Risk assessment of serious crime with fuzzy random theory

Shen, Qiang; Zhao, Ruiqing

Published in:
Information Sciences

DOI:
10.1016/j.ins.2010.07.027

Publication date:
2010

Citation for published version (APA):
Shen, Q., & Zhao, R. (2010). Risk assessment of serious crime with fuzzy random theory. *Information Sciences*, *180*(22), 4401-4411. https://doi.org/10.1016/j.ins.2010.07.027

Risk Assessment of Serious Crime with Fuzzy Random Theory

Qiang Shen Ruiqing Zhao
Department of Computer Science, Aberystwyth University, Wales, SY23 3DB, UK
E-mail: qqs@aber.ac.uk rzz@aber.ac.uk

Abstract

This paper presents a novel approach for assessing the potential risk of serious crime events (e.g. terrorist attack). The modelling and assessment of such risk is carried out under uncertain circumstances because of both the randomness and fuzziness inherent in crime data. The approach is based on fuzzy random theory that complements probability theory, with an additional dimension of imprecision. This allows for potential loss caused by a crime to be expressed as a fuzzy random variable. Crime risk is therefore estimated as the mean chance of a fuzzy random event, where the resulting loss reaches a given confidence level. The concept of the average loss per unit of time is also introduced, in order to calculate the rate at which the loss may increase due to possible crime events. The work is compared with typical existing approaches and supported with examples throughout that illustrate its utility.

Keywords: Risk assessment; Serious crime; Fuzzy variables; Fuzzy random variables

1 Introduction

Serious crime may cause considerable loss of life and damage to property. For example, the terrorist attack on the World Trade Center on September 11, 2001 claimed around 3000 lives [28] and caused an estimated "$120 billion of damage" [22]. Rapid and accurate estimation of the risk of any such potential crime will help to provide a useful means for the establishment of appropriate risk management and loss mitigation strategies. It is therefore crucial to develop reliable methods for risk assessment of serious crime events.

Various approaches have been proposed for risk assessment of crime. In [23], crime risk involves three components (in terms of terrorism): threat to a target, target vulnerability, and the consequence should the target be successfully attacked (from the terrorist's viewpoint). It is abstractly defined as the product of these three factors (all of which are regarded as random variables). Statistical methods are employed to estimate their probability distributions and expected values. An alternative approach is given in [4], which uses possibility theory to address the general issue of

uncertainty. In particular, concepts such as attack, success, and consequence are characterized as discrete fuzzy sets and crime risk is then defined as the convolution of them. The risk of serious crime may also be viewed as an "extreme value event" as in [17]. Thus, it can be measured by using extreme value statistics. In addition, loss analysis caused by serious crime may be carried out with methods drawn from fields such as game theory, social psychology, and network analysis [24]. Clearly, the models of crime risk vary from one approach to another, depending on a variety of issues, including: type of crime, scale of crime, and the uncertainty of crime. Of course, risk analysis and assessment is not limited to the area of crime detection and prevention. It is a general problem that needs to be addressed in many different domains [2, 3, 8].

Estimating the risk of a serious crime event requires consideration of a large amount of uncertainty due to both randomness and fuzziness that are inherent in the crime data. Although different approaches exist for risk modelling, a general methodology is lacking for risk assessment of serious crime under fuzzy random circumstances [21]. In this paper, the occurrence of a serious crime is considered as a random event, while the loss incurred by the crime is considered as a fuzzy set. The proposed approach adopts fuzzy random theory (FRT) [10, 11, 19] to cope with the challenge of assessing the risk of a potential serious crime and to support the consequent loss analysis. The utilisation and integration of fuzzy representation is justified by the observation that it is very difficult, if not impossible, to precisely evaluate the results of serious crime events (e.g. the consequences of a terrorist attack).

This paper is organized as follows. In Section 2, the definition of crime risk is introduced and important properties of this concept are presented in the framework of FRT. The proposed FRT-based risk estimation is compared to typical existing approaches. This section also discusses the potential of practical applications of such estimation and contrasts the proposed approach with representative existing research. In Section 3, the average loss per unit of time is derived to indicate the rate at which loss caused by a possible serious crime may increase. Throughout the paper, examples are given to illustrate the utility of this research. Finally, the paper is concluded in Section 4, where prospects for further research are addressed.

2 Crime Risk Modelling

This section presents a framework for modelling the risk of serious crime under uncertain environments. Important concepts in crime risk management such as loss, expected loss, and crime risk are introduced.

2.1 Basic Concepts

Probability space of crime

Let $\Omega = \{Success, Failure\}$ be a sample space of a potential serious crime, where $\omega = Success$ denotes that the crime occurring within a given time frame of concern and $\omega = Failure$ denotes no crime occurring within a given time frame of concern. For simplicity, let the probabilities

$$\Pr\{\omega = Success\} = p,$$
$$\Pr\{\omega = Failure\} = 1 - p,$$

where $p \in [0, 1]$. Thus, $(\Omega, \mathscr{A}, \Pr)$ forms a probability space for such crime, where $\mathscr{A}$ is a σ-field of Ω.

Loss caused by crime

The loss caused by a crime is considered in two different ways – human cost (death and injuries), and damage to property or business (buildings, building contents, business interruption and so on). Whilst human cost cannot be measured in monetary terms in general, damage to property or businesses can be. For instance, such damage may be estimated by the equivalent cost of the resulting insurance claims for repair and reconstruction. Only the financial loss involving property/business is addressed here.

