Establishing Trust Management in an Open Source Collaborative Information Repository: An Emergency Response Information System Case Study

Evren Eryilmaz  
Claremont Graduate University  
evren.eryilmaz@cgu.edu

Mitch Cochran  
Claremont Graduate University  
mitch.cochran@cgu.edu

Sumonta Kasemvilas  
Claremont Graduate University  
sumonta.kasemvilas@cgu.edu

Abstract

This paper explores the design and evaluation of a trust model to establish trust management in an open source collaborative information repository for an emergency response environment. The proposed model is an instantiation of the SECURE framework and it is based on the characteristics of trust defined by recent information systems research. Evaluation of the model is based on a case study of a drill conducted by a city in Southern California. The results suggest that the proposed model might be useful to provide timely action plans for specific types of incidents based on the level trust and risk. However, a common terminology among involved organizations must exist prior to implementing the proposed model. In addition, information is volatile in an emergency response environment and rapid changes in conditions influence the consensus among entities. Therefore, verifying the accuracy of the emergency information used by the proposed model is essential to establish trust management in this particular context.

1. Introduction

Collaborative information repositories are becoming increasingly common because new open source content management systems allow a cost effective way of creating and maintaining shared content. Within these repositories, collaborating participants are autonomous in regards to what they contribute because any participant can edit information that he or she thinks is incomplete or poorly organized [1]. Prior research considers this particular characteristic as a source of strength as well as weakness [2, 3, 4, 5, 6, 7, 8]. On one hand, participants can express their voices easily by editing and organizing the shared content with a Web browser. Therefore, the contributions of good intentioned and careful participants can expand and improve the content of the shared repository. On the other hand, it is a challenge to convert individual skills and efforts into a collaboratively generated information repository because participants may have different levels of knowledge and writing ability [9]. Thus, information provided by different participants may have varying quality. Furthermore, content accuracy may be transitory due to rapid change [2, 7]. In this context, trust management becomes an important issue because without some form of trust management collaborative information repositories face the difficulty of defending their level of correctness and authoritativeness [4, 10].

Another characteristic of collaborative information repositories is the scale of the group. On one hand, a repository may accept contributions from a diversity of participants who are not known to potential end users. For instance, Wikipedia has 6,827,080 registered users as of April 6, 2008 [11]. This particular repository is based on the assumption that valuable content can be created when good intentioned and careful users outnumber bad intentioned and careless users [12].
Wikipedia puts trust in the collective knowledge of a large-scale distributed community hoping that “given enough eyeballs all bugs are shallow” [3, p. 5]. Hence, Wikipedia’s technical implementation does not provide a gate keeping function to ensure quality material is being contributed [13]. On the other hand, a repository may also allow contributions from only registered users in certain roles to prevent potential vandalism by anonymous users. Furthermore, an editor-in-chief may be responsible for the accuracy of the content. For example, students may write a document collaboratively in a class and the instructor may act as the editor-in-chief.

Recent events such as September 11 and Hurricane Katrina highlighted communication as the primary challenge in responding to emergency situations [14, 15, 16]. Although there have been arguments on the suitability of open source collaborative information repositories for emergency response [17], organizations acting in this particular environment are limited by their institutional and technical capacity when selecting an emergency response information system. Furthermore, the success of Sahana, an open source emergency response information system developed in Sri Lanka immediately after the Indian Ocean tsunami, clearly motivates our intention to use an open source information system in this paper. A group of Sri Lankan IT industry volunteers initially built Sahana in three weeks before it became a part of the official portal for Center of National Operations. Some of the rewards Sahana received include the Red Hat User Award and nomination for the SourceForge Project of the month in June 2006 [18].

This paper focuses on a temporary electronic group of professionals, volunteers, and untrained observers who previously have not worked together respond to an emergency situation, and it seeks to provide a measure of confidence in the accuracy of information developed by this group in a collaborative information repository. We investigate how to enable trust management in an open source collaborative information repository for an emergency response situation while still maintaining the ease and efficiency of user contributions.

There are six sections in this article. The following section describes trust, temporary electronic groups, emergency response information system, and the relationship among them. The third section explains the related scholarship. The fourth section identifies the proposed trust model. The fifth section evaluates the proposed model through a case study approach. The paper concludes with a discussion of the findings and implications for future research.

2. Trust, Temporary Electronic Group, and Emergency Response Information System

This section looks at three core concepts: Trust, temporary electronic group, emergency response information system, and the relationship among them.

