Safety Science 107 (2018) 62–76

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

# Tackling uncertainty in security assessment of critical infrastructures: Dempster-Shafer Theory vs. Credal Sets Theory

Alessio Misuri[a], Nima Khakzad[b,*], Genserik Reniers[b], Valerio Cozzani[a]

[a] Department of Civil, Chemical, Environmental, and Materials Engineering, University of Bologna, Bologna, Italy
[b] Safety and Security Science Group, Faculty of Technology, Policy, and Management, TUDelft, Delft University of Technology, The Netherlands

ARTICLE INFO

*Keywords:*
Security vulnerability assessment
Attack tree
Uncertainty modeling
Dempster-Shafer Theory
Bayesian network
Evidential network
Credal network

ABSTRACT

Securing critical infrastructures is a complex task. Required information is usually scarce or inexistent, and experts' judgments may be inaccurate and biased. In this paper, two methodologies dealing with data scarcity, imprecision, and uncertainty are presented: Evidential network and Credal network. Evidential network is a graphical technique based on Dempster-Shafer Theory to explicitly model the propagation of epistemic uncertainty among variables while Credal network is an extension of Bayesian network to deal with sets of probabilities, known as Credal sets, based on experts' judgments. Both methodologies constitute robust frameworks to account for high degree of imprecision on data, producing informative results despite the low-informative input. In the present study, the power in expressing uncertainty of these two methodologies have been showed, and their differences have been described through their application to a case study of security vulnerability assessment. Results demonstrate the substantial equivalence of the two methodologies in prognostic analysis, thus, an approximate updating procedure of Evidential network through equivalent Credal network has been proposed, to overcome the lack of possibility to compute updating in the context of Dempster-Shafer Theory.

## 1. Introduction

Since the 9/11 terrorist attacks, the concern about malevolent actions against critical infrastructures has remarkably grown. Indeed, before the tragedy of Twin Towers, the perception of risk was limited to unintentional events, as natural disaster or technical failures of critical systems (Baybutt and Ready, 2003). The discipline of security vulnerability assessment (SVA) is relatively young, and has been developed to provide guidelines and methodologies to highlight weaknesses potentially exploitable by adversarial agents to carry out high-consequences detrimental actions against critical assets. The chemical and process industry is one among the first industrial sectors where a number of methodologies were developed to mitigate the risk of security-related events (API (American Petroleum Institute), 2003; CCPS, 2003; Bajpai and Gupta, 2005). According to API RP-70 (API (American Petroleum Institute), 2003), the security risk is defined as the product of the magnitude of consequences caused by an attack, the probability that the attack will be carried out, and the success probability of the attack.

An attack's conditional probability of success has to be estimated considering the security system and its weaknesses. This step is commonly referred to as vulnerability assessment, and is a key step of the analysis. Vulnerability in security risk assessment refers to any weakness which can be exploited by a malevolent agent to gain access to an asset (API (American Petroleum Institute), 2003). Thus, elements to take into account in vulnerability assessment may include the location of the plant, the potential failure of physical protection systems, the equipment and its properties, and personnel practices. According to the majority of these methodologies, the determination of scenarios, and thus vulnerability assessments are based on semi-quantitative calculations, usually relying on experts' judgments. Multilateral competences and high expertise are needed because of the complexity of security issues. The required information embraces various fields, varying from technical to socio-political, whereas available historic data is scarce or even inexistent. Thus, the mission of security research is to develop methodologies able to provide reliable results despite the high level of uncertainty and subjectivity characterizing this field.

Attempts to efficiently deal with the inherent uncertainty of parameters in SVA have been made, usually based on probabilistic techniques and experts' judgement. Argenti et al. (Argenti et al., 2016) propose to adopt Bayesian network (BN) to model the effectiveness of security systems in process installations. Fakhravar et al. (Fakhravar et al., 2017) propose a vulnerability analysis based on attack trees (ATs)

* Corresponding author at: Jaffalaan 5, Delft 2628BX, Netherlands.
*E-mail address:* n.khakzadrostami@tudelft.nl (N. Khakzad).

https://doi.org/10.1016/j.ssci.2018.04.007
Received 16 November 2017; Received in revised form 3 April 2018; Accepted 13 April 2018
Available online 24 April 2018

**Nomenclature**

| | |
|---|---|
| SVA | security vulnerability assessment |
| IED | improvised explosive device |
| PPS | physical protection system |
| AT | attack tree |
| FT | Fault tree |
| BN | Bayesian network |
| DAG | directed acyclic graph |
| CPT | conditional probability table |
| CS | Credal Set |
| CN | Credal network |
| DST | Dempster-Shafer Theory |
| ET | Evidence Theory |
| EN | Evidential network |
| CBT | Conditional belief table |
| BBA | basic belief assignment |
| Pls | Plausibility function |
| Bel | Belief function |

and subsequent mapping through an innovative time-based BN. Clearly, BN is an attractive tool for this aim, because it is able to gather variables of various nature, and to probabilistically depict dependencies, intuitively expressing uncertainty.