Providing an exact evaluation for such costs may be very challenging. However, the utilisation of fuzzy set theory can help to reduce the scale of such challenge and to tackle the underlying difficult problems. For example, on September 21, 2001, approximately 200-300 tons of ammonium nitrate exploded in a fertilizer plant in Toulouse, France, destroying the facility and damaging property several miles away and causing about $1.3-2 billion in insured loss. The result of this event, "about $1.3-2 billion" can be characterised as a fuzzy random variable [14]. The use of such fuzzy random variables manages to capture vaguely described information that cannot easily be represented by conventional probabilistic approaches.

Let $(\Theta, \mathcal{P}(\Theta), \mathrm{Pos})$ be a possibility space [5], where Θ is a universe, $\mathcal{P}(\Theta)$ is the power set of Θ and Pos is a possibility measure defined on $\mathcal{P}(\Theta)$. A fuzzy variable is a mapping from a possibility space $(\Theta, \mathcal{P}(\Theta), \mathrm{Pos})$ to the set of real numbers, with the following membership function [18]:

$$\mu_\xi(x) = \mathrm{Pos}\{\theta \in \Theta \mid \xi(\theta) = x\}.$$

Definition 1 *Let $\mathscr{F}$ be a collection of nonnegative discrete fuzzy variables. Loss caused by a serious crime is defined as a function $\xi : \Omega \to \mathscr{F}$ such that*

$$\xi(\omega) = \begin{cases} \eta_s, & \textit{with probability } \Pr\{\omega = Success\} \\ \eta_f, & \textit{with probability } \Pr\{\omega = Failure\}, \end{cases} \tag{1}$$

where $\eta_s, \eta_f \in \mathscr{F}$.

Example 1 *Consider a saloon car bomb attack occurred with the following probabilities:*

$$\Pr\{\omega = Success\} = p = 5/6,$$
$$\Pr\{\omega = Failure\} = 1 - p = 1/6.$$

Suppose that the minimum evacuation distance is about $457m$ *if the bomb detonates in maximum explosive capacity. The costs* η_s *(in success) and* η_f *(in failure) caused by the bomb attack are represented by fuzzy variables as described in Tables 1 and 2, respectively.*

Table 1: Membership Function of η_s

x_i	0	10	10^2	10^4	10^6	10^8	10^{10}	10^{12}
$\mu_{\eta_s}(x_i)$	0.2	0.4	0.6	0.8	1	0.8	0.6	0.4

Table 2: Membership Function of η_f

y_j	0	10^{-3}	10^{-1}	1	10	10^2	10^3
$\mu_{\eta_f}(y_j)$	0.2	0.4	0.6	0.8	1	0.8	0.4

Then the loss caused by the terrorist attack is

$$\xi(\omega) = \begin{cases} \eta_s, & \textit{with probability } 5/6 \\ \eta_f, & \textit{with probability } 1/6, \end{cases} \tag{2}$$

which is a fuzzy random variable. This is depicted in Fig. 1.

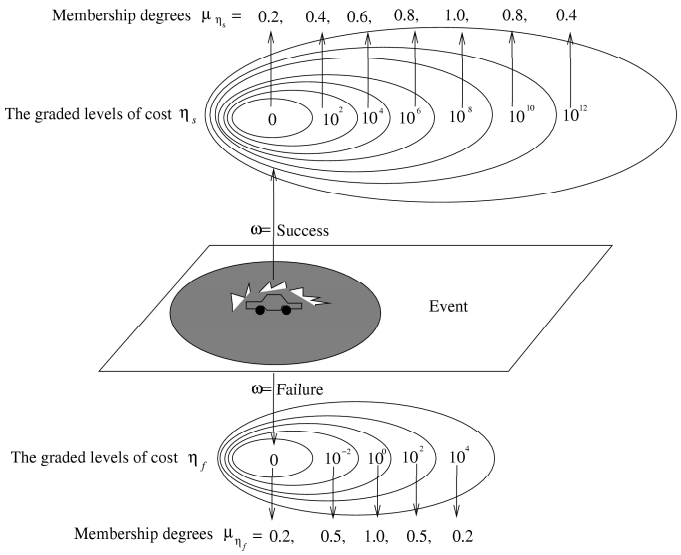

Figure 1: Geometric Interpretation of Loss

Expected loss

Definition 2 *([14]) Let ξ be the loss caused by a serious crime. Then the expected loss caused by the crime is defined as*

$$E[\xi] = E[p\eta_s + (1-p)\eta_f] = pE[\eta_s] + (1-p)E[\eta_f],$$

where $E[\eta_s]$ and $E[\eta_f]$ are the expected value of the fuzzy variable η_s and that of η_f, respectively.

