Modelling the impact of cyber attacks on the traffic control centre of an urban automobile transport system by means of enhanced cybersecurity

Yoana Ivanova[1,*]

[1]Bulgarian Academy of Sciences, Institute of ICT, "Information Technologies for Security" Department, 1000 Sofia, Bulgaria

Abstract. This paper aims to show the major role means of protection play for strengthening the cybersecurity of critical transport infrastructure by using the advanced method of simulation modelling. The simulation model of a Traffic Control Centre (TTC) of an urban Automobile Transport System (ATS) is created by the author in the Riverbed Modeler Academic Edition 17.5 computer networks simulation system and is exposed to the impact of a Denial-of-Service attack. In addition, logical conclusions have been made on the basis of the experimental results obtained and evaluated by comparative analysis with results from analogous previous studies.

1 Introduction

The focus of the present research is on the measures of strengthening and maintaining a secure, operational and sustainable critical transport infrastructure and in particular an urban Automobile Transport System (ATS) by building a reliable cyber protection of its Traffic Control Centre (TCC).

For this purpose, the author has studied and analyzed various advanced simulation environments based on agent-based modelling such as NetLogo [1], Aimsun 8.0, Cisco Packet Tracer and Riverbed Modeler. The capabilities of Riverbed Modeler Academic Edition 17.5 for modelling of computer networks by using a rich palette of realistic network devices and components, which could be precisely configured, make it the preferable software for assessing the impact of a Denial-of-Service attack on the TCC.

It is logical that the choice of an impenetrable protection is preceded by a detection of the vulnerabilities in a system. An example of an adaptive conceptual architecture for critical infrastructure cybersecurity is shown in Fig. 1. As it can be seen, the Topological Vulnerability Analysis (TVA) and the strategies for reducing the vulnerability are carried out at the prevention stage of the overall management, monitoring and analysis process, while the reinforcement of security by technical means is recommended to be done at the last stage.

The advantages of complex systems modelling by using professional simulation software are defined on the basis of a comparison with the other publicly known method of "penetration tests" for assessing the vulnerability of the critical infrastructure against cyber attacks.

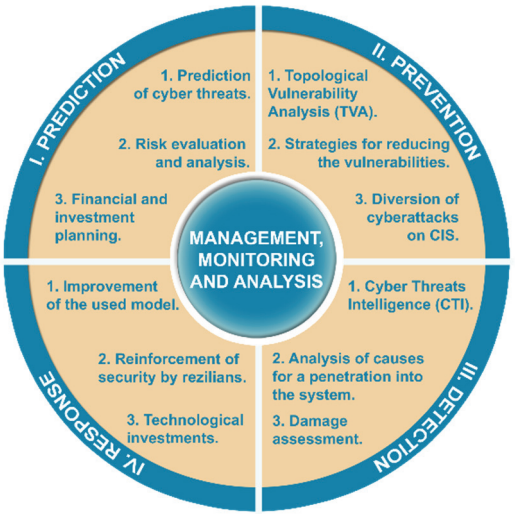

Fig. 1. Adaptive conceptual architecture for critical infrastructure cybersecurity.

2 Advantages of simulation modelling for assessing the vulnerability of critical infrastructure to cyber attacks

Simulation modelling is the main tool of TVA that is expressed in monitoring the state of network assets and maintaining models of network vulnerabilities and residual risk. It combines these to produce models that show the impact of individual and combined vulnerabilities on overall security posture [2].

In Riverbed Modeler Academic Edition 17.5 there is a possibility for specifying the settings of the DoS-attack profile and the vulnerability called "probability of

* Corresponding author: y.ivanova@bas.bg

infection" in percentages, as it can be seen from the screenshot shown in Fig. 2. The study could begin with absence of vulnerability (None) and continue to set the maximum vulnerability of 100 %.

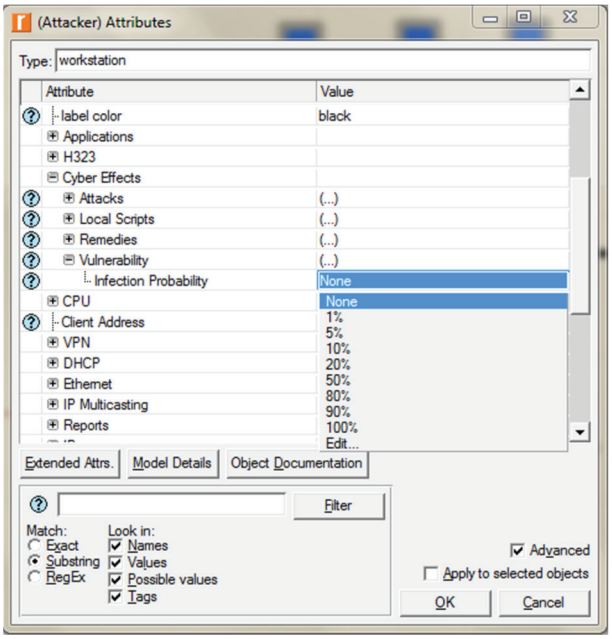

Fig. 2. System vulnerability settings related to a DoS-attack.

