ASSESSMENT OF THE PROBABILITY OF CYBERATTACKS ON TRANSPORT MANAGEMENT SYSTEMS

Yoana A. Ivanova

Department of Informatics, New Bulgarian University
e-mail: yivanova@nbu.bg
Bulgaria

Abstract: This paper is considered to be a continuation of two previous publications devoted respectively to study of the impact of cyber-attacks on a Traffic Control Centre (TCC), (IJIITS, № 2, 2017) and urban Automobile Transport Systems (ATSs), (IJITS, № 3, 2017). The research presents a method for assessing the probability of cyberattacks on Transport Management Systems (TMSs), whose specificity is due to the use of simulation results in qualitative and quantitative risk assessment.

Key words: probability, risk, transport management, cybersecurity, cyberattacks, modelling, simulation, air pollution, harmful emissions.

1. INTRODUCTION

The advanced Transport Management Systems (TMSs) are characterized by improved communications and coordination between the management and control centres, vehicles and the other integrated components that are determined by the type of a transport system. In this paper the focus is on Automobile Transport Systems (ATSs) which operates in the urban environment, whose main components are Traffic Control Centre (TCC), Traffic Signal Control System (TSCS), GPS-based systems for control of vehicles and Video Surveillance Systems (VSSs).

Actually, some essential aspects of evolution of TMSs as a whole are the automation of processes and innovative solutions as virtual and cloud computing. If the term "cloud computing" is discussed two components should be analysed: cloud infrastructure (hardware and network resources for supporting proposed cloud services and cloud software applications. The business on the cloud has some important advantages at moving their data to the cloud and data centers – this permit to centralize the management of data centers, cloud services and applications [1].

Specifically, with regard to TMSs the main benefit of their use is higher efficiency of the transport systems. By accumulating transactional data, these systems can serve as data warehouses as well. When coupled with optimization and

simulation capabilities, the TMS can provide critical support for optimal network design and lane analysis [2]. But it is necessary also to take account of the probable risks, because using cloud technologies could create prerequisites for physical and cybersecurity issues. Consequently, in this case the main efforts should be aimed at strengthening security.

Therefore, it is necessary the traditional approach for assessment and analysis based mostly on experience from past adverse events to be adapted to the new needs due to the dynamic evolution of cyber threats. This does not mean that the model of next-generation cybersecurity excludes conclusions of previous experience, but includes implementing advanced methods for more effective data assessment and analysis. In fact, simulation modelling is an example of a minimizing investment costs contemporary method for obtaining reliable data for various scientific and technical applications. Information resources based on previous experience can be entered in the knowledge bases of expert systems.

The author has used two professional simulation environments (Riverbed Modeler Academic Edition 17.5 and Aimsun 8.0) to make the empirical research which is described in this paper. In Section 2 is presented the expert approach to risk assessment based on the assessment of the probability of a DoS attack on the main components of TMS (TCC and TSCS) and a conditional expert determination of the expected damage. Sections 3 and 4 contain the two consecutive and logical connected stages of the study and the calculations made respectively for TCC and TSCS.

2. EXPERT APPROACH TO RISK ASSESSMENT

Ensuring a reliable protection of TMSs from cyberattacks requires a correct approach to assessing the risk of cyber threats as well as a prediction of the possible adverse consequences. The risk refers to the deviation of one or more results for one or more future events from their expected value.

At the highest expert level, comparatively simplified risk assessment methods are widely used in view of the need for timely action and reducing the decision-making time. Therefore, the expert method to risk assessment is the most widely used. This method of quantifying the risk is based on the Source - Pathway - Recipient - Consequence - S-P-R-C model, which is suitable for risk assessment at all levels. In its essence this is a relatively simplified conceptual model presenting the system and processes that lead to undesirable consequences and damages.

Considering that the probability is a ratio of the number of selected random events to the total number of events, then the risk values can be calculated by a multiplication of probability (P) and the damage (C) ***[R = P*C]*** and presented as a function of P ***[R = f(P)]*** by a probability distribution.

3. ASSESSMENT OF THE PROBABILITY OF CYBERATTACKS ON A TRAFFIC CONTROL CENTRE

In this case the focus is on the number of the adverse events (m) under the impact of a DoS attack on the TCC for each of a total of 10 consecutive scenarios. The used simulation environment is Riverbed Modeler academic Edition 17.5.

The parameter T is interarrival time that specifies the distribution name and arguments to be used for generating random outcomes for times between successive packet generations in the "ON" state [3]. The author sets different values of T respectively in M_{Ref} and under the impact of a cyberattack, while the default values of all other parameters remain unchanged.

