Mathematical Aspects of Risk Management in Interconnected Utility Networks

STEFAN SCHAUER, SANDRA KÖNIG
Digital Safety & Security Department
AIT Austrian Institute of Technology
Lakeside B10a, 9020 Klagenfurt
AUSTRIA
{stefan.schauer, sandra.koenig}@ait.ac.at

STEFAN RASS
Institute for Applied Informatics
Alpen-Adria-Universität Klagenfurt
Universitätsstraße 65-67, 9020 Klagenfurt
AUSTRIA
stefan.rass@aau.ac.at

Abstract: Critical infrastructures together with their utility networks play a crucial role in the societal and individual day-to-day life. Thus, the estimation of potential threats and security issues is a core duty of utility providers. Despite the fact that utility providers operate several networks (e.g., communication, control and utility networks), most of today’s risk management tools only focus on one of these networks. In this article, we will give an overview on the mathematical foundations of Hybrid Risk Metrics, i.e., a novel risk assessment approach explicitly taking the interconnections and the interplay between the different networks into account. This approach has been developed as part of the HyRiM project and is based on a well-defined mathematical basis, considering game theoretic as well as stochastic concepts. We will provide insights on the main ideas behind Hybrid Risk Metrics and sketch the basic mathematical principles.

Key-Words: Risk Management, Game Theory, Percolation Theory, Interconnected Networks, Hybrid Risk Metrics

1 Introduction

Today, critical infrastructures represent the backbone of a large number of supply chains within the society. These critical infrastructures operate on several layers, starting from basic supply networks like water, gas or power, to more complex structures like information and communication networks and up to systems with a high societal impact, like transportation or the shipping of medical supply. Due to the growing and increasingly complex interconnections between these critical infrastructures, they became much more interdependent on each other over the last years, resulting in a very sensitive network (cf. Fig. 1) [1].

It is easy to see that due to this large number of interconnections, a failure within one critical infrastructure does not only affect the infrastructure itself, but potentially has a huge impact on several other dependent infrastructures as well as on the society as a whole. For example, the disruption of electric power in California in 2001 affected several other critical infrastructures, like the production of oil and natural gas as well as the transportation of gasoline through pipelines [2]. In 2003, a major electricity blackout lasting for 12 hours resulted in a financial damage in the order of €1182 million [3].

Fig. 1: Interdependent critical infrastructures [1].

Due to possibly huge consequences that potential failures within a critical infrastructure can have, the infrastructure operators, i.e., the utility providers, have to be very well prepared. In this context, an extensive risk assessment and risk management process represents one of the most important steps a utility provider has to take to be aware of possible threats against the critical infrastructure and the potential consequences of these threats. Unfortunately, most of today’s standard approaches towards risk management have a rather limited
scope and often do not focus on consequences going beyond a specific utility network or critical infrastructure. In this article, we present a novel approach to risk assessment that in particular takes into account the interdependencies among several utility networks and the potential cascading effects originating from a single incident.

In the following section, we will go into more detail on interconnected utility networks as well as the interdependencies within a single utility provider and introduce the notion of Hybrid Risk Metrics. Furthermore, in Section 3 we will describe the mathematical background of the Hybrid Risk Metrics. In more detail, Section 3.1 presents a way to compare different situations to perform a risk assessment, Section 3.2 focusses on a general framework for game theoretic risk assessment and Section 3.3 describes, how stochastic concepts can be used to model the spreading of failure across several networks and thus how to estimate the consequences of specific actions taken during the game theoretic analysis. The results are summarized in the conclusion’s Section 4.

2 Interconnected Utility Networks

2.1 Interdependencies Among Critical Infrastructure

Today, utility providers are well aware of the interconnections and interdependencies among critical infrastructures. There are several approaches in the literature trying to characterize these interdependencies [1][4][5] and various tools to support critical infrastructure protection [6][7][8]. Nevertheless, most of these methods and tools do not use a sound representation of these interdependencies when performing risk assessment and risk management. Thus the way to compute the respective cascading effects of these incidents is not fully comprehensible. In some articles, cross impact analysis [9] is described as one methodology to cover cascading effects but has also been criticized due to the problem of specifying the set of relevant events for the analysis [10].

