Agent-based Security and Efficiency Estimation in Airport Terminals

(Doctoral Consortium)

Stef Janssen
Delft University of Technology
The Netherlands
s.a.m.janssen@tudelft.nl

Keywords

Agent-based Modelling; Airport Terminal; Security Risk Assessment; Efficiency

ABSTRACT

We investigate the use of an Agent-based framework to identify and quantify the relationship between security and efficiency within airport terminals. In this framework, we define a novel Security Risk Assessment methodology that explicitly models attacker and defender behavior in a security scenario. It produces a security risk vector, quantifying the risks to the airport terminal. Efficiency is calculated in the same model using so-called key efficiency indicators. By using this framework, we aim to find and quantify factors that influence both security and efficiency in airport terminals. These factors can then be used to enable informed multi-objective decision making by airport management.

1. INTRODUCTION

Both airport Security Risk Assessment and airport efficiency estimation are well studied in literature. They are mostly studied as separate fields, while intuitively there is a relationship between them. For instance, manual checking of every bag passing the security checkpoint ensures high security standards, but introduces delay and therefore reduces efficiency. In this work, we aim to identify the factors that influence both airport security and efficiency. By identifying these factors one can gain fundamental insights into this relationship, useful for multi-objective decision making concerning security and efficiency.

As Security risk assessment and efficiency estimation are commonly performed using distinct methods, a unifying approach is needed to find a relationship between security and efficiency. Agent-based modelling forms a promising technique to achieve this, as it allows for independent analysis of both security and efficiency, but also enables simultaneous analysis. Agent-based modelling is further capable of incorporating socio-technical processes present within the airport terminal, often not possible in other methods. These socio-technical processes have an influence on both security and efficiency in airport terminals. This leads to the following question that is central to my research.

How can factors that influence the relationships between airport terminal security and efficiency be identified and quantified using Agent-based modelling?

To answer this question, the work is divided into three parts: (1) the development of an Agent-based modelling approach for Security Risk Assessment, (2) modelling of efficiency using Agent-based Modelling, and (3) analysis of the relationship between efficiency and security using Agent-based modelling. We introduce the Agent-based model that forms the basis of the research, and discuss each of these three parts in more detail below.

Appears in: *Proc. of the 16th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2017), S. Das, E. Durfee, K. Larson, M. Winikoff (eds.), May 8–12, 2017, São Paulo, Brazil.*

2. PROPOSED APPROACH

We define an Agent-based model in which we distinguish three blocks: Agent, Environment and Meta-Analysis. In the Agent block we distinguish three types of human agents: Defenders, Attackers and Other Agents. Defender agents are responsible for the defence of the airport terminal. They for instance are X-Ray officers, bag checker agents and walk through metal detector officers, each responsible for a different security element within the system. Defenders interact with each other to find unwanted behavior and unwanted items of attacker agents. Attacker agents execute actions aimed to cause losses to the system. Other Agents are for instance passengers and airport visitors.

The Environment block of the framework contains elements like flight schedules, sensors and physical structures. The Meta-Analysis block of the framework analyses the model to assess the security situation and estimate efficiency, forming the core of this research. This is discussed in more detail below. An overview of the framework is shown in Figure 1.

2.1 Security Risk Assessment

In Security Risk Assessment, one aims to (quantitatively and/or qualitatively) identify the risk(s) to a system. Traditionally, quantitative Security Risk Assessment is performed by using a commonly used Risk function:

$$R(s_i, T) = P(s_i, T) \times P(\mathit{fail}|s_i) \times C(s_i)$$

where we define $R(s_i, T)$ as the risk value of security scenario s_i in some time interval T, often known as *Risk*. Then, the probability that security scenario s_i will happen in interval T is known as *Threat (Likelihood)* and denoted $P(s_i, T)$. $P(\mathit{fail}|s_i)$ is the probability that all defence measures present in the system fail, if s_i were to happens, defined as *Vulnera-*

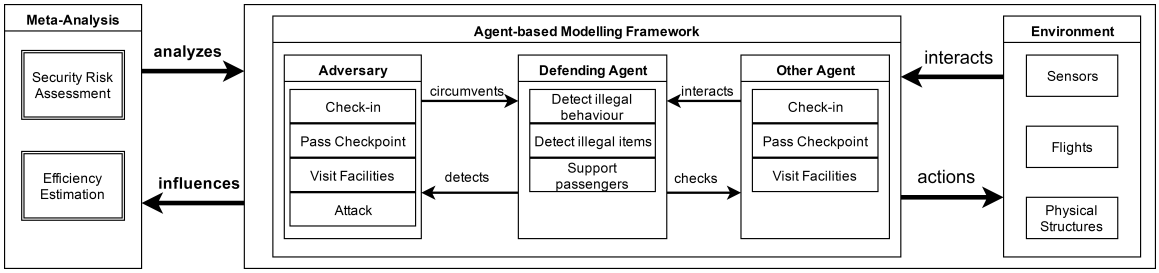

Figure 1: Overview of the Agent-based Modelling Framework, containing Agents, an Environment and a Meta-Analysis block. The agent part of the framework contains three types of agents: attackers, defenders and other agents. The body of each agent shows activities it can execute. The Environment contains airport specific elements like sensors, a flight schedule and physical structures like walls. Meta-Analysis is responsible for security & efficiency analysis of the system, the core of this thesis.

