SIMULATION MODELLING AND ASSESSING THE IMPACT OF CYBERATTACKS ON URBAN AUTOMOBILE TRANSPORT SYSTEMS

Yoana A. Ivanova

"Information Technologies for Security" Department
Institute of ICT, Bulgarian Academy of Sciences
e-mail: y.ivanova@bas.bg
Bulgaria

Abstract: This paper presents the study framework and results in assessing the consequences of cyberattacks on urban automobile transport systems. Consequences in two attack profiles, involving semantic hacking on the one hand and a DoS - attack on the other, are assessed via modelling using the transport simulation system Aimsun. The author compares the negative impact of cyberattacks on urban transport in terms of increased delay and possible traffic accidents, as well as elevated levels of pollutants in the air.

Key words: cybersecurity, cyber threats, cyberattacks, critical infrastructure, urban transport, impact assessment, air pollution, harmful emissions, modelling, simulation software, Aimsun.

1. INTRODUCTION

Intelligent Transportation Systems (ITS) incorporate advanced information and communications technologies and integrated software solutions in order to increase the efficiency of traffic management, as well as user's awareness and mobility. Automation, communications and integrated electronics contribute to improvements of the modern transport systems and provide significant advantages, while at the same time making them vulnerable to effects exercised via cyberspace. There are numerous opportunities for malicious attacks, as well as a variety of methods and means to predict, prevent, and protect against such attacks, as well as to mitigate the consequences, recover the proper functioning of transport systems and/or increase their resilience.

The resources available for that purpose, however, are limited. Risk assessment and risk mitigation provide a widely-used decision-making framework [1, 2]. Its implementation requires rigorous and systematic assessment of possible attacks and their likelihood, as well as their consequences in view of the vulnerabilities of the

system under study. In most practical cases, the respective assessment is challenging, due to the complexities in determining the source of attack, its motives and objectives, the possible rapid escalation of the threat, the complexity and intensity of the modern communications and information processes, the dynamics of the logical and physical links and related uncertainties [3]. The most significant damages are caused by cyberattacks on sectors of the critical infrastructure and vulnerabilities introduced by advanced management and communications systems. For example, a successful cyberattack against the traffic control centre of a transport system can interfere into the normal signalling of the traffic lights, leading to serious and sometimes fatal consequences. The approach to countering such threats involves, *inter alia*, prevention by employing suitable technical equipment, sustainable devices, antivirus software, firewalls, etc. Further, effective resource allocation requires a capacity to assess the threat landscape in its evolution and, respectively, to look for security solutions able to counter continuously developing cyber threats.

There is a body of evidence demonstrating the potential do disrupt critical infrastructures by cyberattacks [4]. The practical approach is to use simulation based on proven and, to the extent possible, verified models of both cyberattacks and transportation management systems.

The next section of this paper provides an overview of the automobile transport, explaining the author's motives to focus on it in the experimental research that is described in Section 6. Section 3 is dedicated to the automobile transport systems and their main characteristics for a better knowledge of the nature and functionality of the simulated complex system, while section 4 describes in what way possible hazards and threats might disrupt its normal operation mode. Section 5 presents the architecture of study. The obtained modelling results are presented and analysed in section 6.

Each section from 2 to 6 can be considered as a separate step of a methodology for conducting the research related to an urban ATS in the following order:

- ***Section 2 (Step 1).*** A reasonable choice of automobile transport for the current research based on its high efficiency and negative environmental effects.

Percentages of cars with petrol, diesel and gas engines relative to the total number of registered cars are entered as input data in the embedded Panis et al Emission Model ***[Section 6]****.*

- ***Section 3 (Step 2)***. Getting acquainted with the basic components of ATS s and their subsystems that could be affected by a cyberattack such as the Traffic Signal Control System.

Only the flow of cars entering the road section has been entered in the input data. The impact of a cyberattack is simulated by changing the value of the input parameter duration of signalling (D) for the green light ***[Section 6]****.*

- ***Section 4 (Step 3).*** A classification of all potential existing threats to transport systems in order to clarify the difference between physical and cyber threats.

The first series of experiments aims to show the impact of a semantic attack by minor changes to the input parameter D. The second series of experiments shows how a DoS – attack stops the operation of traffic lights by setting the minimum acceptable value of D in Aimsun 8.0 ***[Section 6]***.

- ***Section 5 (Step 4).*** Clarifying the main aim of the experimental research: reduction of vulnerabilities by creating policies to strengthen cyber security of the critical infrastructure based on simulation results obtained.

The author refers to an analogous experimental study in a physical environment in order to prove that a DoS – attack on Traffic Signal Control Systems due to specific vulnerabilities which should be reduced ***[Section 6]***.

- ***Section 6 (Step 5).*** Running the simulation.

The conclusion underlines the advantages of using simulations in supporting decision making on resource allocation to enhance security and safety of critical infrastructures. Furthermore, recommendations are given on how the study can be extended.

2. ADVANTAGES OF AUTOMOBILE TRANSPORT AND NEGATIVE CONSEQUENCES OF ITS USE

On one hand, the choice of the automobile transport for this study is determined by its undeniable advantages as the main mode of transport:

- the largest network coverage of roads.
- the greatest variety of vehicles compared with other modes of transport.
- manoeuvrability and comparative independence from environmental conditions.
- no delays due to a large number of initial - end operations [5].

Unfortunately, the benefits of using automobile transport cannot compensate its strong negative effects on the environmental pollution by harmful emissions and respectively on the health of humans and all living organisms.

Furthermore, the road pavement also contributes to the air pollution due to the release of particulate matter and particles of the asphalt coverage. The heavy traffic in the big cities in combination with atmospheric effects (high air humidity, solar radiation, low wind speed, temperature inversion of the air) is one of the main causes of photochemical smog, consisting of particulate matter, soot, lead oxides and photochemical oxidants (ozone, nitrogen dioxide NO_2, sulphur dioxide SO_2, etc.).

3. COMPONENTS OF AN AUTOMOBILE TRANSPORT SYSTEM

The transport system is a combination of all modes, vehicles, roads, transport interchanges, warehouses and repairers. *"Automobile"* means three or more wheeled trackless motor-powered vehicle, used for transportation of passengers and cargo, or for towing other vehicles. The automotive vehicles can be classified according to their technically permissible maximum weight when loaded, specified by the manufacturer depending on their design and performance. The allowable size and weight are determined by the vehicle type. Generally, the permissible maximum weight of vehicles is between 18 and 44 tons.

According to their intended purpose automotive vehicles are:

- *Passenger cars*, used for transportation of passengers, whit the number of passenger seats not exceeding eight.
- *Trucks*, used for freight services and/or towing a trailer.
- *Buses*, for transportation of passengers, with number of passenger seats exceeding eight.
- *Trolleybuses* – buses powered by electricity.
- *Special vehicles* with permanently installed equipment, facilities or machines that do not allow their use for other purposes.