As an alternative, we suggest to use percolation theory [11][12] to describe the propagation of failures through the different networks within a utility provider and to estimate the cascading effects. Percolation theory is a common tool for the analysis of epidemics spreading [13][14][15][16], and only rarely used in the fields of security and risk management so far. Nevertheless, it can be used as a framework to capture cascading effects, as we will show later on in Section 3.3.

2.2 Interdependencies within Utility Providers

The interconnections and interdependencies mentioned in Section 1 and depicted in Fig. 1 above are not only present among critical infrastructures but do also manifest within a specific utility provider. This is due to the fact that a utility provider usually does not just operate the utility network alone. On the contrary, several networks on different layers are required to be able to control and maintain a particular utility network. In general, a utility provider operates three major networks (cf. also Fig. 2):

- the utility’s physical network infrastructure, consisting of, e.g., gas pipes, water pipes or power lines
- the utility’s control network including SCADA (Supervisory Control and Data Acquisition) systems used to access and maintain specific nodes in the utility network
- the ICT network (information and communication technology), collecting data from the SCADA network and containing the organization’s business logic

These different networks exhibit a significant interaction among each other (just like the interaction between the critical infrastructures), which results in a high interdependency. For example, the compromising of a host located in the ICT network of a water provider, e.g., by social engineering or the usage of personally owned devices (bring-your-own-device – BYOD), could give an adversary access to the underlying SCADA network, where s/he may be able to shut down water pumps on the underlying utility network. On the other hand, using a vulnerability within a specific type of power concentrator (which can be easily
identified by the Shodan search engine\(^1\)) could allow an adversary to use the communication links within the smart power grid to get access to the energy provider’s internal ICT network.

### 2.3 Risk Management for Utility Networks and the HyRiM Project

As already mentioned above, the potential effects of a single failure in a specific network need to be addressed in the utility provider’s risk management. Despite the existence of numerous risk assessment tools and standards [17] [18] [19] to support the utility providers in estimating the nature and impact of these potential incidents, contemporary risk management is mostly a matter of best practices. Risk management tools are often focused on just one of the above mentioned networks (cf. Fig. 2) leaving out the specific and important interactions and cascading effects.

A general framework with the potential to model this interplay is game theory. Game theory not only provides a well-sound mathematical foundation but can also be applied without a precise model of the adversary’s intentions and goals. Therefore, a zerosum game and a minimax approach [20] can be used, where the gain of one player is balanced with the loss of the other. This can be used to obtain a worst-case risk estimation. Furthermore, more complex approaches as multi-criteria games can be defined, taking several security goals and their interplay into account [21]. Although game theory has not been extensively used in the field of risk and security management so far, there are solutions for specific problems where game theoretic algorithms provide a sound basis for risk estimation. For example, in the context of communicating in an ICT network, a game theoretic framework was presented, which estimates the risk of achieving a secure transmission while implicitly taking the interdependencies between three security properties (confidentiality, authenticity and availability) into account [20].

In the course of the FP7 project HyRiM\(^2\), we are focusing on these sensitive interconnection points between the different networks operated by a utility provider. As a main objective of the project, we are defining Hybrid Risk Metrics to assess security risks in these interconnected infrastructure networks. The major challenge lies in the variety of the utility networks and the different nature of threats acting on these networks. To go beyond the application of best practices and mostly qualitative risk assessment, the aim is to find a well-sound mathematical foundation for the Hybrid Risk Metrics and the interplay between the various networks. The application of game theory provides a suitable mathematical basis and also comes with the benefit to yield optimal defenses against worst case scenarios. Thus, game theory takes the uncertainty about the adversary’s intention into account and gives an optimal defense strategy against an adversary causing as much damage as possible. Since nature is intrinsically random, the outcome of these defense measures can also be random in some way. Thus, the HyRiM project focused on the definition of a general framework for decision-making based on a high degree of uncertainty, not only regarding the adversary’s strategy/intentions but also the defender’s payoffs [20], which marks a novel approach in the field of game theory.

