

Agent-based Simulation of the Diffusion of Warnings

Cindy Hui¹, Mark Goldberg², Malik Magdon-Ismael², William A. Wallace¹

¹Dept of Decision Sciences and Engineering Systems, ²Dept of Computer Science
Rensselaer Polytechnic Institute

huic@rpi.edu, wallaw@rpi.edu, goldberg@cs.rpi.edu, magdon@cs.rpi.edu

Keywords: Diffusion, Dynamic Networks

Abstract

Diffusion occurs in various contexts and generally involves a network of entities and interactions between entities. Through these interactions, some property, e.g. information, ideas, etc., is spread through the network. The network may become dynamic as entities in the network interact and information, ideas, etc. flow through the network. This paper presents a general model of diffusion in dynamic networks. We use the model to examine how network structure, seeding strategy, and population inhomogeneity as defined with trust, affects the diffusion process. We simulate an evacuation scenario where the network structure represents a network of households. There are multiple sources that initiate the broadcasts of evacuation warnings and the goals are for the households to propagate the message and perform evacuation. The network dynamics observed are the result of the diffusion, where households may leave the network some time after receiving the warning. The results provide interesting observations on the effects of trust asymmetry and trust differentials. When we introduce population inhomogeneity using trust, the diffusion was more effective. The network structure and the seeding strategy used in delivering the initial broadcast also affect the effectiveness of the diffusion.

1. INTRODUCTION

Diffusion occurs in various contexts and generally involves a network of entities and interactions between entities. These networks can consist of entities like individuals or organizations. The interactions could be physical contact, collaboration, innovation adoption, or some form of verbal or written communication depending on the circumstances. Through these interactions, some property, e.g. information, idea, innovation, disease, etc., is spread through the network. The flow of these information, ideas, etc. may in turn have an effect on the entities in the network as well as the network itself. For example, through the diffusion of a product review, individuals may become curious and browse for additional reviews on the product, or they might become convinced and adopt/purchase the product. In addition, individuals may join/form user groups to discuss the product and through these groups, form new relationships and change their social networks.

In this paper*, we present a general model of diffusion in dynamic networks, where the network may change as a result of the diffusion that occurs. We apply our model to the context of evacuation warnings. The network in this case is a social network of households nodes and the property being diffused is an evacuation warning. As warning messages propagate through the network, households may seek additional information, spread the information, or take action, i.e. perform evacuation. This context demonstrates one form of network dynamics where nodes may leave the network and remove their edges. Observing this form of dynamics may reveal disruptions in the spread of information, and identify areas in the network that assist in the spread of the warning as well as identify areas that fail to evacuate. We use the model to explore how the network structure, population inhomogeneity, and the seeding strategies affects the diffusion process. We introduce population inhomogeneity by assigning household nodes to social groups and quantifying the relations between household nodes using trust. The population inhomogeneity is the product of varying trust levels between specified groups.

2. BACKGROUND AND RELATED WORK

Social networks play a significant role in the spread of information, ideas, emotions, diseases, innovations, etc. As a result, the flow of this information, these ideas, etc. affect the way people think, act, and bind together in a society. Modeling information flow through various social networks is an active research area, with work on diffusion of innovation and technology [5, 8, 17, 34, 37, 40], viral marketing [25, 26], the spread of computer viruses [3, 10], and the spread of diseases [27, 29].

2.1. Epidemiology models

The spread of infectious diseases and the spread of infectious ideas have common characteristics in terms of their diffusion process. For this reason, many diffusion models for studying the spread of ideas were developed based on models from epidemiology [7]. Many of the epidemiology models are derived from the Susceptible/Infected/Removed (SIR) model,

*This paper expands on the work from "Micro-Simulation of Diffusion of Warnings" in proceedings of ISCRAM 2008 and "The Impact of Changes in Network Structure on the Diffusion of Warnings" presented at the Workshop on Analysis of Dynamic Networks at SDM 2009.

which was formulated by Lowell Reed and Wade Hampton Frost in the 1920s [32]. The SIR model divides the population into three possible categories (susceptible, infected, and removed) that reflect the status of the individuals. Susceptible are individuals who are not infected but may become infected when they gain contact with an infected individual. Infected are individuals who are carrying the disease and have the potential to spread it. Removed are individuals who have either recovered from the disease or died, and cannot spread the disease. The model assigns a disease transmission probability based on a given average rate of contact, and assumes that all individuals are equally likely to become infected. Mathematical models can then be used to infer population average parameters such as contact rates and duration of infectious periods.

