Sandra König

Simultaneous Treatment of Risk and Resilience

HICL

Published in: Adapting to the Future:
Wolfgang Kersten, Christian M. Ringle and Thorsten Blecker (Eds.)
ISBN 978-3-754927-70-0, September 2021, epubli

Simultaneous Treatment of Risk and Resilience

Sandra König[1]

1 – Austrian Institute of Technology

Purpose: *Supply chain management has a clear focus on risk management, but recent developments have shown that it is also important to pay attention to resilience. This paper introduces a systematic approach to simultaneously treat the two correlated quantities and can incorporate various notations of risk and resilience.*

Methodology: *A game theoretic model that allows simultaneous risk minimization and resilience maximation is proposed. Integration of existing supply chain risk and resilience measures is described to show its applicability. The intrinsic uncertainty of consequences of actions is explicitly taken into account by probabilistic payoffs.*

Findings: *The model provides a set of actions that provide optimal protection, depending the weight put on risk vs. resilience (i.e., how much weight is put on which of the two goals). The problem of putting such theoretical results into practice is discussed and illustrated with an example.*

Originality: *This work aims at improving existing best practice techniques to increase resilience by providing a systematic optimization method. It allows integration of existing resilience measures and is thus flexible to use.*

First received: 13. Apr 2021 *Revised: 29. Aug 2021* *Accepted: 31. Aug 2021*

1 Introduction

Resilience has become a topic of high interest in the context of supply chains (Dubey et al., 2019). This is also due to recent incidents that caused disruption of flows, such as the NotPetya attack that heavily affected container logistics (Tills, 2018). The strong relation between risk and resilience is well-known, but a concrete description of the relation is very challenging to find. There are approaches that identify explicit relations when building a resilient supply chain (Wicher and Lenort, 2012) and approaches that use simulation to design a framework for risk, resilience, and performance (Macdonald et al., 2018). This paper uses a different approach that applies game theoretic methods to simultaneously optimize risk and resilience without the need to explicitly model the relation between the two quantities. The proposed method is very general in the sense that users can choose their own measures of risk and resilience to be used during the analysis. This increases both the willingness to apply the method and the understanding of the results.

The paper is organized as follows. Section 2 provides a short overview on risk and resilience in the context of supply chains, including some measures that may be used during the upcoming analysis. Section 3 describes how to set up the game theoretic model and how to perform the analysis. The approach is illustrated with a small example to demonstrate the workflow. Section 4 concludes with remarks on limitations and potential future directions.

2 Risk and Resilience in Supply Chains

This section summarizes different approaches of risk and resilience in supply chains (SCs), providing input to the optimization framework. Users are free to use their own risk and resilience measures but might like to have a look at current approaches and adapt their measures based on these.

2.1 Supply Chain Risk

A critical review on different definitions and measures of supply chain risk is provided in (Heckmann, Comes and Nickel, 2015) in order to close the gap in the literature regarding a definition of risk in the context of supply chain risk management. This review demonstrates that most authors work with informal concepts, and only few authors (less than 20%) use explicit definitions. While these explicit definitions all consider risk to be triggered by an event, the actual definitions differ. Some focus on probability and outcome, while others consider the deviation from expected behavior or the (in)ability to cope with consequences of an event. If an explicit definition is available, the next question is how to measure the defined risk. For example, if the likelihood of occurrence is part of the definition, the question is how to estimate the likelihood - quantitative based on empirical data or on quantitative based on expert assessment.

A more recent survey still states that so far there is no generally accepted definition of supply chain risk (Baryannis et al., 2019). Correspondingly, there are numerous measures of risk in the context of supply chain, depending on the perspective of the researcher, on the specific sector and on the circumstance, e.g., in light of the experiences during COVID-19 (Deaton and Deaton, 2020).

Existing supply chain risk definitions and measures are heterogeneous, not least due to adoption of approaches from related fields (Heckmann, Comes and Nickel, 2015). The game theoretic approach described in the following can integrate any of these concepts, but qualitative measures allow an intuitive understanding of the approach. The user is free to choose a risk definition and measure on his own, which should also increase the understanding of the results (which are described in terms of the chosen risk measure).

