Micro-Simulation of Diffusion of Warnings

Cindy Hui
Rensselaer Polytechnic Institute
huic@rpi.edu

Mark Goldberg
Rensselaer Polytechnic Institute
goldberg@cs.rpi.edu

Malik Magdon-Ismail
Rensselaer Polytechnic Institute
magdon@cs.rpi.edu

William A. Wallace
Rensselaer Polytechnic Institute
wallaw@rpi.edu

ABSTRACT

This paper presents a unique view of modeling the diffusion of warnings in social networks where the network structure may change over time. Since the characteristics and actions of people in a community have significant influence on the flow of information through a network, we present an axiomatic framework for modeling the diffusion process through the concept of trust. This ongoing work provides a micro level view of the behavior of individuals and groups in a community. Preliminary experiments were made to explore how model parameters such as trust and the social network structure affect warning message belief and evacuation.

Keywords

Modeling, Simulation, Warnings

INTRODUCTION

In the event of a natural disaster or technological hazard, it is important that warnings are disseminated effectively and efficiently through the affected population. In other events, warning messages may serve as a flag alerting the population of potential but not immediate danger. The assumption here is that given a warning, individuals will have some time to spread the warning and take the recommended action.

Warning systems play an important role in notifying the population of the future danger and providing precautionary and safety information so that necessary actions can be taken. Even with the most detailed warning broadcast, the message might not reach the entire targeted audience. In addition, social and economic factors may hinder individuals to comply with the recommendations. It is essential to understand the social interactions and human behaviors involved in hazardous events in order to have a successful warning system. The notion of trust is an important component in these situations. The diffusion framework incorporates this concept of trust that quantifies the likelihood that individuals will believe the message being conveyed to them (Kelton et al., In Press, Kelton and Wallace, 2000, Kelton and Wallace, 2003).

RELATED WORK

Research on warning response behavior dates back about 40 years (Mileti, 1999). The overall conclusion is that warning is a social process where receiving a message sets into motion a complex set of social interactions that may or may not result in the population taking the desired protective action. The warning sequence process model (Sorensen, 2000, Sorensen and Mileti, 1987, Sorensen et al., 1987) posits that there are six phases extending from disseminating the warning to the protective action. Previous work has also involved analyzing the decision making process that occurs in response to environmental threats and dangerous events (Lindell and Prater, 2004, Perry and Lindell, 2003).

People's response to warnings is a function of social, economic, and demographic factors (Aguirre, 1994), including physical environment, population, technology, social relations, and culture (Ding, 2006, Golden and Adams, 2000, Lindell and Prater, 2007, Sorensen, 2003). Warning systems must consider people's perception, interpretation, and reaction to the warnings. It requires significant knowledge of the local population, in terms of their demographics, societal culture, and past events that have occurred in the location. In studying warning systems, issues like message distortion, level of detail in the message, as well as interference with normal activities play an important part on the recipient's analysis of their situation (Lindell and Prater, 2004, Lindell and Prater, 2007, Sorensen, 2000, Sorensen

and Mileti, 1987, Sorensen et al., 1987). Incomplete information leads to lower compliance with emergency recommendations (Perry and Lindell, 2003).

The warning time distribution has two components: the official broadcast component and the information diffusion component. The broadcast component is easy to identify but there are many uncertainties relating to the diffusion component (Perry and Lindell, 2003, Rogers and Sorensen, 1991, Sorensen, 1992). There has been considerable research in estimating warning time distributions by modeling the warning network, however there are difficulties because the diffusion component is dynamic, depending on the social and demographic structure (Ding, 2006, Rogers and Sorensen, 1991, Sorensen and Mileti, 1987, Sorensen et al., 1987).