In the following section, we will present the central building blocks of Hybrid Risk Metrics, describing how distribution-valued situations can be compared, how a novel game-theoretic framework based on distribution-valued payoffs can be formalized and how the propagation of failures in a network can be described.

### 3 Hybrid Risk Metrics

#### 3.1 Comparing Distribution-valued Consequences

A main task of risk management consists of choosing actions that yield to situations with minimal risk. In order to do this, it must be possible to compare between different situations, either due to expert opinions about the potential risk of these situations or due to the estimated damage it may cause. We introduce a new way to compare different situations applicable to both cases that allows us later on to find a situation with minimal risk.

Risk elicitation is often based on human expertise. A standard problem in risk assessment is how to deal with the diversity contained in such data. It is common practice to use a maximum principle, i.e., to identify a risk as “high” if at least one expert considered the risk to be “high”. While this method corresponds to the general intuition of ‘being on the safe side’ a lot of information is lost (i.e., it cannot be retraced how many experts agreed with this opinion). Thus, a new approach described in [20] allows a more accurate way of comparing elicitation of different situations.

The main idea behind this approach is not to aggregate several opinions into a single value (as it is done using the above mentioned maximum

---

1. [www.shodan.io](http://www.shodan.io)
2. Hybrid Risk Metrics for Utility Networks, [www.hyrim.net](http://www.hyrim.net)
principle) but rather to use all of the available data. More explicitly, assume we have a fixed number of categories to describe a situation’s risk, e.g., from “very low” to “very high”. We then record the number of occurrences of each such risk category in the expert opinions at hand and construct a preference relation \( \preceq \). For example, preferences based on these occurrences work by comparing the number of extreme opinions. In that special case (only), we have:

A situation \( S_1 \) is preferred to a situation \( S_2 \), i.e., \( S_1 \preceq S_2 \), if fewer experts consider the risk as “very high”. In case these counts are equal we compare the second-worst category and so on.

Analogously, the idea of focusing on the worst possible outcome (without ignoring the less extreme events) can be applied to situations where some information about the expected damage due to a security incident is given: we think of a situation to be ‘better’ if an extreme outcome is less likely than in another situation. The so constructed preference relation can thus be used to compare probability distributions and hence applies to the estimated loss-distributions.\(^3\)

These considerations in particular apply to situations where we can simulate the expected loss, e.g., by inspecting the effects of an event using percolation theory (cf. Section 3.3). Even if the simulated data is discrete, then we can compare the scenarios by counting and comparing the numbers of extreme outcomes as described in the previous section.

As this new preference relation allows us to compare two situations and decide which yields the smaller likelihood of extreme events, we are able to optimize our actions and even find an upper bound for the remaining risk as described in the next section.

### 3.2 Game Theory with Uncertain Payoff

Given a set of attack scenarios and a set of defense strategies, game theory provides a convenient way to optimize the defense. Considering an adversary who causes as much damage as possible (i.e., considering a worst case scenario), then this corresponds to a zero-sum game.

Optimization of multiple security goals simultaneously, can be deduced from the simple case of one goal: cast the two-person game where the defender pursues \( d \) goals into a \((d + 1)\)-person game, in which the defender is faced with \( d \) adversaries, each of which refers to a single security goal. This “one-against-all” game is called the “auxiliary game” [25] and is a theoretical vehicle to simultaneously deal with \( d \) mutually interdependent security goals (by using \( d \) copies of the original adversary).

Applying game theory to security goals has two main advantages (in the sense of having the following provable properties of the outcome):

1) **Assurance**: the resulting strategies are optimal in the sense that regardless the adversary’s behavior, the defender never suffers more damage than predicted by the game theoretic model approach. In particular, this corresponds to an upper risk bound for any situation.