Remark 1 *To illustrate the calculation of $E[\eta_s]$ and $E[\eta_f]$, for simplicity, let η be a discrete fuzzy variable with membership function $\mu_\eta(a_i) = \mu_i$ for $i = 1, 2, \ldots, n$. Assume that $a_1 < a_2 < \cdots < a_n$. Definition 2 implies that:*

$$E[\eta] = \sum_{i=1}^{n} \omega_i a_i, \tag{3}$$

where the weights $\omega_i, i = 1, 2, \ldots, n$ are given by:

$$\omega_1 = \frac{1}{2}\left(\mu_1 + \max_{1\le j\le n} \mu_j - \max_{1<j\le n} \mu_j\right),$$

$$\omega_i = \frac{1}{2}\left(\max_{1\le j\le i} \mu_j - \max_{1\le j<i} \mu_j + \max_{i\le j\le n} \mu_j - \max_{i<j\le n} \mu_j\right),\ 2 \le i \le n-1,$$

$$\omega_n = \frac{1}{2}\left(\max_{1\le j\le n} \mu_j - \max_{1\le j<n} \mu_j + \mu_n\right).$$

It is obvious that $\sum_{i=1}^{n} \omega_i = 1$.

Example 2 *Let ξ be a loss defined by (2). The procedural results of calculating $E[\xi]$ are summarised in Table 3, where π_i and ρ_i are instances of the ω_i given in Equation (3).*

Table 3: Expected Loss $E[\xi]$

x_i	0	10^2	10^4	10^6	10^8	10^{10}	10^{12}
π_i	0.1	0.1	0.1	0.1	0.2	0.2	0.2
$E[\eta_s]$	$= \sum_{i=1}^{7} \pi_i x_i$=202020101010						
y_i	0	10^{-2}	10^0	10^2	10^4		
ρ_i	0.1	0.15	0.5	0.15	0.1		
$E[\eta_f]$	$= \sum_{i=1}^{5} \rho_j y_j = 1015.5015$						
$E[\xi]$	$= pE[\eta_s] + (1-p)E[\eta_f] = 168350084344.25$						

2.2 Crime Risk

Risk is generally defined in the Oxford English Dictionary as "a chance or possibility of danger, loss, injury, or other adverse consequences". Traditionally, in mathematical modelling, risk is defined as

the probability of a specified, unwanted event. Following this approach, but taking into account fuzzy random cases, the risk is defined herein as the mean chance of a crime occurring.

Definition 3 *([15]) Let ξ be a fuzzy random variable. Then the mean chance, denoted by* Ch*, of a fuzzy random event characterised by A is defined as*

$$\mathrm{Ch}\{\xi \in A\} = \int_0^1 \Pr\left\{\omega \in \Omega \,\middle|\, \mathrm{Cr}\left\{\xi(\omega) \in A\right\} \geq \alpha\right\} \mathrm{d}\alpha, \tag{4}$$

where Cr *is a credibility measure (which is the average of the conventional possibility and necessity measures) [13].*

Definition 4 *Let ξ be the potential loss caused by a possible serious crime. The risk caused by such a possible crime is defined by:*

$$\begin{aligned} \mathrm{Risk}(x) &= \mathrm{Ch}\{\xi \geq x\} \\ &= \int_0^1 \Pr\left\{\omega \in \Omega \,\middle|\, \mathrm{Cr}\left\{\xi(\omega) \geq x\right\} \geq \alpha\right\} \mathrm{d}\alpha, \end{aligned} \tag{5}$$

where $x \in \Re^+$ is a given confidence level.

Remark 2 *If ξ degenerates to a random variable, then the crime risk* $\mathrm{Risk}(x)$ *degenerates to*

$$\Pr\left\{\xi \geq x\right\},$$

which is just the probability of the random event $\{\xi \geq x\}$. If ξ degenerates to a fuzzy variable, then the crime risk $\mathrm{Risk}(x)$ *degenerates to*

$$\mathrm{Cr}\left\{\xi \geq x\right\},$$

which is just the credibility of the fuzzy event $\{\xi \geq x\}$. Thus, the definition of crime risk in this work is a generalised version of the conventional approach.

Remark 3 *Let $P(\alpha) = \Pr\left\{\omega \in \Omega \,\middle|\, \mathrm{Cr}\left\{\xi(\omega) \geq x\right\} \geq \alpha\right\}$. $P(\alpha)$ is a non-increasing and left-continuous function with respect to the given parameter α [15]. Thus, crime risk defined above can be interpreted as the area of the shadowed region in Fig. 2.*

Theorem 1 $\mathrm{Risk}(x)$ *is a decreasing function of x, $\forall x \geq 0$.*

Proof. For any $x_1 > x_2 \geq 0$, it is clear that

$$\begin{aligned} \mathrm{Risk}(x_1) &= \mathrm{Ch}\{\xi \geq x_1\} \\ &= \textstyle\int_0^1 \Pr\left\{\omega \in \Omega \,\middle|\, \mathrm{Cr}\left\{\xi(\omega) \geq x_1\right\} \geq \alpha\right\} \mathrm{d}\alpha \\ &\leq \textstyle\int_0^1 \Pr\left\{\omega \in \Omega \,\middle|\, \mathrm{Cr}\left\{\xi(\omega) \geq x_2\right\} \geq \alpha\right\} \mathrm{d}\alpha \\ &= \mathrm{Ch}\{\xi \geq x_2\} \\ &= \mathrm{Risk}(x_2). \end{aligned}$$

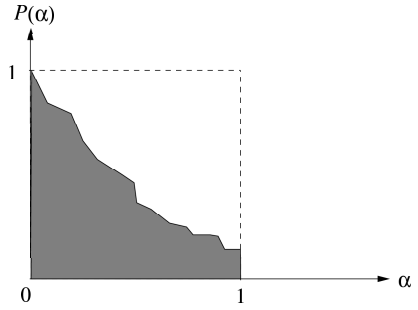

Figure 2: Geometric Interpretation of Crime Risk

Thus, Risk(x) is a decreasing function of x.