By understanding the communication patterns and social network structure, information can be passed on more efficiently and effectively. This form of communication is crucial when dealing with hazardous situations, natural disasters, or other emergencies. Along with quick communication, warnings have to be communicated effectively so that the target audience would act upon receiving the message and take the necessary measures. Upon receiving a warning message, people, in general, do not panic but instead try to act based on their limited knowledge of the situation. People evaluate the message in terms of their own personal experiences and values. They seek additional information and confirmation through observation and direct contact (Mileti, 1999, Sorensen, 2000, Sorensen and Mileti, 1987, Sorensen et al., 1987). Furthermore, people do not necessarily react immediately when they receive a warning message. The time to action depends upon the situation, the type of warning, as well as other factors (Sorensen et al., 1987).

The source of the message is an important factor. Warning messages may come from many sources, such as television, radio, or simply word of mouth. The message receiver may have a different value of trust for each source. If the message is very important, i.e. potential for saving a life, the message receiver will be more likely to be influenced by the message. The quality and the content of the message is also an important factor. People are more hesitant to comply with emergency measures when they are provided with incomplete information (Perry and Lindell, 2003).

In certain situations, individuals may decide to leave the community after a certain time, when they feel it is necessary to leave. Therefore the social network is dynamic in the sense that when individuals leave, we assume that all connections to their neighbors are terminated, possibly disrupting future routes for additional messages.

THE MODEL

The agent-based model is based on an axiomatic foundation for studying the diffusion process in dynamic social networks. The social network described here is dynamic and in the case of evacuation warnings, when an individual node evacuates, the individual is removed from the network eliminating all its interaction edges, and perhaps disrupting the flow of information.

The diffusion network defined here is comprised of three hierarchical layers. The bottom layer is the physical network. The physical layer represents all the possible forms of communication. In theory, the layer could be a complete graph in which each node has the potential ability to contact any other node in the network. The definition of the physical layer depends on the context of the model, for example, the geographical region being modeled. The second layer is the social network. The social layer is the layer where the diffusion of information occurs and is an induced sub graph of the physical layer. Lastly, the top layer is the interaction network. The interaction layer consists of a series of evolving graphs that are produced when information flows through the social network. Analyzing the evolving graphs in the interaction layer will provide insights into the diffusion process that occurs in the social network.

Parameters

Each node in the network represents a single entity, each with configurable attributes. These entities may be uninformed individuals or information sources. Source nodes initiate the original message. Once the message is initiated by a source, it carries along with it a source-value pair, storing the message source and information value.

Types of nodes can be defined to introduce variety into the network population. These types can be used to represent subsets of the population that share similar traits, e.g. based on occupation. The trust values between types of individuals can be configured based on social relationships, e.g. in terms of kinship, affiliations, or authoritative power. The desired action consists of spreading the warning to their social contacts and making the decision to

perform protective action. There is a parameter to represent the evacuation preparation time, i.e. how much time elapses between the evacuation decision and its enactment.

A source node is a specific type of node. It is defined to mimic the sources, such as television, radio, external family member, etc. The sources can broadcast messages with varying information value to represent the type of warning message, e.g. precautionary warning or high-risk alert. Each source has its own value of trust, which may be viewed differently by individuals. Their action is guaranteed in the sense that they introduce the initial message into the network. The source node may leave the network when the broadcast of the information is a one-time event or send messages in time intervals, e.g. sending news updates. The model assumes that the source nodes receive their information from resources outside of the network's scope.

The properties of the individual nodes are updated based on a set of defined axioms for the diffusion process. The weight on each interaction edge symbolizes the trust value between two individual nodes. Between two nodes in the network is a pair of directed edges with possibly two different weights, since trust does not have to be symmetric.

Axioms

The framework described here uses axioms to model the behavior of individuals as they receive and propagate information through the social network The individuals in the network diffuse information based on the following four axioms: Information Loss Axiom, Source Union Axiom, Value Min-Max Axiom, and Threshold Utility Axiom.

Information Loss Axiom

The Information Loss Axiom states that 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, not just a function of distance.

Source Union Axiom

The Source Union Axiom states how source-value pairs are updated in a receiver node. The resulting source set should be a union of the source sets of the incoming messages. This ensures that messages from the same source are accounted for only once.

