10.20378/irb-58521

Mobility in Computer Science

Prof. Dr. Wilfried Honekamp

Academy of Hamburg Police, Carl-Cohn-Straße 39, 22297 Hamburg,
wilfried.honekamp@polizei-studium.org

Prof. Günter Koch

Humboldt Cosmos Multiversity, Tenerife, Canary Islands, Spain

Mobility in modern times is almost always accompanied by the application of computer science. In relation to this year's focus on mobility and security, the following three contributions show one commonality: different aspects of organising, exercising and maintaining security in the public space. The scope of the three topics reached from protection of public infrastructure, in concrete the Hamburg Sea Port and its logistics, then switch to the aspect of police force operation planning, and finally ending at the individual level of protection of individuals using near-field communication (NFC) technology in payment systems infrastructure.

A different aspect in applying automated algorithms is presented by Tobias Cors and his co-authors: They describe their approach on how to find an optimal solution in making best use of capacities of police force organised in so-called shifts, in combining a multitude of aspects to be considered as are

- district organisation (technically defined by radio areas),
- availability of police forces in the districts,
- availability of patrol cars,
- distances to arrive at a location of incident,
- frequency and intensity of occurrences – predictable, e.g. in case of events and by daily profiles, as well as unpredictable caused by random incidents,
- type of mission (162 mission causes have been identified), and
- mission variances and mission mixes.

The approach taken by the simulation building team is to conceive a simulation solution based on a stochastic process model which includes the following functions in stepwise sequence:

- ABC classification of incident = mission cause,
- analysing probability of mission occurrence by matching it against profile data available,
- travelling time calculated taking into account the resources available as well as using empirical data,

- identifying the mission profile fitting to the given case, also using prior cases for comparison, and
- documentation effort in the course of finalising a mission.

The simulation program is instantiated by a discrete event simulation model which, for inputs, uses the many different aspects mentioned above and tries to bring them in balance thereby finding the optimum. No question that the "algorithmisation" must be based on rules as have been designed by the programmers versus human-based experience. I.e. the validity of the solution by the simulation developed is to be measured by comparing the prediction made by the simulation program versus the real case. As for now, the predictions by simulation prove to come close to the real cases, however, this comparison also provides hints which parameters need special attention to be adapted. Future improvements are foreseen w.r.t. a) target KPI values making best use of the police force, b) inclusion of heuristics and c) finding best solutions by playing with a variety of capacity plans. As a consequence from this experiment, optimisation considerations will be started on the organisation and dimensioning of districts, as well as to find optimal shift plans.

The contribution by Lars Damm and Wilfried Honekamp starts from the widest perspective addressing the vulnerability of large and complex infrastructures as is the Hamburg Sea Port, Europe's second largest port after Rotterdam. The Hamburg port logistics is operated by the HHLA (Hamburger Hafen und Logistik AG) and its IT department which covers the operation of the whole process from the container ship, via the container bridge, the container portal crane transport to the storage location and finally to the transfer of the containers to trucks and trains in their specific stations. From a data perspective three dimensions need to be covered which are

- workflow data for managing the different processes steering the flow of containers,
- allocation data maintaining the consistency between storage location and specific containers, and
- business data associated with the contents of containers.

All software and data are run in the HHLA-own system, the HHLA network. Due to the size and complexity of this system there exists a multitude of points of attack for outside intruders which may enter e.g. through web portals or communication connections as well as through usual user interfaces. Malware from outside can be infiltrated potentially through mail attachments, mobile data media (e.g. USB flash drive) or by access processes attempting phishing attacks or simply by human operators with doubtful intentions. In consequence the management of the HHLA IT is challenged to monitor and to discover cyberattacks applying a variety of methods as are

- general risk analysis,
- integrative analysis of data received from end points and sensors,
- intelligent combination of recognising different occurrences indicating an attack,
- identification of risks / attacks by means of artificial intelligence (AI), especially deep learning algorithms usually implemented through neural networks, and
- permanent observation of data traffic and identifying abnormalities at the firewall interface.

The challenge is not only to apply these different techniques rather than a) to continuously build or purchase own intelligent algorithms for recognition and defence of attacks, b) to exchange information with other institutions employed in defending against cyberattacks as are malware defence software producers, internet security service providers or partnering companies with which complementary insights gained on their side is being exchanged. Acquiring information, data and software for defending cyberattacks is a permanent activity operated by HHLA's IT, i.e. a permanent activity in producing prototype algorithms to be tested in different scenarios and, of course, even more in the case of a current attack. In order to obtain an idea on the dimension of damage produced by a cyberattack, the authors quote cases in which a container transport company had to suffer a decrease in turnover of up to $ 300 Mio. or cases when drug trafficking using containers remained undiscovered due to manipulations introduced by hackers smuggled into the IT organisation.

A case touching the question of personal risk management is discussed in the paper of Jonathan Reimers and Wilfried Honekamp on the use of near-field communication (NFC) in payment applications, first hand using credit cards. NFC is based on RFID (Radio Frequency Identification) and allows two types of communication

- peer-to-peer: two active NFC units communicate actively with each other, and
- reader/writer mode: an active NFC unit communicates with a passive one which acts as a transponder.

The second case is the most commonly used application in practice and is best known by using credit cards with an element for touchless communication for payment e.g. at cashpoints. The point discussed in this paper in respect of security is that the physical radio signal distance between an active reader and a corresponding passive unit can be > 50 cm, however, in practice 30 cm and less are common. Such distance is large enough so that a person with an active reader as could be a smart phone can interfere with the transponder on a credit card.

The project reported is about tests reading data from a credit card using a smart phone with an NFC reader function as is available for free as an app (e.g. "Contactless Credit Card Reader"). The number of tests under each condition were 100 and the objective

was, if and how much and which data could be read from a corresponding transponder on a credit card under different physical circumstances. In the different conditions in the test series it turned out, that a single credit card with transponder function could be read with success at ~ 80% if loosely carried e.g. in a jeans or jacket or backpack pocket. Success in building communication goes down at < 25% if carried in a leather bag and is 0% when protected by an aluminium foil or a special protection box.

The paper describes which data can be extracted from a credit card and how this data can be used for credit card payment e.g. for internet orders. The objective of this research project is to identify and to recommend protection measures to avoid NFC data stealing, as are

- usage of special credit card boxes blocking RFID communication,
- putting credit cards in bigger container units such as large handbags,
- observing credit card transaction on bank account, and
- creating public awareness on the possibility of being pickpocketed.

In sum, as pointed out at the beginning, this panel session covered all dimensions from very large infrastructures down to urban districts and further down to a personal level discussing the question of how to protect against criminal data theft, data manipulation and cyberattacks. All the three papers explore “objects on the move” and how criminal intervention can damage the moving targets. The excitement of this panel is to learn about the dimensionalities of such problems as well as about the methodologies to cope with the challenges raised.