2.1 Trust

As an interdisciplinary research area, trust has many definitions in a wide range of domains from sociology and psychology to political and business science, and these definitions may change according to the application domain [19, 20, 21]. For instance, sociologists consider trust as a social structure; psychologists recognize trust as a personal trait; economists see trust as a mechanism of economic choice and risk management [21]. Recent information systems research referred to the following definitions to describe trust.

- A particular level of the subjective probability with which an agent will perform a particular action both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action [22, p. 217].
- The willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party [23, p. 712].
- A subjective assessment of another’s influence in terms of the extent of one’s perceptions about the quality and significance of another’s impact over one’s outcomes in a given situation, such that one’s expectation of, openness to, and inclination toward such influence provide a sense of control over the potential outcomes of the situation [24, p. 43].

These definitions point out that trust is subjective because every individual makes his or her own decision to trust.

Other characteristics of trust used in recent information systems papers are context dependent, composite property, dynamic, and measurable. Context dependent means that trust in one environment does not directly transfer to another environment [25]. For instance, Alice may trust Bob as her car mechanic to repair her car, but not as a baby sitter. Composite property indicates that trust is based on a composition of different factors depending on the environment [21]. Dynamic specifies that trust is sensitive to the changes...
in a context [26]. Finally, measurable states that the level of trust can be represented by a continuous real number [27]. This characteristic also provides the foundation for trust modeling. However, it should be noted that trust may have other characteristics based on the application domain. In this context, Rousseau, et al. [28] examined the overlap and synthesis in the scholarship on trust.

This paper views trust as a dynamic domain-specific belief or attitude held by an individual concerning confidence in the accuracy of collaboratively created and updated content. Trust is essential for professionals and volunteers operate as a collective in a crisis because it promotes open, substantive, and influential information exchange [29], which increases the likelihood that constructive controversy among entities will result in information useful for decision making.

2.2 Temporary Electronic Group

A temporary electronic group is formed around a clear purpose and common task with a finite life span [30] and its members interact primarily through computer-mediated communication. The term “temporary” means that members may have never worked together before and they may not expect to work together again as a group [31].

In an emergency response environment, the nature of a crisis is the primary factor that often requires forming temporary electronic groups. Furthermore, the members of these groups are trained to perform a number of different roles because it is never certain who will take on which role or which combination of roles in a crisis [32].

Since temporary electronic groups for emergency response come together to help victims in high stress situations, group members have a limited amount of time to become familiar with each other [33]. Therefore, they rely on a high level of activity in order to manage ambiguity, risk, and points of vulnerability regarding a collaboratively evolving information repository.

2.3 Emergency Response Information System

An emergency is typically characterized as unpredictable in terms of unforeseen events which evolve as a result of the nature of a crisis, exact actions and responsibilities of individuals, and exceptions to a planned response [34]. Information systems aid in the management of emergency response by facilitating the information flow, decision making, and coordination management [35, 36]. According to [32], an emergency response information system is a structured group of communication systems where the protocols and communication structures are provided, but there is little content about a particular crisis situation except as an integrated electronic library of external data and information sources (p. 10).

An effective emergency response information system should provide timely access to comprehensive, relevant, and reliable information in order to help emergency responders to collect, analyze, disseminate, and act on key information to better meet the needs of victims [15, 17]. Although it is never certain who will perform which role or which combinations of roles in a crisis, actions and privileges of the roles need to be well defined in the software. In addition, emergency responders must be trained to act as a collective by using the software when they assume multiple or changing roles [32].

3. Related Literature

This work is based on general literature in two areas: designing an effective emergency response information system and the issue of trust for collaborative information repositories.

From an emergency management perspective, prior research considers coordination and dissemination of timely and accurate information as major challenges for designing effective emergency response information systems [37]. In this context, Shen et al. [38] used coordination theory and theory of task-technology fit to examine the impact of information system design on emergency coordination requirements. Their findings suggest that the capabilities of an emergency response information system should support coordination mechanisms. Turoff [32] provided a framework based on nine premises to assist researchers and practitioners think about issues prior to designing a flexible and dynamic emergency response information system. Following Turoff [32], Chen et al. [37] investigated both single- and multi-incident scenarios and they presented a set of principles for designing an effective emergency response information system.