Value Min-Max Axiom

The Value Min-Max Axiom provides a method for computing the information value set for a receiver node. When a source is found in multiple messages, the combined information value for the source at the node is at least the maximum of the information values for this source over all the messages. Furthermore, the combined information value is at most the sum of all the information values of this source, but cannot exceed 1. The combined information value is scaled by a lambda parameter that determines where the value fall in the defined range, i.e. to what extent the information values are merged together.

Threshold Utility Axiom

The Threshold Utility Axiom is used to determine the states of the nodes. In this configuration, each individual node can be in one of four possible states. The following table summarizes the four basic states and defines the corresponding behavior.

State	Description	Behavior
Uninformed	Individual has not received the message	No action
Disbelieved	Individual does not believe the message	No action
Undecided	Individual received the message and is uncertain of what to do	Query
Believed	Individual received the message and believes the value of the message	Take necessary action

Table 1. Node States

After computing new source sets and their corresponding information values, the receiver node will combine the values into a single information fused value. This value determines the state of the node. Each node has two defined threshold levels, a lower and upper bound, which determine the boundaries for when the node will acknowledge the message and/or take action.

The Threshold Utility Axiom also states that the threshold level is a function of the utility of the message. In the case where the utility of the message is high, the individual is more likely to acknowledge the message but might be hesitant to take action (evacuate) immediately since there are high costs and consequences associated with this situation. Therefore, the lower bound threshold should be relatively low and the upper bound threshold should be somewhat high. On the contrary, if the utility of the message is rather low, both thresholds should be relatively low, since individuals may be more eager to take action (spread the message) since there are low costs and consequences to the action.

SIMULATION EXPERIMENTS

Preliminary experiments were made to explore how population demographics, trust and the social network structure affect evacuation. For the experiments, the social communication network was constructed an Erdos-Renyi graph with 600 nodes, where nodes are connected randomly with probability of 0.006. This resulted in an average of 3.6 neighbors for each individual node and a total of 1102 edges. A network of 600 nodes seem sufficient based on past evacuation studies of hazardous events (Rogers et al., 1990, Vogt and Sorensen, 1999) that analyzed survey data sets in the scope of hundreds of households. The population is heterogeneous and consists of two equally sized groups of nodes, A and B. For simplicity, one source node was incorporated into the network. This source node was randomly connected to 60 nodes from group A and 60 nodes from group B. This source is assumed to be a trustworthy source with a very high information value (0.95). Individual nodes from either group have high trust in the source (0.90). In addition, it is assumed that this source would reach all its connected individual nodes when it sends the initial warning message.

The two groups of nodes are identical in the sense of node characteristics, but the social relationships between them, namely, the trust values, are varied. The nodes have a lower bound threshold of 0.1, which suggests low tendency to disbelieve a warning message, and an upper bound of 0.5. Even though two individual nodes may be connected in the social network, it is possible that communication between them may not occur. To include this aspect, a probability of successful communication between two nodes is incorporated. In this case, there is a 75 percent probability that an individual node would be able to reach and propagate the message to its neighboring node. When an individual node enters the believer state, the node will propagate the message to its neighboring nodes and evacuate after 5 time steps.

The following scenarios were modeled to incorporate heterogeneity in the degree of trust between nodes. These models are applicable, for example, multi-ethnic communities. In Scenario 1, the trust levels between all node types are equal (0.75). This represents a homogeneous network where everyone has the same trust in everyone else. In Scenario 2, individuals who belong to the same type have higher trust in each other. However, they have a lower level of trust in individuals of a different type. In Scenario 3, recipients have higher trust in senders who belong to one specific type, regardless of the recipient's node type. Recipient nodes have high trust in senders from group A and low trust in senders from B.