Many variations of the SIR model have been proposed to incorporate more realistic factors, for example implementing a social structure for contact based spread, [4, 13, 23, 28, 33], or varying disease transmission probability [32]. In general, these models depict the disease spreading process by tracking the average number of infected individuals and identifying individuals who are prone to become infected with the disease. These models can also identify the specific characteristics, at the population level, that play a significant role in the transmission process. Such characteristics include age, variable infection rates and variable infection periods. These characteristics introduce a heterogeneous population, which also leads to more complex models.

2.2. Diffusion of innovation models

Diffusion models are used to study the adoption of products and spread of innovation influence by viewing them as a process of social interactions. The diffusion of innovation theory, introduced by Everett Rogers in 1962, defines stages of product adoption process (knowledge, persuasion, decision, implementation, and confirmation). The product adoption curve classifies adopters into five categories: innovators, early adopters, early majority, late majority, and laggards. The theory suggests that the adoption curve follows an S-curve, in which a small proportion of individuals initially adopt the innovation, followed by relatively quick adoption by the early and late majority, and then levels off as the laggards finally adopt. This theory introduces the concept that for most individuals in the social network, the decision to adopt the innovation is dependent upon the other individuals in the network. Early adopters have a profound effect on the adoption decisions of the later adopters. Recent research utilized the categories of adopters as introduced in Roger's theory to analyze how the adoption process affects the information flow of product recommendation [35]. The Bass model for diffusion of innovation is a mathematical model for estimating the adoption of new products. This model introduces fac-

tors such as product market potential and interaction rate between consumers and prospective consumers into the model. Early models for innovation diffusion ignore the consumer decision-making activity that occurs in each individual. The characteristics of consumers are an important factor for product adoption. A consumer's decision is highly affected by social influences and interactions that occur over time. The concept of "word of mouth" is commonly used in marketing. It builds on the observation that a consumer's decision to accept a new product depends on what they hear from others[15].

2.3. Threshold and cascade models

In general, the existing diffusion models in the literature focus on two types of approaches, cascade models and threshold models. The most basic models are the Independent Cascade Model and the Linear Threshold Model. The cascade models are similar to the models of the spread of epidemic diseases [21, 26, 28, 32]. In the Independent Cascade Model, each node gets a chance to influence each of its inactive neighbors with a given probability of success. If the transmission is successful, the neighbor will become active at the next time step. In general, this process continues until there are no more possible transmissions. In the Linear Threshold Model, an individual is infected based how many of their neighbors are already infected. There is a weight on the edge between two nodes, which defines a measure of influence. Each node has a threshold value, which is drawn randomly from some specified probability distribution. This threshold determines how many neighboring nodes have to be activated before the node itself becomes active. If the sum of the weights of all active neighbors exceeds the threshold, then the node will become active [16, 40]. The cascade and threshold approaches form the basis for many diffusion models and extensions to these models have been made to study different diffusion processes [12, 15, 21, 25], as well as identifying variables that affect the diffusion process in cascade models [9] and observing information cascade in viral marketing [25, 26].

2.4. Network structures

The structure of the social communication network is a very important factor in the diffusion process. At the two ends of the spectrum of graphs are regular graphs and random graphs. In regular graphs, all nodes have the same degree, i.e. every node is connected to the same number of nodes. Random graphs are generated based on some random process and are often used for proving the existence of certain graph properties. However, these graphs often do not represent how actual social networks are structured.

Scale-free networks and small-world networks are commonly used in studying social network structures. They appear to be more realistic and reflect the characteristics of biological and technological systems. In scale-free networks,

most nodes have a low degree while a small subset have high degree. This addresses the phenomenon of the existence of highly connected individuals in a network. The degree distribution follows a power-law relationship in which the structural dynamics are independent of the number of nodes in the network. In small-world networks, nodes are highly clustered with small path lengths between nodes. This phenomenon is commonly found in biological, social, and synthetic systems [30, 38] and also appears when analyzing patterns of scientific collaboration [31] and actor collaboration in films [2, 36, 39]. Small-world networks have been used in studying algorithmic routing of messages in communication networks [22]. The speed in which information spreads changes with the degree of randomness in the network and has found to increase in small-world networks [12].

Most previous research assumes the network to be static and does not consider the changes that may occur over time. Dynamic networks are becoming more popular in the recent research literature [6, 11, 24] which study evolving communication graphs conditioned on a static social group structure. In dynamic networks, nodes and edges may appear and disappear with time. There are multiple aspects of dynamics to consider. The local dynamics describe how nodes interact and how the diffusion may spread. This includes changes at the individual node level, e.g. changes in node thresholds or infection probabilities. The group dynamics describe the social group evolution that may occur over time. New nodes and edges may appear as individuals make new friends or join social groups, and/or disappear as individuals relocate or leave groups. When diffusion occurs over a social network, the dynamics of the social network determine who is interacting at each time step (e.g. [14]), which in turn determines how the diffusion may spread at that particular time step. In addition, the network may change due to the diffusion that occurs through the network.