On the basis of previous summary evaluations of the results the author makes the assumption that these adverse events are expressed in anomalous values of "traffic sent" ($T_{S, max}$) and "traffic received" ($T_{R, max}$) compared to the reference model M_{Ref}. The sent and received traffic are measured in packets per second [packet/s]. The number of all events for each scenario is n = 6, because the duration of the simulation is divided into 6 equal intervals of 5 seconds.

Table 1 contains the calculated probabilities of a DoS attack (P) and the possible damage (C), as well as a quantitative risk assessment (R). The author makes a conditional expert determination of the expected damage based on the number of registered adverse events for each scenario. It is logical that the greater number of adverse events should cause more damage. Practically, if m = 0, then C = 0 and if m = n = 6, then C is taken as a maximum of 1 (100 %). Consiquently, if m = 1 and n = 6, then C is a ratio of 1 to 6. Its value is respectively 2, 3, 4 or 5 times more if m = 2, 3, 4, 5.

The probability distribution is graphically represented in Figure 1.

Table 1.

Scenario	***T [s]***	***m***	***P***	***C***	***R***
1	2	1	0.17	0.17	0.03
2	1	1	0.17	0.17	0.03
3	0.5	1	0.17	0.17	0.03
4	0.25	2	0.33	0.33	0.11
5	0.2	3	0.50	0.50	0.25
6	0.15	2	0.33	0.33	0.11
7	0.1	1	0.17	0.17	0.03
8	0.05	2	0.33	0.33	0.11
9	0.025	2	0.33	0.33	0.11
10	0.02	1	0.17	0.17	0.03

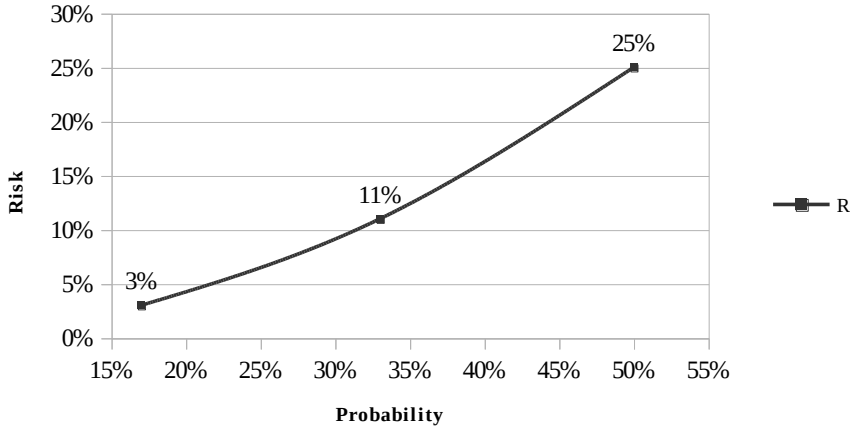

Fig. 1. Graphical interpretation of R=f(P) for TCC / ATSs.

The maximum values of P and R are registered in Scenario 5. A qualitative assessment of the risk can be made based on generally accepted standards for the risk areas. The average risk value in this case is 8 %. It is accepted that R < 20 is admissible and special measures for its reducing are not required. Actually, if the average risk of 8 % is low or high is relative, because the simulation duration is 30 [s], while a cyberattack may take much longer.

For reducing the risk the same simulation process can be repeated after the placement of a an additional protection between the attacker and the switch in the modelled TCC. The number of the adverse events with a firewall insertion are shown in Table 2 respectively for Scenarios 1 (initial), 5 (intermediate) and 10 (final). The simulation results ffrom the selected three scenarios are presented in Table 3 to show the better filtration due to the firewall placed on the way of the DoS attack. Consequently, the registered adverse events are also reduced when there is a firewall insertion.

The comparison between the average risk value for the selected three scenarios in this case and the average risk value for the relevent scenarios 1, 5 and 10 with a built-in protections only shows reducing the risk from 10,3 % to 4,67 % which is more than 2 times less.

Table 2.

Scenario	***T [s]***	***m***	***P***	***C***	***R***
1	2	0	0	0	0
5	0.2	2	0.33	0.33	0.11
10	0.02	1	0.17	0.17	0.0

Table 3.

Scenario	***T [s]***	***Buili-in protections***		***Firewall insertion***	
		$T_{S,\,max}$ ***[pack/s]***	$T_{R,\,max}$ ***[pack/s]***	$T_{S,\,max}$ ***[pack/s]***	$T_{R,\,max}$ ***[pack/s]***
1	2	10	9	9	3.4
5	0.2	20	13.5	16.6	7.7
10	0.02	60	41	56	26.