Scenarios	**A to A**	**A to B**	**B to A**	**B to B**
Scenario 1	SAME	SAME	SAME	SAME
Scenario 2	HIGH	LOW	LOW	HIGH
Scenario 3	HIGH	LOW	HIGH	LOW

Table 2. Trust levels between node types

DISCUSSION

The results from the average of 10 replications are presented in Figure 1. The trust differential is referred to, as the difference between the high and low trust values. The network in Scenario 2 with trust differential 0.3 ended with the largest proportion of individuals evacuating. This observation suggests that tightly connected social communities

may be preferable in message diffusion. The homogenous network where trust values between all individual nodes are identical, Scenario 1, resulted in the lowest proportion of individuals evacuating.

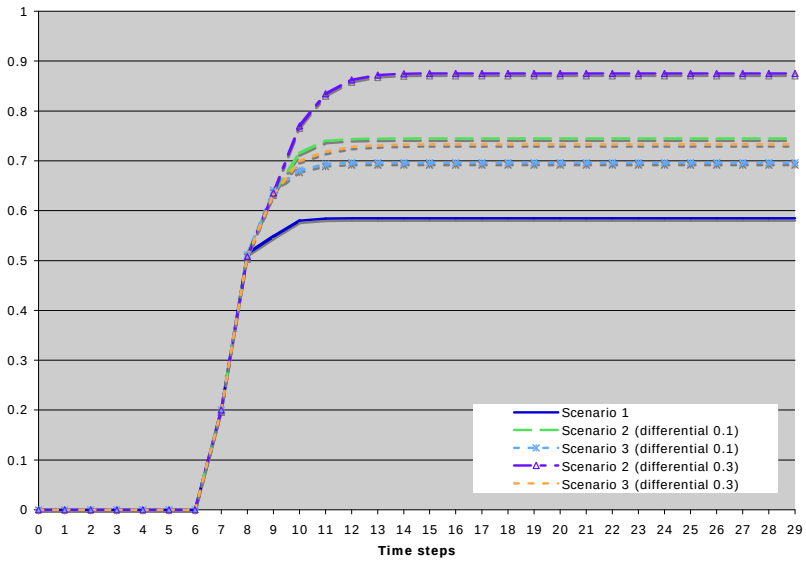

Figure 1. Proportion of Evacuated Nodes

The trust differential introduces a measurement of how symmetric the trust relationships between individual nodes may be. A large trust differential would suggest possible occurrences of highly asymmetric trust relationships. In this case, the initial direction of message would have a potential impact on the overall effectiveness of the flow. Further analysis is needed to observe these dynamics.

Comparisons of the trust scenarios are displayed in Figure 2. In Scenario 2, where nodes have higher trust in others of the same group, a larger trust differential results in a higher proportion of evacuated nodes. In Scenario 3, where nodes have higher trust in only nodes from group A, the larger trust differential does not have as great of an effect as observed in Scenario 2.

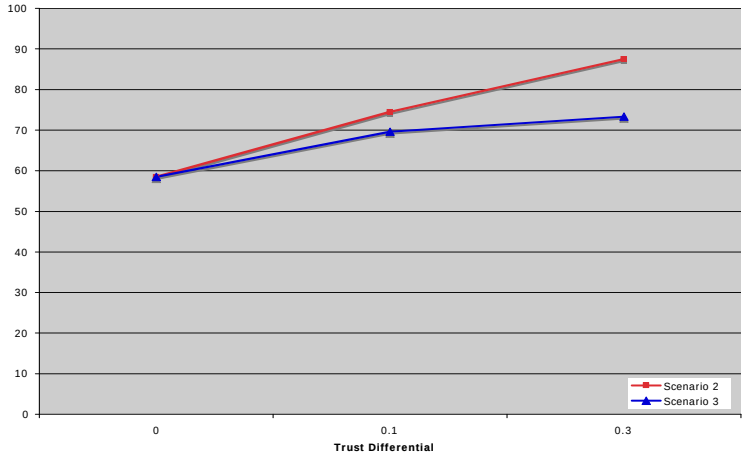

Figure 2. Comparison of Scenarios

CONCLUSION

The results presented are preliminary findings to explore the effects of variation in trust among the population. The basic scenarios introduce two groups of individual nodes. The social interactions between along with variables of trusts and perceived information values would bring about individuals to evacuate the network. A major assumption made is that after entering the believer state, the individual will attempt to propagate the warning information to members of its social network prior to evacuating. The findings bring upon an interesting observation on the effect of the trust differentials and the symmetry of the trusts. In certain situations, highly connected social communities may be preferable in message diffusion. The asymmetric trust relationships among individuals also have an interesting effect on message diffusion. These observations may have interesting implications for warnings belief and evacuation in heterogeneous multi-ethnic communities.