3. DIFFUSION MODEL

The model of diffusive processes in dynamic networks described in this paper is motivated by the existing diffusion models. The key concepts found in the SIR models used in epidemiology and the standard threshold and cascade models are reflected in the axiomatic framework. The proposed diffusion model is a general framework and these particular models can be incorporated as special cases.

3.1. Parameters

The diffusion process occurs on a network whose nodes represent individual entities and edges represent interactions between nodes. This network may be a directed or undirected. Through the interactions between nodes, some property is diffused through the network. We refer to the property as messages. External sources introduce messages into the network.

Multiple sources may exist for a message, each with its corresponding perceived information value. The perceived value of the message may be different for each source, i.e. trustworthiness of source.

The weight on each edge represents a trust value between two nodes. This value is used to quantify the social relations based on a notion of trust in information and information sources [20]. Note that in other contexts the weight on the edge may represent other concepts. For example, in the spread of diseases, the weight on the edge can reflect on how infectious of contagious the disease may be. Each node in the network has configurable attributes. The properties of each node are updated over time as interactions occur and messages are propagated.

3.2. Axioms

The model for diffusion on dynamic graphs is based on four axioms: Information Loss Axiom, Source Union Axiom, Information Fusion Axiom, and Threshold Utility Axiom. These axioms define the diffusion process by specifying: what happens to the message as it is propagated, how the nodes handle information they receive, and nodes update their properties based on their interactions and the information they receive.

Information Loss Axiom. If (S, V) is a source-value pair at node i which is propagated to node j then the source-value pair at node j is $(S, \alpha(i, j)V)$, where $0 \leq \alpha(i, j) < 1$ is the propagation loss from i to j . $\alpha(i, j)$ quantifies the trust relationship between nodes i and j .

When a message is passed from one node to another, the information value of the message is non-increasing. The information value of the message at the receiver node is a function of the social relationship between the sender and the receiver and not just a function of distance. The social relationship may be asymmetric, i.e. the trust weights on the edge may be different depending on the direction of the information flow.

Source Union Axiom. If multiple nodes propagate a message to a node j , then the source set at j after propagation is the union of the source set which was already at j with the union of the source set arriving from the multiple nodes.

Information Fusion Axiom. A. If a source S_i appears in multiple incoming messages with values V_i^1, V_i^2, \dots , the information from this particular source, V_i^* , is fused into the single source-value pair (S_i, V_i^*) , where $\max_k V_i^k \leq V_i^* \leq \sum_k V_i^k$. The value V_i^k corresponds to the information value of source i at node k . **B.** Suppose that node k has source set (S_1^k, S_2^k, \dots) with information values (V_1^k, V_2^k, \dots) . The fused information value at the node is at least the $\max_i V_i^k$ and at most $\sum_i V_i^k$.

Each node stores a list of source-value pairs representing the information they have received. At the end of each time step, the node will merge the information they received and update their properties. There are two components to consider when merging the information, as described by the *Information Fusion Axiom*. The first part **A.** is to fuse information from the same source appearing in multiple messages. When a source is found in multiple messages, the combined information value for the 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 second part **B.** outlines how to compute the information fused value at a node. To specify how to combine the information values from all the different sources, we can use a weighted convex combination of the sum and maximum of the values according to a parameter λ . The fused value at node k would be $\lambda * \sum_i V_i^k + (1 - \lambda) * \max_i V_i^k$. When $\lambda = 1$, the fused value is equal to the sum of the information values of all the sources. When $\lambda = 0$, the fused value is equal to the max of the information values. Exactly where V^* should sit in this range will depend on the nature of the diffusion, for example gossips (which spread fast) will have V^* closer to the sum. The fused information value is at least the maximum of the information values (having more information cannot hurt) and at most the sum.

Threshold Utility Axiom. After computing the fused information value, the node state is determined based on whether the information value exceeds certain thresholds. Each node has two defined threshold levels, a lower bound and an upper bound, which determine the boundaries for when the node will acknowledge the message and/or take an action. Table 1 summarizes the possible node states along with its corresponding behaviors in the context of evacuation warnings. The lower bound threshold lies between the disbelieved and uninformed states, while the upper bound threshold lies between the undecided and believed states.