A criticism against the use of probabilities is that they may not be easy to be assessed as point values. On the other hand, it may be more natural for experts to represent their opinion through comparative judgments, intervals of probability, or degrees of belief. Moreover, even if experts were able to directly convert their statements in probability values, numbers would be affected by epistemic uncertainty due to the impossibility of practically obtaining some information or clearly shaping dependencies. The objective of this paper is to specifically examine the applicability of two methodologies to deal with epistemic uncertainty and imprecision in SVA, and then comparing their features and outlining the differences between the two approaches. The present paper proposes a comparison between Dempster-Shafer Theory (DST) and Credal network (CN). DST allows to explicitly model the propagation of epistemic uncertainty among the variables of a system, depicted as an Evidential network (EN). This methodology may offer an intuitive framework to use low informative judgments to obtain reliable outcomes, keeping track of effects of the vagueness of input information on the obtainable results, through simple mathematical functions. On the contrary, CN is conceptually more similar to BN, and is based on the specification of sets of probabilities rather than on point values. These sets can be defined through geometrical figures whose edges can be directly reconstructed starting from comparative judgments, through mathematical procedures based on standardized interpretation of natural language. Both methodologies are suitable to produce robust outcomes from low informative input data. Therefore, these methodologies may be of great application to the field of SVA since SVA usually suffers from qualitative judgments, biased subjective data, and imprecise information.

As such, EN may allow to evaluate the quality of results, producing optimistic and pessimistic estimations of vulnerability via plausibility and belief concepts while CN may allow the specification of probabilities of primary events in a more robustly in the form of set of possible values. That being said, the novelty of the present study lies in the application of EN and CN to uncertainty modelling which has been unprecedented not only in SVA but also safety risk assessment.

After revisiting the background of AT, BN, CN, and DST in Section 2, the methodologies are applied to a case study in Section 3. Section 4 is reserved for the discussion of results, comparing the methodologies, and pointing out their shortcomings. Conclusions are reported in Section 5.

## 2. Background

### 2.1. Attack tree

AT is a hierarchical graphical framework to model attacks against a system, given some security constraints (Brooke and Paige, 2003). ATs have been outlined for the first time by Schneier (Schneier, 1999, 2000) in the field of informational technology. In his definition, ATs are powerful tree-shaped representations and offer a clear view of the security system and its components. For a solid mathematical definition of AT, the reader is referred to (Gribaudo et al., 2015). For the scope of this paper, it is sufficient to indicate that ATs are analogous to Fault trees (FTs) (US Nuclear Regulatory Commission, 1981) but that they are used for security risk assessment rather than of safety risk assessment (in case of FTs). AT makes it possible to model failure sequence of countermeasures, or success of intermediate steps of attack via AND and OR gates, shedding light on the vulnerabilities of security systems. It is worth noting that there are some differences between ATs and FTs. For example, the FT's structure is linked to the architecture of the system, so it is not mutable unless there is a change in the system, while AT's structure depends on the effect of countermeasures on attackers' preferences, and so it may change radically after each improvement of the security system (Gribaudo et al., 2015).

Fig. 1 depicts an AT for opening a safe. As shown in the figure, leaf nodes are various types of attacks, and the root node "Open Safe" is the goal the attacker wants to achieve. Actually, leaf nodes can also represent states of elements of the security system, and so their effectiveness to stop an attack. As can be noted from Fig. 1, originally the semantic rules adopted by Schneier (Schneier, 2000) are opposite to the ones usually adopted in FT analysis (i.e., the "Open Safe" node should be a leaf node depicting a top event). Since in the field of process engineering FTs are widespread and well-known tools, for the rest of the paper the semantics of FT was adopted also for ATs. Thus, in the rest of the paper the basic events (i.e., types of attack, or state of elements of security system) will be labelled as root nodes, while the vulnerability (i.e., the probability of success of an attack) will be the top event, or leaf node. This notation is more intuitive considering that ATs in this paper will be mapped into directed acyclic graphs similar to BN.

ATs can be used both for qualitative and quantitative analysis of the security system. Qualitative analysis is performed based on the graph depicting dependencies, and allows experts to brainstorm knowledge,

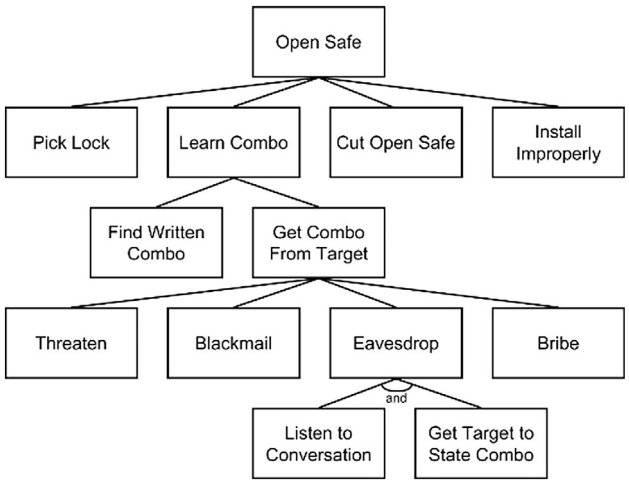


**Fig. 1.** AT for opening a safe (Schneier, 2000).