2) **Efficiency**: there is no alternative strategy that would improve the predicted risk bounds in all matters of interest. Thus, the so-obtained defense strategies are optimal.

Traditionally, the above concepts are used for real-valued payoffs, where each specific attack and defense strategy yields an exact predictable damage. Still, the implicit assumption of actions leading to deterministic consequences is often violated. In many cases, actions have uncertain consequences thus making the risk control intrinsically random. Under these circumstances, the payoffs are described through probability distributions \( F_{ij} \) if defender and adversary choose scenarios \( i \) and \( j \), respectively. Thus, also the overall damage is described by a probability distribution,

\[
P(R \leq r) = F(r) = \sum_{i,j} F_{ij}(r)C_{pq}(i,j).\tag{1}\]

where \( R \) can be thought of as risk response (or repair cost, reliability or some similar quantity) and \( C_{pq}(i,j) \) describes the probability of this particular choice depending on their strategies \( p \) and \( q \). For actions being taken stochastically independent, we have \( C_{pq}(i,j) = Pr_q(j) \).

This makes the application of game theoretic models extremely difficult since the utility functions are probability-distribution-valued. To tackle this problem, a new kind of game in which uncertainty applies to the payoff functions rather than the player’s actions is introduced [21]. Based on that and on the preference relation introduced above, a framework is built to compute risk assurances on games with distributions as payoffs.

Roughly speaking, the basic algorithm to compute the optimal security strategy consists of two steps:

\(^3\) To avoid computational difficulties in the continuous case it is necessary to approximate the probability densities by their Taylor-polynomial approximations (up to a fixed order).
1) The loss distributions are estimated either based on records of earlier losses or on categorical data describing the intensity of the expected loss (such as “low”, “medium” and “high”).

2) A gameplay is “simulated” in which both the defender and the adversaries (each of which corresponds to another security goal) record each other’s actions and optimize their choices with respect to these empirical distributions. This algorithm is known as fictitious play (FP) [22] and can be adapted to the case of random payoffs, if we replace the ordinary order relation by the preference relation ≼ introduced above.

As the situation with multiple goals can be deduced from the one of a single goal, this algorithm can as well be generalized to find an optimal defense strategy in that case.

While this algorithm yields an optimal strategy for the defender, it does not deliver a concrete equilibrium strategy for the (physical) adversary but rather returns worst-case behavior strategy options for each of his goals. Thus, the result may pessimistically underestimate what happens in reality (as the true adversary is forced to choose a specific option out of many, thus necessarily deviating from some of the equilibrium strategies).

The sought risk bound \( r_k \) for goal \( k \) with expected payoff distribution \( F(k) \) is computed by

\[
r_k = F(k)(p^*, q^*) \geq F(k)(p^*, q^n) \quad (2)
\]

where \( p^* \) and \( q^* \) are the optimal strategies found by fictitious play concerning goal \( k \). For any other strategy \( q \) of the adversary, the risk will decrease due to optimality of the equilibrium \( (p^*, q^*) \).

Furthermore, the above algorithm allows prioritization of security goals (by setting parameters intrinsic to the equilibrium computation algorithms).

### 3.3 Propagation of Failures

A central concern of network operators is that an incident affects a significant part of the network and thus may yield to a complete breakdown. As pointed out above, percolation theory can be used to model how a failure of either a node or an edge will affect the rest of the network. The model developed in the HyRiM project requires only two basic inputs, i.e., the topology of the network and the chances of failure of its components, making it very general and easily applicable in different fields.

To understand how certain events trigger other events in a network, percolation theory has evolved into an indispensable tool. So far, these models do not entirely represent the structure of the network as they assign the same probability of failure to each component.