There have been a number of studies that address the trust challenge in collaborative information repositories and, due to its popularity, most of them were quantitative studies focused on Wikipedia. Although these approaches were not intended to support trust management in emergency response, this paper uses an open source system similar to Wikipedia and to the best of our knowledge establishing trust management in an open source collaborative information repository for emergency response has not been investigated. Therefore, we reviewed the
literature on Wikipedia to identify how researchers approached the issue of trust in Wikipedia and to what extent these approaches could be applicable to emergency response. Lih [13] approached Wikipedia from a participatory journalism perspective and he found that when Wikipedia articles are cited by the press their quality, which was measured indirectly by the total number of edits (rigor) and the total number of unique editors (diversity), increased quickly. Viegas et al. [2] used a history flow visualization tool to identify five types of vandalism that could reduce the quality of active Wikipedia articles: (1) Mass deletion suggests removing all or a significant percent of an article; (2) Offensive copy refers to adding inappropriate words; (3) Phony copy means inserting text that is not related to a page topic; (4) Phony redirection implies redirecting to an unrelated page; (5) Idiosyncratic copy indicates adding biased information. Stvilia et al. [3] considered quality as fitness for use and the authors identified ten information quality problem types encountered by the Wikipedia community and the types of user information activities that might be affected by those problems. McGuiness et al. [4] indicated that user rating schemes may not be sufficient to determine the trustworthiness of a collaborative information repository because an article rated trustworthy may not still be trustworthy if modified. In this context, McGuiness et al. [4] assumed that Wikipedia articles could be segmented into a sequence of text fragments and they considered a fragment of an article as a collection of text in the article which was contributed by one author in one revision. To address trust issues, McGuiness et al. [4] used two citation-based trust algorithms, the link-ratio algorithm and the page-rank algorithm. Citation-based trust suggested that a well cited article might be more trustworthy than an article with no citations. On one hand, the authors defined the link ratio of an article (i.e., the page with title x) as the ratio between the number of citations and the number of non-citation occurrences of the encyclopedia term x. On the other hand, the authors viewed page-rank as a reflection of the relative popularity of an article in a collection of articles. However, the authors indicated that neither the link-ratio algorithm nor the page-rank algorithm was effective enough alone for computing trustworthiness. The authors found that the link-ratio result could be dependent on how common a term was and how much it required supplemental information. Therefore, the authors could not determine whether low link-ratio was due to untrustworthiness. In addition, the authors showed that a page with a low rank value could have a higher link ratio value than a page with a high rank value. Zeng, et al. [10] investigated the revision history of a Wikipedia article to compute trust value for the article. Their main assumption was that an article might gain or lose trustworthiness based on author trustworthiness. Therefore, the researchers used author trustworthiness as an input. In order to model how trust evolved through article revisions, the authors used dynamic Bayesian networks. The results of the study showed a significant improvement over citation based trust. In comparison to Zeng et al. [10], Adler et al. [39] computed author reputation as output and suggested that author reputation could be used for two purposes: (1) An indicator of quality of fresh text; (2) To manage author activity by means such as preventing low reputation authors from editing certain pages. Dondio et al. [6] argued that the fast changing nature of Wikipedia articles complicated calculating trust values based on past evidence. They supported their claim by referring to another study which found that user past experience with a Web site is only the 14th most important among the criteria used to assess the quality of a Web site [40]. In this context, Dondio et al. [6] investigated how to evaluate the trustworthiness of Wikipedia articles by relying exclusively on their present state. These Wikipedia-oriented studies point out two factors to calculate trust in an emergency response environment. The first factor, author trustworthiness, implies that a piece of information gains or loses trustworthiness based on author trustworthiness. In an emergency response situation, decisions are made with incomplete and sometimes contradictory information because accurate and complete information is rarely available in the beginning and only over time does a more clear picture emerge [37]. Therefore, emergency responders are more likely to trust to professionals than volunteers. The second factor is considering the present state of information. Emergency response is a dynamic environment that is measured in minutes and seconds [16]. Sudden and unexpected changes in a crisis can affect the validity of the present information available in the collaborative repository for decision making. Hence, the time nature of the present information available in the repository should be taken into consideration when calculating a trust value for emergency response information.

4. Trust Model

This section identifies the conceptual model of a trust algorithm based on the SECURE framework and
it presents a common incident as an example to facilitate our discussion on the proposed model.