2.2 Supply Chain Resilience

The term resilience can be understood from various perspectives, and the understanding of resilience changes over time (de Bruijn et al., 2017). Resilience may focus on providing a certain level of service despite disruption, on recovery time after a shock, or on reaching a stable state over time. Resilience concepts may focus on specific threats (e.g., extreme weather conditions) or on all possible sources of disruptions, depending on the goal of

the analysis. In essence, most resilience concepts in the context of supply chains capture the ability of a system to recover from disruptions, but the ways to actually measure resilience differ a lot. A systematic review of supply chain and supply network resilience based on 84 studies has been conducted in (Datta, 2017), finding that detailed explanations are often missing.

In other domains, such as critical infrastructures, more precise concepts are available, but consensus is still missing. A finding of the EU Horizion 2020 project IMPROVER is that a crucial part of critical infrastructure resilience is the ability to provide a minimum level of service and quick recovery after a shock (Petersen et al., 2020). Supply chain resilience could be defined similarly. A more concrete measure is the resilience triangle proposed in (Bevilacqua, Ciarapica and Marcucci, 2017). This triangle is drawn by plotting the performance of the system after a disruption over time. The name stems from the fact that after a sharp drop in performance, the system steadily recovers during a certain time interval, so that the area above the curve has approximately the shape of a triangle.

The main challenges in addressing resilience, as in risk research, are uncertainties and interdependencies, and sparse data (Sun, Bocchini and Davison, 2018). Uncertainty and the increasing number of interdependencies hamper prediction, and limited availability of data limit the use of empirical methods. A decision support framework to assess supply chain resilience to disasters is presented in (Falasca, Zobel and Cook, 2008). The authors define resilience as the ability to reduce the probabilities of disruption and to reduce both the consequences of disruptions and the time to recover and measure these through three determinants (density, complexity and node criticality). These determinants are integrated in the resilience triangle, and the objective of the framework is to reduce the size of the triangle.

3 Optimization of Risk and Resilience

Considering risk and resilience optimization as a game between two players allows identification of strategies that simultaneously minimize risk and maximize resilience without the need to explicitly model the relation between risk and resilience. In the context of risk management, it is common to consider a worst-case scenario where the

attacker tries to cause as much damage as possible (Monga and Zhu, 2016). The main contribution of this paper is such a zero-sum game model. The approach is described on a high level in the next subsection and applied afterwards.

3.1 Methodology

On a high level, protecting a system can be regarded as a game between a defender, i.e., the operator or authorities, who wants to protect the system and an attacker that tries to cause damage to the system. The key components of the model are

- Strategies for the defender (player 1) and the attacker (player 2). For the defender, this includes all countermeasures that reduce risk and increase resilience, while for the attacker, the list includes events that threaten the system.
- For each pair of defense and attack strategy the payoffs need to be estimated for each goal, i.e., risk and resilience need to be evaluated for each scenario.

Digitalization has increased the complexity of such kind of analysis, since a precise prediction of a system's reaction is almost impossible. Therefore, classical game theory can be extended such that it allows distribution-valued payoffs rather than real-valued payoffs (Rass, König and Schauer, 2015). This way, the user no longer needs to provide crisp estimates of the quantity of interest but can provide his believes over various values. In order to keep the approach practical, the payoffs are proposed to be measured on a qualitative scale, e.g., a 5-tier scale, such that the distribution over the possible outcomes becomes a simple histogram. The optimization algorithm requires that both risk and resilience are measured on the same scale.

An algorithm to solve such zero-sum games with random payoffs has been implemented in the statistical software R (R Core Team, 2018) in course of the EU project HyRiM (Rass and König, 2018). It is based on the fictitious play algorithm (Berger, 2005) that imitates the game and records how often players choose which strategy. In the case of qualitative payoffs, the algorithm compares two payoffs by comparing the values in each category with increasing importance, i.e., it prefers actions with a lower likelihood of the highest risk. The main functions of the R package 'HyRiM' needed to set up and solve the game are described in Section 3.3.

In the remainder of this section, we demonstrate how to perform such a game theoretic analysis. First, the strategies of both players are defined, and the payoffs are estimated. Then the optimization is done using the statistical software R and the output is interpreted.

3.2 Actions to Reduce Risk and Increase Resilience

Once the goal of the analysis is clear (in our case risk minimization and resilience maximization), the next step is to collect all possible and relevant actions each player can take, i.e., define the set of strategies.