Further work will be done to observe the effects of components such as trust variants in various sources, information value perceptions, and evacuation times. The use of multiple message sources will bring into effect how message information values incorporate together. An interesting matter would be the compare the effectiveness of sources with varying trustworthiness. The model axioms have dependencies on the initial social communication network, which abstractly describe how people communicate with each other. The message diffusion based on the axioms will vary accordingly to the defined network's density and connectivity.

ACKNOWLEDGMENTS

The authors acknowledge John H. Sorensen and Barbara Sorensen from Oak Ridge National Labs for their advice and expertise in natural hazards, emergency management, and warning systems. This material is based upon work partially supported by the U.S. National Science Foundation (NSF) under Grant Nos. 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 Center for Dynamic Data Analysis for Homeland Security 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, and no official endorsement should be inferred or implied.

REFERENCES

1. Aguirre, B. E. (1994) In U.S.-Russia Seminar on Social Research on Mitigation for and Recovery from Disasters and Large Scale System Hazards Newark, Delaware: The University of Delaware Disaster Research Center, pp. 210-240.
2. Ding, A. W. (2006) JDMS: The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 3.
3. Golden, J. H. and Adams, C. R. (2000) Natural Hazards Review, 1, 107-118.
4. Kelton, K., Fleischmann, K. R. and Wallace, W. A. (In Press) Journal of the American Society for Information Science and Technology.
5. Kelton, K. and Wallace, W. A. (2000) Computational & Mathematical Organizational Theory, 6, 361-379.
6. Kelton, K. and Wallace, W. A. (2003) In Proceedings of the 36th Hawaii Int. Conference on Systems Science.
7. Lindell, M. K. and Prater, C. S. (2004) In National Institute for Standards and Technology Workshop on Building Occupant Movement During Fire
8. Emergencies.Gaithersburg, MD, pp. 91-95.
9. Lindell, M. K. and Prater, C. S. (2007) Journal of Urban Planning and Development, 133, 18-29.
10. Mileti, D. S. (1999) Disaster by Design: A Reassessment of Natural Hazards in the United States, Joseph Henry Press, Washington, D.C.
11. Perry, R. W. and Lindell, M. (2003) Journal of Contingencies and Crisis Management, 11, 49-60.
12. Rogers, G. O., Shumpert, B. L. and Sorensen, J. H. (1990) Oak Ridge National Laboratory, Oak Ridge, TN.
13. Rogers, G. O. and Sorensen, J. H. (1991) Diffusion of Emergency Warning: Comparing Empirical and Simulation Results, Plenum Press, New York.
14. Sorensen, J. H. (1992) Oak Ridge National Laboratory, Oak Ridge, TN.

15. Sorensen, J. H. (2000) Natural Hazards Review, 1, 119-125.
16. Sorensen, J. H. (2003) In DIMACS Working Group on Modeling Social Responses to Bio-terrorism Involving Infectious Agents DIMACS Center, CoRE Building, Rutgers University.
17. Sorensen, J. H. and Mileti, D. S. (1987) International Journal of Mass Emergencies and Disasters, 5, 33-61.
18. Sorensen, J. H., Vogt, B. M. and Mileti, D. S. (1987) In Federal Emergency Management Agency Oak Ridge National Laboratory.
19. Vogt, B. and Sorensen, J. H. (1999) Oak Ridge National Laboratory, Oak Ridge, TN.