bility. Finally, $C(s_i)$ is known as *Consequence* and quantifies losses in case security scenario s_i happens. Each of these factors is determined by security experts, often relying on probabilistic tools, relevant data and experiences [5].

It is often noted that this method is unable to incorporate intelligent and dynamic properties of an adversary [1, 3]. It further strongly relies on the skills of the security experts.

To overcome this problem, we propose a novel Security Risk Assessment methodology to estimate both *Vulnerability* and *Consequence* by using Agent-based modelling. Compared to other methods found in literature, this agent-based method for Security Risk Assessment is capable of more realistic representation of socio-technical processes present within the system. It further reduces dependency on security experts and results in potentially more accurate quantitative results. Results of this Security Risk Assessment can be used for both the traditional method described above, but can also be used as payoff values for game theoretic methods, as for instance defined by Tambe and his colleagues [2].

The method is defined as follows. We estimate *Vulnerability* using a so-called Fail function.

$$F(m_i^j) = \begin{cases} 1 & \text{Defender fails.} \\ 0 & \text{Attacker unsuccessful.} \end{cases}$$

Where m_i^j represents instance j of simulation model m_i. *Consequence* is estimated using a (real-valued) Consequence function $C(m_i^j)$ that quantifies the direct and indirect losses of the system.

We define attacker behaviour in simulation model m_i to correspond to attacker behaviour as defined in some identified security scenario s_i. Defenders and other agents like passengers are modelled as well. We perform Monte Carlo simulations to estimate *Vulnerability* $\hat{F}(m_i)$ and *Consequence* $\hat{C}(m_i)$ of security scenario s_i based on the repeated outcomes of the Fail function and Consequence function. These values can then be used to estimate a risk value r_i for the security scenario s_i. By applying this method to a set of security scenarios, a vector of risks $R = (r_1, ..., r_n)$ can be obtained, quantifying the different risks for a system.

2.2 Efficiency Estimation

We take a terminal oriented view on airport efficiency, commonly referred to as *terminal efficiency*. We define terminal efficiency $E = (e_1, ..., e_m)$ as a vector of Key Efficiency Indicators (KEIs), based on the work of Martens [4]. KEIs represent efficiency-related variables considered important by an airport. This can for instance be space efficiency, revenue per passenger, revenue per employee and so on. The above defined Agent-based model can then be used to estimate these parameters under different circumstances. Airport efficiency data will be used to validate these findings.

2.3 Security and Efficiency Interactions

After gaining insights into security and efficiency independently, we will aim to find factors that influence the relationship between them. To do this, we will use the above described methods for security risk assessment and efficiency estimation. These methods generate a vector of risks $R = (r_1, ..., r_n)$ and Key Efficiency Indicators $E = (e_1, ..., e_m)$ that quantify security and efficiency respectively. Factors like number of employees, X-Ray machine type and airport layout will then be analysed to determine their influence on these output vectors. This can for instance be done by using methods of global sensitivity analysis. After these factors are identified, a structure of direct and indirect relations between these factors will be determined. This structure will support multi-objective decision making concerning both security and efficiency.

REFERENCES

[1] G. G. Brown and L. A. T. Cox Jr. How probabilistic risk assessment can mislead terrorism risk analysts. *Risk Analysis*, 31(2):196–204, 2011.

[2] M. Brown, A. Sinha, A. Schlenker, and M. Tambe. One size does not fit all: A game-theoretic approach for dynamically and effectively screening for threats. In *AAAI conference on Artificial Intelligence (AAAI)*, 2016.

[3] L. A. T. Cox Jr. Some limitations of "risk = threat× vulnerability× consequence" for risk analysis of terrorist attacks. *Risk Analysis*, 28(6):1749–1761, 2008.

[4] R. Martens. Benchmarking the efficiency of terminal processes at regional airports. In *Air Transport and Operations: Proceedings of the Second International Air Transport and Operations Symposium 2011*, page 327. IOS Press, 2012.

[5] A. Washington. *All-Hazards risk and resilience: prioritizing critical infrastructures using the RAMCAP Plus SM approach*. ASME, 2009.