SECURE is a trust/risk-based security framework that aims to provide entities with a basis for reasoning about trust and risk when there is uncertainty about the outcome of an interaction [41]. Two high level processes run parallel to each other in the SECURE framework. The first high level process, the decision making process, helps an entity to decide what action to take due to a request made by another entity. There are two components in the decision making process: Trust engine and risk engine. The trust engine dynamically assesses the trustworthiness of the requesting entity based on evidence such as observation or recommendation [41]. The risk engine dynamically evaluates the risk involved in the interaction and chooses the action with appropriate cost-benefit for the decision maker. The second high level process, evidence processing, gathers recommendations and comparisons between expected outcomes of the chosen actions and real outcomes [42]. This evidence is used for trust and risk related calculations and it is collected in the evidence store.

Based on Cahill et al. [43], SECURE can be adapted to a variety of application scenarios. The model proposed below is an instantiation of the SECURE framework to establish trust management in an open source collaborative information repository for an emergency response environment.

The trust model shown in Figure 1 acknowledges that an algorithm which establishes trust management for collaboratively created and modified information repositories should reflect the characteristics of trust, consider the factors that influence trust, and support trust management in a feasible way [21]. We consider trust management as the activity of collecting, codifying, analyzing and evaluating evidence relating to competence, honesty, security, or dependability with the purpose of making assessments and decisions regarding trust relationships [44, p. 147].

In this model, assessing the trustworthiness of collaboratively created and modified information starts with the monitoring module by noticing a change in a collaboratively written page and notifying the data retrieval module to collect information from the database. Then, the context recognition module examines the retrieved information to identify its context. The trust calculator needs context information because context influences weight of trust factors. For instance, trust in shared content may be influenced by information quality problems defined by Stvilia et al. [3], but the impact of different problems could be various in dissimilar contexts.

Based on the context information, the trust calculator acquires trust factors and their weights in the relevant context from the evidence store. This model uses two trust factors: author trustworthiness and information timeliness. The first trust factor, author trustworthiness, refers to the identity of the emergency responder who provided the information. Author trustworthiness may provide confidence on a piece of information to a decision maker because emergency responders rapidly process incomplete and sometimes contradictory information to take immediate mitigating action under conditions where error tolerance is extremely low. In this model, the weight of the author trustworthiness depends on emergency responders’ role. A role can be professional, certified volunteer, or untrained observer.

The second trust factor, information timeliness, indicates when an author contributed a piece of information to the collaborative information repository. Due to the time dependence of emergency response, a piece of information may lose its validity over the course of minutes based on the dynamic nature of a particular situation. Therefore, providing the timeliness of the present information available in the collaborative repository may assist emergency responders to determine whether they are using the most current information to make a decision. In this model, the weight of the information timeliness decreases as time passes to indicate that a piece of information may not reflect the changes in an incident.

Afterward, the trust calculator analyzes the information content by using the trust factors and it estimates a continuous real number trust value which represents confidence in the accuracy of information content.

The risk evaluator needs context information too because context also influences situations involving risk. Similar to Grandison et al. [44], this paper views risk as “probability of failure with respect to the context of the interaction” (p.147). The model links trust to risk because the degree of trust implies a certain amount of risk which an entity may or may not
accept. In general, if there is low trust in the information, then the higher the risk. From this perspective, the purpose of the risk evaluator is to recognize the risks properly and communicate them effectively to all entities in an emergency response situation. To do this, the risk evaluator refers to the evidence store to get the knowledge acquired from similar prior incidents to estimate the probability for a hazard to occur in the current emergency situation.

The evidence store contains all trust and risk related data defined by local rules. Entities with certain roles could use the specification editor to either create and/or edit the data stored in the evidence store. The algorithm has two outputs: The context specific continuous real number trust value and the probability of a hazard to occur in the current emergency situation.

Although trust is subjective in nature, the output of this algorithm could provide information that will enable one to make a better decision whenever a decision is to be made. Furthermore, trust is also dynamic in nature. Therefore, the monitoring module is dedicated to observe the changes in the collaborative information database and it starts the entire process again when an entity changes a collaboratively written page.

To facilitate our discussion on the proposed model, we have developed a scenario involving a fire department response. In this scenario, we imagine a resident (untrained observer) detecting an incident and creating a new page in the collaborative information repository with the title “sighting of smoke”. The monitoring module recognizes this newly created page and it notifies the data retrieval module to collect the information posted on the page such as incident name, source of information, actions needed, and time stamp from the collaborative information repository database. Then, the context recognition module uses natural language processing techniques to look for phrases such as single family residence fire or hazardous material incident to identify the context of the incident.

