TRENDS IN ANALYTICS FOR PROTECTING CRITICAL INFRASTRUCTURE

Adam Zagorecki[1], Jozef Ristvej[2], Krzysztof Klupa[3]

ABSTRAKT

V rámci článku sa zaoberáme trendmi spojenými s aplikáciou informačných technológií a najmä analýzou dát na problém ochrany kritickej infraštruktúry. Zameriavame sa na technológie zamerané na automatický zber údajov a analýzy, ktoré môžu rozšíriť zvyšovanie poskytovania zabezpečenia kritickej infraštruktúry do budúcnosti. Ďalším záujmom sú technológie, ktoré sú na začiatku vývoja a ktoré majú podľa nás potenciál na podporu zabezpečenia do budúcna. Začíname technológiami, ktoré podporujú fyzické aspekty zabezpečenia, biometrické technológie, ďalej analýza videa, senzorov a integrácia/fúzia dát. V závere rozoberáme stručne analýzy v rámci kybernetickej bezpečnosti.

Kľúčové slová:
Kritická infraštruktúra, analýzy, bezpečnosť.

ABSTRACT

In this paper we review the key trends related to application of information technology and in particular automated data analysis to the problem of protecting critical infrastructure. We will focus on technologies that use automated data collection and analyses that can be exploited for improving security provision for critical infrastructure in the future. Of our particular interest are technologies that are at relatively early stage of adaptation and in our judgement have potential to significantly affect how the security is provided in the future. We start our discussion with technologies that support physical aspect of security: biometric technologies, video analytics, sensors and integration/data fusion. Then we briefly discuss analytics in context of cyber-security.

Key words: Critical infrastructure, analytics, security.

[1] Dr. Adam Zagorecki, Senior Research Fellow, Cranfield University / Defence Academy of the UK, Shrivenham SN6 8LA, United Kingdom, email: a.zagorecki@cranfield.ac.uk.
[2] Ing. Jozef Ristvej, PhD., odborný asistent, Katedra krízového manažmentu, Fakulta špeciálneho inžinierstva Žilinská univerzita v Žiline, Slovensko, e-mail: Jozef.Ristvej@fsi.uniza.sk.
[3] płk dr Krzysztof Klupa, doktor nauk wojskowych, Prodziekan Wydziału Nauk o Bezpieczeństwie Wyższej Szkoły Oficerskiej Wojsk Lądowych we Wrocławiu

1 INTRODUCTION

The terrorist attacks on September 2001 have changed the perception of critical infrastructure security. These attacks were characterised not only by sophistication of planning and execution but as well the selection of targets – a diverse set of critical infrastructure buildings that included government, defence and commercial [1]. Those were followed shortly by London bombings and attack on trains in Spain, proving that complex attacks on critical infrastructure are becoming a new trend in terrorism [2].

In this paper we review the key trends related to application of information technology and in particular automated data analysis to the challenge of protecting critical infrastructure. We focus on technologies that use automated data collection and analyses that can be exploited for improving security provision for critical infrastructure in the future. Of our particular interest are technologies that are at relatively early stage of adaptation and in our judgement have potential to significantly change how the security is provided in the future. We mostly focus our discussion on technologies that support physical aspect of security: biometric technologies, video analytics, sensors and integration/data fusion. Then we briefly discuss analytics in context of cyber-security. We focus on the man-made threats to critical infrastructure. These are typically divided into two categories: physical threats and cyber threats. We want to emphasise that this division does not imply that these two categories are separate in fact one should expect that more sophisticated attacks in the future should combine the two domains.

2 DATA ANALYTICS FOR SECURITY

Data analytics [3] is the process of discovery and communication of meaningful patterns in data typically with use of data-mining techniques [4]. It has become a very prominent trend especially in business context (often referred as business intelligence). The premise behind the analytics is that the use of (objective) data gathered on multiple aspects of the problem (data fusion) should improve understanding of the problem and provide new insights. In the context of providing security to critical infrastructure, one should be able to use data coming from various sensors, cameras and other data sources (for example: authorised users database) to improve provision of security by enhanced capability of identifying security breaches, reducing costs of providing security and supporting security personnel in their tasks [5]. Below we review key classes of technologies that in our opinion are becoming prominent for providing security and rely upon or explicitly use analytics.

