# MODELING THE IMPACT OF CYBER THREATS ON A TRAFFIC CONTROL CENTRE OF URBAN AUTO 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 a realistic simulation model of an advanced Traffic Control Centre of urban Auto Transport Systems (ATSs), created using the computer networks simulation system Riverbed Modeler Academic Edition 17.5. The author examines the impact of a Denial-of-Service attack on the reference model and makes a comparative analysis based on the simulation results obtained in a normal operation mode and in the case of a cyberattack.

**Key words:** cybersecurity, simulation, modelling, auto transport, traffic control.

## 1. INTRODUCTION

Auto Transport Systems (ATSs) are chosen by the author for this study, because the automobile transport is the main type of contemporary transport due to several advantages like the largest network coverage of roads, the greatest variety of vehicles compared with other modes of transport, manoeuvrability and comparative independence from environmental conditions and no delays due to many initial - end operations.

The most effective protection of the automated control systems from various hazards and potential threats can be achieved by appropriately combining means of physical and cyber security. Being main components of an Intelligent Transportation System (ITS), the Traffic Signal Control Systems and Traffic Control Centres (TCCs) are exposed to a potential risk of becoming targets of attackers, which can use the cyberspace as a conductor of malicious software.

Transportation efficiency applications focus on improving traffic flow, because any disruption in the normal functioning of an ATS related to navigation, road guidance, signalling of traffic lights, traffic information services, traffic assistance and traffic coordination leads to major inconvenience, delays and even road accidents. An example of this are Traffic Information Services (TIS) which rely on Embedded On-board Infotainment Systems (OISs), also known as In-Vehicle Communications and Entertainment System (IVCES). OISs combine entertainment, multimedia and driver information in one module [1] but at the same time providing Internet connectivity make them vulnerable to cyber threats.

It should be noted that one of the main purposes of implementing innovative Information and Communication Technologies in ITSs is to strengthen cybersecurity of the critical transport infrastructure and accordingly its safety, efficiency and stability in general. In terms of good practices for prevention, minimizing potential risks and reduced financial investments the simulation modelling is the most reliable and effective method for examination of complex systems, as well as detecting vulnerabilities of network devices and configurations in a safe virtual environment.

The main goal of this paper is to present convincing arguments in favour of using simulation modelling as an auxiliary high technology for strengthening critical infrastructure cybersecurity. This is achievable when investing in professional simulation systems like Riverbed Modeler Academic Edition 17.5 which provides rich opportunities for conducting various simulations. It is important to be noted that such financial investments are considerably smaller than the potential costs of dealing with possible consequences of cyber terrorism.

The next section of this paper provides an overview of urban Traffic Management and Control Systems. Section 3 is devoted to simulation modelling and its role and importance in the field of cybersecurity. Section 4 presents the essence and stages of the TCC modelling process, followed by simulation results in section 5. The conclusion underlines the advantages of using simulations in supporting decision making on resource allocation towards increased security and safety of transport critical infrastructures.

## 2. CONCEPTUAL FRAMEWORK FOR URBAN TRAFFIC MANAGEMENT AND CONTROL SYSTEMS

Generally, in practice Traffic Control Centres (TCCs) and Traffic Management Centres (TMCs) are accepted for synonymous designations, because the two terms are very similar in meaning. TCC usually refers to actual control centres used by road concessionaires and municipalities whereas TMS refers to a more generic management facility.

A TCC is the core of a Traffic Management System (TMS) where traffic management is performed by decision making, as well as additional services and operations. TMS ensures traffic management operation process, obtaining input data from the roadside (traffic data, weather data, reports regarding the traffic status) that are processed by a specialized software. TCCs are responsible for receiving, monitoring and analysing the information about the road conditions.

The ISO International Standard 148130-1 on ITSs [2] determines traffic management as "The Management of the movement of vehicles, travellers and pedestrians through the road transport network".