For the attacker, the set of strategies contains all actions that threatens the system. This includes both intentional attacks (e.g. malware attacks, as in the NotPetya case) and natural disasters (such as a flood). Since the attacker is an abstract representation of threats, the strategies should reflect the threats the user is most concerned about. It is not necessary to estimate the likelihood of occurrence in this setting, rather a likelihood assessment is part of the result of the analysis, as we describe at the end of this section.

For the defender, this list includes all actions that can be taken to reduce the risk or increase the resilience. Due to the correlation between the two quantities, a strategy will typically affect both risk and resilience to some extent. The model requires to assess the effects for each goal individually, as described in the next subsection.

Threats and protective actions against supply chain risks have been discussed in the literature (Rajagopal, Prasanna Venkatesan and Goh, 2017) and build the ground for the illustrative example. According to the review, the main concerns are disruption of the SC and operational risk (e.g., risk of damage during transportation). Frequently discussed counteractions are construction of a robust SC network design (SCND) and risk propagation analysis (RPA). SCND methods describe how a supply chain can be designed effectively to recover from disruptions. RPA analyses how risks propagate through a system and affect different parts, which helps to understand operational risks better.

For the illustrative example, these two threats are chosen as attack strategies, and SCND and RPA are selected as defense strategies, as shown in Table 1.

Table 1: Strategies

	Attacker	Defender
Strategy 1	Disruption	SCND
Strategy 2	Operational	RPA

Note that the enumeration of strategies does not reflect their relevance, the analysis selects strategies depending on their effects regarding the considered goals. Further, it is possible to include a "no action" strategy that describes the current state (i.e., evaluating whether a strategy reduces the risk or increases the resilience compared to the status quo).

The final task to set up the game is an assessment of the payoffs, that is, for each combination of attack and defense action the expected impact needs to be estimated for each goal. It is recommended to measure risk on a qualitative scale (Münch, 2012) to represent the fact that an exact assessment is hardly possible in practice. If enough data is available, quantitative approaches may be used as well. In any case it should be made clear how to deal with inconsistent data, i.e., wether outliers are removed, or different assessment are aggregated. In this model, we chose to include all data available (including potentially inconsistent expert assessments) and work with probability distributions over all possible values. Non-probabilistic approaches like fuzzy logic usually perform very well in practice, but the interpretation of the underlying concept is not always obvious. The decision on whether to use qualitative or quantitative data is up to the user, since it is often a question of taste. The optimization algorithm requires that payoffs are measured on the same scale for all the goals, which is not a limitation in our case, since resilience is equally hard to measure as risk. We suggest using a 5-tier scale, where the levels have different interpretations for the different goals. The payoffs are collected in two payoff matrices (one for each goal).

Since the algorithm that solves the game has been implemented in the context of risk minimization, it is important that lower levels refer to a better situation than larger ones.

In practice, this means that experts who do the assessments (not necessarily one person alone) interprets 1 as low risk or a high resilience and 5 as high risk or low resilience. The algorithm then aims at minimizing the maximal risk and minimizing the lowest resilience (and therefore increasing it). The payoff matrices shown below in Figure 1 and Figure 2 show the probability distributions over the 5 categories, i.e., the x-axis shows the categories and the y-axis the corresponding probabilities.

Based on the description of the defense strategies in (Rajagopal, Prasanna Venkatesan and Goh, 2017) and references therein, the payoffs for the running example are chosen based on the assumption that SCND reduces the risk of disruption more than RPA (see first column of the matrix in Figure 1) because disruptions are less likely to occur in a network with robust network design. Further we assume that RPA reduces the risk of operational problems more than SCND (second column of the matrix in Figure 1), because such an analysis might identify causes of the problems that can be resolved and hence reduce the risk in the future. Note that these assessments depend on the specific use case, this work is based on a researcher's best guess, but expert knowledge will be crucial in practical applications.

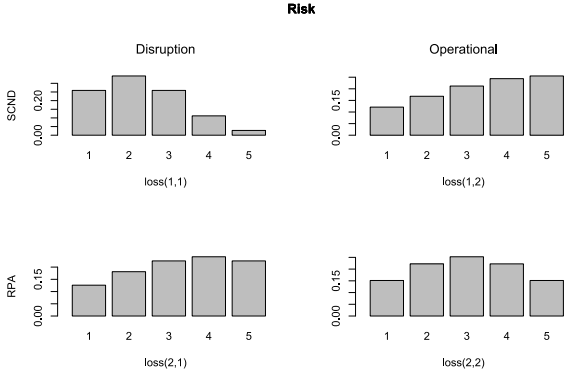

Figure 1: Payoff matrix for goal "Risk"

Similarly, it is assumed that SCND increases the resilience against disruption more than RPA (i.e., yields more likely lower values, see first column of Figure 2) while RPA increases

the resilience against operational problems more than SCND (second column of Figure 2). The concrete numbers in this example are artificial, and the assessment requires expert's knowledge in practice.

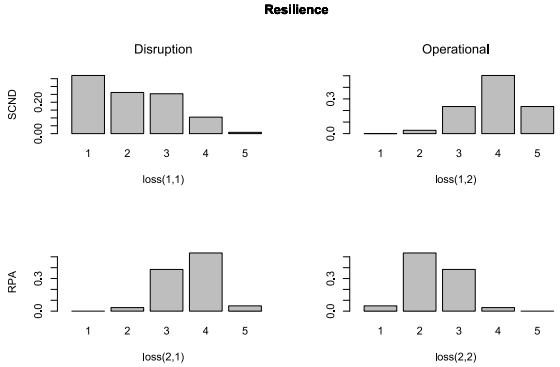

Figure 2: Payoff matrix for goal "Resilience"

3.3 Identification of Optimal Actions

Identification of an optimal choice among the possible strategies is done using the R package 'HyRiM' (Rass and König, 2018). The core functions of this package are:

- *lossDistribution*: constructs a loss distribution from raw data such that it fits the framework (in particular, all goals use the same scale); if necessary, smoothing is applied
- *mosg*: a Multi-Objective Security Game is constructed from the number of goals, number of strategies and a list of payoffs; description of goals and strategies are optional but recommended
- *mgss*: for a given game, this algorithm determines probability distributions over the actions of each player, indicating how frequently they should be used to get optimal results. Further, it provides a distribution over the expected damage, called *assurance* since this is the expected damage if the attacker acts in his best (the defender's worst) possible way, which will not always happen.

By default, the algorithm treats both goals as equally important. However, the user is free to adapt this by putting weights on the various goals and therefore prioritizing one over the other.

In case of the considered example, the R code looks as follows:

```
# load package HyRiM
library(HyRiM)
# number of strategies
n<-m<-2
# number of goals
d<-2
# description of strategies
defensesDescr<-c("SCND","RPA") # PS1
attacksDescr<-c("Disruption","Operational") # PS2
# raw data for payoff
obs111, …, obs122, obs211, …, obs222
# payoff distribution from raw data
ld111 <- lossDistribution(obs111, discrete=TRUE,supp=c(1,5),smoothing="ongaps")
…
ld222 <- lossDistribution(obs222, discrete=TRUE,supp=c(1,5),smoothing="ongaps")
# collect in list of payoffs
payoffs<-list(ld111,ld112,ld121,ld122, ld211,ld212,ld221, ld222)
# set up game
G <- mosg(n=2,m=2,goals=2, goalDescriptions=c("Risk","Resilience"),
losses=payoffs, byrow=TRUE,
defensesDescr<-c("SCND","RPA"), attacksDescr<-
c("Disruption","Operational"))
# compute optimal solution for chosen accuracy eps
eq <- mgss(G,eps=0.01)
```

The main result of the analysis is a guide on which defense actions should be used, i.e., which defense strategies should be played how often. The uppermost histogram in Figure 3 shows the recommended relative frequency of use for the defense actions.

