A CBRN Detection Framework Using Fuzzy Logic

Ahmed Nagy
SCK•CEN
ahmed.nagy@sckcen.be

Lusine Mkrtchyan
SCK•CEN
lmkrtchy@sckcen.be

Klaas van der Meer
SCK•CEN
kvdmeer@sckcen.be

ABSTRACT

Identifying a chemical, biological, radiological, and nuclear incident (CBRN) is a challenge. Evidence and health symptoms resulting from CBRN malevolent incident overlap with other normal non malevolent human activities. However, proper fusion of symptoms and evidence can aid in drawing conclusions with a certain degree of credibility about the existence of an incident. There are two types of incidents directly observable, overt, or indirectly observable, covert, which can be detected from the symptoms and consequences. This paper describes a framework for identifying a CBRN incident from available evidence using a fuzzy belief degree distributed approach. We present two approaches for evidence fusion and aggregation; the first, two level cumulative belief degree (CBD) while the second is ordered weighted aggregation of belief degrees (OWA). The evaluation approach undertaken shows the potential value of the two techniques.

Keywords

Data mining, Crises management, Decision support, Disaster management, Fuzzy set theory.

INTRODUCTION

The danger of launching chemical, biological, radiological, and nuclear (CBRN) malevolent incidents has grown in the previous years (Van der Meer 2003). A malevolent CBRN incident can easily disrupt social life. Several governments have set up initiatives to be prepared for CBRN malevolent crisis, few to mention, the United States of America, India and the United Kingdom (Fisher 2007). Our work aims at developing a framework for the discovery of CBRN malevolent incidents. In this paper, we focus on the radiological malevolent incidents, also known as an RDD (Radiological Dispersion Device) incident. However, the framework presented is capable of handling and fusing evidence relevant to CBN incidents, as well. We start by presenting a decision support system based on cumulative belief degree approach. We collect the relevant attributes to make decisions about the existence of an RDD incident. It is essential to have an estimate for the existence of a radiological attack or the possibility of one happening since this triggers several crises management procedures. The main procedures relevant to a radiological incident are the sheltering, evacuation, medical screening, external and internal decontamination, risk communication and stress relief (Hardeman, Rojas-Palma, Sohier, Van Der Meer, and Bendam 2007).

In this study we apply cumulative belief degree fuzzy set approach for CBRN event identification. Our contributions can be stated as presenting an effective approach to deal with uncertain, missing and incomplete data. The rest of the paper is organized as follows. We start by analyzing several definitions of terrorism. Then we present our framework and problem modeling. The section identifies the observable indicators discussed by the CBR Central Intelligence Agency (CIA) handbook (CIA 1998) and the Triage monitoring and treatment (TMT) Handbook (Rojas-Palma et al 2009). Afterwards, we explain the two techniques developed for evidence fusion and aggregation. The last section presents our conclusions and future work.

TERRORISM DEFINITION

This section analyses several definitions of terrorism. This will help perceive the core goals of a terroristic attack. As a result, we can develop more efficient techniques for evidence fusion and situation assessment (Biermann 2009). Ganor defines terrorism as actions that seek to achieve political goals by instilling fear and

anxiety among the target population (Ganor 2005). On the other hand, Horgan refers to terrorists through the following quotation: "while they have some ultimate set of political objectives, it is an immediate goal of most terrorist groups to cause terror" (Horgan 2005). On the other hand, Hoffman defines terrorism as "deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change. All terrorist acts involve violence or the threat of violence. Terrorism is specifically designed to have far-reaching psychological effects beyond the immediate victim(s) or object of the terrorist attack. It is meant to instill fear" (Hoffman 2006). It is clear from the definitions presented that spreading fear, doubt and insecurity is a main goal for any terroristic attack or threat.

The challenge is to process several small pieces of information and evidence to assess the risk of launching an attack or discovering an existing one; thus, limit the impact of an attack and contain it as early as possible. Reducing the effect of a terroristic attack entails discovering it rapidly, which is part of our goal through presenting the evidence fusion framework. Orphan sources present valuable examples of radiological incidents that can be used with malevolent intentions. An orphan source is defined as "a self-contained radioactive source that is no longer under proper regulatory control" (UNSCEAR Report 2008). We observe that covert incidents were usually discovered through the medical consequences resulting from exposure to the radiological source.