The main traffic management services are related to:

- *Planning:* involving services like defining the road network layout and structure (or its evolution), planning multimodal interfaces, determining fixed signalling elements, the roadside TMSs and the actual traffic management procedures or public transport routes.
- *Operating:* involving activities like monitoring and patrolling, resolving traffic incidents or emergencies, managing demand, anticipating or predicting future situations, providing information and assistance to drivers, repairing damages to the infrastructure, managing parks and other facilities, enforcing and policing or managing multimodal public transport.
- *Analysing:* evaluating the results of the operating activities and, in case of need, determining if these can be positively influenced by applying changes to the results of the planning stage [3].

Particularly regarding the urban traffic environment is important to note that it is located in big cities and metropolitan areas which have network of streets and roads with different capacities and typical traffic densities. This determines the need of Urban Traffic Management and Control (UTMC) Systems representing improved Urban Traffic Control (UTC) Systems which are one of the most important components of the advanced ITSs.

The framework for UTMC adds updated basic features to the existing UTC, as follows:

- *Adaptive Traffic Signal Control (ATSC) Systems* – the main concept of ATSC is avoiding the green traffic signals when there are no cars passing. This can be realized locally at a single traffic sign, as well as, usually, coordinated across areas or an entire city.
- *Automatic Incident Detection (AID) Systems* – they are based on image processing or processing traffic flow data. Their main applications are to detect a great variety of problems related to the traffic as stopped or low-speed vehicles, wrong-way drivers, fire, smoke, etc.
- *Real-time traffic information* – there are two widely used TMS architectures which are client-server based: *event-based* and *data-store*. The event-based TMS can provide real-time information that the client stores, filters and visualizes to the operator whereas a data-store TMS reserves all data on a server and cannot provide real-time information.

Besides the above components there are trends for implementation of additional functionalities like:

- *Air pollution monitoring and control.*
- *Prioritization of public transport.*
- *Enforcement measures monitoring.*
- *Using online data with ensuring a high level of cybersecurity.*

On the base of these advantages UTMC can be defined as the next generation of traffic systems.

## 3. APPLICATIONS OF SIMULATION MODELING FOR THE PURPOSES OF CYBERSECURITY

The author has chosen to simulate a Denial-of-service (DoS) attack on the TCC of an urban ATS in the experimental part of this paper (Section 5), because the statistics show that this type attacks to computer systems connected to the Internet are the most widespread. There is a variety of DoS attacks directed against the sectors of critical infrastructure, because of their great importance for the national security in general.

Computer networks consist of clients and servers for information exchange. Servers offer services, such as a Web or File Transfer Protocol (FTP) service, with which clients can interact to share or obtain information. When servers or services cannot respond to client requests, a situation called a DoS attack condition arises.

The most common form of a DoS attack is sending so intensive traffic (flooding) from the attacker that processing the requests to be impeded. In this case the most sent requests cannot rich their intended destinations. Attackers use communication protocols like User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), and Transmission Control Protocol (TCP) to flood the target with network traffic.

Another form of DoS attack is overutilization of system resources like central processing unit (CPU), memory, or data structures stored in memory, causing a system failure. System failure of a network device (firewall, router, switch) has devastating results because it causes network traffic congestion resulting in performance degradation or an outage. There are also examples of DoS attacks caused by configuration changes.

The analysis of the different types of DoS attacks shows that their prediction is a serious challenge to the cybersecurity experts. The effective prevention requires:

- *Reliable means of protection* – patching of systems that reduces the known vulnerabilities that can potentially cause a DoS through exploitation. Unfortunately, this method is not useful for detection of unknown vulnerabilities. Therefore, the best way is filtering out erroneous traffic at edge routers and firewalls.

- *Timely detection* – it can be realized by monitoring of network traffic patterns and roadworthiness of the connected devices into it.
- *Adequate response planning* – for example VeriSign is a good solution for traffic monitoring. It provides mitigation by filtering out the overwhelming traffic [4].