In real life, hardly any network will have components that will fail at uniform randomness (if they fail). To take this diversity (i.e., non-uniformity of failures) into account, the existing models have been refined in the HyRiM project in the following way: we classify all components into different types due to their nature (e.g., links of different kind, say wireless, physical, logical by email-communication, etc.). Then, we assigning a specific probability of failure to each type (based on expert opinions or on data from earlier incidents) and model the error/problem propagation based on these probabilities (e.g., malware spreading by email communication is different from its propagation over wireless links, etc.). This model allows us to compute the probability that an error affects a significant number of components, i.e., it causes an epidemic or even pandemic, as well as how many nodes are indeed affected in this case.

A pandemic (i.e., unbounded infection) is avoided if only the network’s error propagation properties obey certain conditions. Hence, we need to compute the expected size of an outbreak (measured in number of affected nodes) \( S_i \) due to failure of a component of type \( i \) and investigate under which circumstances this number remains finite in the long run. It shows that these expected values can be derived by solving a linear equation system which can be done in a straightforward way. The only ingredients required to formulate this equation system are the topology of the network in terms of how likely the existence of a connection of type \( i \) is and how likely a problem is to propagate over a connection in the network. Once this expected number of infections is known, we can characterize a pandemic as a case where these expectations become infinite.

A well-known model to describe the structure of a (random) network is due to Erdős and Rényi [23]. If we adapt this model to characterize the existing network with \( n \) nodes, the procedure described above yields a simple criterion: let \( q_i \) denote the probability that an edge of type \( i \) exists in the network and by \( p_i \) the probability that this edge fails. Then, a pandemic will not occur if

\[
np_1q_1 + \cdots + np_nq_n < 1. \quad (3)
\]

With this we are able to predict the influence of a single failure based on basic information about the network. Furthermore, this model allows computing
the probability that such an epidemic is triggered by failure of a single component.

Regardless of whether a pandemic occurs or just a few nodes are affected, a system of equations is available to determine the expected number of affected nodes. While in the case of a large scale outbreak this system might be non-linear and hence hard to solve, an explicit solution can be found for the Erdős-Rényi model.

Once we are able to model error propagation through a network consisting of non-uniform error propagation, this provides us with a tool to simulate which nodes are affected due to a single failure, and a direct criterion to decide about the risk of a pandemic. This further allows to estimate the consequences of changes to the network as we can carry out another simulation (or invoke the criterion) under these changed conditions. The results can be compared by the preference relation $\preceq$ introduced earlier and thus indicate which changes are worth implementing.

On the other hand, we are able to compare the consequences of different possible failures. These comparisons might indicate which components are more sensitive and thus require an increase protection.

4 Conclusion

In this article, we presented a novel approach towards risk assessment in interconnected utility networks defining the notion of Hybrid Risk Metrics. This concept addresses in detail the “hybrid” nature of the different networks (ICT, SCADA and physical utility network) operated by utility providers. These networks are often highly interconnected and an extensive interplay is given among these networks, such that a risk assessment focusing on each network separately would be insufficient.

Where common risk assessment and risk management tools are usually relying on best practices and qualitative assessments to estimate potential incidents and their impact, our approach uses sound mathematical concepts to evaluate threat scenarios. One of these concepts is game theory, which can be used to identify worst-case scenarios. Going beyond standard game theoretic models, we described a novel approach which takes distribution-valued payoffs in account, thus modelling the high degree of uncertainty regarding the intention and actions of an adversary, as well as nature itself.

As a second concept percolation theory is applied in our approach. This tool can be used to describe the propagation of a failure as well as its consequences not only in one of the networks operated by a utility provider, but it can also model the impact on the interconnected networks.

The combination of these two approaches represents a fundamental building block for our novel risk assessment approach, which is specifically suited for the requirements of utility providers and critical infrastructure operators. Planned next steps of the research in this field are the adaption of the general methodology onto specific areas of application (with the help of use cases identified within the HyRiM project) and the integration of additional information, e.g., on organizational and human factors, to refine the mathematical framework and to go beyond purely technical aspects.

Acknowledgement

This work was partially supported by the European Commission’s Project No. 608090, HyRiM (Hybrid Risk Management for Utility Networks) under the 7th Framework Programme (FP7-SEC-2013-1).

References:


