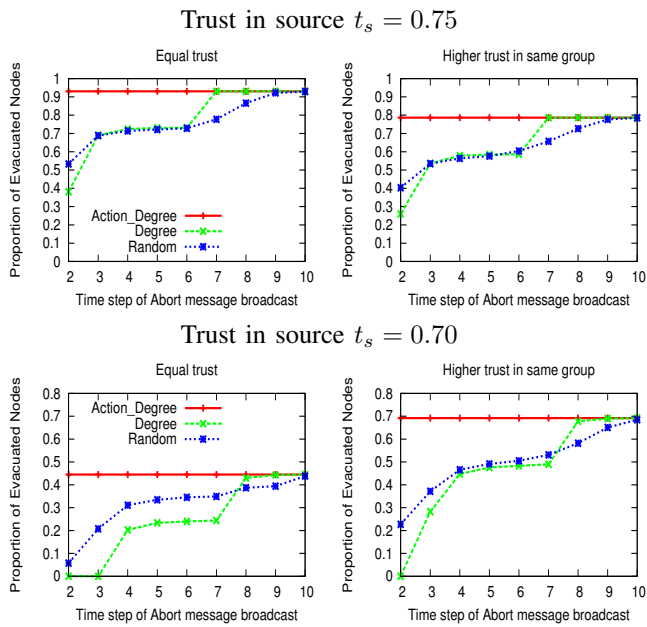


Fig. 2. Simulation results for the Scale-free network where the Action messages are broadcast by highest degree nodes. Average trust of the network was 0.75. Information values of the Action and Abort messages are 0.95. Node thresholds are  $L = 0.4$ ,  $U = 0.7$ .

delivered to the highest degree nodes.

The results show that a retraction is only effective if the Abort messages are broadcast soon after the Warning information, when the information value of the messages are high and the trust in the information source is also high (0.75). 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 the Believed state upon receiving the Warning message broadcast directly from the source and immediately propagate the Warning information. This results in the Warning messages spreading very quickly through the network. We can observe that the more effective the Warning diffusion is the more difficult it is to retract or minimize the spread. In most of the cases, broadcasting the Abort information after soon after the Warning messages (time steps  $\leq 3$ ) is most effective in minimizing the number of evacuated nodes. The Abort message becomes less effective if it is delivered after nodes have already started to leave the network. Retraction becomes ineffective if Abort messages are broadcast after the seed nodes have already taken action, i.e. time steps  $\geq 7$ . In other words, the seed nodes receive the Warning at time step 1, enter Believed state at time step 2, propagate the Warning for 5 time steps, and are removed by time step 7.

The results also show that when the Warning diffusion performs very well, broadcasting Abort messages randomly in the network is not preferred and that the Abort messages should be targeted as well in order to counter the Warning. Under certain scenarios, e.g. when dominating set seeding strategy is used for broadcasting Warnings in the group mode network and  $t_s = 0.70$ , the retraction strategy for spreading

Abort information works in the equal trust scenario. However, retraction is no longer effective when there is higher trust within the group. This suggests that seeding strategies will need to incorporate the distribution of trust in order to have a useful mechanism for spreading Abort messages in a inhomogeneous trust network.

## VI. CONCLUSION AND FUTURE WORK

We presented a diffusion model where Abort messages were introduced into a network to negate an ongoing diffusion process and stop the action that was prescribed by the original Warning messages. The Abort messages are diffusive and propagate over the network that evolved from the spread of the Warning messages. We performed empirical experiments to investigate strategies for broadcasting the counter message. In particular, we studied how to select a set of individuals, i.e. seed nodes, that should receive the counter message directly from the information source.

The experiments presented some interesting observations. Since the Abort information is introduced into the network after the Warning information, the Abort message should be sent out as soon as possible after the Warning 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 Warning message. The information value of the Abort messages should be high and the sources from which they originate from should be trusted. However, this implies that there is a tradeoff between a rapid spread of the Warning message and the possible need to Abort because of new information. If the Warning 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 by sending Abort information to the same seeds as the Warning information, is only effective if Abort messages are broadcast soon after the Warning 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 the distribution of trust in designing a useful mechanism for spreading Abort messages. It would be interesting to investigate dynamic strategies for spreading information, i.e. selecting seed nodes over time while considering the network dynamics and changes due to the ongoing information flow. In addition, it would also be interesting to explore the effects as we increase the number of groups and vary the group sizes.