In this context simulation modelling provides great opportunities for researching computer networks and their functionalities by using professional software products. The methods of simulation modelling allow investigating the cyberattack itself and respectively the subsequent damages which depend on its nature and duration [5].

The simulation analysis is a powerful problem-solving technique. Its origins lie in statistical sampling theory and analysis of complex probabilistic physical systems [6]. Simulation models can describe systems which are still not constructed in the physical environment. Computer models with high level of realism are very useful for preventing potential problems and errors.

Agent-based modelling is the most advanced and widely used method which is the basis of professional simulation software. Some of the main characteristics of agent-based modelling are: “object-based” architecture; time model; networks and links between agents; communication between agents, as well as between agents and environment; dynamic creation and destruction of agents; statistic collection on agent population [7]; data visualization; possibilities for animation. For example, the author has used Riverbed Modeler Academic Edition 17.5 for modelling and simulation of a DoS attack on the TCC of an urban ATS that are presented in Sections 4 and 5.

## 4. MODELING A TRAFFIC CONTROL CENTRE IN A SIMULATION ENVIRONMENT

The model of a Traffic Control Centre of an urban ATS is created by the author using the simulation software Riverbed Modeler Academic Edition 17.5 specialized for designing computer networks. Simulations are run by representing real world devices as nodes and links. This software provides an environment on which attributes of these nodes and links can be configured and used as inputs in the simulation run, after which results are analysed. Each project can contain at least one scenario that can be edited in the project editor where subnets, nodes, links, utilities, and application traffic can be included for the simulation study [8].

The author has chosen this simulation software for the experiments, because the generated results are reliable and do not require mandatory of comparison with results obtained from experiments performed using a real hardware prototype.

Actually, the designed network configuration is based on a detailed study of practically implemented TCCs and includes carefully considered as being compatible and conventional devices according to the requirements for network design [9]:

- *Workstations* – they represent personal computers designed to work intensively at high load. In the simulation model the author has chosen to connect three workstations (type *ethcoax_station*) to a bus (type *eth_coax_adv*) by a cable (type *eth_tap*) according to the requirements for the compatibility of the physical components in a linear bus network.
- *Servers* - every computer that shares resources across the network at a particular moment plays the role of server, but not every computer is able to perform the functions of a specialized server that is characterized by large capacity, fast processor and large amount of memory. In the model are connected three servers (type *ethernet_server_adv*): control server; database server; server for strategic control in the sense of operational control, which is expressed in the formulation and implementation of strategic plans.
- *Physical network components:*
  ✓ *transmission mediums* – they can be cables, lasers, infrared rays, wireless communications (radio and satellite), microwave. The networks with a bus topology commonly use thick or thin coaxial cable and Ethernet architecture 10Base2 (speed of 10 Mbps in cable length 200 m) or 10Base5 (speed of 10 Mbps in cable length 500 m). In the simulation model the author has used a bus and a cable respectively type *eth_coax_adv* and *eth_tap*.
  ✓ *network devices* – the most configurations of TCCs are implemented using a switch that directs the packets on a route to their destination. The simulation model includes an advanced type of switch (*ethernet 128_switch_adv).*

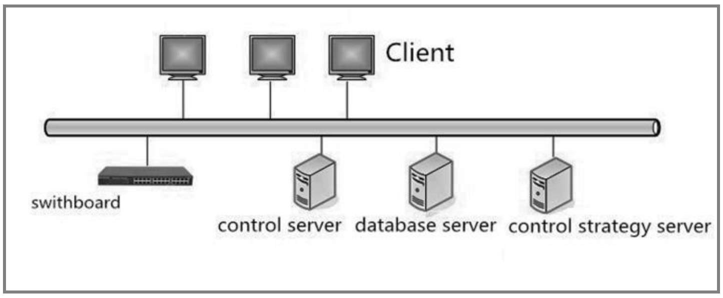

*Figure 1. Scheme of a typical TCC.*

The author has chosen to build a model of a typical TCC according to the conceptual architecture of one of the leaders in the field – Huawei (Figure 1) [10]. There are many examples of similar TCCs with bus topology, which differ in the number of servers, workstations and means of protection. The control centre of Tyco Integrated Systems (UK) Ltd. has a very simple structure, including two operator workstations [11]. On the contrary, the control centre of HiCON Adaptive Urban Traffic Control System is realized by only one Client and five servers [12]. Therefore, the exemplary architecture has been preferred as optimal, because it includes an equal and sufficient number of workstations and servers.

A screenshot of the reference model in a normal mode ($M_{Ref}$) is shown in Fig. 2.

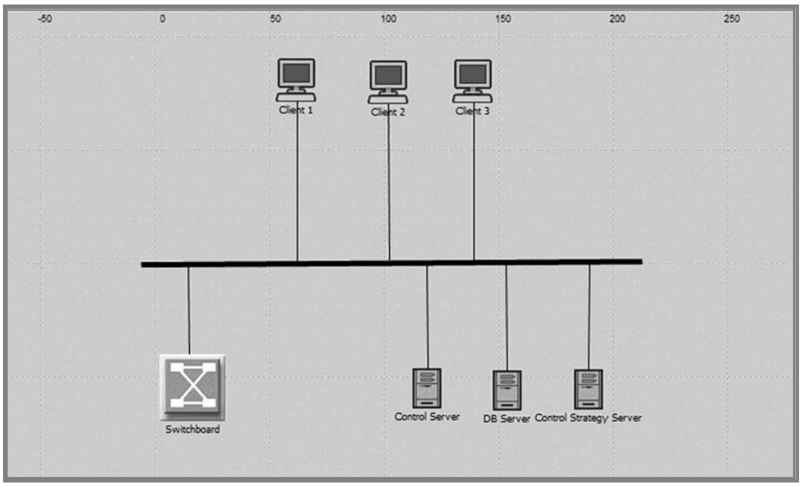

*Figure 2. The reference model of the Traffic Control Centre in a normal mode ($M_{Ref}$).*

For running the simulation is required to be made optimal settings of the main input parameters, as follows:

- *Network scale* - the order of 200 x 200 [m], as a standard office.
- *Network topology* – linear bus.
- *Network architecture* - Ethernet 10Base2.
- *Physical network components* – they are selected from the palette of objects *"ethernet_advanced"*.
- *Time delay of the bus $T_D$* - this attribute specifies the propagation delay in [sec/m] which will be incurred by packets sent over the bus. The default velocity of propagation is assumed to be equal to [0.65 * (speed of light)]. Initially, the author has specified an arbitrary value of the parameter $T_D$ = 0.005 [sec / m].
- *Thickness* - this attribute specifies the thickness of the line used to draw the bus link. It is default value of 5 units remains unchanged.
- *Traffic Generation Parameters* – the parameters of the traffic pattern that will be generated by this traffic source:
  ✓ *Start time* – this is a constant $T_0$ = 5.0 [s].

✓ *ON state time $T_{ON}$* - specifies the distribution name and arguments to be used for generating random outcomes for time spent in the "ON" state. Packets are generated only in the "ON" state. For Client 1 $T_{ON}$ = 100 [s].
✓ *OFF state time $T_{OFF}$* - specifies the distribution name and arguments to be used for generating random outcomes for time spent in the "OFF" state. No packets are generated in the "OFF" state. For Client 1 $T_{OFF}$ = 0.00001 [s].

- *Packet Generation Arguments* - specifies the parameters that determine the rate of the packet generation and the size of these generated packets:
  ✓ *Interarrival time T* - specifies the distribution name and arguments to be used for generating random outcomes for times between successive packet generations in the "ON" state. The initial value of this parameter is 2 [s] for Clients 1, 2 and 3 in the first scenario. In the next scenarios the author sets different values of T respectively in $M_{Ref}$ and under the impact of a cyberattack C, while the default values of all other parameters remain unchanged.
  ✓ *Packet Size* - specifies the distribution name and arguments to be used for generating random outcomes for the size of generated packets in [bytes]. In this case the default value „exponential (1024)" remains unchanged.
- *Duration* – this simulation has a duration of 30 [s].