At this point, the context of the example is the sighting of smoke detected by an untrained observer, but not verified by a professional. The normal response of the fire department to this situation is to send a single fire engine to investigate the sighting of smoke. Based on this context information, the trust calculator acquires trust factors and their weights in this particular context from the evidence store. The first trust factor is author trustworthiness, and untrained observers will generally have a weight less than certified volunteers and professionals because the information they provide may be biased by their lack of training, lack of comprehension, background, and/or verbalization [37]. However, the specific numerical value of the weight will depend on the priority of the incident because a higher priority incident such as a wildfire or freeway accident in some sense requires more resources (fire engines, personnel) than a single trashcan fire.

The second trust factor is information timeliness, and it indicates the time incident detection took place by an untrained observer at a given time. Although the completeness of information at this stage is low, it is the most current information to this point. Therefore, the weight of information timeliness of the incident detection will be high. But this weight will decrease over time depending on the dynamic nature of the type incident determined in the evidence store.

Based on these two factors, the trust calculator will use a mathematical formula which reflects the relationship between author trustworthiness and information timeliness within the given context, and it will estimate a continuous real number trust value to represent confidence in the accuracy of information content.

In this scenario, the sighting of smoke could indicate the following situations: Barbeque, trash fire, house fire, factory fire which could possibly include hazardous components. We assume hazardous materials as a risk in fire department response because the detection of hazardous materials requires fire fighters to change their strategy when dealing with the fire. In order to assess the probability of detecting hazardous materials within the given context, the risk evaluator examines past responses to similar incidents in the evidence store and calculates the probability of detecting hazardous materials in the current incident based on city zoning guidelines. The risk factor would change depending on the location of the smoke. For example, a light industrial zone would have a higher risk of hazardous material compared to residential area.

In emergency response, decisions are time sensitive [16]. From this perspective, incorrect decision making can lead to a fault in resource allocation and it will take time to recover the resources for other uses [32, 45]. Therefore, the focus of the model is to both help lower response times and provide a more efficient resource allocation. The model has two outputs in this scenario. The first output is to provide decision makers confidence in the accuracy of information that they use when they make a decision. The second output is to assist emergency responders with their risk assessments by making the potential risk involved in this scenario explicit. The table below represents possible responses to the scenario based on the level of trust and risk.
Table 1. Responses for trust and risk levels.

<table>
<thead>
<tr>
<th></th>
<th>Low Trust</th>
<th>High Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Risk</td>
<td>Response depends on available resources</td>
<td>Full or greater response</td>
</tr>
<tr>
<td></td>
<td>If there is good availability then full response for that type of incident</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If there is poor availability then limited response for that type of incident</td>
<td></td>
</tr>
<tr>
<td>Low Risk</td>
<td>Send one fire engine to investigate</td>
<td>Full response for that type of incident</td>
</tr>
</tbody>
</table>

5. Evaluation of the Trust Model

This section identifies how the proposed model could be implemented in an emergency response environment. The case study explained below is based on a mass casualty drill and small city Emergency Operations Center (EOC) activation.

The mass casualty drill was held at the training tower of Monrovia Fire Department’s Station 102. The stated objective of the drill was to address lack of communication among agencies during an emergency response. The participants in the mass casualty drill and EOC activation included:

- City of Monrovia: Fire Department, Police Department, and all departments as part of the EOC
- Monrovia Unified School District
- Schafer Ambulance: Responsible for transporting medical patients within the City of Monrovia
- American Red Cross: Disaster Coordinator
- Arcadia Methodist Hospital: Emergency room, Continuing Education Coordinator

To improve communication among these participants, we used Drupal as an open source content management system to build a collaborative information repository as a proof of concept with three main parts: volunteer tracking, patient tracking, and incident tracking.

The first part, volunteer tracking, focused on capturing volunteers’ capabilities, their present locations, and the tasks they are involved in during the drill. The second part, patient tracking, aimed at monitoring the number of patients, their conditions, and the hospitals they go to.

The last part, incident tracking, addressed sharing necessary and current information among all entities to manage incidents. This feature of the system was similar to a Wikipedia article in the sense that each incident became a written description about what was happening. All entities affected by the information on an incident page were encouraged to update anything that they thought was incomplete, inaccurate, or poorly organized.

The access to the system was controlled by a virtual private network connection into the City’s network. The remote participants only needed a browser and connection to the internet.