The structure of an automobile transport system includes also the following integrated components:

- *Traffic Signal Control Systems* coordinating individual traffic signals to achieve network-wide traffic operations objectives. These systems consist of intersection traffic signals, a communications network to tie them together, and a central computer or network of computers to manage the system. Coordination can be implemented through several techniques including time-base and hardwired interconnection methods. Coordination of traffic signals across agencies requires the development of data sharing and traffic signal control agreements. Therefore, a critical institutional component of Traffic Signal Control is the establishment of formal or informal arrangements to share traffic control information as well as actual control of traffic signal operation across jurisdictions [6].

Effective day-to-day operation of the control system requires several routine tasks and procedures to assure continuity of operation; obtain and retain archival data, assure security of the system database and software, and ensure that the system is operated by authorized personnel [7].

- *Freeway Management Systems* are strategy-based and consist of components and technologies combined to monitor, control, and manage freeway traffic more effectively. Strategies/system components and technologies in use include: ramp control (e.g., ramp metering, ramp closure); freeway mainline metering; freeway-to-freeway metering;

reversible roadway control (e.g., lane control, variable speed control); priority control for high-occupancy vehicles (HOV) (e.g., priority access control, HOV facilities); transportation management during reconstruction; surveillance and detection (e.g., vehicle detectors, call boxes, CB monitoring, weather and environmental detection, over height vehicle detection, automatic truck warning system, closed circuit television (CCTV); driver information systems (e.g., changeable message signs (CMS), lane-use control signals, highway advisory radio, call boxes and commercial telephone, in-vehicle systems); communications (e.g., media types, data and voice, video).

Freeway management includes a Freeway Management Centre (or multiple centres where responsibility for the freeway system is shared by more than one operating entity in a metropolitan area) and links to other ITS components in the metropolitan area. From these centres, staff electronically monitors traffic conditions, activates response strategies, and initiates coordination with interagency and interagency resources, including emergency response and incident-management providers when necessary [8].

- *Transit Management Systems* include Automatic Vehicle Location (AVL) technologies and computer-aided dispatch systems to help keep buses on schedule and improve service. Some cities have integrated the bus system with the traffic light system at key intersections. This increases the green lights along these routes by only a few seconds, but results in a valuable reduction in transit travel time [9].

Transit-management software is designed to optimize the use of all implemented technologies. It is a part of an integrated management system often located in Transportation/Transit Management Centres [10].

- *GPS-based systems for control of vehicles* are developed especially for the transport sector and use GPS tracking and GPRS data transfer through mobile operator. The monitoring and control of each vehicle is performed by a compact GPS device, which consists of a GPS receiver and GPRS module. Each automobile can be observed from a computer with Internet access. The location information is updated at intervals. The detailed information for the traffic and routes can be obtained daily, weekly or monthly according to the customer needs. Such GPS-based systems provide current location data; data for the technical parameters of the vehicle at any time of the motion; history of motion; working hours of the vehicle; consumed fuel; routes and many other parameters; graphical and textual data visualization.
- *Video Surveillance Systems* perform wireless transfer of video signals from vehicles in real time. Their main components are video cameras and GPS navigation module connected to a digital video recorder, whose output is

connected to a 3G modem. The monitoring system uses global mobile networks, using GPRS – 3D to transfer video via an encrypted link. The system stores a local record in the vehicle. This function continuously connects the vehicle to the central server regardless of the distance.

Transport management systems may include in addition electronic fare payment technologies, electronic toll/ fee collection, incident management systems, traveller information services, links to emergency management services, etc.

4. EXTERNAL INFLUENCES ON THE FUNCTIONING OF ITS

Intelligent transport systems (ITS) function in an environment characterized by various hazards and potential threats. For the purposes of this the author distinguishes two types of threats – physical and cyber.

The *physical threats* can be intentional, accidental or caused by natural disasters. Data storages and hardware are most vulnerable to a number of internal and external forces that can damage or destroy them: material instability; climatic and environmental factors (temperature, humidity, light, dust); continuous exploitation; infrastructure failure (plumbing, electrical, climate control); inadequate hardware maintenance; hardware malfunction; human error) [11].

Cyber threats come in many forms and continuously evolve. At current, the threats in cyberspace can be classified as follows:

- *viruses* – boot sector virus, file-infecting virus, macro virus, polymorphic virus, stealth virus, etc.
- *malicious software (malware)* – exploit, dropper, logic bomb, crime ware (Trojan, worm), spyware (Trojan), ransomware, botnets, etc.
- *web attack* – SQL injection, Cross-site scripting, DNS cache poisoning.

The most common cyberattack is *DoS* (Denial-of-Service), in which the attacker overloads the server with requests and user queries cannot be processed. In a *DDoS* (Distributed Denial-of-Service) attack the attacker uses not one, but multiple computers [12]. The principle of action can be likened to a "chain reaction" in which the infected computer becomes a conductor of the attack to other computers.

In a particular form of attack via cyberspace, the attacker manipulates the incoming sensor information [e.g. 13] in a way that the result is incorrect, yet a casual or even an attentive viewer may be seeing it as correct [14]. This attack can be caused by someone, who has gained access to the sensor reading or the stored sensor data. Then the sensor data are modified in a way that is not too obvious. That may involve changing the data values or their timing, e.g. by introducing delays. The idea behind such attacks is that the attacker wants to manipulate sensor data, but s/he cannot alter too much the values or postponing too much time slots, otherwise can easily be detected.

The most common threat to transportation management centres is from malware that can cause damages to a system, even when a centre is not connected to Internet. Portable media players, cell phones, and compact disks can be conductors of malware [15].

Generally, the simulated cyberattack can be determined as semantic hacking. For its realization is necessary the attacker to gain access to the Traffic Control Centre, the communications link transmitting the signal, or the controller of the traffic light. The control signals are manipulated by him in a way that is not too obvious by reducing or increasing the duration of the green light signal in comparison to a reference model signal, that has been optimised in some sense.

In particular, this cyberattack is a form of an Advanced Persistent Threat (ATP) – a relatively new class of cyber threats has some certain characteristics that distinguish it from the traditional threats. Specific characteristics of APTs are: specific targets and clear objectives; highly organized and well-resourced attackers; long latency period; and difficulty in detecting the intrusion. At the stage of initial intrusion of a malware into the target system, detection is still possible. Sandboxing execution, for example, is a proven technique for analysing malware's behaviour, which allows defenders to identify unknown advanced malware [16]. Actually, cyber-threats evolve and are no longer limited to a single malware executable, but often comprise targeted, multi-stage attacks that are difficult to spot using only file- and signature-based malware detection systems.

5. IMPORTANCE OF POLICIES FOR CYBERSECURITY OF CRITICAL INFRASTRUCTURE

The policies for protection of critical infrastructures from cyberattacks are particularly important for overall strengthening the national security.

Formulation, as well as implementation of policy is based on sound understanding of the threat landscape. Here, the role of cyber threats intelligence is to help network defenders, threat hunting teams, and incident responders to research and analyse trends and technical developments in the following directions: *cybercrime, cyber activism, cyber espionage* (advanced persistent threat – APT).

Four types of CTI can be distinguished: *tactical*, related to attacker methodologies, approaches and means and relevant actions against suspicious actors; *technical*, indicators of malware; *operational*, aimed to assess the organisation's ability in determining the future cyber threats on the base of previous experience related to successful cyberattacks; and *strategic*, i.e. high-level information on changing risk (strategic shifts), senior leadership is required for thorough determination to critically assess threats.

If reliable information about cyber threats and system vulnerabilities is available, the next step is Topological Vulnerability Analysis (Fig. 1). It involves

understanding of the actor and his motivation, as well as knowledge on vulnerabilities and ways to exploit them. Then, simulation results facilitate the consideration of measures to reduce vulnerabilities through evaluation of their impact, measures to monitor and detect attacks, as well as response measures.

In the next section of this paper will be discussed an experimental research, that includes the processes of modelling, simulation and visualization related to the impact of a cyber threats.

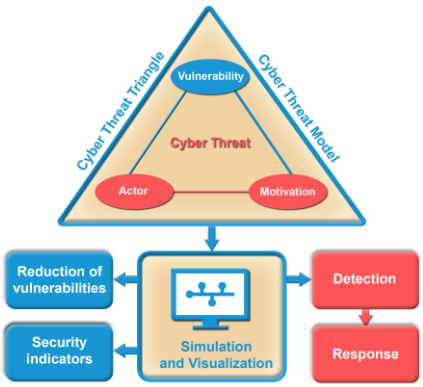


Fig. 1. The overall flow of Topological Vulnerability Analysis (TVA).

6. MODELLING THE IMPACT OF CYBERTHREATS ON URBAN AUTOMOBILE TRANSPORT SYSTEMS

The concept of the experimental research aims to show the comparative characteristics between the generated output data from the use of a reference model in a regular mode and respectively under the impact of a cyber threat. The author considers a special case of potential infringements of the light signalling as a consequence of a cyber threat on the specific transport system. The used reference simulation model is the result of efficient work of a group of scientists, studying the automobile traffic in urban environments and its optimization [17, 18].

Aimsun 8.0 has three components that allow dynamic simulations, the Microscopic Simulator, the Mesoscopic simulator and the Hybrid Simulator. They can deal with different traffic networks: urban networks, freeways, highways, ring roads, arterials and any combination thereof. The dynamic simulators have been designed and implemented as a tool for traffic analysis to help traffic engineers in the design and assessment of traffic systems. They have proven to be very useful for testing new traffic control systems and management policies, based either on traditional technologies or as implementation of Intelligent Transport Systems.

The input data required by Aimsun Dynamic simulators is a simulation scenario, and a set of simulation parameters that define the experiment. The scenario

is composed of four types of data: network description, traffic control plans, traffic demand data and public transport plans. The simulation parameters are fixed values that describe the experiment (simulation time, warm-up period, statistics intervals, etc.) and some variable parameters used to calibrate the models (reaction times, lane changing zones, etc.).

The following tables 1, 2, 3, 4, and 5 present output data from the simulation for some of the main parameters of the model of urban automobile transport:

- *Flow* - vehicles per unit time or the ratio between the number of vehicles passing some designated roadway (n) point during time t and the duration of a time interval (t). Flow is often measured over the course of an hour in which case the resulting value is typically referred to as volume (vehicles per hour) [19].
- *Speed* - the distance that a vehicle travels (S) per unit of time (t). Each vehicle on the roadway travels with an individual speed. Therefore, the average speed value is calculated by averaging the individual speeds of all the vehicles in the section of road, which is the object of study. The speed is measured in units km/h and m/s [20].
- *Delay* - average delay time per vehicle per kilometre. This is the difference between the expected travel time (the time it would take to traverse the system under ideal conditions) and the travel time. It is calculated as the average of all vehicles and then converted into time per kilometre.

There are three different kinds of delay time:

  - *Fixed* - pedestrians will remain stopped for a fixed time;
  - *Wait Until* - pedestrians will remain stopped until a certain time;
  - *Variable* - pedestrians will remain stopped for a variable time, defined with a mean and a deviation.

- *Mean Queue* - average length of the queue in that section, expressed as the number of vehicles per lane. It is calculated as a time average.
- *Number of Stops* - average number of stops per vehicle per kilometre or while travelling in the section... Each interval value will be calculated considering the pedestrians that reached their destination in the specified interval [21].

The average value of *the duration of signalling (D)* for the examined crossroad in the reference model is calculated to be approximately 20 seconds. For the purposes of our research is conditionally accepted that cyberattacks 1 and 2 change the duration of signalling respectively with – 10 and + 10 seconds compared to the reference model. The presented simulations have been made for a time interval from 10:00:00 to 11:00:00 am. Table cells include the maximum and the reference value

of the relevant parameters, as well as the relevant ratios. The dependencies of selected parameters on the duration of signalling are graphically visualized by 3D bar charts in Figures 2, 3, 4, 5 and 6.

Table 1.

Impact	***D [s]***	***F [veh/h]***	***F/ F_{max} [%]***	***F/ F_{ref} [%]***
C_1	10	3171	77.45%	77.45%
M_{Ref}	20	4094	100.00%	100.00%
C_2	30	2653	64.80%	64.80%

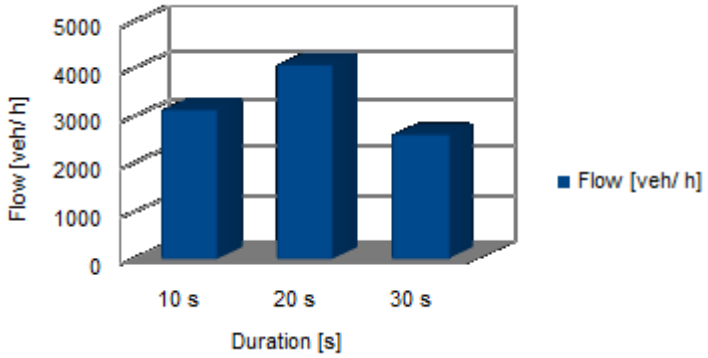


Fig. 2. F = f (D)

Table 2.

Impact	***D [s]***	***T_D [s/km]***	***T_D/ $T_{D, max}$ [%]***	***T_D/ $T_{D, ref}$ [%]***
C_1	10	169.47	100.00%	310.21%
M_{Ref}	20	54.63	32.24%	100.00%
C_2	30	52.7	31.10%	96.47%

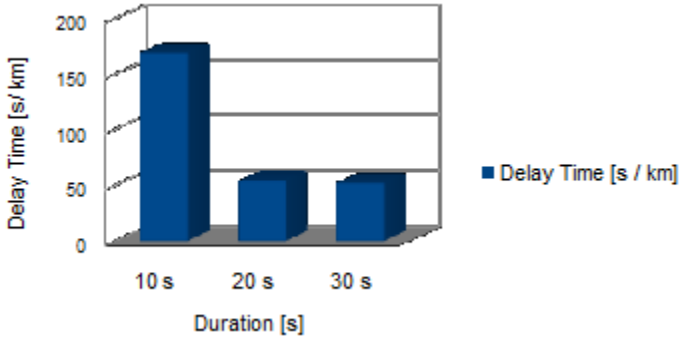


Fig. 3. T_D = f (D)

Table 3.

Impact	***D [s]***	***V [km/h]***	***V/ V_{max} [%]***	***V/ V_{ref} [%]***
C_1	10	28.14	81.75%	84.23%
M_{Ref}	20	33.41	97.07%	100,00%
C_2	30	34.42	100.00%	103.02%

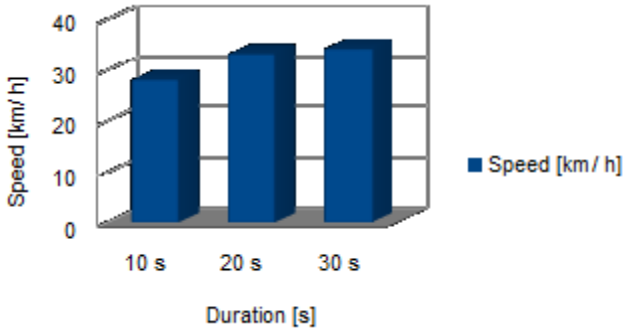


Fig. 4. V = f (D)

Table 4.

Impact	***D [s]***	***Q [veh]***	***Q/ Q_{max} [%]***	***Q/ Q_{ref} [%]***
C_1	10	158.75	100.00%	497.34%
M_{Ref}	20	31.92	20.11%	100.00%
C_2	30	138.22	87.07%	433.02%

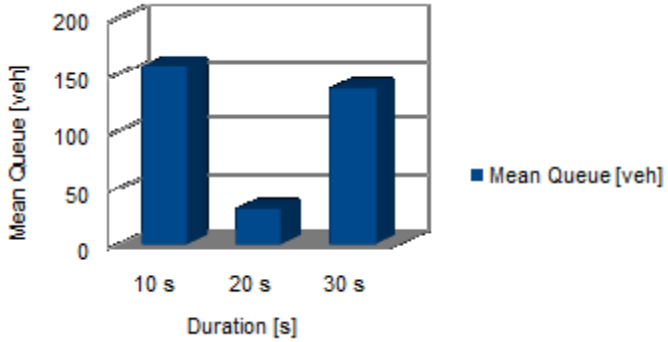


Fig. 5. Q = f (D)

Table 5.

Impact	***D [s]***	***N [#/veh/km]***	***N/ N $_{max}$ [%]***	***N/ N $_{ref}$ [%]***
C_1	10	0.25	100.00%	147.06%
M $_{Ref}$	20	0.17	68.00%	100.00%
C_2	30	0.16	64.00%	94.12%

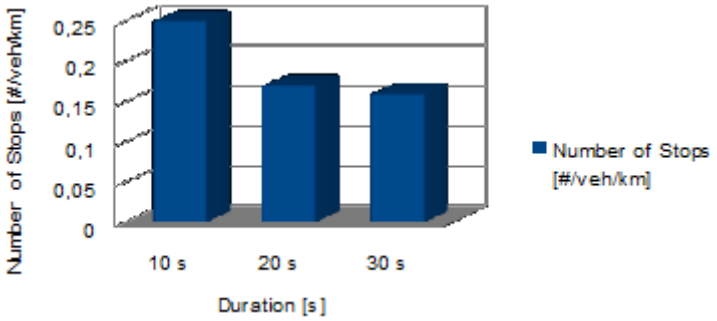


Fig. 6. N = f (D)

Summary evaluation

When the duration of signalling has been reduced by 10 s (for green light) compared to the duration of signalling for the reference model, the ratio F/ F_{ref} is equal to 77.45 %. This means that under the impact of Cyberattack 1 the flow F decreases with approximately 23 %. In this case the delay time T_D increases more than 3 times compared to $T_{D, ref}$ and the speed decreases with approximately 16 % compared to V_{ref}. Mean queue Q increases almost 5 times compared to Q_{ref}. The Number of stops N is 1,5 times more compared to N_{ref}.

When the duration of signalling is increased by 10 s (for green light) compared to the duration of signalling for the reference model, the delay time T_D, the speed V and the number of stops N do not change substantially. Actually, the mean queue Q changes substantially, increasing over 4 times, and the flow F decreases with 35 %.

In conclusion, the flows F decreases and the mean queues Q increases multiple under the impact of the two cyberattacks, which means that under the impact of potential APTs or some kind of semantic attacks can be observed accumulations, that could lead to traffic accidents.

In support of the analysis of simulation results, the author presents a 2D/ 3D visualization (Fig. 7) of a traffic accident under the impact of Cyberattack 1, when the duration of signalling is -10 s compared to the reference model.

Fig. 7. 2D / 3D visualization of a traffic accident under the impact of Cyberattack 1.

Except the parameters selected by the author, because of their importance to characterize traffic, Aimsun 8.0 generates data for Density, Harmonic Speed, Missed Turns, Total Travel Time, Total Travelled Distance, Travel Time, etc. The research can be expanded with exploring other parameters and analysing dependencies between them.

The next stage of the experiment is related to the obtained results for various pollutants and harmful emissions [g] in the air for a certain mileage [g / km]. Objects of the study can be particulate matter (PM), carbon oxides CO_x, NO_x, volatile organic compounds (VOC) etc.

For the generation of correct data on concentrations of certain pollutants in the air, is required to be entered input data as follows:

- *Percentages of cars with petrol, diesel and gas engines relative to the total number of registered cars.*
  Publicly available statistics show that the total amount of harmful air emissions from the petrol engines is the highest compared to the diesel and gas engines. According to information from Open data Bulgaria from 01.01.2017, the total number of registered cars in the country is 3 113 190. 215 from them are electrical and for this reason environmental-friendly. Therefore, they are not considered in the research. 202 996 of them are hybrid cars and can operate in two ways. If they are assigned to one of the three major groups according one of the ways, then the number of the cars will be as follows: petrol cars - around 1 674 119 (53.78%); diesel cars – around 1 237 910 (39.77%); gas cars – around 200 946 (6.46%).
- *Flow* – the resultant values of that parameter from Table 1 are used again at this stage of the study.

In the simulation environment Aimsun 8.0 the amount of emitted airborne contaminants is included in the tables of results under the name IEM Emission (Integral Equation Model Emission). The experiment is realized by the embedded *Panis et al Emission Model* that generates data about pollution by certain substances in a time interval from all cars above the research section.

Table 6 contains the obtained values on concentrations of pollutants (CO_2, NO_x, VOC and PM), released into the air from one car in [g] and measured using the reference model of the same urban section respectively in a normal mode (M_{Ref}) and under the impact of two potential cyberattacks (C_1 and C_2), as well as the embedded Panis et al Emission Model. The ratios between the concentrations of pollutants respectively for the reference model and under the impact of two cyberattacks are presented in Table 7.

Table 6.

Impact	***D [s]***	***M_{CO} [g]***	***M_{NO} [g]***	***M_{VOC} [g]***	***M_{PM} [g]***
C_1	10	1332.89	12.166	0.852	0.402
M_{Ref}	20	1020.85	7.218	0.529	0.290
C_2	30	1159.31	11.267	0.796	0.318

Table 7.

Impact	***D [s]***	***CO_2/ $CO_{2,Ref}$ [%]***	***NO_x/$NO_{x,Ref}$ [%]***	***PM/ PM_{Ref} [%]***	***VOC/ VOC_{Ref} [%]***
C_1	10	130.56	168.55	138.62	161.06
M_{Ref}	20	100.00	100.00	100.00	100.00
C_2	30	88.09	156.10	109.66	150.47

The tabular data and the charts in Fig. 8, 9, 10 and 11 clearly show that in cases of change in the duration of signalling respectively with – 10 and + 10 seconds compared to M_{Ref} the simulation software registers elevated levels of pollutants in the air above the considered section.

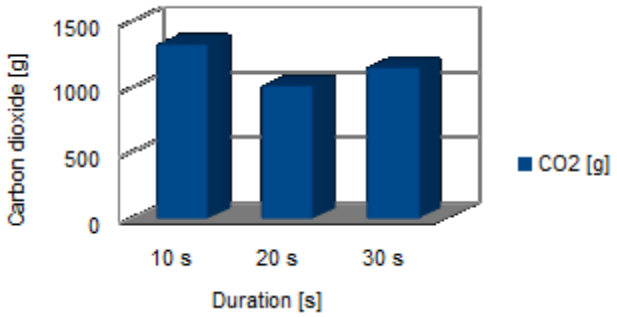


Fig. 8. $M_{CO} = f(D)$

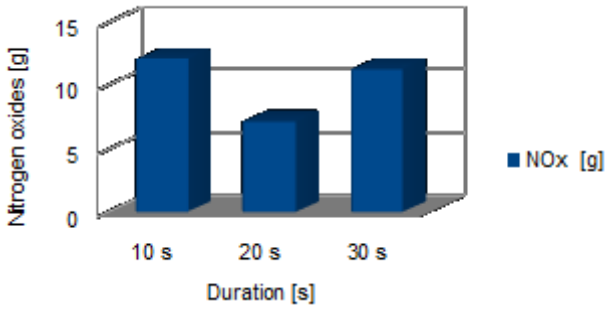
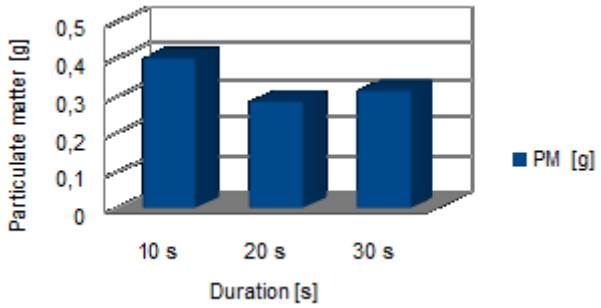


Fig. 9. $M_{NO} = f(D)$



|Fig. 10. $M_{PM} = f(D)$

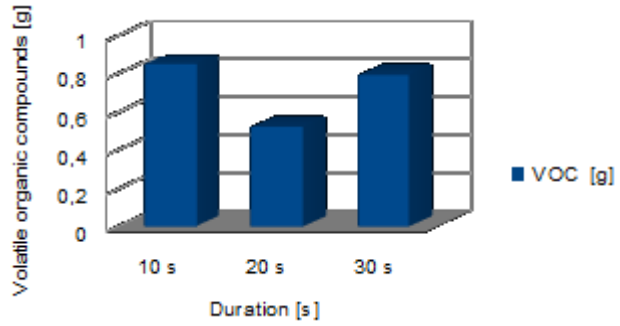


Fig. 11. $M_{VOC} = f(D)$

The research continues with a comparative analysis of the simulation results for the levels of pollutants in the air based on the accepted norms according to Ordinance №12 (from 15 July 2010) of the Ministry of Environment and Water and the Ministry of Health of Bulgaria [22]. Table 8 consists of sub-tables A, B, C, D, E, F, G, which contain: the simulation results for concentrations of harmful

substances (M_x) in [g]; relevant norms (N_x) for each substance per unit volume (V), measured in [m^3]; ratios between them ($R_x = M_x / N_x$).

Considering that the software does not provide information about the volume of the air, in which the concentrations of air pollutants are measured, the author calculates the ratios for particulate matter, carbon and nitrogen oxides per volume in the range of 1 to 1 000 000 [m^3]. Volatile organic compounds are not considered further in the upcoming part of the study, because the source does not contain an unambiguous norm for their permissible concentrations in the air.

In Fig. 12, 13 and 14 the functional dependencies of the ratios R_x of the volume of air V [m^3] are graphically presented.

Table 8 (A, B, C, D).

A		***C_1***	***M_{Ref}***	***C_2***
Pollutant	***N_x [g/m^3]***	***R_x [V = 1 m^3]***	***R_x [V = 1 m^3]***	***R_x [V = 1 m^3]***
CO_2	1.10^{-2}	133 289	102 085	115 931
NO_x	2.10^{-4}	60 830	36 090	56 335
PM	$2,5.10^{-4}$	1 608	1 160	1 272
B		***C_1***	***M_{Ref}***	***C_2***
Pollutant	***N_x [g/m^3]***	***R_x [V =10 m^3]***	***R_x [V = 10 m^3]***	***R_x [V = 10 m^3]***
CO_2	1.10^{-2}	13 328.9	10 208.5	11 593.1
NO_x	2.10^{-4}	6 080.3	3 609.0	5 633.5
PM	$2,5.10^{-4}$	160.8	116.0	127.2
C		***C_1***	***M_{Ref}***	***C_2***
Pollutant	***N_x [g/m^3]***	***R_x [V = 100 m^3]***	***R_x [V = 100 m^3]***	***R_x [V = 100 m^3]***
CO_2	1.10^{-2}	1 332.89	1 020.85	1 159.31
NO_x	2.10^{-4}	608.03	360.9	563.35
PM	$2,5.10^{-4}$	16.08	11.60	12.72
D		***C_1***	***M_{Ref}***	***C_2***
Pollutant	***N_x [g/m^3]***	***R_x [V =1000 m^3]***	***R_x [V = 1000 m^3]***	***R_x [V = 1000 m^3]***
CO_2	1.10^{-2}	133.289	102.085	115.931
NO_x	2.10^{-4}	60.803	36.09	56.335
PM	$2,5.10^{-4}$	1.1608	1.160	1.272

Table 8 (E, F, G).

E		***C_1***	***M_{Ref}***	***C_2***
Pollutant	***N_x [g/m³]***	***R_x [V = 10000 m³]***	***R_x [V = 10000 m³]***	***R_x [V = 10000 m³]***
CO_2	1.10^{-2}	13.3289	10.2085	11.5931
NO_x	2.10^{-4}	6.0803	3.609	5.6335
PM	$2,5.10^{-4}$	0.11608	0.116	0.1272
F		***C_1***	***M_{Ref}***	***C_2***
Pollutant	***N_x [g/m³]***	***R_x [V =100000 m³]***	***R_x [V = 100000 m³]***	***R_x [V = 100000 m³]***
CO_2	1.10^{-2}	1.33289	1.02085	1.15931
NO_x	2.10^{-4}	0.60803	0.3609	0.56335
PM	$2,5.10^{-4}$	0.011608	0.0116	0.01272
G		***C_1***	***M_{Ref}***	***C_2***
Pollutant	***N_x [g/m³]***	***R_x [V = 1000000 m³]***	***R_x [V = 1000000 m³]***	***R_x [V = 1000000 m³]***
CO_2	1.10^{-2}	0.133289	0.102085	0.115931
NO_x	2.10^{-4}	0.060803	0.03609	0.056335
PM	$2,5.10^{-4}$	0.0011608	0.00116	0.001272

Table 9.