2.1. BIOMETRICS

The biometric technologies [6] are aimed at verifying personal identity – ensuring that only authorised personnel is able to access the area or perform tasks by measuring some physical aspect of a person. The most popular biometric techniques focus on the following aspects: finger prints, face recognition, and iris scans. All of

them make use of sophisticated digital data analysis. Below we will briefly discuss all four types.

Finger prints have been recognised as a useful tool of identification individuals as early as 19th century. It has been recognised that this method of biometrics is relatively easy to bypass and susceptible to noise while reading, often requiring multiple scans. However, it is accepted that this technique can be successfully used as an additional security measure in order to increase security by diversifying methods.

Face recognition is considered as natural and least invasive method of biometric identification. Facial recognition systems range from software based solutions to complete close circuit TV systems. The technology relies on samples of images of an individual stored in the database against which the pictures taken by cameras are compared. In practice high-quality enrolment material is essential, with quality of the enrolment material determining the performance of the system. The face recognition systems have advantage for environments with a large number of people – public transportation to mass events. However, one should remember that this technology is relatively easy to be fooled and therefore not suitable for situations where high reliability is required from a biometric system.

Iris recognition is believed to be the most promising of the biometric methods. The iris patterns are believed to be unique to an individual, constant over time and not subject to changes caused by medical conditions. Scanning process is performed using a camera (visible or near-infrared light) and therefore is non-invasive (unlike retina scanning). In terms of accuracy it has low occurrence of false positives and extremely low of false negatives. The iris recognition systems have been fielded in some environments, however at the current stage they have not been widely accepted with some systems being withdrawn (e.g. UK Iris Recognition Immigration System). Particular challenges include requirement for good quality samples and relative ease to fool the system by presenting an image.

In summary the biometric technologies are considered to be immature and not sufficiently reliable to provide definitive ways of authentication in large scale and general setting. However, with time they may become more mature and they are likely to provide increased levels of authentication, especially when their accuracy and speed will be increased.

2.2. VIDEO ANALYTICS

The sophistication and costs related to digital imagery have drastically dropped due to advancements in related technologies. In the result, modern digital imagery systems may not only record high quality images and videos, but as well allow for more and more sophisticated means of image analysis [7]. The types of image analyses vary in complexity which translates into ability of automated systems to address those problems. We can identify four key types of analytics that relate to security-based tasks:

- Motion detection – a simple task of detection of changes in an otherwise static image. This task is extremely useful for identifying situation that may potentially require security officer's attention in order to analyse the scene.
- Object detection and classification – a task of automated interpretation of images in order to identify particular types of objects of an interest (e.g. a person or a van).
- Object recognition – for example face recognition. A task of identifying a particular instance (e.g. person) of an object.
- Object tracking – a task of following an object on an image, or even following the object in a series of images (using views from different cameras).

Automated image analysis is a relatively new domain with first more sophisticated practical applications (such as face recognition) being fielded no more than 15 years ago. More sophisticated functionalities such as object tracking are still on relatively early stage of maturity. One of interesting problems with the image processing techniques are differences between reported performance of algorithms achieved in the laboratory setting and actual fielded applications. Similarly, it has been often reported that the performance claimed by suppliers is much higher to that achieved by fielded systems. These may be not necessarily due to intentional actions, but due to the nature of phenomena related to algorithm evaluation and it emphasises the fact that a proper scientific approach to evaluation of such systems is necessary. From practical perspective, substantial research is needed till such systems will achieve desirable performance. Another challenge with video analytics is that they require relatively large computational power due to sheer amount of data encoded in an image. Therefore further computational performance improvements can make video analytics even more prominent for providing security in the future.

2.3. SENSING TECHNOLOGIES

During the recent decade a revolution in development of sensing technologies has taken place. Examples of different sensors include:

- Accelerometers – which are so affordable, that often they are installed 'just in case' in other electronic devices
- Digital cameras – experiencing dramatic lowering of costs and improvements in terms of resolution
- Transmitters/receivers -- which allow for communication between sensors and the information infrastructure
- Other sensors such as temperature, pressure, light, etc.