Generally speaking, Risk(x) is neither right-continuous nor left-continuous. However, the following theorem holds.

Theorem 2 *For any $x \in R^+$ and $x_i \uparrow x$,*

$$\lim_{i\to\infty} \text{Risk}(x_i) = \text{Risk}(x)$$

if for any $\omega \in \Omega$, either of the following conditions is satisfied:

$$(a) \quad \text{Cr}\{\xi(\omega) \geq x\} \geq 0.5; \quad (b) \quad \lim_{i\to\infty} \text{Cr}\{\xi(\omega) \geq x_i\} > 0.5.$$

Proof. By the credibility semi-continuity law [12], if either condition (a) or (b) holds, then

$$\lim_{i\to\infty} \text{Cr}\{\xi(\omega) \geq x_i\} = \text{Cr}\{\xi(\omega) \geq x\}.$$

Applying the above to (5) leads to

$$\begin{aligned}
&\lim_{i\to\infty} \text{Risk}(x_i) \\
&= \lim_{i\to\infty} \int_0^1 \text{Pr}\left\{\omega \in \Omega \,\middle|\, \text{Cr}\left\{\xi(\omega) \geq x_i\right\} \geq \alpha\right\} \text{d}\alpha \\
&= \int_0^1 \lim_{i\to\infty} \text{Pr}\left\{\omega \in \Omega \,\middle|\, \text{Cr}\left\{\xi(\omega) \geq x_i\right\} \geq \alpha\right\} \text{d}\alpha \\
&\qquad \text{(by dominated convergence theorem)} \\
&= \int_0^1 \text{Pr}\left\{\omega \in \Omega \,\middle|\, \lim_{i\to\infty} \text{Cr}\left\{\xi(\omega) \geq x_i\right\} \geq \alpha\right\} \text{d}\alpha \\
&\qquad \text{(by probability continuity theorem)} \\
&= \int_0^1 \text{Pr}\left\{\omega \in \Omega \,\middle|\, \text{Cr}\left\{\xi(\omega) \geq x\right\} \geq \alpha\right\} \text{d}\alpha \\
&\qquad \text{(by credibility semi-continuity law)} \\
&= \text{Risk}(x).
\end{aligned}$$

The theorem is thus proven.

Interpretation of risk levels

To reflect what is typically employed in risk-modelling in the anti-terrorism domain, the following interpretations will be adopted for subsequent discussions in this paper:

1) $0.8 \leq \text{Risk}(x) \leq 1$ means that a fuzzy random event $\{\xi \geq x\}$ will almost certainly occur; in this case, the crime risk is very high.

2) $0.6 \leq \text{Risk}(x) < 0.8$ means that a fuzzy random event $\{\xi \geq x\}$ will occur with some certainty; in this case, the crime risk is high.

3) $0.4 \leq \text{Risk}(x) < 0.6$ means that occurrence of a fuzzy random event $\{\xi \geq x\}$ is less certain but still of moderate likelihood; in this case, the crime risk is medium.

4) $0.2 \leq \text{Risk}(x) < 0.4$ means that a fuzzy random event $\{\xi \geq x\}$ is somewhat unlikely to occur; in this case, the crime risk is low.

5) $0 \leq \text{Risk}(x) < 0.2$ means that a fuzzy random event $\{\xi \geq x\}$ is rather unlikely to occur; in this case, the crime risk is very low.

Example 3 *Consider Examples 1 and 2 further. To illustrate the computation of* $\text{Risk}(x) = \text{Ch}\{\xi \geq x\}$*, suppose* $x = 10^2$*. It is straightforward to obtain that*

$$\begin{aligned}\text{Cr}\{\xi(\omega) \geq 10^2\} &= \begin{cases} \text{Cr}\{\eta_s \geq 10^2\}, & \text{if } \omega = Success \\ \text{Cr}\{\eta_f \geq 10^2\}, & \text{if } \omega = Failure \end{cases} \\ &= \begin{cases} 0.9, & \text{if } \omega = Success \\ 0.25, & \text{if } \omega = Failure. \end{cases}\end{aligned}$$

Hence,

$$\begin{aligned}\Pr\left\{\omega \in \Omega \,\middle|\, \text{Cr}\left\{\xi(\omega) \geq 10^2\right\} \geq \alpha\right\} &= \begin{cases} \Pr\{\Omega\}, & \text{if } 0 \leq \alpha \leq 0.25 \\ \Pr\{Success\}, & \text{if } 0.25 < \alpha \leq 0.9 \\ \Pr\{\phi\}, & \text{if } 0.9 < \alpha \leq 1 \end{cases} \\ &= \begin{cases} 1, & \text{if } 0 \leq \alpha \leq 0.25 \\ 5/6, & \text{if } 0.25 < \alpha \leq 0.9 \\ 0, & \text{if } 0.9 < \alpha \leq 1. \end{cases}\end{aligned}$$