	C_1			***M_{Ref}***			***C_2***		
V [m³]	***R_{CO}***	***R_{NO}***	***R_{PM}***	***R_{CO}***	***R_{NO}***	***R_{PM}***	***R_{CO}***	***R_{NO}***	***R_{PM}***
1	133 289	60 830	1608	102 085	36090	1160	115931	56335	1272
10	13 328.9	6 080.3	160.8	10 208.5	3609.0	116.0	11593.1	5 633.5	127.2
100	1 332.89	608.03	16.08	1 020.85	360.9	11.60	1159.31	563.35	12.72
1000	133.289	60.803	1.1608	102.085	36.09	1.160	115.931	56.335	1.272
10000	13.3289	6.0803	0.11608	10.2085	3.609	0.116	11.5931	5.6335	0.1272
100000	1.33289	0.60803	0.011608	1.02085	0.3609	0.0116	1.15931	0.56335	0.01272
1000000	0.133289	0.060803	0.0011608	0.102085	0.03609	0.00116	0.115931	0.056335	0.001272

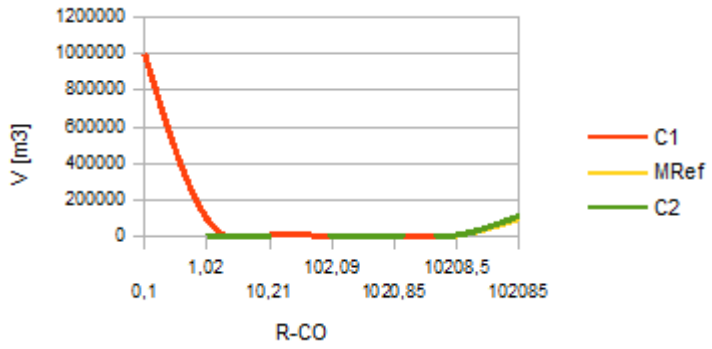


Fig. 12. $R_{CO} = f(V)$

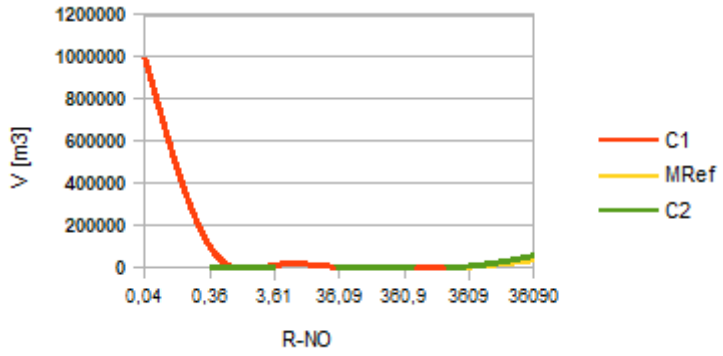


Fig. 13. $R_{NO} = f(V)$

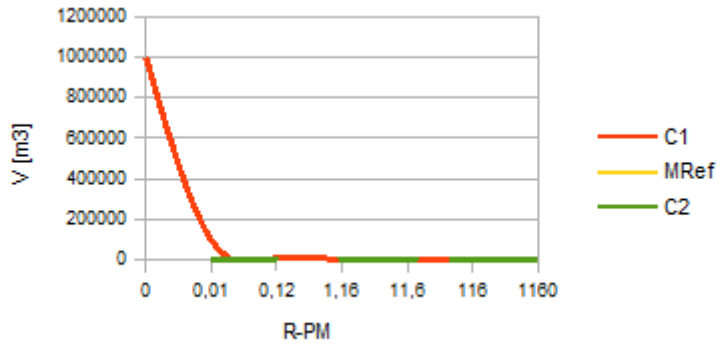


Fig. 14. $R_{PM} = f(V)$

The tables and charts show that the ratios R_x are inversely proportional to the volume of air for which has been made the conditional admission. Therefore, R_{CO},

R_{NO} and R_{PM} significantly decreased with increasing the volume of air that is naturally. Table 10 contains the results of the comparative analysis at the conditionally accepted maximum volume of air in the particular research - 1 000 000 [m^3]. The bar chart in Figure 15 aims to visualize the dependencies of the ratios R_{CO}, R_{NO} and R_{PM} from changes in the duration of signalling for reference model M_{Ref} and under the impact of two cyberattacks C_1 and C_2.

Table 10.

Impact	***D [s]***	***R_{CO} [%]***	***R_{NO} [%]***	***R_{PM} [%]***
C_1	10	13.33	6.08	0.12
M_{Ref}	20	10.21	3.61	0.12
C_2	30	11.60	5.63	0.13

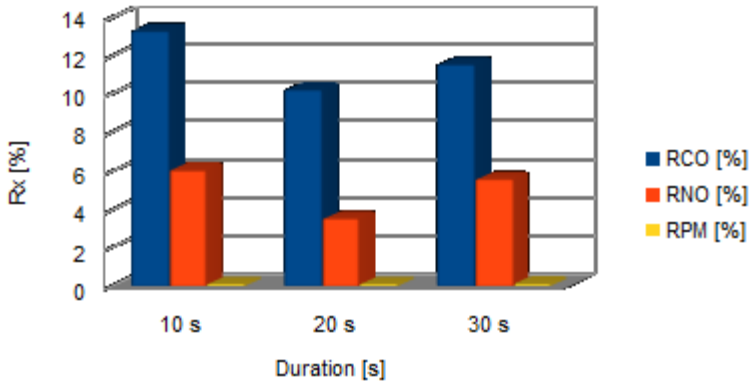


Fig. 15. $R_{PM} = f(V)$

Summary evaluation

The registered increase in the concentrations of PM compared to thresholds values can be defined as negligible, because it is below 1 % in the three cases. The amount of carbon dioxide CO_2 in the reference model M_{Ref} of the section increases by approximately 10 % compared to the accepted norm, while under the impact of cyberattacks C_1 and C_2 - respectively by 13 % and 12.6 %. The concentration of nitric oxide NO increases by 3.6 % in the reference model M_{Ref} compared to the norm and by 6 % and 5.6 % under the impact of cyberattacks C_1 and C_2.

This study can be expanded by assessing and analysing the impact of a DoS – attack on the simulation model of the Traffic Control Centre of an urban ATS developed in the simulation software Riverbed Modeler Academic Edition 17.5 [23]. In this case the author has proposed the two simulation software to be combined in order to present the full impact of a DoS – attack on the urban ATS.

The transition between the two studies represents a logical connection (implication). The claims regarding the progress and consequences from the DoS - attack on the urban ATS made by the author are supported by the research of Prof. J. Alex Halderman's team from the University of Michigan. His analogous study has been conducted in a physical environment in a cooperation with a road agency located in Michigan [24].

According to this study the destructive impact of a DoS – attack continues on the traffic lights after the server has stopped working due to the communication between the server and the signal controllers controlling the traffic lights. Stopping the operation of traffic lights under the impact of the DoS - the attack occurs when manipulating the traffic lights signalling at an intersection compared to others, which can be done for both red and green light. In Aimsun 8.0 this change is only possible for the green light only.

The detected vulnerabilities of the controllers have been determined as follows: *unencrypted radio signals; use of usernames and passwords by default; a debug port that is easy to be attacked; using an older version of the installed software.*

The simulation results for the main parameters which characterize the congestions, are presented in tabular and graphical form in Tables 11, 12 and13 and in Figures 16, 17 and 18. The potential impact of C_{DoS} is shown by an unevenly and significantly change of the value of D for all 4 signals from traffic lights at the intersection. Actually, one of the main differences between the initially simulated semantic attacks and a DoS – attack is the more notable effect of the second one. The average value of D for M_{Ref} set in the first series of experiments is used again in this experiment. 1 [s] is the minimum acceptable value of the parameter D in Aimsun 8.0.

Table 11.

Impact	***D [s]***				***F [veh/h]***	***F/ F_{max} [%]***	***F/ F_{Ref} [%]***
M_{Ref}	20				4094	100.00	100.00
C_{DoS}	1	3	2	1	1300	31.75	31.75
	1	1	1	1	1076	26.28	26.28

Table 12.

Impact	***D [s]***				***T_D [s/km]***	***T_D/ $T_{D, max}$ [%]***	***T_D/ $T_{D, Ref}$ [%]***
M_{Ref}	20				54.63	20.50	100.00
C_{DoS}	1	3	2	1	266.53	100.00	487.88
	1	1	1	1	248.46	93.22	454.81

Table 13.

Impact	***D [s]***				***Q [veh]***	***Q/ Q $_{max}$ [%]***	***Q/ Q $_{Ref}$ [%]***
M $_{Ref}$	20				31.92	6.73	100.00
C_{DoS}	1	3	2	1	443.82	93.61	1390.41
	1	1	1	1	474.13	100.00	1485.37

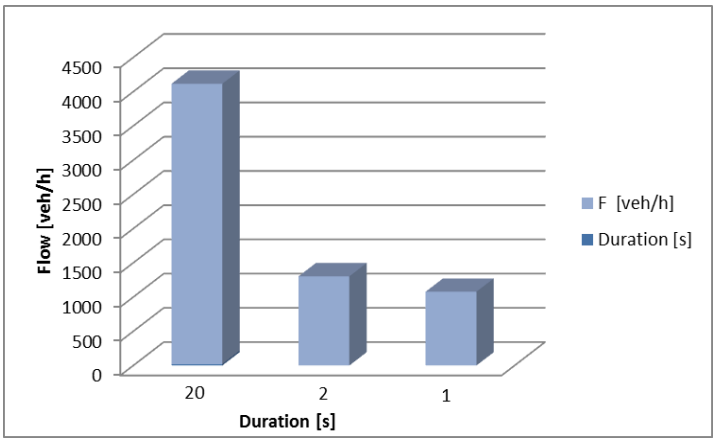


Figure 16. F = f (D)

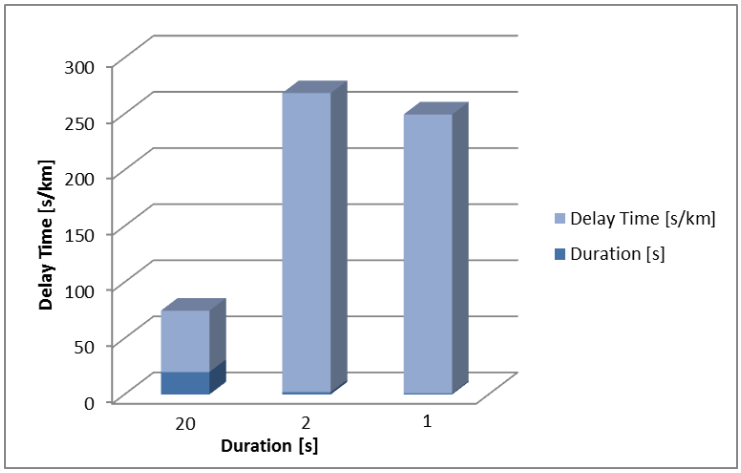


Figure 17. T_D = f (D)

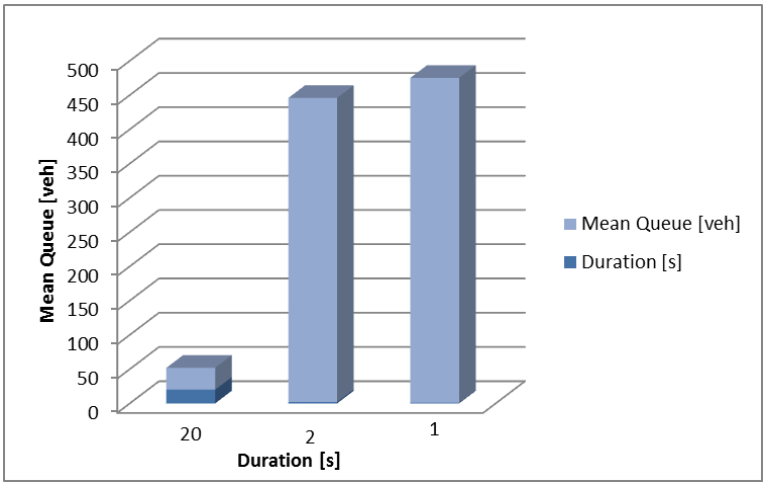


Figure 18. Q = f (D)

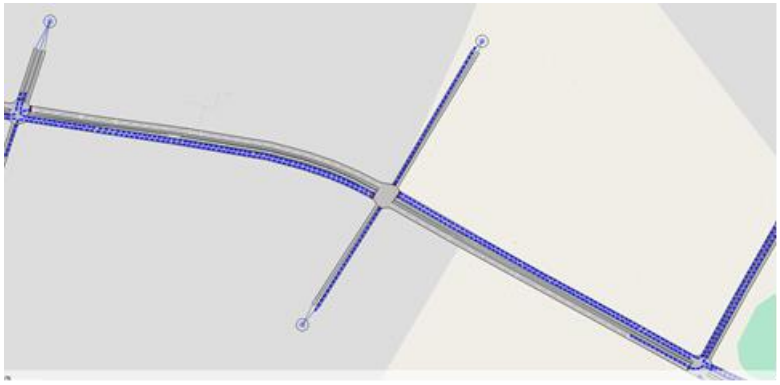


Figure 19. A 2D visualization of the traffic situation under the impact of C_{DoS}.

Summary evaluation

From the tabular data and comparative diagrams, when the average D is approximately 2 [s] for green light, the ratio F / F_{Ref} is equal to 31.75%. This means that the flow F decreases by approximately 68 % compared to M_{Ref} under the impact of the DoS - attack. In this case, the delay time T_D is increased approximately 5 times compared to $T_{D, Ref}$. The mean queue Q is increased nearly 14 times compared to Q_{Ref}.