FRAMEWORK FOR INCIDENT DISCOVERY

Figure 1 shows the high level design of the proposed framework. There are different types of information sources such as reports (first responders, witnesses, etc.), inspections (experts) and open sources (newspapers, television, social media, etc.). The framework does not compute the credibility of the source which is out of the scope of this work; for further details on credibility calculating and ranking the reader can refer to (Rein, Frey, Schade, and Kawaletz 2010). Each source has a credibility value per category. This reflects the specialization of knowledge for each expert regarding a topic or category (explained in subsection "Credibility Values for the Experts"). The experts and the first responders give their evaluations for the attributes with different data structures, such as, linguistic terms, crisp numbers, interval values and belief distribution over linguistic terms. In general the number of linguistic terms to be used depends on the problem domain.

In our problem we chose three level linguistic values (High, Medium, and Low) for the attribute importance and five level linguistic terms (Very Low, Low, Medium, High, Very High) for the attribute evaluation. The expert distributes his/her beliefs regarding a set of linguistic terms when he/she hesitates between linguistic terms. For example, the expert may have belief of 80% that the given attribute is 'High', and 20% belief for 'Very High'. Notice that the sum of belief degrees for a given attribute may be also less than 100%, which indicates the incompleteness of the evaluations. The incompleteness can have several reasons; for example, it can be due to the lack of knowledge about the attribute, or the lack of expertise of the expert. Evaluating the attributes relevant to a specific category is dependent on the expertise of the expert. Even if the expert has low expertise to judge an attribute according to its relevance to the problem this should be mitigated by collecting information from different experts and sources; thus, the redundancy in the data collected should guard for misleading information; for more details on specifying values for an attribute (Kabak and Ruan 2011).

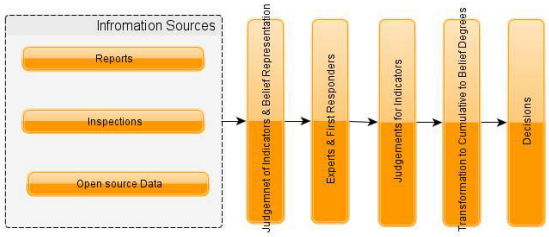

Figure 1. Process of Data Collection and Decision Making

Table **1** provides a comprehensive list of observable attributes that reflect the existence of an RDD incident. The attributes collected are based on the CIA and TMT handbooks for radiological incidents. We further asked two radiological experts to evaluate the importance of the attributes collected in assessing the existence of an RDD incident. The attributes collected are clustered in six categories. We present two approaches for aggregating the values of the attributes either per category or through following a flat hierarchy, where we aggregate the values for all the attributes presented without enforcing hierarchies on them. In the hierarchical framework there is a possibility to choose the categories included in the final aggregated summation. The choice

of the categories can be further tuned by specifying how many attributes should be receiving a specific value for example a high to include the category above them in the aggregation.

Category	Observable Symptoms & Reported Attribute	Importance
Dispersion technique	Spill fire	High
	Explosion	High
	Spray of Aerosol	Low
Measurements	Alarming dosimeter	Medium
	Elevated reading on dose rate meter	High
	National Radioactivity Surveillance System	High
	Elevated reading on a contamination monitor	High
Health	People with symptoms consistent with radiation exposure	High
	Vomiting frequently	High
	Diarrhea	Low
	Nausea	Low
	Burns	High
Signs	Containers or packages having radiation symbols	High
	Geographically spatially correlated individuals experiencing similar health symptoms.	Medium
	Presence of unjustified metallic packages with no obvious reason	Medium
	Transport accident involving a vehicle with radiation	High
Material	Heat emitting material	High
	Glowing material/particles	High
Miscellaneous	Intelligence information	High
	Stolen/ Lost sources	High

Table 1. The List of Radiological Dispersion Device Categories and Attributes.