4. EXPERIMENTS

We illustrate the concepts of the model by simulating the spread of evacuation warnings in a social network. The context of the experiments are motivated by the evacuation warnings scenario described in [18, 19]. In the case of evacuations, warnings are broadcasted from information sources to the at-risk population. We assume that the initial broadcasted messages will reach a certain proportion of individuals from the population, referred to as seeds. These selected individuals (seeds) will then attempt to propagate the evacuation warning to the rest of the population. Applying the model to the diffusion of warnings captures network dynamics as a result of the diffusion, i.e. receiving the evacuation warning may

Table 1. Node States for Evacuation Warnings

State	Description
Uninformed	Node has not received any messages. (No action.)
Disbelieved	Node has received a message but does not believe the message. (No action.)
Undecided	Node has received the message and is uncertain of what to do. (Query neighbors in the network.)
Believed	Node has received the message and believes the value of the message. (Spread the message to its neighbors and evacuated after x time steps.)
Evacuated	Node is no longer in the network.

cause individuals to leave the network and disrupt the flow of information. In a structural sense, nodes are removed from the network and incoming and outgoing edges from the nodes are removed as well. We simulate the diffusion of evacuation warnings in multiple network structures under various model settings and observe the ultimate proportion of evacuated nodes.

4.1. Network Structures

Random graph. The random graph is a Erdos-Renyi network where nodes are linked randomly with an edge probability p . Here, $p = 0.00004$.

Scale-free network. To generate scale-free networks, we used the Barabasi-Albert model for generating random scale-free networks using preferential attachment [1, 2]. The degree distribution of the resulting graph follows a power law of the form $P(k) \sim k^{-3}$.

Random group model. Individuals are more likely to communicate with certain individuals and less frequently with other individuals. In the random group model, nodes are more likely to be connected to other nodes belonging to the same group than to nodes of a different group. Nodes are assigned to k groups of size m where the total number of nodes is $n = k * m$. The edge probability between nodes from the same group is p_s and the edge probability between nodes from different groups is p_d . We assume that p_s is much greater than p_d . Here, $p_s = 2 * p_d$.

Grid network. The nodes are arranged in a two-dimensional grid, where most nodes have 4 neighbors.

Regular graph. In the random regular graph, all nodes have 4 randomly selected neighbors.

4.2. Node Characteristics

Node thresholds. For evacuation warnings, the goal of the diffusion process is to spread the warning message and have the nodes take action and evacuate. There are high risks,

Table 2. Summary of Network Structures

Network	Size	Density
Grid	100,000	0.00003987
Regular (d=4)	100,000	0.00004000
Random (p=0.00004)	100,000	0.00004000
Scale-free (m=2, k=2)	100,000	0.00003900
Group (k=2, m=50000)	100,000	0.00003994

costs, and consequences to an individual or household associated with evacuation, i.e. being in Believed state. Therefore, nodes that reach this state will have preformed information seeking before deciding to evacuate. This is modeled by setting a large difference between upper and lower thresholds for the Undecided state. Further, it is assumed that when a node enters Believed state, they will spread the warning to its neighbors and will evacuate and leave the network after 5 time steps.

4.3. Seeding Strategies

We refer to the subset of nodes that receive messages directly from sources as the *seed set*. The messages are then spread from the seed set to the rest of the network. Each source is connected to an equal number of nodes in the network. In these experiments, we define 5 trustworthy sources (*trust_value* = 0.90). Each source will broadcast evacuation warnings represented as messages with high information value of 0.95. We assume that the initial messages sent from the sources will reach all its intended recipients. We look at two ways of selecting the seed set of nodes to receive the initial broadcast: randomly selecting a set of nodes, or selecting a set of nodes with the highest degree. We consider three values for the size of the initial seed set: 5%, 10%, 20% of the node population. Since there are 5 sources, each source will connect to $|seed_set|/5$.

4.4. Trust Scenarios

The following scenarios were modeled to incorporate population heterogeneity, in terms of differences in trust between nodes and the degree of trust differences. The trust values between nodes are assigned depending on the sender and receiver’s social group membership. We split the population into two social groups *A* and *B* of equal size. There are four types of links showing the direction of information between any two neighboring nodes in the network: (*A* to *A*), (*A* to *B*), (*B* to *A*) and (*B* to *B*). Each link represents the trust between the two nodes when information is transferred from the sender to the recipient. As a benchmark, we assign an average trust value t_{avg} . We define high trust links with value $t_{high} = t_{avg} + \epsilon$ and low trust links with value $t_{low} = t_{avg} - \epsilon$. We refer to ϵ as the trust differential, which is the difference from the aver-

age trust. In these scenarios, the average trust of the entire network will be approximately t_{avg} since the two groups have equal sizes.