Thus,

$$\begin{aligned}
\text{Risk}(10^2) &= \text{Ch}\{\xi \geq 10^2\} \\
&= \int_0^1 \Pr\left\{\omega \in \Omega \,\middle|\, \text{Cr}\left\{\xi(\omega) \geq 10^2\right\} \geq \alpha\right\} \mathrm{d}\alpha \\
&= \int_0^{0.25} \Pr\left\{\omega \in \Omega \mid \text{Cr}\left\{\xi(\omega) \geq 10^2\right\} \geq \alpha\right\} \mathrm{d}\alpha \\
&\quad + \int_{0.25}^{0.9} \Pr\left\{\omega \in \Omega \mid \text{Cr}\left\{\xi(\omega) \geq 10^2\right\} \geq \alpha\right\} \mathrm{d}\alpha \\
&\quad + \int_{0.9}^{1} \Pr\left\{\omega \in \Omega \mid \text{Cr}\left\{\xi(\omega) \geq 10^2\right\} \geq \alpha\right\} \mathrm{d}\alpha \\
&= \int_0^{0.25} 1 \mathrm{d}\alpha + \int_{0.25}^{0.9} \frac{5}{6} \mathrm{d}\alpha + \int_{0.9}^{1} 0 \mathrm{d}\alpha = 0.79 > 0.5,
\end{aligned}$$

which means that the crime risk is high. The estimated risk of this possible crime can be interpreted as the shadow area depicted in Fig. 3.

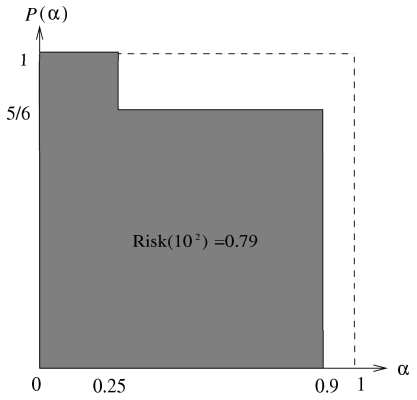

Figure 3: Geometric Interpretation of Risk(10^2)

2.3 Discussion

As indicated previously, risk assessment has a wide range of practical applications [2, 3, 8, 17, 23, 24]. In particular, it has a major implication in the area of serious crime modelling and analysis. For example, in developing intelligent systems for intelligence data monitoring [1, 21], an important trade-off needs to be considered: On the one hand, it is essential not to miss out any potentially significant scenarios that may later explain the observed evidence; on the other hand, too many unsorted and particularly, spurious scenarios may confuse human analysts. Thus, it is desirable to filter the created scenario space with respect to certain quality measures of the generated scenario descriptions. Risk estimation provides a useful means for the development of appropriate risk management and loss mitigation strategies. In particular, preferences over different hypothetical scenarios can be determined on the basis of the estimated risk levels for individual scenarios. For instance, given a plausible terrorist scenario with an estimated large risk value, prioritised actions

to prevent its occurrence must be taken.

When faced with a possible serious crime event, effective and efficient decision-making commonly requires consideration of a variety of hypotheses that may have led to certain observed evidence [6]. The utilisation of scenario descriptions, which may each individually explain a particular type of evidence, has received significant attention recently. However, such work typically considers the uncertainty involved in the description of both the evidence and the hypothesis using just random variables. Yet, working with human intelligence analysts, it is clear that much of this information is only available in vaguely described terms. Thus, in addition to the need for probabilistic representation and inference, there is also a need for the variables and their influences to be expressed in fuzzy forms. The present research addresses such a combined need in describing fuzzy random events.

Importantly, any extension to the existing (probabilistic) techniques should ensure that when events are crisply described, the extended representation and its associated inference mechanism must be consistent with the conventional approach. The risk assessment method introduced here satisfies this constraint, as verified previously.

2.4 Comparison with Possibilistic Risk

Possibilistic risk [4] is the most relevant existing work that extends probabilistic risk to address uncertainty. This subsection empirically compares the present research with the possibilistic approach.

Following possibility theory, possibilistic risk is computed by [4]:

$$\text{Possibilistic\_Risk} = \text{Attack} \times \text{Success} \times \text{Consequence}, \tag{6}$$

where all three factors: Attack, Success, and Consequence, are generally characterised as discrete fuzzy sets. For instance, they may be defined on the following three domains respectively: $\{0, 10^{-5}, 10^{-4}, 10^{-3}, 10^{-2}, 10^{-1}, 1, 10\}$ where each element has the dimension of number of times per year; $\{0, 10^{-3}, 10^{-2}, 10^{-1}, 1\}$ where each element is dimensionless; and $\{1, 10^{1}, 10^{2}, 10^{3}, 10^{4}, 10^{5}, 10^{6}, 10^{7}, 10^{8}, 10^{9}, 10^{10}, 10^{11}, 10^{12}\}$ where each element has the dimension of US dollars.

Defined upon such discrete fuzzy sets, Possibilistic_Risk is also a discrete fuzzy set, whose membership function can be calculated through the use of the extension principle [25] such that

$$\mu_{Possibilistic\_Risk}(r) = \max_{xyz=r} \mu_{Attack}(x) \wedge \mu_{Success}(y) \wedge \mu_{Consequence}(z).$$

If the factor Attack is ignored (or assumed to be true) in (6), then the Possibilistic_Risk defined in (6) is very similar to the loss as given in Definition 1. The difference is that Success is characterised by fuzziness alone in (6) while it is fundamentally represented by randomness in this paper. The

present approach is based on the observation that the chance of Success (in terms of probability) of a serious crime event occurring may be estimated by conventional statistical means. For example, consider the following timeline of bomb attacks which occurred in India from 2003 to 2007:

Table 4: List of Attacks in India from 2003 to 2007

Attack	Date	Location	State
Bombing	August 26, 2007	Hyderabad, Andhra Pradesh	Success
Bombing	May 18, 2007	Mosque in Hyderabad, Andhra Pradesh	Success
Train bombing	February 19, 2007	Train from New Delhi to Pakistan	Success
Bombing	September 8, 2006	Mosque in the Southwest of India	Success
Train bombing	July 11, 2006	Bombay	Success
Bombing	March 7, 2006	Varanasi, Uttar Pradesh	Success
Bombing	October 29, 2005	New Delhi	Success
Bombing	August 15, 2004	Assam	Success
Bombing	August 15, 2004	Assam	Success
Bombing	January 26, 2004	Reported by police station in New Delhi	Failure
Bombing	January, 2004	Reported by police station in New Delhi	Failure
Train bombing	May 13, 2003	Bombay	Success

From this table, it follows that

$$\begin{aligned} \text{Total number of bomb attacks} &= 12, \\ \text{Number of successful attacks} &= 10, \\ \text{Number of failed attacks} &= 2. \end{aligned}$$

Hence, the probability p of Success of a bomb attack in India can be estimated by the frequency:

$$\hat{p} = \frac{\text{Number of success}}{\text{Total number of bomb attacks}} = \frac{5}{6}.$$

Importantly, the expectation for Possibilistic_Risk in [4] is defined as an interval

$$[E_*[\text{Possibilistic\_Risk}], E^*[\text{Possibilistic\_Risk}]], \tag{7}$$

where

$$\begin{aligned} E_*[X] &= \sum_i x_i[\text{Pos}\{X \leq x_i\} - \text{Pos}\{X \leq x_{i-1}\}], \\ E^*[X] &= \sum_i x_i[\text{Pos}\{X > x_{i-1}\} - \text{Pos}\{X > x_i\}] \end{aligned}$$

with $x_{i-1} < x_i$. However, the expected loss computed using Definition 2 of this paper is a crisp number. It is obviously much more convenient to rank different terrorist scenarios [21] by crisp risk values than by interval-valued ones.

Example 4 *To further contrast the proposed approach with the work on possibilistic risk, consider Examples 1 and 2 again.*

Recall that in Example 1, the loss caused by the terrorist attack is computed by

$$\xi(\omega) = \begin{cases} \eta_s, & \textit{with probability } 5/6 \\ \eta_f, & \textit{with probability } 1/6, \end{cases} \tag{8}$$

where η_s and η_f are the costs caused by a successful or failed bomb attack, respectively (see Tables 1 and 2). In addressing the same problem using the possibilistic approach for risk assessment, the notion of "with probability 5/6" is characterised as a fuzzy set "about 5/6". Denote it by "Success" for shorthand. Without loss of generality in illustration, suppose that the membership function of "Success" is represented by the fuzzy set given in Table 5. Thus, the Consequence term of (6) can be

Table 5: Membership Function of *Success*

y_i	0.75	0.8	0.85
$\mu_{Success}(y_i)$	0.5	1	0.5

reasonably assumed to be η_s given that a certain attack has, or will have, been carried out (i.e. the term of Attack in (6) is of a full membership value for its underlying element that represents truth). From this, it follows that the possibilistic risk defined in (6) is a fuzzy set whose membership function can be calculated as shown in Table 6. Obviously, the main difference between the possibilistic risk and the loss defined in the paper is that the former is a fuzzy set while the latter is a fuzzy random variable.

Table 6: Membership Function of *possibilistic_risk*

r_i	0	7.5	$10^2 \times 0.75$	$10^4 \times 0.75$	$10^6 \times 0.75$	$10^8 \times 0.75$	$10^{10} \times 0.75$	$10^{12} \times 0.75$
$\mu_{possibilistic\_risk}(r_i)$	0.2	0.4	0.5	0.5	0.5	0.5	0.5	0.4
r_i	0	8	$10^2 \times 0.8$	$10^4 \times 0.8$	$10^6 \times 0.8$	$10^8 \times 0.8$	$10^{10} \times 0.8$	$10^{12} \times 0.8$
$\mu_{possibilistic\_risk}(r_i)$	0.2	0.4	0.6	0.8	1	0.8	0.6	0.4
r_i	0	8.5	$10^2 \times 0.85$	$10^4 \times 0.85$	$10^6 \times 0.85$	$10^8 \times 0.85$	$10^{10} \times 0.85$	$10^{12} \times 0.85$
$\mu_{possibilistic\_risk}(r_i)$	0.2	0.4	0.5	0.5	0.5	0.5	0.5	0.4

Note that the expected value of the possibilistic risk is the following interval:

$$[E_*[\text{Possibilistic\_Risk}], E^*[\text{Possibilistic\_Risk}]] = [161646.5, 341666160000].$$

In order to obtain a single value in assessing the risk (which may be better understood than an interval by the user [21]), a simple way is to calculate the arithmetic average of E_*[Possibilistic_Risk] *and*

E^*[Possibilistic_Risk]*:*

$$\frac{1}{2}(E_*[\text{Possibilistic\_Risk}] + E^*[\text{Possibilistic\_Risk}]) = 170833160823.$$

This is an interesting figure which will be further discussed in the next section, where a method of estimation of average loss is introduced.

3 Average Loss Estimation

Estimation of average loss for serious crime is a very difficult task. This section tackles a particular type of average loss estimation, which is of practical significance in dealing with serious crime under certain conditions.