When the average D is equal to 1 [s] for green light T_D is increased by 4.5 times. It can be seen that Q increases dramatically (15 times), while F decreases by nearly 74 % compared to M_{Ref}.

As can be seen, the conclusions based on the obtained results are like the previous ones. Stopping the traffic lights under a DoS – attack causes stopping the traffic with a possibility of road accidents (Figure 19).

7. CONCLUSION

The presented experimental research illustrates the great capabilities of the professional simulation products and the advantages of their use for solving a wide range of issues and global problems related to the security of critical infrastructure and respectively the national security in general.

Financial investment in simulation products are entirely justified because they are significantly lower compared to the potential costs of dealing with the serious consequences of a major breakthrough in the systems. The great possibilities for realistic visualizations undoubtedly support the research activities. For the summary evaluations of the results the author uses the method of the logical analysis, showing their reliability for application in other similar researches. The tabular and graphical results show the negative impact of the cyberattacks on the section of an urban ATS and in particular the increased delay and the risk of traffic accidents. The additional study of environmental effects contributes to the main research, presenting the higher levels of pollutants in the air (CO_2, NO and PM) under the impact of simulated cyberattacks compared to the reference model.

For the summary evaluations of the results the author uses the method of the logical analysis in order to show their reliability for application in other studies related to enhance cybersecurity of transport critical infrastructure and in addition to traffic optimization and reducing the concentrations of pollutants in the air.

The research can be extended by testing different means of protection installed in the Traffic Control Centre of the urban ATS such as firewalls integrated with VPN (Virtual Private Networks) or IDS (Intrusion Detection System), Honeypots computer systems and Honeynets computer networks, complex solutions to strengthen protection against cyber threats UTM (Unified Threat Management), etc. These simulations can be performed in a suitable simulation environment such as Riverbed Modeler 17.5.

Furthermore, a methodology for vulnerability assessment and planning of measures to strengthen the resilience of he selected critical infrastructure can be developed. For this purpose, the author recommends again the aforesaid software for simulation modelling of computer networks.

REFERENCES

[1] ISO 31000:2009, Risk management – Principles and guidelines.

[2] IEC 31010:2009, Risk management – Risk assessment techniques.

[3] Sharkov, G., From Cybersecurity to Collaborative Resiliency. *Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense*, Vienna, Austria, 2016, https://doi.org/10.1145/2994475.2994484.

[4] ENISA. *Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations*, www.enisa.europa.eu, 2016, https://www.enisa.europa.eu/publications/good-practices-recommendations (access date: 1 January, 2017).

[5] Mutafchiev, L. *Economy of transport (in Bulgarian)*, Sofia, 2001.

[6] Department of Transportation. *Federal Highway Administration, Manual on Uniform Traffic Control Devices for Streets and Highways*, 2009, https://www.gpo.gov/fdsys/pkg/FR-2009-12-16/pdf/E9-28322.pdf (access date: 12 January 2017).

[7] DEA & SITS. *Traffic Control Systems Handbook*, 2005, http://www.ops.fhwa.dot.gov/publications/fhwahop06006/fhwa_hop_06_006.pdf (access date: 12 January 2017).

[8] U.S. Department of Transportation. *Federal Highway Administration. Freeway Management and Operations Handbook.* Final Report, September 2003 (Updated June 2006), FHWA Publication, http://ops.fhwa.dot.gov/freewaymgmt/publications/frwy_mgmt_handbook/fmoh_complete_all.pdf (access date: 1 February 2017).

[9] Genesee County. *Intelligent Transportation Systems Summary*, http://gcmpc.org/wp-content/uploads/pdf/LRTP_pdfs/ITSSum.pdf (access date: 15 January 2017).

[10] Kaufman, Sarah M. *Co-Monitoring for Transit Management*, 2014, https://wagner.nyu.edu/rudincenter/wp-content/uploads/2014/02/CoMonitoringForTransit_web.pdf (accessed at 12 January 2017).

[11] ENISA. *Digital Preservation Management*, 2016, http://www.dpworkshop.org/dpm-eng/oldmedia/threats.html (accessed: 5 January 2017).

[12] US-CERT. Security Tip (ST04-015). *Understanding Denial-of-Service Attacks*, 2013, https://www.us-cert.gov/ncas/tips/ST04-015 (access date: 20 January 2017).

[13] Yan, R., Xu, T., and Potkonjak, M. *Semantic Attacks on Wireless Medical Devices*, 2014, https://doi.org/10.1109/ICSENS.2014.6985040 (access date: 20 January 2017).

[14] Nabil, S., and Benmohamed, M., *Security Ontology for Semantic SCADA*, 2012, http://ceur-ws.org/Vol-867/Paper19.pdf (access date: 20 January, 2017).

[15] Fok, E. An Introduction to Cybersecurity Issues in Modern Transportation Systems, *ITE Journal*, **3** (vol. 83), 2013, pp. 19. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.377.199&rep=rep1&type=pdf

[16] Chen, P., Desmet, L., and Huygens, Ch. *A Study on Advanced Persistent Threats*, 2014, https://lirias.kuleuven.be/bitstream/123456789/461050/1/2014-apt-study.pdf (access date: 3 February, 2017).

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

[18] 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*, Bulgaria, **3** (vol.16), 2016, pp. 165 - 184.

[19] Mannering, Fred L., and Washburn, Scott S., *Chapter 5. Fundamentals of Traffic Flow and Queuing Theory. Principles of Highway Engineering and Traffic Analysis* (6th ed.), Wiley, 2016, pp. 135 - 169.

[20] Hall F. L., Gartner N., Messer C. J., Rathi A. K. *Traffic stream characteristics. In Traffic Flow Theory: State-of-the- Art Report*, Federal Highway Administration/Transportation Research Board/Oak Ridge National Laboratory, Chapter 2, 2001, https://www.researchgate.net/profile/Nathan_Gartner/publication/248146380_Traffic_flow_theory_A_state-of-the

[21] TSS - Transport Simulation Systems. *Aimsun 8 Dynamic Simulators Users' Manual*, 2014.

[22] Yablanski, Ts., Petkov, G. *Mannual Book of Applied Ecology*, Norwegian Cooperation Programme with Bulgaria, Trakia University, Faculty of Agriculture, Stara Zagora, 2011, pp. 22 – 39.

[23] Ivanova, Y., Modeling the Impact of Cyber Threats on a Traffic Control Centre of Urban Auto Transport Systems, *International Journal on Information Technologies and Security (IJITS)*, № 2 (vol. 9), June 2017, pp. 83-95.

[24] Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J. & Halderman, A. J., Green Lights Forever: Analyzing the Security of Traffic Infrastructure, *Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT'14)*, 2014, https://jhalderm.com/pub/papers/traffic-woot14.pdf.

Information about the author:

Yoana A. Ivanova – Assistant and a PhD student in the Department of Information Technologies for Security at IICT of BAS; 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; Professional area: 5.3. "Communication and computer equipment"; Doctoral Program: "Automated Systems for Information processing and Management".

Manuscript received on 04 July 2017