Scenario A. Same trust between all nodes. This scenario represents a homogeneous network where everyone has the same trust in everyone else. There are essentially no social groups and no differences in trust between nodes, i.e. $\epsilon = 0$ and $t_{high} = t_{low}$.

Scenario B. Higher trust in nodes from the same group. This scenario represents a population where people have higher trust in others who are in the same group or similar to them. This is such a case, for example, in the dissemination of hazard information in populations with ethnic groups. Individuals who belong to the same group have t_{high} in each other and have t_{low} in individuals of a different group.

Scenario C. Random trust between all nodes. There is no structure in how trust is distributed in the network in this scenario. The values t_{high} and t_{low} are randomly assigned onto links throughout the network with probability 0.5. As a result, individuals have higher trust about 1/2 of the population.

4.5. Parameters

Information Fusion. A. When a source appears in multiple messages with different information values, we use the maximum of all the information values. **B.** When computing the information fused value at the node, we take a linear combination of the sum and maximum of the information values: $\lambda * \sum_i V_i^k + (1 - \lambda) * \max_i V_i^k$ using $\lambda = 0.5, 0.75, 1.0$.

Edge probability. When a node (that is not a source) tries to query for information or spread a message, there is a 75% chance that the message will be received or shared.

5. RESULTS AND DISCUSSION

Each simulation run lasts 50 time steps and is repeated 100 times. Based on these experiments we report the average proportion of evacuated nodes at the end of the simulations.

5.1. Network Structures, Seeding Strategies, and Information Fusion

Figure 1 shows the proportion of evacuated nodes for each network structure under the homogeneous trust scenario, *A*. As we increase the size of the seed set, the resulting proportion of evacuated nodes also increases. The results also show that the network structure and the seeding strategy used both have an impact on the proportion of evacuated nodes. Using the highest degree nodes as seeds was more beneficial in spreading the evacuation message than when using a randomly selected set of nodes. The effect of the seeding strategy is also dependent on the network structure. In the grid network and the regular network, there is little difference since

most nodes share the same degree. In scale free networks, seeding using high degree nodes results in a drastic increase in the proportion of evacuated nodes. Seeding using the highest degree nodes also showed improvement in the random network and the random group network.

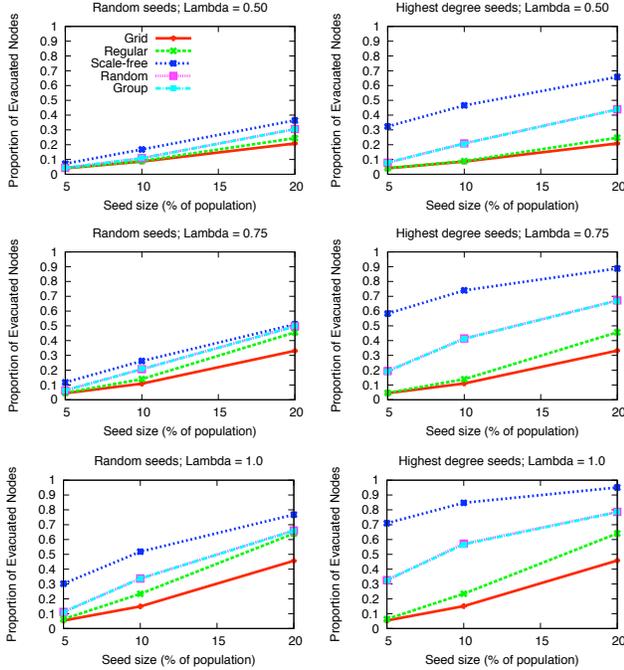


Figure 1. Proportion of evacuated nodes as we increase the size of the seed set, for information fusion parameters $\epsilon = 0.50, 0.75, 1$.

When we perform information fusion with $\lambda = 1$, the fused value is more likely to exceed the lower and/or upper thresholds. As a result, the messages diffuses to a larger proportion of nodes. As we decrease the value of λ the fused value gets closer to the maximum of the individual bits of information. Treating each source independently and adding their information values results in the largest spread. The value for λ would depend on whether the nature of the diffusion is fast spreading or not.