One limitation of the proposed framework is that it does not take into account the order in which types of messages arrive at the node. In the current framework, receiving an Warning

Trust in source  $t_s = 0.75$

Trust in source  $t_s = 0.70$

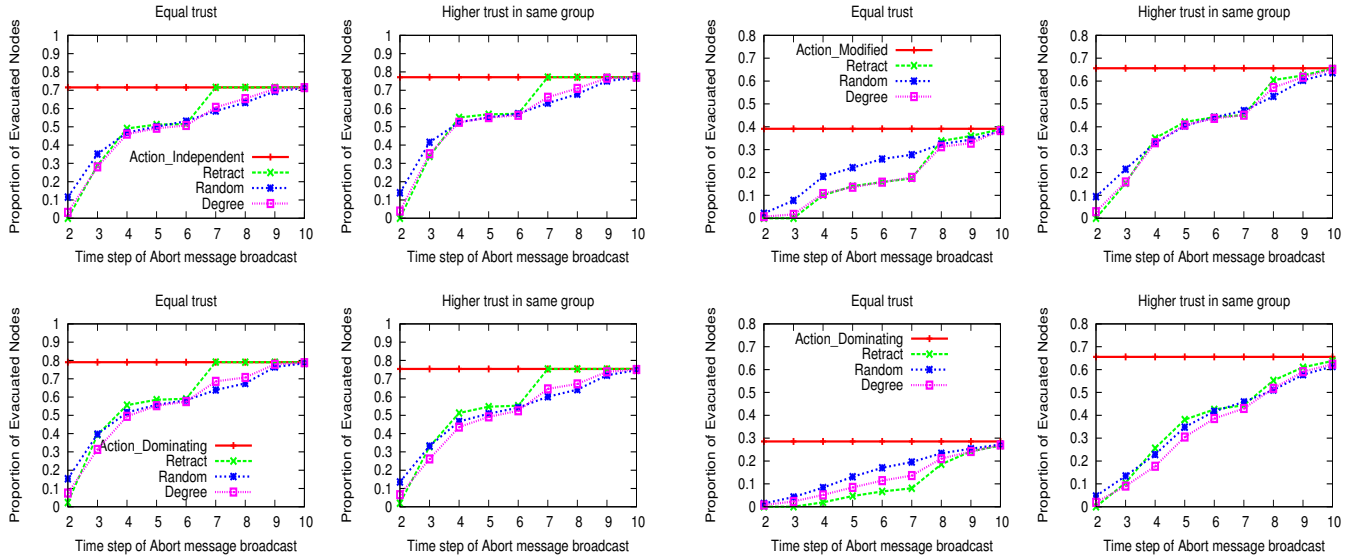


Fig. 3. Simulation results for the Group model network where the Action messages are broadcast by independent set of nodes, modified independent set, and dominating set. Average trust of the network was 0.75. Information values of the Action and Abort messages are 0.95. Node thresholds are  $L = 0.4$ ,  $U = 0.7$ .

message followed by an Abort message is treated the same as an Abort message followed by an Warning message. The current model only takes into consideration the information value associated with the message and not the order in which they are received or the time between messages. The order in which messages arrive at the node may affect the nodes decision-making process. There is a trade off between a fast effective spread of Warning information and the ability to effectively utilize an abort. The presented framework can be used to investigate such trade offs in various scenarios. First, a series of strategies for spreading Warning information can be identified for a given constraint, e.g. the minimum proportion of the network that must take action. The next step would be to analyze various strategies for spreading Abort information, such as, how to seed the Abort information, assuming that the action strategy is fixed.

#### ACKNOWLEDGMENT

This material is based upon work sponsored by the Army Research Laboratory under Cooperative Agreement Number W911NF-09-2-0053 and by the Department of Homeland Security through the Command, Control, and Interoperability Center for Advanced Data Analysis Center of Excellence. 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.

#### REFERENCES

- [1] R. Cohen, S. Havlin, and D. ben Avraham, "Efficient immunization 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] D. H. Zanette and M. Kuperman, "Effects of immunization in small-world epidemics," *Physica A: Statistical Mechanics and its Applications*, vol. 309, no. 3-4, pp. 445–452, 2002.
- [5] E. Terzi, P. Tsaparas, G. Giakkoupis, and A. Gionis., "Models and algorithms for network immunization," Department of Computer Science, University of Helsinki, Tech. Rep. Technical Report C-2005-75, 2005.
- [6] L. K. Gallos, F. Liljeros, P. Argyrakis, A. Bunde, , and S. Havlin, "Improving immunization strategies," *Physical Review E*, vol. 75, 2007.
- [7] G. Hartvigsen, J. Dresch, A. Zielinski, A. Macula, and C. Leary, "Network structure, and vaccination strategy and effort interact to affect the dynamics of influenza epidemics," *Journal of Theoretical Biology*, vol. 246, no. 2, pp. 205 – 213, 2007.
- [8] 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.
- [9] 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.
- [10] C. Budak, D. Agrawal, and A. E. Abbadi, "Limiting the spread of misinformation in social networks," Department of Computer. Science, UCSB, Tech. Rep., 2010.
- [11] M. Broecheler, P. Shakarian, and V. Subrahmanian, "A scalable framework for modeling competitive a scalable framework for modeling competitive diffusion in social networks," in *IEEE International Conference on Social Computing*, 2010, pp. 295–302.
- [12] C. Hui, M. Goldberg, M. Magdon-Ismael, and W. A. Wallace, "Simulating the diffusion of information: An agent-based modeling approach," *Special Issue on Agent-Directed Simulation, International Journal of Agent Technologies and Systems*, vol. 2, no. 3, pp. 31–46, 2010.