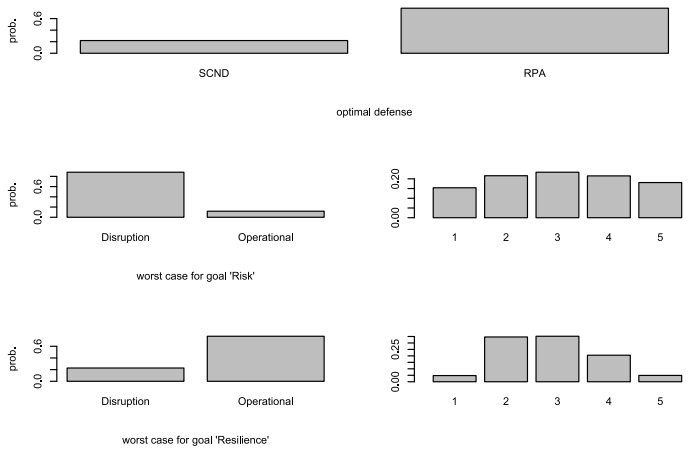

Figure 3: Results of game theoretic analysis

The practical implementation of such results depends a lot on the actual strategies. If they can be implemented with reasonable effort, they should be applied according to this relative frequency (e.g., in the case of quality checks, software updates etc.) In this concrete example, the analysis yields a frequency of 0.22 for SCND and 0.78 for PRA, so that on average SCND should be applied 22% of the time and PRA 78% of the time. Changing the network design might be costly, so that it cannot be done regularly. In this case, the numbers can be interpreted in terms of priority, i.e., applying RPA is more urgent than SCND. However, if it is not possible to switch between strategies in order to meet the relative frequencies in the long run, the defense is no longer optimal, and a different choice of strategies should be considered (the analysis needs to be redone in this case).

Besides instruction on how to act, the analysis provides information on the best actions from the attacker's point of view, i.e., on the worst-case attack from the defense's point of view. Similar as for the defender, the analysis provides relative frequencies over the attack strategies. However, this optimal/worst attack depends on the goal that the attacker has in mind. If he focuses on increasing the risk, his best action is characterized through the second row in Figure 3 (left side), if he focuses on reducing resilience his optimal choice is described in the last row in Figure 3 (left side). For both goals, the resulting payoff is given (right-hand side of second and third row in Figure 3). This should be understood as a distribution over the damage in case both the attacker and the defender play their optimal strategies. For the goal 'Risk', this attack most likely yields a risk of 3, but other risk levels are also likely to happen. For the goal 'Resilience', the optimal attack is very unlikely to yield a resilience level of 1 or 5, with levels 2 and 3 being most likely. These risk and resilience levels are reached if the attacker follows the optimal strategy, however he may not be able to do both attacks at the same time (if the optimal strategy profile differs for the two goals) or may not even be rational (e.g., in the case of natural disaster). In this case, the expected impact will be less bad. Therefore, the provided distribution is understood as an assurance, meaning that this is an upper bound to the observed values. The provided assurances are not valid any longer if the defender deviates from his optimal strategy given in the first row.

4 Conclusion

As every model, the proposed approach has its limitations, which at the same time show some potential directions of future work. From a modelling point of view, the approach is conservative in the sense that it considers the worst-case scenario. While this is appropriate for intentional attacks, it might be too strong for natural disasters, potentially resulting in spending more resources than strictly necessary. Further, it might be worth distinguishing agents that try to protect the system, i.e., have more than two players. From a practical point of view, open topics include identification of strategies (e.g., based on standards, maybe atomized) and the implementation of the results in practice. Finally, refinements for specific users might be useful.

Acknowledgement

This work was supported by the research Project ODYSSEUS ("Simulation und Analyse kritischer Netzwerk-Infrastrukturen in Städten") funded by the Austrian Research Promotion Agency under Grant No.873539.

References

Baryannis, G., Validi, S., Dani, S. and Antoniou, G., 2019. Supply chain risk management and artificial intelligence: state of the art and future research directions. International Journal of Production Research, 57(7), pp.2179–2202. https://doi.org/10.1080/00207543.2018.1530476.

Berger, U., 2005. Fictitious play in $2\times n$ games. Journal of Economic Theory, 120(2), pp.139–154. https://doi.org/10.1016/j.jet.2004.02.003.

Bevilacqua, M., Ciarapica, F.E. and Marcucci, G., 2017. Supply Chain Resilience Triangle: The Study And Development Of A Framework. [online] https://doi.org/10.5281/ZENODO.1131597.

de Bruijn, K., Buurman, J., Mens, M., Dahm, R. and Klijn, F., 2017. Resilience in practice: Five principles to enable societies to cope with extreme weather events. Environmental Science & Policy, 70, pp.21–30. https://doi.org/10.1016/j.envsci.2017.02.001.