5.2. Network Structures, Trust Scenarios, and Trust Differentials

The results for information fusion $\lambda = 1$ using the two seeding mechanisms are shown in Table 3 and 4. The scenarios with inhomogeneous trust, B and C, resulted in larger proportions of evacuated nodes when compared to scenario A, when there was same trust between all nodes. This suggests that scenarios with differences in trust is better for evacuation diffusion than a homogeneous trust scenario. In particular, the higher trust differential $\epsilon = 0.15$ resulted in larger proportions of evacuated nodes than $\epsilon = 0.05$. This suggests

that large asymmetries in trust have a positive effect. Under these configurations, the results for scenarios B and C are very similar for most of the networks. The similarities may have been caused by the fact that there were equal number of individual nodes in both groups and the nodes were randomly assigned to groups A and B. Therefore, there may not be observable differences between randomly assigning high and low trust values and assigning trust values based on group membership when group membership was also randomly assigned. The results suggest that having differences in values of trust based on social groups is beneficial for the spread of the evacuation warnings. For the random group network, the nodes from group A are more likely to be connected to others from group A and likewise, nodes from group B connected to others from group B. In this case, having higher trust in nodes from the same group is shown to be much better than just randomly assigning high and low trust values. This suggests that the distribution of the node groups in the network have an effect on the diffusion process.

Table 3. Proportion of Evacuated Nodes (Random Seeds; Information Fusion Lambda = 1)

Network	A	B		C	
		$\epsilon = 0.05$	0.15	$\epsilon = 0.05$	0.15
Grid	0.457	0.481	0.548	0.488	0.570
Regular	0.640	0.659	0.731	0.658	0.729
Scale-free	0.768	0.798	0.848	0.797	0.848
Random	0.661	0.686	0.756	0.685	0.756
Group	0.659	0.741	0.836	0.685	0.756

Table 4. Proportion of Evacuated Nodes (Highest Degree Seeds; Information Fusion Lambda = 1)

Network	A	B		C	
		$\epsilon = 0.05$	0.15	$\epsilon = 0.05$	0.15
Grid	0.458	0.482	0.549	0.490	0.571
Regular	0.641	0.659	0.730	0.659	0.729
Scale-free	0.951	0.960	0.948	0.960	0.948
Random	0.787	0.801	0.814	0.801	0.813
Group	0.784	0.833	0.861	0.799	0.812

For most of the network structures, the nodes were randomly assigned to one of two groups, A and B, throughout the network. In a more realistic model, nodes from the same social group are more likely to communicate with each other and form clusters in the network. The random group network captures this component in some sense, where nodes from the same group are more likely to be connected to each other than nodes from different groups. Figure 2, presents simulation results for random node assignment and the group as-

segmentation on the random group network. Random Assignment refers to randomly assigning nodes to groups and the Group Assignment refers to the node assignment that resulted when we were constructing the random group network. For a small seed size of 5%, the group assignment appears to have a greater effect on the diffusion process than with random assignment. As the seed size increases, the effect is not as drastic.

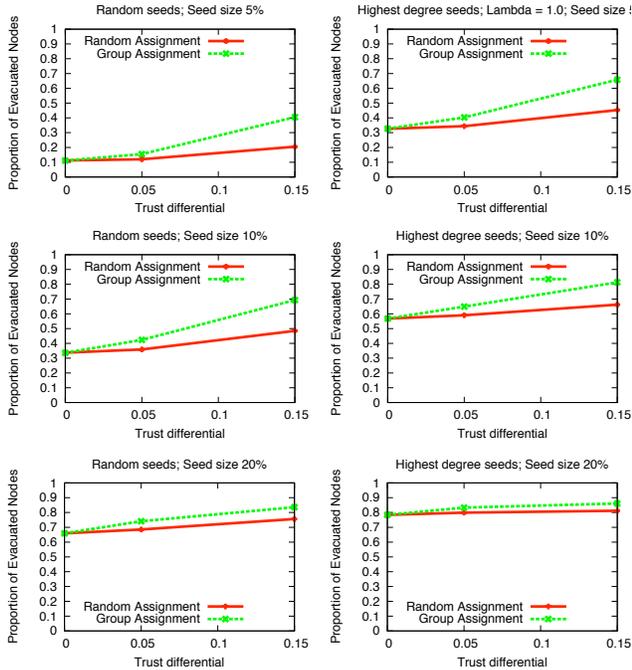


Figure 2. Comparison of the proportion of evacuated nodes for Random Assignment and Group Assignment, as we increase the trust differential and vary the seed sizes.