The model captures the limitation of knowledge of an expert through giving him/her the option to assign no knowledge and no information to a given attribute. In case of no information the expert did not collect evidence regarding the attribute at hand yet no knowledge means that the expert does not have enough skills to give an estimate for the value of the attribute.

Credibility Values for the Experts

For the CBD the experts are given credibility weight per process, while for OWA the experts' credibility is not taken into account. CBD captures the specialization of the experts through ranking their credibility for different categories. In other words, each expert has a specific degree of expertise and knowledge related to a process. For example, a medical doctor is considered to have a high credibility factor for categories relevant to health. The same medical doctor will have lower credibility value with respect to measurements. A credibility matrix is defined as an $n * m$ matrix, where the credibility of n experts or information sources is recorded for m type of categories, which reflects the concept of specialization per expert per category.

AGGREGATION ALGORITHMS

Our framework relies on two aggregation algorithms 1) two level cumulative belief degree (CBD) and 2) ordered weighted aggregation of belief degrees (OWA). The main differences between the two approaches are presented in Table 2. As we have already discussed in the previous sections, in this framework the data is collected from different sources that provide their evaluations with different data structures. Each data structure is transformed to a belief degree distribution structure. We build our work on the belief structures presented in (Kabak et al. 2011). Note that we do not detail the algorithms here; we only describe the main procedures. The output for the CBD module is a graph showing the following bars (category name, aggregation score, aggregated reliability). The category name belongs to the field category illustrated in Table 1. While aggregated score is the score accumulated describing the existence of attributes relevant to the category at hand.

Aggregated credibility is the combined reliability in the decision factor that results from summing the credibility of a piece of information fed as described in subsection "Credibility Values for the Experts". For example, a graph showing the value of measurement "4" on a scale of "6" with a reliability of 90% can be considered as a high level of radioactivity and that is pretty reliable evidence (measurement, 4/6, 90%). Including other categories in the interpretation to judge the existence of an RDD is important. However, a high radioactivity measurement might be due to other reasons, for example, rain. As a result, it is important to inspect all categories thoroughly. On the other hand, OWA offers an aggregated score for the existence of an RDD. There are several ways, where this can be helpful. For first responder that suggests a need for wearing proper

protective equipment whenever an RDD is suspected to be taking place. Fast first aid and risk communication plans can be triggered to be delivered for the crowd. Thus, it is a useful approach to deal with terroristic threats at an early stage of the crises. The difference that OWA would offer is instead of calculating a score for every category all the categories are accumulated to contribute to one score, which can be used to judge the absence or the presence of an RDD incident. Table 2 offers detailed differences between CBD and OWA.

	CBD	OWA
Categories	Can be composed of several categories in our case (dispersion technique, measurement, health, material signs, miscellaneous) where the categories constitute the upper hierarchy and the attributes compose the lower hierarchy.	All attributes contribute to the aggregated belief degrees unconditionally. No category activation rules need to be specified.
Activation rules	There are activation rules that are used to consider the category active to include it in the belief aggregation.	We have a flat hierarchy no aggregation based category is presented.
Expert (Source) Credibility	Expert or source credibility is specified in rules that capture the credibility of an expert in a specific category.	The credibility of the experts is not captured in the model. Only expert evaluation is considered without including an evaluation of their skills in the model.

TABLE 2. DIFFERENCES BETWEEN CBD AND OWA

The Preparation Phase

This phase is common for both algorithms. The first stage of the framework models the problem and the indicators are specified. The data is collected from the sources and the experts give their evaluation for the values of the attributes for an incident. Algorithm 1 specifies the steps necessary to prepare the data model, the attributes and the measurements. Note that modeling the important attributes is done manually. However, there are automatic natural language processing techniques that can be used to extract important features from text in case of written reports. After the preparation phase the CBD algorithm can be run on the data collected or the OWA.

Preparation Phase

Step 1 Attribute specification and modeling

1. Attributes are specified for assessing the category.
2. Types of indicators are specified and the indicators are grouped according to these types.
3. Number of linguistic terms is determined, i.e., three level linguistic values or five etc...
4. Expectation values related to linguistic terms are specified i.e., the values to be specified for each attribute.

Step 2. Gathering expert evaluations

1. Experts investigate the evidence from several sources and make judgments for relevant RDD attributes.
2. The expert judgments are represented by belief structures according to approach presented in (Kabak et al. 2011).

ALGORITHM 1. COMMON PREPARATION PHASE

Cumulative Belief Degrees Approach

Following we list the main steps for calculating the cumulative belief degrees for a set of categories with attributes specified. Algorithm 2 describes the CBD algorithm that we modeled for the RDD incident at hand. The belief degrees are represented per category. This can give the first responders an overview of the situation which can be used to make decisions for triggering more investigations for either specific category or the whole incident in general.

Cumulative Belief Degree Calculation

Specify rules related to the activation of the category to include it in the final summation

Credibility of experts is specified per category as described in Table 1.

Belief structures of the experts are aggregated by using the belief structure related to each attribute.

Fulfillment of each activation rule is calculated.

Accumulated belief degree per category at each linguistic term is computed.

The final result is computed by aggregating the belief degrees.

Presentation of the results to the decision maker(s).

Algorithm 2. Cumulative Belief Degree Calculation

Aggregations of Indicator Results through OWA Operators

For an RDD, it is crucial to use every piece of information. Since concluding the existence of an incident when there is no RDD threat is very costly. We prefer to give higher weights to high belief degree scores. However, we do not neglect low belief degrees since we use all possible information.

OWA calculation

1. Belief structures of the experts are aggregated by using the belief structure related to each attribute.
2. Accumulated belief degree for all the attributes specified at each linguistic term is computed.
3. The final result is calculated by aggregating the belief degrees.
4. Presentation of the results to the decision maker(s)

Algorithm 3. OWA Calculation

CONCLUSION

In this work, a new approach for evidence fusion for fuzzy linguistic terms is proposed. Two level cumulative belief degree and ordered weighted aggregation of belief degrees were proposed and applied on an RDD incident to reach a better understanding of the situation at hand (not presented due to space limitations). The importance of the techniques developed is to early detect threats of unconventional terroristic attacks, CBRN incidents. The benefit of the approach can be clear in helping first information receptors such as computer-aided dispatchers (CAD), who can look for more information and details from reporting citizens. It can also trigger preparation for emergency procedure. For the future work we aim at automating credibility ranking and applying the techniques developed in other incidents such as the chemical and biological case. Further, we will apply the approaches on real life scenarios to aid first responders.

ACKNOWLEDGMENTS

This work has been supported by SCK•CEN. We thank Dr. Johan Campus for the discussions we had with him which added to the value and the depth of the work. We are also thankful to the advice of Dr. Catrinel Turcanu which will enhance our further research. I am also grateful for Dr. Mercy Njima for checking the work.

REFERENCES

1. Klaas van der Meer. (2003) The radiological threat: verification at the source. Verification Yearbook.
2. Jochaim Biermann. (2009) Understanding military information processing Tan approach to support intelligence in defense and security. Harbour Protection through Data Fusion Technologies, pages 127-137.
3. CIA. (1998) Chemical, biological, radiological incident handbook.
4. U. Fisher. (2007) Deterrence, terrorism, and American values. Homeland Security Affairs, 3(1):1-17.
5. UNSCEAR Report . (2008) "Sources and Effects of Ionizing Radiation", United Nations.
6. B. Ganor. (2005) The counter-terrorism puzzle: A guide for decision makers. Transaction Pub.
7. F. Hardeman, C. Rojas-Palma, A. Sohier, K. Van Der Meer, and K. Bendam. (2007) Monitoring in case of emergency situations related to orphaned sources. International Journal of Emergency Management,

4(3):376-393.

8. K. Rein, M. Frey, U. Schade, and S. Kawaletz. (2010) Alarm for early warning: A lightweight analysis for recognition of menace. In Information Fusion (FUSION), 2010 13th Conference on, pages 1-7. IEEE.
9. Rojas-Palma, Carlos, et al. (2009) "TMT handbook: triage, monitoring and treatment of people exposed to ionising radiation following a malevolent act." Print: Lobo Media AS.