An example of a sensor platform is a smart phone – a typical smart phone includes all the above sensors – and typically it is not strictly required by the primary function of the device (making phone calls) but the sensors are included just because they are affordable and can provide value added to the user making the model more competitive on the market. Sensors are able to produce large volumes of data which can be used by data-mining algorithms to derive automatically new knowledge of the

domain. However a common misconception should be clarified here – the data produced by sensors do not imply the useful knowledge – this should be extracted from the data through the analytical processes that are not trivial. Therefore the sensors should be considered as an enabling technology with analytics required to make efficient use of the data generated by sensors.

2.4. INTEGRATION

The key trend in security systems is integration [8] – security systems are becoming more integrated and it can be observed at several levels:

- Monitoring of several buildings or structures from the same location by exploiting remote sensing and telecommunication infrastructure that allows for transferring video streams. The primary benefit of such integration is lowering security costs by reducing number of personnel and facilities.
- Integration with other building systems (such as HVAC, electrical systems, etc.). The purpose of it is utilising common infrastructure and useful information about the state of the monitored infrastructure that can be used to inform security.
- Integration with business processes – for example integration with organisational data warehouse to use up to date personnel data for the security purposes. The purpose of such integration is reduction of organisational costs and enhancing security by means of data fusion.

3 CYBERSECURITY

In the recent decades the rise of cyberspace and related threats associated with this domain has been observed and widely discussed in the literature [9]. In particular it is the networked nature of the monitoring systems and their connectivity to the Internet that creates a bridge between providing physical security and the cyberspace. This is not intention to discuss cyber-security threats and application of analytics in this paper, however automated intrusion detection systems based on constant monitoring and automated interpretation of data are an active and very promising research field [10].

4 CONCLUSIONS

In this paper we outlined the trends in analytics for the problem of providing protection for critical infrastructure. The field of analytics is currently dynamically developing and in our opinion it is at a relatively immature not only for security applications but for a wide spectrum of applications in general. The trends from other domains (especially business) indicate that the data fusion and the concept of ‘big data’ carry a promise of revolutionary changes in analytics in general. If it will be the case – it is yet to be seen. But certainly some more basic applications and concepts outlined here have a potential to substantially affect how the security for critical infrastructure will be implemented.

Cyber threats and cyber-security are emerging phenomena. Even though that the immense number of strategies, reports, white-papers and both professional and academic papers have been proposed and published, we are yet to see the development of these threats into a security daily reality.

Príspevok vznikol ako súčasť projektu výskumu:
„Táto práca bola dofinancovaná Agentúrou na podporu výskumu a vývoja na základe zmluvy č. DO7RP-0025-12“.

REFERENCES

[1] EDWARDS, M., Critical Infrastructure Protection, Volume 116 of NATO Science for Peace and Security Series - E: Human and Societal Dynamics, M. Edwards (ed.), IOS Press, 2014.
[2] LEWIS, T.G., Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Wiley, May 2006, ISBN: 978-0-471-78628-3.
[3] KOHAVI, R., ROTHLEDER, N.J., and SIMOUDIS, E., Emerging Trends in Business Analytics. Communications of the ACM 45 (8): 45–48, 2002.
[4] HAN, J., KAMBER, K. and PEI, J., Data mining: concepts and techniques. Morgan Kaufmann, 2006.
[5] SHANKAR, M. RAO, N. and BATSELL, S. Fusing intrusion data for detection and containment. In Proceedings of the 2003 IEEE conference on Military communications - Volume II (MILCOM'03), Vol. II, 2003. IEEE Computer Society, Washington, DC, USA, 741-746.
[6] JAIN, A.K.; ROSS, A.; PANKANTI, S., Biometrics: a tool for information security. Volume: 1 Issue: 2, Issue Date: June 2006, page(s): 125 – 143
[7] KO, T., A survey on behavior analysis in video surveillance for homeland security applications. In Applied Imagery Pattern Recognition Workshop, 2008. AIPR'08. 37th IEEE, pp. 1-8. IEEE, 2008.
[8] BASS, T., Intrusion Detection Systems and Multi-sensor Data Fusion. Communications ACM 43, 4, April 2000, 99-105.
[9] MILLER, R.A. Cyber war realities—What lies ahead, International Journal of Critical Infrastructure Protection, Volume 5, Issue 2, July 2012, Pages 84-85, ISSN 1874-5482.
[10] DI PIETRO, R., and MANCINI, L. V.. Intrusion detection systems. Springer, 2008.

Článok recenzovali dvaja nezávislí recenzenti.