6. CONCLUSION

In this paper, we presented a general model of diffusion in dynamic networks. We used the model to simulate the diffusion of evacuation warnings in various network structures. Each node in the network, representing a household, is assigned into one of two groups. The network is dynamic as a result of the diffusion, where households who believe the warnings they receive will evacuate and leave the network. We examined how network structure, seeding strategy, and population inhomogeneity based on trust, impact the diffusion process. Network structure and the seeding strategy used in sending the initial broadcasts affects the effectiveness of the diffusion. The results show that when nodes have higher trust in nodes of their same group, the evacuation is greater than when trust is the same between all nodes. Increasing the trust differentials leads to larger proportions of evacuated nodes.

The diffusion model presented in this paper can be tuned to represent various diffusion scenarios by specifying the parameters to fit the particular context. Future work includes calibrating the model parameters using data from specific applications. Further experimentation include investigating concepts, such as network density and connectivity, and trust variants in sources. We will investigate the interactions between parameters such as the node thresholds, information fusion, and seed size. We will also perform experiments to look at the broadcast of warnings over time, as opposed to the one-time broadcast simulated in these experiments.

ACKNOWLEDGEMENTS

This material is based upon work partially supported by the U.S. National Science Foundation (NSF) under Grant No. IIS-0621303, IIS-0522672, IIS-0324947, CNS-0323324, NSF IIS-0634875 and by the U.S. Office of Naval Research (ONR) Contract N00014-06-1-0466 and by the U.S. Department of Homeland Security (DHS) through the Command, Control, and Interoperability Center for Advanced Data Analysis administered through ONR grant number N00014-07-1-0150 to Rutgers University. The content of this paper does not necessarily reflect the position or policy of the U.S. Government, no official endorsement should be inferred or implied.

REFERENCES

- [1] Albert, R. and A. Barabasi, 1999, “Emergence of scaling in random networks”. *Science* 286: 509–512.
- [2] Albert, R. and A. Barabasi, 2002, “Statistical Mechanics of Complex Networks”. *Reviews of Modern Physics* 74(1): 47–97.
- [3] Albert, R., H. Jeong, and A. Barabasi, 2000, “Error and attack tolerance of complex networks”. *Nature* 406(6794): 378–382.
- [4] Barthélemy, M., A. Barrat, R. Pastor-Satorras, and A. Vespignani, 2004, “Velocity and hierarchical spread of epidemic outbreaks in scale-free networks”. *Phys. Rev. Lett.* 92(17): 178701.
- [5] Bass, F., 2004, “A new product growth for model consumer durables”. *Management Science* 50(Supplement 12): 1825–1832.
- [6] Berger-Wolf, T. Y. and J. Saia, 2006, “A framework for analysis of dynamic social networks”. In *Proc. of the 12th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining*, Philadelphia, Pennsylvania, pp. 523–528. ACM Press.
- [7] Bettencourt, L., A. Cintron-Arias, D. Kaiser, and C. Chavez, 2006, “The power of a good idea: Quantitative Modeling of the spread of ideas from Epidemiological models”. *Physica D* 364: 513–536.
- [8] Brown, J. and P. Reingen, 1987, “Social ties and word-of-

