Markov Based Decision Support for Cost-Optimal Response in Security Management

Jutta Hild
Fraunhofer IOSB
jutta.hild@iosb.fraunhofer.de

Jonathan Ott
Karlsruhe Institute of Technology (KIT)
j.ott@kit.edu

Yvonne Fischer
Karlsruhe Institute of Technology (KIT)
yvonne.fischer@kit.edu

Christian Glökler
Fraunhofer IOSB
christian.glökler@iosb.fraunhofer.de

ABSTRACT

In this contribution, we introduce a prototype of a decision support tool for cost-optimal response in security management. The threat situation of a closed infrastructure, exposed to multiple threats, and the corresponding response actions are modeled by a continuous-time Markov decision process (CMDP). Since the CMDP cannot be solved exactly for large infrastructures, the response actions are determined from a heuristic, based on an index rule. The decision support tool's user interface displays the infrastructure's current threat state and proposes the heuristic response actions to the decision maker. In this way, global situation awareness can be enhanced and the decision maker is able to initiate an almost cost-optimal response action in short time.

Keywords

Security management, decision support tool, situation awareness, cost-optimal response, continuous-time Markov decision process, user interface.

INTRODUCTION

Critical infrastructures are the backbone of every industrialized society and thus demand extraordinary protection. Multiple threats such as accidents, natural hazards, crime, or terrorism menace these infrastructures. Avoiding disastrous impact from these threats requires early threat detection and correct assessment of the current threat situation in order to initiate the best response.

First choice to achieve these aims is surveillance of an infrastructure. This can be best accomplished by combining the complementary capabilities of human beings and state-of-the-art sensor and computer technology to form man-machine systems. Figure 1 illustrates such a surveillance system.

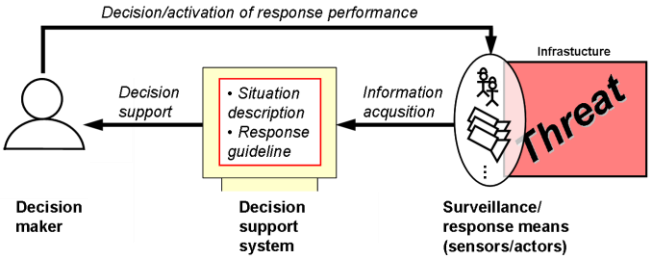

Figure 1. Man-Machine System to Accomplish a Surveillance Task

During surveillance, sensor equipment and security personnel acquire information about the infrastructure's threat state. From this information, a decision support system generates a description of the current threat situation that improves the decision maker's situation awareness. Additionally, the system provides response

Reviewing Statement: This paper represents work in progress, an issue for discussion, a case study, best practice or other matters of interest and has been reviewed for clarity, relevance and significance.

guidelines. Supported in this way, the decision maker selects and initiates the currently most appropriate response action. The key point of the framework is how to tailor the decision support to provide maximum benefit for the decision maker, i.e. how to get the best situation description from the acquired information and how to get the best response action for a particular situation.

Here, we focus on a surveillance task serving to protect a closed traffic infrastructure like a train station, an airport or a logistics center. In these domains, state-of-the-art surveillance is implemented primarily through security personnel, monitoring cameras, and alarm-triggering sensors. State-of-the-art decision support consists of operation guidelines, which define response rules for particular threat situations, usually based on extensive risk assessment and experience gathered through previous threat events. This might be sufficient and efficient in a single-threat situation where all response means can be focussed on one response task. In case of a multiple-threat situation with numerous threat events, all of them requiring prompt response, refined decision support considering the global threat situation might be necessary. Providing global situation awareness should support the decision maker to choose the globally best response action.

On the other hand, a comprehensive surveillance of a large infrastructure produces an abundance of situation reports. Particularly in a multiple-threat situation, this would result in information overload for the decision maker. In consequence, it is necessary to choose a representation of the situation description that draws the decision maker's attention to the most important site.

APPROACH

The first section of this chapter outlines how the previously defined aims, mainly a global view on the threat situation providing globally optimal response actions, can be accomplished by mathematical modeling of an infrastructure's global threat situation using a continuous-time Markov decision process (CMDP). The second section shows how to use the CMDP-model as a base for decision support. A decision support tool prototype is introduced, providing a representation of the current threat situation and the corresponding best response actions. The interface of the tool strives to provide global situation awareness for the decision maker, while avoiding information overload at the same time.

Providing a Global View and Globally Optimal Response with a CMDP-Model Defining a Threat Scenario

Modeling the Global Threat Scenario

In general, a threat scenario can be described by a controlled stochastic process. The infrastructure's threat situation, i.e. its current threat state, changes according to random threat events and is influenced by the chosen response actions. To model the threat scenario globally, we use the rich mathematical theory of continuous-time Markov decision processes (CMDP) (Puterman, 2005). A CMDP consists of a set of parameters describing the process states, its stochastic dynamics, available actions and corresponding costs. In our threat scenario, process states are the possible threat states of the infrastructure. They are defined by parameters describing the overall structure of the infrastructure (sectors and their dependencies) and a finite number of threat levels: A threat state is given by the set of threat levels of all sectors. The threat levels range from "no threat" to "immediate threat" and result from the occurrence rates of a finite number of threat events. Besides threat events, the stochastic dynamics of the process are modeled by parameters defining a set of response actions and available resources (e. g., a finite number of sensors and security personnel). Finally, parameters describe the corresponding costs for threat events and response actions respectively.

Global situation awareness is primarily provided by the infrastructure's threat state, which aggregates all sectors' threat levels. Threat state changes are triggered by events from outside (threat events and response actions). In addition, we model that changes are also influenced by the sectors' dependencies. Thus, the impact of an event is not only in the sector, in which it occurs, but also in dependent sectors. Considering the impact of a threat in such an extended way, the model definition facilitates early detection of threat to sectors that have not been threatened directly. For a detailed description of all parameters and their relations see (Bauer, Hild and Ott, 2009).

Determination of the Global Response Policy

Based on the model parameters, a solution of the CMDP is calculated by linear programming. The result is an optimal response policy that minimizes the expected total discounted costs of the CMDP; for formulas see

(Bauer et al., 2009). Since the definition of the threat scenario in the CMDP is global, the response policy is global as well. The policy contains the cost-optimal response action for every defined threat state of the infrastructure. It represents the recommendation of the decision support tool.

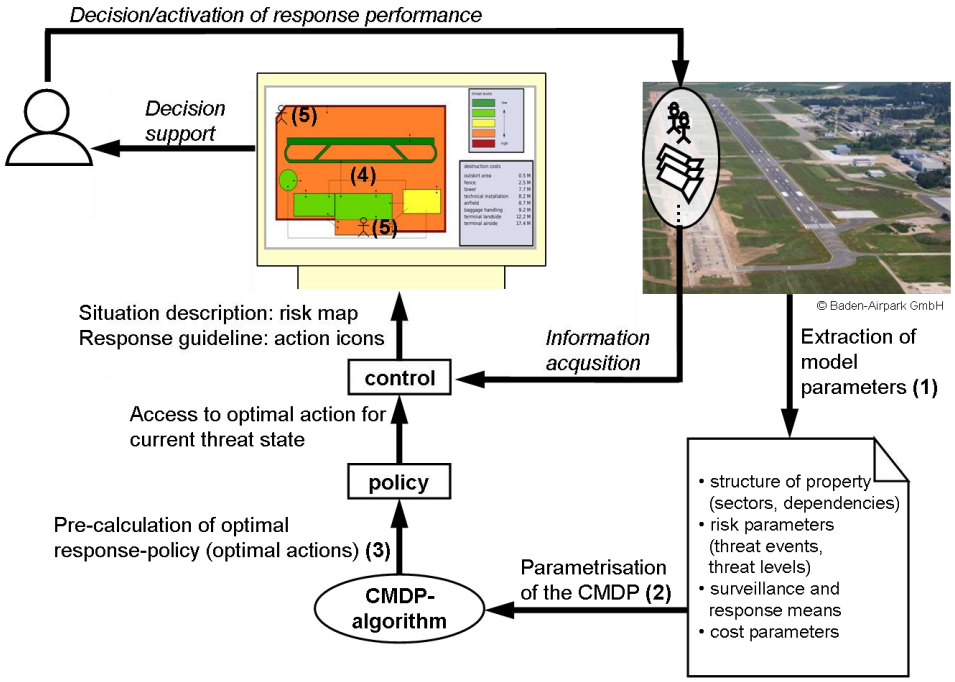

Figure 2. Decision Support in a Surveillance Framework Based on a CMDP

The Decision Support Tool Prototype

Applying the CMDP-Model in Operation

Figure 2 shows how a CMDP-model can be employed to provide decision support in a surveillance framework, using an example for a regional airport.