4. ASSESSMENT OF THE PROBABILITY OF CYBERATTACKS ON URBAN AUTOMOBILE TRANSPORT SYSTEMS

This empirical research is another example of probability assessment based on simulation results obtained using Aimsun 8.0. It is a logical continuation of the situation described in Section 3, because the realization of a DoS attack on the TCC could cause a disruption in the normal signalling of the traffic lights. The assessment method is also analogous of the previous one, but in this case the adverse events are related to the road traffic and ecological issues.

In this sense congestions and accidents are observed as a result of changing certain parameters characterizing the road traffic like: Flow (F) in vehicles per hour [veh/h], Delay time (T_D) in seconds per kilometer [sec/km], Mean queue (Q) in vehicles [veh]. The lowest crash rates (crashes per vehicle mile traveled per lane) tend to occur at intermediate levels of flow. Controlling for traffic density – rather than flow – also is key, since low flows can occur under both uncongested (high speed) and congested (low speed) conditions [4].

As well as imposing high costs on industry and road users through wasted time and fuel, delayed deliveries and reduced reliability, congestion increases air pollution. Ecology is the scientific study of the interrelationships between living organisms and their environment [5]. Therefore, another object of the current simulation research are harmful emissions like particulate matter (PM), carbon oxides CO_x, NO_x, volatile organic compounds (VOC) and etc. In this way the author aims to show their increasing concentration in grams [g] in the air for a certain mileage [g/km] as another negative effect of cyberattacks.

The main aim of this part of the simulation research is to show how the levels of the selected air pollutants increase under the influence of cyberattacks on the TSCS. These levels are measured in the simulation environment Aimsun 8.0 using the embedded in *Panis et al Emission Model*. Actually, the concentrations of harmful emissions in the air can depend on the climatic conditions. Therefore, the selected simulation system provides the opportunity to choose among a few working modes, including various meteorological settings. But for the purpose of unambiguous analysis of the impact of a DoS attack the simulation measurements are made for dry

weather without counting other external factors as precipitation or fog. In the particular case the pollution should not have an additional negative impact on cybersecurity, because the time interval of the impact of a DoS attack is short for observing any side effects related to the normal functioning of the systems. The physical protection the transportation modes, routes, terminals and communication and information systems must be reliable enough to meet the national security requirements remaining well protected against a direct impact of common and accidental environmental factors. For example, the Intelligent Disaster Decision Support System (IDDSS) provides a platform for integrating a vast range of road network, traffic, geographic, economic and meteorological data as well as dynamic disaster and transport models. Recent development in sensor networks, spatial data analysis procedures and traffic models provide an opportunity for improving the management of traffic during disaster events [6].

Consequently, the adverse events observed by the author mainly in two crossroads under the impact of a cyberattack can be classified into three main categories:

- *Traffic congestions* – they are observed in one time interval respectively in Scenarios 1 and 2. There are prerequisites for congestions in two time intervals in Scenarios 3 and 4 which are also reported as adverse events.
- *Accidents* – an accident is simulated in Scenario 1.
- *Elevated levels of pollutants* – the pollution is particularly intense in Scenario 1 due to the elevated levels of all pollutants mentioned above.

The selected road section is modelled by a team of scientists [7, 8] in the simulation environment Aimsun 8.0 and includes three crossroads. It is assumed that the cyberattacks cause changing the average duration of signalling for green light respectively with – 10 and + 10 seconds compared to the reference model M_{Ref} when D is equal to 20 [s]. Table 4 consists anomalous values registered in each of all 5 scenarios based on analysing the simulation graphical results. The simulations are executed for a time interval from 10:00:00 to 11:00:00 am which is divided into 6 equal intervals of 10 minutes. Therefore, the number of all events for each scenario is n = 6.

In Aimsun 8.0 D = 1 [s] in Scenario 5 is simulated the potential fatal situation when the traffic lights stop functioning absolutely under the negative impact of a DoS attack. Based on the simulation graphical and tabular results generated for the parameters mentioned above it is assumed that m = n = 6 in the last scenario. Obviously the values of the risk in the interval from 25% to 100% can be determined and analysed based on the graphic shown in Figure 2.

Table 4.