- mouth referral behaviour”. *J. Consumer Research* 14(3): 350–362.
- [9] Centola, D., V. M. Eguiluz, and M. W. Macy, 2007, “Cascade dynamics of complex propagation”. *Physica A* 374: 449–456.
- [10] Chen, L. and K. Carley, 2004, “The impact of countermeasure propagation on the prevalence of computer viruses”. *IEEE Trans. on Systems, Man, and Cybernetics* 32(2): 823–833.
- [11] Cortes, C., D. Pregibon, and C. Volinsky, 2003, “Computational methods for dynamic graphs”. Technical report, AT&T Shannon Labs, Florham Park, New Jersey.
- [12] Delre, S., W. Jager, and M. Janssen, 2006, “Diffusion Dynamics in Small-World Networks with Heterogeneous Consumers”. *Computational & Mathematical Organizational Theory* 13(2): 185–202.
- [13] Girvan, M. and M. Newman, 2002, “Community structure in social and biological networks”. *Proc. Natl. Acad. Sci. USA* 99(12): 7821–7826.
- [14] Goldberg, M., S. Kelley, M. Magdon-Ismail, K. Mertsalov, and W. A. Wallace, 2008, “Communication Dynamics of Blog Networks”. In *Proc. SIGKDD Workshop on Social Network Mining and Analysis*, pp. ACM Digital Library.
- [15] Goldenberg, J., B. Libai, and E. Muller, 2001, “Talk of the network: a complex systems look at the underlying process of word-of-mouth”. *Marketing Letters* 12(3): 211–223.
- [16] Granovetter, M., 1978, “Threshold Models of Collective Behavior”. *Amer. J. Sociology* 83(6): 1420–1443.
- [17] Hill, S., F. Provost, and C. Volinsky, 2006, “Network-Based Marketing: Identifying Likely Adopters via Consumer Networks”. *Statistical Science* 21(2): 256–276.
- [18] Hui, C., M. Goldberg, M. Magdon-Ismail, and W. A. Wallace, 2008, “Micro-Simulation of Diffusion of Warnings”. In F. Fiedrich and B. V. de Walle (Eds.), *Proc. of the 5th Int’l Conf. on Information Systems for Crisis Response and Management ISCRAM2008*, pp. 424–430.
- [19] Hui, C., M. Magdon-Ismail, W. A. Wallace, and M. Goldberg, 2009, “The Impact of Changes in Network Structure on the Diffusion of Warnings”. In *Proc. Workshop on Analysis of Dynamic Networks at the SIAM Int’l Conf. on Data Mining*, Sparks, NV.
- [20] Kelton, K., K. R. Fleischmann, and W. A. Wallace, 2008, “Trust in digital information”. *J. Amer. Society for Information Science and Technology* 59(3): 363–374.
- [21] Kempe, D., J. Kleinberg, and É. Tardos, 2003, “Maximizing the spread of influence through a social network”. In *Proc. of the 9th ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining*, Washington, DC, pp. 137–146. ACM Press.
- [22] Kleinberg, J., 2000, “The small-world phenomenon: An algorithmic perspective”. In *32nd ACM Symp. on Theory of Computing*.
- [23] Kuperman, M. and G. Abramson, 2001, “Small world effect in an epidemiological model”. *Phys. Rev. Lett.* 86(13): 2909–2912.
- [24] Lahiri, M., A. Maiya, R. Sulo, Habiba, and T. Y. Berger-Wolf, 2008, “The Impact of Structural Changes on Predictions of Diffusion in Networks”. In *ICDM Workshop on Analysis of Dynamic Networks*, Pisa, Italy.
- [25] Leskovec, J., L. A. Adamic, and B. A. Huberman, 2006, “The dynamics of viral marketing”. In *Proc. of the 7th ACM Conf. on Electronic Commerce EC06*, New York, NY, USA, pp. 228–237. ACM Press.
- [26] Leskovec, J., A. Singh, and J. Kleinberg, 2006, “Patterns of Influence in a Recommendation Network”. In *Proc. Pacific-Asia Conf. on Knowledge Discovery and Data Mining (PAKDD)*.
- [27] Meyers, L. A., M. Newman, and B. Pourbohloul, 2006, “Predicting epidemics on directed contact networks”. *J. Theoretical Biology* 240: 400–418.
- [28] Moore, C. and M. Newman, 2000, “Epidemics and percolation in small-world networks”. *Phys. Rev. E* 61(5): 5678–5682.
- [29] Morris, S., 2000, “Contagion”. *Rev of Economic Studies* 67(1): 57–78.
- [30] Newman, M., 2000, “Models of the small world”. *J. Statistical Physics* 101(3/4): 819–841.
- [31] Newman, M., 2001, “The structure of scientific collaboration networks”. *Proc. Natl. Acad. Sci. USA* 98: 404–409.
- [32] Newman, M., 2002, “The spread of epidemic disease on networks”. *Phys. Rev. E* 66(1): 12.
- [33] Pastor-Satorras, R. and A. Vespignani, 2001, “Epidemic Spreading in Scale-Free Networks”. *Phys. Rev. Lett.* 86(14): 3200–3203.
- [34] Rogers, E., 1995, *Diffusion of Innovations*. New York, NY: Free Press.
- [35] Song, X., B. L. Tseng, C.-Y. Lin, and M.-T. Sun, 2006, “Personalized Recommendation Driven by Information Flow”. In *29th Annual Int’l ACM SIGIR Conf. on Research and Development in Information Retrieval*, pp. 509–516.
- [36] Strogatz, S. H., 2001, “Exploring complex networks”. *Nature* 410: 268–276.
- [37] Valente, T., 1995, *Network Models of the Diffusion of Innovations*. Hampton Press.
- [38] Watts, D. J., 1999, “Networks, Dynamics, and the Small-World Phenomenon”. *Amer. J. Sociology* 105(2): 493–527.
- [39] Watts, D. J. and S. H. Strogatz, 1998, “Collective dynamics of small-world networks”. *Nature* 393: 440–42.
- [40] Young, H. P., 2000, “The Diffusion of Innovations in Social Networks”. *Economics Working Paper Archive* 437, Johns Hopkins University.