## 5. ASSESSING AND ANALYSING THE IMPACT OF A CYBERATTACK ON A TRAFFIC CONTROL CENTRE

### 5.1. Related work

The present experimental research by using Riverbed Modeler Academic Edition 17.5 has been conducted after exploring the experience in this area, which confirms that the theme meets the requirements of authenticity.

Actually, an example of a DDoS (Distributed Denial-of-Service) attack on a campus network is very suitable to show the large capacity of Riverbed Modeler Academic Edition 17.5 for simulating cyberattacks. The main purpose of the software developers is to help experts in various fields to simulate a cyberattack on computer networks. The Cyber Effects model and framework allow the execution of cyberattacks and remedies in the simulation. This project is built to demonstrate some of the implemented features and capabilities of this model, like script definitions, attack profiles configuration, remedy profiles configuration and vulnerability configuration.

The network components are:

- *"Attacker"* - conducts the attacks.
- *System administrator node "sys_admin"* - executes remedy actions.
- *Server under DDoS attack "Server"* - this node has its IP address.

- *Client nodes* – run HTTP application from "Server".
- *Potentially infected nodes.*

All the nodes are connected to the network through routers and/or switches and all the nodes in the network can reach each other. The scenario has configured an example of an attacker remotely changing the IP forwarding rate of all four routers. The "Cyber Effects Config" node has the necessary script and attack definitions to modify remotely the router settings altering their IP processing rate. The statistic shows the "Cyber Effects" traffic received by each one of the four routers.

### 5.2. Modelling the impact of a DoS attack on a TCC.

Simulating the impact of a DoS attack on the reference model of a TCC is expressed in “Decrease forwarding rate” and modifying „IP forwarding rate“ of the switch by the attacker. As a result, the workstations are "infected" and the corresponding servers are exposed to the cyber threat.

The cyberimpact on the reference model is simulated by using the configuration *cyber_effects_attrib_definer* (Figure 3). The link between the workstation of the attacker (type *cyber_ethernet_wkstn_adv*) and the switch is *10BaseT_adv*, because this specification is widely used in local area networks of all sizes. All parameter settings of the switch and the servers are accepted by default, that helps to more accurate and unambiguous subsequent analysis, based only on the assessing the impact of cyber threats without considering any additional external or internal factors.

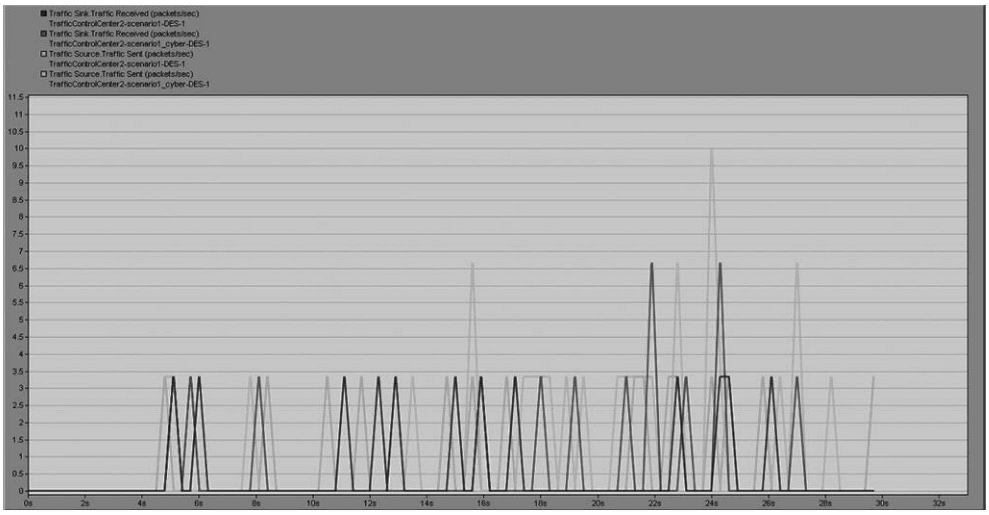

*Figure 3.* $T_S = f\,(T)$ *and* $T_R = f\,(T)$ *at* $T = 2$ *[s].*

Table1 contains simulation results from all scenarios for peak levels of "traffic sent" ($T_{S,\ max}$) and "traffic received" ($T_{R,\ max}$), depending on the interarrival time (T) respectively for the reference model ($M_{Ref}$) and under the impact of a cyberattack (C).

*Table 1.*

| | | $M_{Ref}$ | | C | |
|---|---|---|---|---|---|
| ***Scenario*** | ***T [s]*** | $T_{S,\ max}$ **[packets/s]** | $T_{R,\ max}$ **[packets/s]** | $T_{S,\ max}$ **[packets/s]** | $T_{R,\ max}$ **[packets/s]** |
| 1 | 2 | 3.3 | 3.3 | 10 | 6.7 |
| 2 | 1 | 3.3 | 3.3 | 10 | 6.7 |
| 3 | 0.5 | 6.7 | 10 | 10 | 13.5 |
| 4 | 0.25 | 13.5 | 13.5 | 16.5 | 13.5 |
| 5 | 0.2 | 20 | 20 | 16.8 | 13.5 |
| 6 | 0.15 | 27 | 23 | 27 | 13.5 |
| 7 | 0.1 | 26.5 | 20 | 33.5 | 20 |
| 8 | 0.05 | 44 | 40 | 44 | 37 |
| 9 | 0.025 | 80 | 50 | 80 | 50 |
| 10 | 0.02 | 90 | 84 | 84 | 58 |

The comparative diagrams on Figures 3, 4 and 5 show at which second of running the simulation are registered peak levels of $T_S$ and $T_R$ respectively for the reference model ($M_{Ref}$) and under the impact of a cyberattack (C).