Using the CMDP-model as base for a decision support tool in operation of surveillance of a real infrastructure, parameter modelling and policy computation have to be done during a setup phase. At first, the threat scenario has to be described by parameter data as required by the CMDP model definition (see above) **(1)**. The parameters are similar to those which would have been collected for a state-of-the-art risk analysis of the infrastructure to formulate operation guidelines for security personnel. For this work, obtaining high-quality parameter data for the model parameters has been a challenging task. As the data in question is security-relevant, operators of infrastructures are reluctant in providing it. Even though our data has been reviewed by security experts it remains an educated guess at present. Based on the parameter data **(2)**, a solution of the CMDP is calculated by linear programming, resulting in an optimal response policy **(3)**.

In operation, the decision support tool links currently acquired information about the infrastructure's threat situation, the predefined model parameters and pre-calculated response policy. The result is a risk map **(4)** of the infrastructure plus a graphical representation of the recommended response action **(5)**.

Heuristic Policy for Large Infrastructures

Simple access to the policy as described above is possible if the computation of the optimal policy results in a two-column table that lists for every threat state the corresponding optimal action. An example introducing an exact computation of the policy can be found in (Bauer et al., 2009). Considering a real-sized infrastructure consisting of lots of sectors, the number of threat states grows exponentially with the number of sectors. Due to this curse of dimensionality, it is impossible to solve the minimization problem defined by the CMDP for large infrastructures. Therefore, one has to find a way to solve it as good as possible, such that the resources for computation suffice to obtain an approximation of the optimal policy in acceptable time.

In this section, we propose a heuristic which is based upon an index rule. Such heuristics compute indices for projects the decision maker is working on and choose to work on those projects with the highest indices. They are, for instance, considered in approximately solving so-called restless bandit problems (cf. (Whittle, 1988)). Earlier, (Gittins, 1979) has shown that a policy based upon an index is indeed optimal if the problem is a so-called multi-armed bandit, which is a special case of a restless bandit.

For our surveillance problem, assume that there are only a limited number r of security personnel available to the decision maker. To obtain the heuristic, all sub-infrastructures of size $m \geq r$ are considered as independent projects that can be worked on. Based on a threat state of the original infrastructure, we define an index for every sub-infrastructure which depends only on the corresponding state of the sub-infrastructure. Then the heuristic action is defined as the optimal action of the sub-infrastructure with maximal index. The size m of the considered sub-infrastructures should be chosen large enough to incorporate the essential dependencies of the original infrastructure. On the other hand, m should be sufficiently small as well, such that the optimal response policies of the sub-infrastructures are still computable. For large r, where there is no $m \geq r$ for which the problems corresponding to the sub-infrastructures are computable, other heuristics have to be used.

To get an idea of the quality of the heuristics in comparison to an optimal policy we consider the following numerical example. The infrastructure consists of four sectors and we define five threat levels for each sector.. The restrictions are $r = 1, 2$, i.e. the staff consists of one or two persons, respectively. In these cases, the infrastructures are not too large and exact solutions for the problems are available. Table 1 shows the minimal, average and maximal relative errors of the heuristic in comparison to the optimal costs. As one would expect, the quality of the heuristic increases with m for fixed r. On the other hand, the error seems to be small enough to use the heuristic policy as base for decision support.

r	m	Minimal relative error	Average relative error	Maximal relative error
1	1	5.01 %	5.49 %	7.13 %
1	2	0.25 %	0.34 %	0.73 %
1	3	0.11 %	0.16 %	0.58 %
2	2	1.72 %	2.00 %	3.30 %
2	3	1.12 %	1.28 %	2.53 %

Table 1. Results of the Numerical Example

The User Interface: Providing Situation Awareness

Figure 3 shows a user interface of the decision support tool giving a picture of the global threat situation of a regional airport. All sectors are depicted by idealized contour lines. The fill colour of a sector changes according to the sector's current threat state. The threat coding is done by five different threat levels, from "no threat" (dark green) to "immediate threat" (dark red). This mapping, commonly used for representation of warnings, ensures that the viewer's attention is directed to the most threatened sectors.