Datta, P., 2017. Supply network resilience: a systematic literature review and future research. The International Journal of Logistics Management, 28(4), pp.1387–1424. https://doi.org/10.1108/IJLM-03-2016-0064.

Deaton, B.J. and Deaton, B.J., 2020. Food security and Canada's agricultural system challenged by COVID-19. Canadian Journal of Agricultural Economics/Revue canadienne d'agroeconomie, 68(2), pp.143–149. https://doi.org/10.1111/cjag.12227.

Dubey, R., Gunasekaran, A., Childe, S.J., Papadopoulos, T., Blome, C. and Luo, Z., 2019. Antecedents of Resilient Supply Chains: An Empirical Study. IEEE Transactions on Engineering Management, 66(1), pp.8–19. https://doi.org/10.1109/TEM.2017.2723042.

Falasca, M., Zobel, C.W. and Cook, D., 2008. A Decision Support Framework to Assess Supply Chain Resilience. In: Proceedings of the 5th International ISCRAM Conference. ISCRAM. Washington DC, USA.pp.596–605.

Heckmann, I., Comes, T. and Nickel, S., 2015. A critical review on supply chain risk – Definition, measure and modeling. Omega, 52, pp.119–132. https://doi.org/10.1016/j.omega.2014.10.004.

Macdonald, J.R., Zobel, C.W., Melnyk, S.A. and Griffis, S.E., 2018. Supply chain risk and resilience: theory building through structured experiments and simulation. International Journal of Production Research, 56(12), pp.4337–4355. https://doi.org/10.1080/00207543.2017.1421787.

Monga, A. and Zhu, Q., 2016. On solving large-scale low-rank zero-sum security games of incomplete information. In: Information Forensics and Security (WIFS), 2016 IEEE International Workshop on. [online] IEEE.pp.1–6. Available at: <http://ieeexplore.ieee.org/abstract/document/7823923/>.

Münch, I., 2012. Wege zur Risikobewertung. In: P. Schartner and J. Taeger, eds. DACH Security 2012. syssec.pp.326–337.

Petersen, L., Fallou, L., Reilly, P. and Serafinelli, E., 2020. Public expectations of critical infrastructure operators in times of crisis. Sustainable and Resilient Infrastructure, 5(1–2), pp.62–77. https://doi.org/10.1080/23789689.2018.1469358.

R Core Team, 2018. R: A Language and Environment for Statistical Computing. [online] Vienna, Austria: R Foundation for Statistical Computing. Available at: <https://www.R-project.org/>.

Rajagopal, V., Prasanna Venkatesan, S. and Goh, M., 2017. Decision-making models for supply chain risk mitigation: A review. Computers & Industrial Engineering, 113, pp.646–682. https://doi.org/10.1016/j.cie.2017.09.043.

Rass, S. and König, S., 2018. HyRiM: Multicriteria Risk Management using Zero-Sum Games with vector-valued payoffs that are probability distributions. https://cran.r-project.org/package=HyRiM. Available at: <https://hyrim.net/software/>.

Rass, S., König, S. and Schauer, S., 2015. Uncertainty in Games: Using Probability-Distributions as Payoffs. In: M. Khouzani, E. Panaousis and G. Theodorakopoulos, eds. Decision and Game Theory for Security: 6th International Conference, GameSec 2015, London, UK, November 4-5, 2015,

Proceedings. [online] Cham: Springer International Publishing.pp.346–357. https://doi.org/10.1007/978-3-319-25594-1_20.

Sun, W., Bocchini, P. and Davison, B.D., 2018. Resilience metrics and measurement methods for transportation infrastructure: the state of the art. Sustainable and Resilient Infrastructure, 5(3), pp.168–199. https://doi.org/10.1080/23789689.2018.1448663.

Tills, C., 2018. Case Study: A.P. Møller-Maersk and NotPetya. [online] Available at: <https://www.clairetills.com/single-post/2018/05/20/Case-Study-AP-M%C3%B8ller-Maersk-and-NotPetya> [Accessed 7 May 2019].

Wicher, P. and Lenort, R., 2012. The ways of creating resilient supply chains. Carpathian Logistics Congress. pp.688–694.