Scenario	***D [s]***	***m***	***P***	***C***	***R***
1	10	3	0.50	0.50	0.25
2	30	1	0.16	0.16	0.03
3	10	2	0.33	0.33	0.11
4	30	2	0.33	0.33	0.11
5	1	6	1	1	1

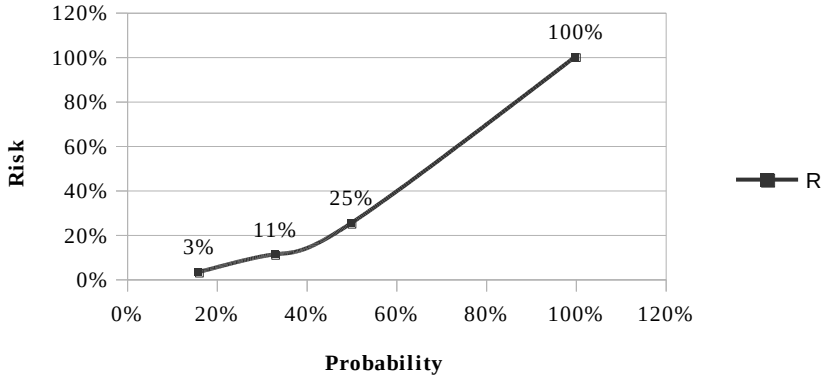

Figure 2. Graphical interpretation of R=f(P) for TCC / ATSs

5. CONCLUSION

The described method can be a basis for a series of sequential algorithms which can be used in the process of predicting the preliminary risk of cyberattacks on TMSs. For example, the randomness in agent based modelling can be presented schematic by block diagrams [9]. For a stochastic model it is recommended multiple scenarios to be performed in order to the effective study of complex systems.

Besides, since cloud computing depending on virtualization, this class of vulnerability can affect not only a single virtualization system but also any system that operates within the same virtual infrastructure. A vulnerability in an operating system or an application may lead to the compromise of a single server within an infrastructure [10]. Consequently, if data for the vulnerabilities of TMSs are available, then the risk assessment can be made by the „method of the three factors" (3F) that is analogical to the expert approach to risk assessment, but includes also a vulnerability assessment.

The main advantage of this method is that it allows use of data generated during the simulation process. Another advantage of the method is that it gives a possibility for a conditional expert analysis of the damage. It should be noted that the application of the method is associated with some conditions as a resource provision including a professional simulation software and suitable computing equipment to create a

quality end product. For example, it can represent an assessment and analysis, as well as recommendations for the selection of appropriate means of protection of TMSs.

REFERENCES

[1] Romansky, R., *A Survey on Digital World Opportunities and Challenges for User's Privacy*, International Journal on Information Technologies and Security (IJITS), Issue №3 (December), 3 (Vol. 9), 2017, pp. 103 - 104.

[2] Griffis, S. E. and Goldsby, T., *Transportation Management Systems: An Exploration of Progress and Future*, Journal of Transportation Management, The Ohio State University, 2007, pp. 28.

[3] Riverbed Technology, Inc. *Introduction to Riverbed Modeler Academic Edition: Common procedures when using Riverbed Modeler Academic Edition,* USA, 2014.

[4] Kockelman, K., *Chapter 12. Traffic Congestion in the Handbook of Transportation Engineering*, McGraw Hill, 2004, pp. 5.

[5] O'Flaherty, C. A., Bell, M. G. H., Bonsall, P.W., Leake, G.R., May, A. D. and Nash, C. A., *Transport Planning and Traffic Engineering,* Elsevier Butterworth-Heineman, Oxford, UK, 2006, pp. 16 - 37.

[6] Kaviani, A., Thompson, R. G., Rajabifard, A., Griffin, G. and Chen, Y., A *Decision Support System for Improving the Management of Traffic Networks During Disasters,* Department of Infrastructure Engineering, the University of Melbourne, Victoria Police, Sydney, Australia, 2015.

[7] Vachova, B., Boneva, Y. & Paunova, E. Optimization and intelligent management of traffic - Traffic modeling (in Bulgarian), Sofia: IICT – BAS, 2015, pp. 144 - 153.

[8] Balabanov, A., Stoilov, T., and Boneva, Y. Linear-Quadratic-Gaussian Optimization of Urban Transportation Network with application to Sofia Traffic Optimization, Cybernetics and Information Technologies, Sofia: IICT – BAS, 3 (vol.16), 2016, pp. 165 - 184.

[9] Borshchev, A., The Big Book of Simulation Modeling, Multimethod Modeling with AnyLogic6, AnyLogic North America, 2013, pp. 277, 577.

[10] Graham, J., Howard, R., Olson, R. Cyber security Essentials, CRC Press, Taylor & Francis Group LLC, London, United Kingdom, 2011, pp. 30 - 40.

Information about the author:

Eng. Yoana A. Ivanova – Teaching assistant in the Department of Informatics at NBU; Area of scientific research: Applications of Information Technologies in Security, Communication and Information Systems and Technologies in Security;

Manuscript received on 11 October 2018