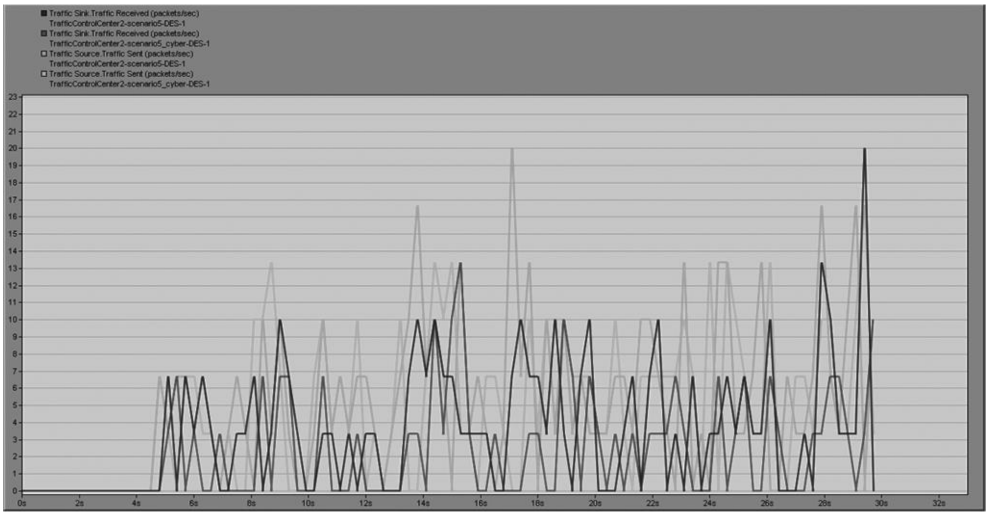

*Figure 4. $T_S = f\,(T)$ and $T_R = f\,(T)$ at T = 0.2 [s].*

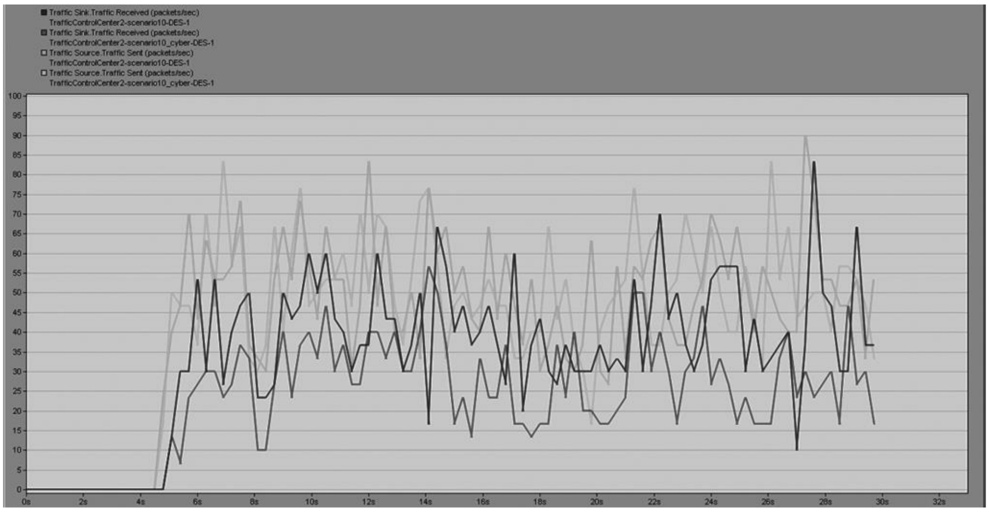

*Figure 5. $T_S = f(T)$ and $T_R = f(T)$ at $T = 0.02$ [s].*

Table 2 contains the summary results of all three charts, showing in what time intervals R in [s] are registered peak levels of $T_S$ and $T_R$ as functions of the selected three values of the interarrival time ($T_1$ = 2 [s], $T_2$ = 0.2 [s] and $T_3$ = 0.02 [s]), respectively for the reference model ($M_{Ref}$) and under the impact of a cyberattack (C). The duration of this simulation is divided into six equal intervals of 5 seconds.

*Table 2.*

| | $T_1$ | | | | $T_2$ | | | | $T_3$ | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $M_{Ref}$ | | C | | $M_{Ref}$ | | C | | $M_{Ref}$ | | C | |
| **R [s]** | $T_{S,\,max}$ | $T_{R,\,max}$ | $T_{S,\,max}$ | $T_{R,\,max}$ | $T_{S,\,max}$ | $T_{R,\,max}$ | $T_{S,\,max}$ | $T_{R,\,max}$ | $T_{S,\,max}$ | $T_{R,\,max}$ | $T_{S,\,max}$ | $T_{R,\,max}$ |
| [1, 5] | 3.3 | 3.3 | 3.3 | 0 | 3.3 | 3.3 | 3 | 3 | 45 | 10 | 50 | 13 |
| [5, 10] | 3.3 | 3.3 | 3.3 | 3.3 | 10 | 10 | 13.5 | 6.7 | 73 | 60 | 84 | 37 |
| [10,15] | 3.3 | 3.3 | 3.3 | 0 | 16.7 | 10 | 13.5 | 10 | 84 | 66 | 76 | 56 |
| [15, 20] | 3.3 | 3.3 | 6.7 | 3.3 | 20 | 10 | 13.5 | 13.5 | 66 | 60 | 66 | 40 |
| [20, 25] | 3.3 | 3.3 | 10 | 6.7 | 13.5 | 6.7 | 13.5 | 6.7 | 70 | 70 | 76 | 50 |
| [25, 30] | 3.3 | 3.3 | 6.7 | 3.3 | 16.7 | 20 | 16.7 | 10 | 90 | 84 | 85 | 47 |

Based on the tabular and graphical results the author makes the following conclusions. Under the impact of a DoS attack in the time interval [25, 30] and $T_3$ = 0.02 [s] can be seen that the number of the received compared with sent packets ($T_{R,\,max}/T_{S,\,max}$) decreases by approximately 45 %, while the received packets are only 7

% less than sent packets for $M_{Ref}$. It is observed a problem with receiving the sent packets.