The optimal response action is directly represented in the risk map. In this example, the resources are restricted to two parallel response measures, which are either inspection by security personnel or analysis by camera. This corresponds to two elementary response actions in the model. Clear symbols ask for the appropriate action. To further enhance situation awareness, the interface also shows the sectors' dependencies (arrows) as well as their values (in million €). Thus, the decision maker is not only subject to the fixed policy recommendation, but they are supported in deciding differently, if necessary. The representation aims to avoid information overload by the following means:

- The representation abstracts from the single items of sensor information and integrates them to a single threat level. This results in clear action recommendations for the decision maker.
- Uncertainties, which are present in every information system, are not shown in the user interface as they are already considered by the threat event occurrence rates within the model definition.
- The user interface provides only model information which is relevant to enhance situation awareness.

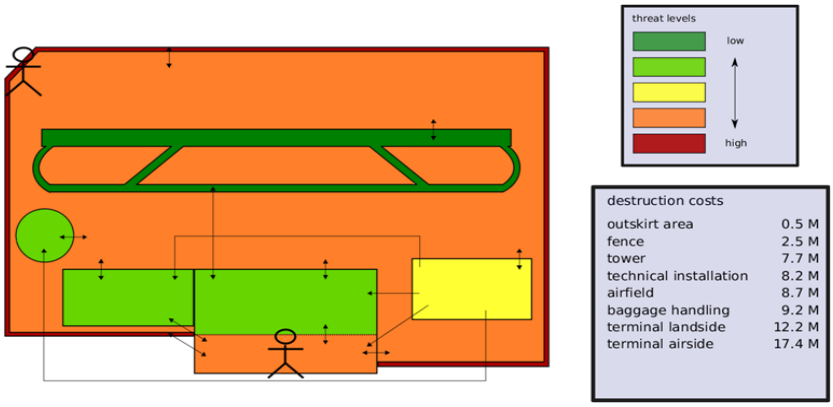

Figure 3. User Interface of the Decision Support Tool Prototype

CONCLUSION

In this contribution, a proposal has been made to improve decision support in security management by providing a global view of and globally optimal response to an infrastructure's threat situation. The rich mathematical CMDP theory seems to provide a promising method to meet this challenge. Our prototype generates a near-optimal response policy with respect to our simplified threat scenario model. The overall quality of the system will depend on the degree to which a real world threat scenario can be matched by the assumptions in the underlying model.

FUTURE WORK

In the near future, we will conduct an experimental evaluation of our prototype. Participants are security staff of a local company. The parameter data modelling the company's threat scenario has been revised by security experts. The aim is to determine to which extent the use of the decision support tool enhances the choice of the response action in a simulated threat scenario. As mentioned above, obtaining high-quality parameter data for the model parameters has been a challenging task. Future projects will strive for partners able to share their knowledge as "real" input to our model.

ACKNOWLEDGMENTS

We thank the German Federal Ministry of Education and Research, who kindly fund our work by the underlying projects 03BAPAC1 and 03GEPAC2. We thank the BIG Company, who kindly supports us with their knowledge in security management.

REFERENCES

1. Bauer, A., Hild, J. and Ott, J. (2009) Decision Support to Facilitate Cost-Optimal Response in Time- and Safety-Critical Situations, *Proceedings of Future Security 2009*, 322-338
2. Gittins, J. C. (1979) Bandit Processes and Dynamic Allocation Indices, *Journal of the Royal Statistical Society. Series B (Methodological)*, 41, 2, 148-164
3. Puterman, M. L. (2005) Markov Decision Processes: Discrete Stochastic Dynamic Programming, John Wiley & Sons
4. Whittle, P. (1988), Restless Bandits: Activity Allocation in a Changing World, *Journal of Applied Probability*, 25, 287-298