Let T_i denote the interarrival time between the $(i-1)$th and ith potential criminal activities, $i = 1, 2, \ldots$, respectively. Suppose that T_i are independent and identically distributed (iid) exponentially distributed random variables with parameter $\lambda > 0$, i.e. T_i, $i = 1, 2, \ldots$, have a common probability density function

$$f(x_i; \lambda) = \begin{cases} \lambda e^{-\lambda x_i}, & x_i \geq 0 \\ 0, & x_i < 0, \end{cases}$$

with the expected value

$$E[T_i] = \frac{1}{\lambda}.$$

Let $S_0 = 0$ and

$$S_n = T_1 + T_2 + \cdots + T_n, \qquad \forall n \geq 1. \tag{9}$$

Thus, S_n denotes the time of the nth crime event (or criminal activity). The number of possible crime events up to time t is denoted by

$$N(t) = \max_{n \geq 0}\{n \mid 0 < S_n \leq t\}. \tag{10}$$

Note that $\{N(t), t \geq 0\}$ is a Poisson process with parameter λ [20]. As such, for any nonnegative integer n,

$$\Pr\{N(t+s) - N(s) = n\} = e^{-\lambda t}\frac{(\lambda t)^n}{n!}.$$

In particular,

$$E[N(t)] = \lambda t.$$

Let ξ_i denote the loss caused by the ith potential criminal activity. Suppose that $\{\xi_i, i \geq 1\}$ is a sequence of iid nonnegative fuzzy random variables [7, 12], independent of $\{T_i, i \geq 1\}$. Then, the aggregated loss up to time t is

$$C(t) = \sum_{i=1}^{N(t)} \xi_i. \tag{11}$$

It can be proven (by following the work of [9], [27] and [26]) that

$$\begin{aligned} E\left[C(t)\right] &= E\left[\sum_{i=1}^{N(t)} \xi_i\right] \\ &= E[N(t)] \cdot E\left[\xi_1\right] \\ &= \lambda t \cdot E\left[\xi_1\right]. \end{aligned} \tag{12}$$

Obviously, $\lim_{t\to\infty} E[C(t)] = +\infty$ provided that $E\left[\xi_1\right] > 0$. Note that

$$\lim_{t\to\infty} \frac{E[C(t)]}{t} = \lim_{t\to\infty} \frac{\lambda t \cdot E\left[\xi_1\right]}{t} = \lambda \cdot E[\xi_1] = \frac{E[\xi_1]}{E[T_1]}. \tag{13}$$

This states that the average loss per unit of time is just the expected loss caused by the first criminal activity, divided by the expected interarrival time for the first event to take place.

Remark 4 *If fuzzy random variables ξ_i degenerate to random variables, then the result in (13) degenerates to the form*

$$\lim_{t\to\infty} \frac{E[C(t)]}{t} = \frac{E[\xi_1]}{E[T_1]},$$

which is just the conventional result in the stochastic case [20].

Example 5 *Consider the modelling and analysis of a sequence of compact saloon car bomb attacks. The interarrival times between the $(i-1)$th and ith attack T_i may be represented by iid positive random variables with the following exponential density function*

$$f(x_i;\lambda) = \begin{cases} \lambda e^{-\lambda x_i}, & x_i \geq 0 \\ 0, & x_i < 0, \end{cases}$$

where $\lambda = 0.0001$. The average period between two occurrences of bomb attacks is $E[T_i] = 1/\lambda = 10000$ (day). Suppose that the losses ξ_i $(i = 1, 2, \ldots)$ caused by the corresponding i terrorist attacks are iid fuzzy random variables, and that they have a common form as with ξ defined in (2). Given these conditions, $E[\xi_i] = 168350084344.25$ (in British Pound Sterling), $i = 1, 2, \ldots$ That is, the average loss caused by each saloon bomb attack is £168350084344.25.

Note that this figure is close to the arithmetic average of the lower and upper bounds of the expected interval of the possibilistic risk. As calculated in Example 4 of Section 2.4, the latter is: £170833160823. This shows that the present estimation method produces a single-valued outcome that is compatible to the expected risk value which is obtainable using the possibilistic approach, although the latter is an interval of a rather wide width.

Continuing the current example, let $N(t)$ denote the total number of terrorist attacks that have occurred up to time t. Then, $C(t) = \sum_{i=1}^{N(t)} \xi_i$ represents the total amount of losses accumulated up to time t. It follows from (13) that the average loss per unit of time can be calculated as

$$\lim_{t\to\infty} \frac{E[C(t)]}{t} = \frac{E\left[\xi_1\right]}{E[T_1]} = \lambda E[\xi_1] = 16835008.43.$$

*In other words, the loss caused by the terrorist attacks increases at the rate of £*16835008.43 *per day.*

As stated previously, estimation of average loss for a serious crime event is a very challenging task. This is particularly true when considering possible terrorist attacks, as little historical data is available to model the events precisely and accurately. Yet, an approximate estimate of the aforementioned form offers additional insight into a hypothesised scenario which can help experienced human analysts to refine any competing demands for potential resource deployment.

4 Conclusion

This paper has presented a novel technique to evaluate the potential risk of possible serious crime events under fuzzy random circumstances. The technique uses the fuzzy random theory to represent the uncertainty that pervades the domain of such events. In particular, the risk is defined as the mean chance that loss reaches a given confidence level. The average loss per unit of time is also considered in the paper.

This work has produced encouraging results, but further developments will help to enhance its potential and applicability. For instance, an important issue is to generalise the proposed approach to address risk estimation problems in other areas of serious crime (e.g. series rape or drug trafficking). Also, it would be very interesting to create a more robust interpretation of risk levels. That is, instead of using hard thresholds in defining the levels, a better approach might be to introduce soft boundaries between such levels. This will allow for more user-friendly explanation of the resultant risk estimates. Finally, risk of a possible crime may be estimated over different types of loss (e.g. range of geometric destruction and number of casualties). Estimates obtained using different criteria (e.g. reliability and urgency) may be integrated to assess an overall situation risk. Such measures may then be utilised as flexible constraints [16] to be imposed, say, over an automated emergency planning process for efficient resource deployment.

Acknowledgments

This work was supported by UK EPSRC grant EP/D057086. The authors are grateful to all members of the project team for their contribution whilst taking full responsibility for the views expressed in the paper. The authors are also grateful to the Editor and the anonymous reviewers for their constructive comments that are helpful in directing the revision of this paper.

References

[1] T. Boongoen, Q. Shen, C. Price, Disclosing false identity through hybrid link analysis. *Artificial Intelligence and Law*, 18 (2010) 77-102.

[2] G. Buyukozkan, D. Ruan, Choquet integral based aggregation approach to software development risk assessment, Information Sciences 180 (2010) 441-451.

[3] S. Chen, Y. Huang, Relative risk aversion and wealth dynamics, Information Sciences 177 (2007) 1222-1229.

[4] J.L. Darby, Estimating terrorist risk with possibility theory, http://www.doe.gov/bridge, 2004.

[5] D. Dubois, H. Prade, Possibility Theory, Springer, 1988.

[6] X. Fu, T. Boongoen, Q. Shen, Evidence directed generation of plausible crime scenarios with identity resolution. *Applied Artificial Intelligence*, 24 (2010) 253-276.

[7] J. Gao, B. Liu, New primitive chance measures of fuzzy random event, International Journal of Fuzzy Systems 3 (2001) 527-531.

[8] C. Huang, H. Inoue, Soft risk maps of natural disasters and their applications to decision-making, Information Sciences 177 (2007) 1583-1592.

[9] T. Huang, R. Zhao, W. Tang, Risk model with fuzzy random individual claim amount, European Journal of Operational Research, 2007, doi:10.1016/j.ejor.2007.10.035.

[10] H. Kwakernaak, Fuzzy random variables – I, Information Sciences 15 (1978) 1-29.

[11] H. Kwakernaak, Fuzzy random variables – II, Information Sciences 17 (1979) 253-278.

[12] B. Liu, Uncertainty Theory, 3rd ed., http://orsc.edu.cn/liu/ut.pdf.

[13] B. Liu, Y. Liu, Expected value of fuzzy variable and fuzzy expected value models, IEEE Transactions on Fuzzy Systems 10 (2002) 445-450.

[14] Y.K. Liu, B. Liu, Fuzzy random variables: a scalar expected value, Fuzzy Optimization and Decision Making 2 (2003) 143-160.

[15] Y.K. Liu, B. Liu, On minimum-risk problems in fuzzy random decision systems, Computers & Operations Research 32 (2005) 257-283.

[16] I. Miguel, Q. Shen, Fuzzy rrDFCSP and planning, Artificial Intelligence, 148 (2003) 11-52.

[17] H. Mohtadi, Assessing the risk of terrorism using extreme value statistics, Proceedings of the institute of food technologists' first annual food protection and defencse conference, Atlanta, Georgia, 2005.

[18] S. Nahmias, Fuzzy variables, Fuzzy Sets and Systems 1 (1978) 97-110.

[19] M.L. Puri, D.A. Ralescu, Fuzzy random variables, Journal of Mathematical Analysis and Applications 114 (1986) 409-422.

[20] S.M. Ross, Stochastic Processes, John Wiley & Sons, Inc, New York, 1996.

[21] Q. Shen, J. Keppens, C. Aitken, B. Schafer, M. Lee, A scenario-driven decision support system for serious crime investigation, Law, Probability and Risk **5**: 87-117, 2006.

[22] B.S. Wesbury, The Economic Cost of Terrorism,
http://usinfo.state.gov/topical/econ/mlc/02091004.htm

[23] H. Willis, A. Morral, T. Kelly, J. Medby, Estimating terrorism risk, RAND Corporation, Report from Center for Terrorism Risk Management Policy, 2005. http://www.rand.org

[24] G. Woo, Terrorism Risk, Wiley Handbook of Science and Technology for Homeland Security.

[25] L.A. Zadeh, Fuzzy sets as a basis for a theory of possibility, Fuzzy Sets Sys-tems 1(1978) 3-28.

[26] J. Zhang, R. Zhao, W. Tang, Fuzzy Age-Dependent Replacement Policy and SPSA Algorithm Based-on Fuzzy Simulation, Information Sciences 178 (2008) 573-583.

[27] R. Zhao, W. Tang, C. Wang, Fuzzy random renewal process and renewal reward process, Fuzzy Optimization and Decision Making 6 (2007) 279-295.

[28] September 11, 2001: A day of terror,
http://www.cnn.com/2003/US/03/10/sprj.80.2001.terror/index.html