Under the impact of the cyberattack in the same time interval and $T_2 = 0.2$ [s] the number of received packets compared to send packets decreases by 40 %, while the number of received packets is larger compared with sent packets for $M_{Ref}$. However, the peak levels at $T_2 = 0.2$ [s] for $M_{Ref}$ are registered in the time range [15, 20] and in this case the number of received packets compared to send packets decreases by 50 %. Consequently, the author assumes that the packets had arrived with a delay in the time range from 20-th to 30-th second without an evidence of malfunction of the network.

In the same time interval and $T_1 = 0.02$ [s] under the impact of a cyberattack the number of received compared to send packets is reduced by approximately 50%, while the number of received packets is equal to the sent packets for $M_{Ref}$ . In this case the peak levels are in the time range [20, 25], when the number of received packets decreases by 36% compared to the sent packets. Besides, the number of received packets decreases by about 43% compared to the sent packets from 15-th to 30-th second. Accordingly, the packets are not received even with some delay, which can be explained with the simulated cyberattack.

## 6. CONCLUSION

The strategic vision for ITSs is as the integrator of transportation, communications and intermodalism on a regional scale. Transportation fundamentals include the concept of transportation as a complex system and a framework for analysis of this system [13]. In this sense the TCC can be viewed as the heart of this complex system, whose understanding includes statistical methods, complex mathematical algorithms and various network analysis tools.

Constructing this simulation model of a TCC, the author aims to show that a correct connection of compatible structural components leads to the realization of a simulation that runs successfully. Besides, the model and obtained results can be used as a basis for researches and developments in order to recommend effective means and methods of cybersecurity that can be applied in the area of ITSs. Simulation modelling is useful for minimizing potential risks and detection of vulnerabilities of devices and configurations. Therefore, the advanced methods of simulation and visualization can contribute to finding the best cyber security and IT security solutions under optimal conditions.

## REFERENCES

[1] Picone, M., Busanelli, S., Amoretti, M., Zanichelli, F., Ferrari, G. *Advanced Technologies for Intelligent Transportation Systems*, Springer International Publishing, Switzerland, 2015.

[2] ISO 14813-1: 2007. *Intelligent transport systems – Reference model architecture(s) for the ITS sector – Part 1: ITS service domains, service groups and services.* ISO, 2007.

[3] Perallos, A., Hernandez-Jayo, U.,Onieva, E., Garcia-Zuazola, I. J. *Intelligent Transport Systems. Technologies and Applications (1st ed.),* John Wiley &Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, United Kingdom, 2016.

[4] Graham, J., Howard, R., Olson, R. *Cyber security Essentials*, CRC Press, Taylor & Francis Group LLC, London, United Kingdom, 2011.

[5] Ivanova, Y., Simulation Modeling of a Cyber Attack Against a Governance Structure. *Military Journal.* 4, 2015, pp. 113–126.

[6] Hoover, S. V. *Simulation: A Problem-solving Approach,* Addison-Wesley, 1989.

[7] Borshchev, A. *The Big Book of Simulation Modeling, Multimethod Modeling with AnyLogic6*, AnyLogic North America, 2013

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

[9] Shinder, D. L., *Computer Networking Essentials*, Cisco Press, 2001.

[10] http://e.huawei.com

[11] http://www.itsinternational.com/categories/detection-monitoring-machine-vision/features/computer-technology-increasingly-aids-traffic-management/

[12] http://www.hisense-transtech.com/plus/view.php?aid=49

[13] Sussman, J. M., *Perspectives on Intelligent Transportation Systems*, Springer, USA, 2005.

### *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 30 March 2017**

**Revised version received on 21 April 2017**