Considering the small scale of the drill and the explorative nature of our study, we conducted semi-structured interviews with Monrovia Fire Department personnel at the mass casualty scene, Monrovia City EOC. Feedback received from the Monrovia City EOC indicates that the main issue during the drill in regards to trust was information inaccuracy. The community services director stressed that

*After the briefing I can come back and say that the information we received is actually not accurate. We need to verify what has been said.*

Therefore, the Monrovia City EOC staff specified that they need to have some form of corroborative evidence to verify the accuracy of the information.

In a crisis there are requests for resources and incident commander has to decide if a request can be satisfied right away or has to be denied or delayed [34]. In this drill, the incident commander’s evaluation of the request was based in part on his trust of the information contained in the request and in part on the source of request. In regards to the source of the request, the battalion chief indicated that he had little trust in untrained observers (public) who report seeing smoke or smelling gas, more trust in certified volunteers and outside firefighters, and full trust in Verdugo Dispatch (joint dispatch for thirteen cities) and Monrovia Fire Department personnel.

When evaluating risks in dangerous and dynamic environments, the battalion chief expressed that a commanding officer uses his or her field experience that may not be a part of the regular training activity. An incident commander places a high level of trust in his or her own experience because a person probably trusts in himself or herself more than others. From this perspective, transforming tacit knowledge into explicit knowledge and storing the resulting explicit knowledge in a repository (evidence store) must be taken into consideration for the risk evaluator module in the proposed model.

As for the application of the trust model to this particular case, the Information Systems Manager in the EOC staff remarked that the trust model could be integrated to the open source collaborative information repository as a decision support tool for all agencies participating the drill. Thus, he suggested that the evidence store should be pre-loaded with response
policies, rules, and pre-action plans so it can provide timely action plans for specific types of incidents based on the level of trust and risk.

Although Monrovia Fire Department personnel, Monrovia City EOC staff, and American Red Cross staff played different roles in the mass casualty drill, they all agreed on three areas. First, the incident information put into the system was volatile due to rapid changes in conditions. Therefore, users trusted a piece of information more when it received more updates since there would be corroborative evidence. Second, interoperability was an issue on the pages because different organizations used different terminologies and drill participants did not trust the information that they did not understand. In this context, communication difficulties led to lower trust. Third, the proposed model and the developed system were more applicable to larger incidents because small incidents are cleared before the application or resources could be deployed.

6. Conclusion

Trust is difficult to understand because it is influenced by many factors and the weight of the factors could change depending on the context. Although trust management and Wikipedia as a common collaborative information repository have received a lot of attention, to the best of our knowledge, establishing trust management in an open source collaborative information repository that aims to improve communication among various organizations in an emergency environment has not been investigated.

This explorative study proposed a trust model and evaluated it through a case study which took place during a mass casualty drill and small-city Emergency Operations Center (EOC) activation. In an emergency environment, information is volatile due to rapid changes in conditions. This characteristic is important for assessing trustworthiness of collaboratively created and maintained information because the changes in conditions influence the consensus among entities. This is why the Monrovia City EOC staff wanted to see some form of verification in order to trust the information posted on an incident page because information inaccuracy implied to them the risk of making inefficient resource allocations. In this context, establishing a checkpoint within certain time intervals to synchronize the information among entities could verify that the trust model is using accurate information and provide corroborate for reported information.

Another implication of this study is the need to establish a common terminology among participating organizations. This assertion echoes the work of [45, 46]. In this drill, each organization used its own terminology when contributing information to collaboratively written pages. Not understanding the terminology used on a page implied lack of trust on the information content.

A decision support system for emergency response should have mechanisms to provide decision makers appropriate inputs to resolve emerging conflicts and propose optimal solutions [37]. The model proposed in this paper used trust calculator and risk evaluator as mechanisms to help decision makers under conditions where error tolerance is low.

The application of the trust model to this particular case suggests that the proposed model might be useful to provide timely action plans for specific types of incidents based on the level of trust and risk.

A limitation that we acknowledge in this study is the generalizability of the proposed model. Trust is context dependent, therefore the proposed model may not be applicable to other situations. Furthermore, the following issues must be taken into consideration before the proposed model can support the main objective of the current work: Establishing a common terminology among participating organizations, building a knowledge repository for the risk evaluation module, and testing the proposed model in a larger scale drill.

7. Acknowledgments

We would like to thank to the participants in our study for their cooperation and Lorne Olfman for his critical comments that have improved the paper.

8. References


Information, Communication, and Transportation,”  


[38] S. Y. Shen and M.J. Shaw, “Managing Coordination in Emergency Response Systems with Information Technologies,”  