Penetration tests are used to verify security and, in particular to detect vulnerabilities in security systems by attacking them in the same way as a potential hacker would. One of the main differences between the two methods is that penetration tests must be implemented in "virtual machines" with vulnerable applications in order to safely test different techniques that target a system breakthrough, using publicly available tools [3]. This can be considered as an advantage of simulation modelling as compared to penetration tests, because the direct installation of simulation software on a personal computer does not pose a threat of infection.

Indeed, both methods in their essence are intended to detect vulnerabilities in the system but differ in the purpose of taking this action. In simulation modelling vulnerability assessment precedes simulation execution, while in penetration tests the attacker wastes time looking for weak points in the system. Practically, every complex system of great importance such as a TCC is protected in some way and it takes the attacker a relatively long time to overcome these means of protection. In this case, the advantage of simulation modelling is the possibility for the impact of a cyber attack to be seen instantly by relevant settings for ignoring the protection.

Actually, the full process of penetration testing is executed in seven successive phases as follows: ***Pre-engagement, Information gathering, Threat modelling, Vulnerability analysis, Exploitation, Post exploitation, Reporting [3].*** An analogous sequence of five phases in modelling a DoS-attack on a TCC in Riverbed Modeler Academic Edition 17.5 can be presented as a comparison: ***Gathering information about the DoS-attack, Attack modelling, Vulnerability assessment, Simulation execution, Summary evaluation of the results.*** By using the method of simulation modelling the phases become fewer as there is no direct and continuous communication with the client who has commissioned the penetration testing. This can be considered as another advantage of simulation modelling, because the client is not constantly involved in the process of performing a penetration test, but gets a finished end product. Additionally, penetration testing is usually conducted on site at the institution or organization that has commissioned it and this causes a disruption of its normal functioning during this process.

3 Means of protection against cyber attacks based on the potential vulnerabilities

The first step in defining an optimal protection strategy is to determine precisely the vulnerability of the specific management system which could be related to lapses in:

- ***network configuration*** – not using flow management methods; unencrypted passwords; bad device configuration in terms of security.
- ***network hardware*** – unsafe physical ports and unreliable physical protection.
- ***means of protection*** – misconfigured firewalls, undefined network security perimeter.
- ***software*** – buffer overflow, DoS-attacks, lack of Intrusion Detection System (IDS), failure to maintain Logs and monitor them in real time.
- ***hardware*** – insufficient testing, unreliable physical protection, unauthorized access, insecure remote access, Electromagnetic Interference (EMI).
- ***communication system*** – unsuitable Logs of firewalls and routers, lack of monitoring, authentication and verification of data integrity.
- ***security policies and procedures [4].***

On the basis of the classified main vulnerabilities the author recommends the following means for overall improvement of cybersecurity:

- ***antivirus software*** – constant update of the software is required to prevent penetration into the system.
- ***router*** – this autonomous device working with IP addresses can be defined as a smart device compared to the switch, because except for distributing the traffic it is also able to reduce the vulnerability of the system to cyber threats from Internet.
- ***Virtual Private Networks (VPN)*** – they ensure remote access, preserving the high quality and integrity of the output information. For example, IP VPN is a service designed to meet the needs of corporate business, where high quality, security and rich capabilities for integrated data, voice, video and multimedia transmission should be guaranteed.
- ***Firewall*** – this is an advanced approach to cybersecurity that is implemented as a strong authentication instead of static passwords through software and hardware complexes, routers, and other security measures. The interpretation of rules is implemented consistently by filters that allow for or prohibit the transmission of data (packets) to the next filter or protocol level.
- ***Honeypots and Honeynets*** – honeypots represent fake computer systems, setup as a "decoy", that are used to

collect data on intruders. This "decoy" appears to contain operating system vulnerabilities that make it an attractive target for hackers. While it appears vulnerable to attack, it actually prevents access to valuable data, administrative controls and other computers. Administrators can collect data on the identity, access, and compromise methods used by the intruder. Honeynets are networks, where all inbound and outbound data is analyzed and collected [5].

- ***Unified Threat Management (UTM)*** – complex solutions for cyber threat protection including all necessary modules**.**

4 Modelling the impact of a DoS-attack on the Traffic Control Centre of an urban Automobile Transport System through a firewall insertion

Being a professional simulation software Riverbed Modeler is widely used in security and defense for modelling all networks types and technologies (VoIP, TCP, OSPFv3, MPLS, IPv6) and analysing networks. It is suitable for testing and demonstrating technology designs before production; increasing network R&D productivity; developing proprietary wireless protocols and technologies; and evaluating enhancements to standards-based protocols [6].

For a comparison NetLogo is an open source multi-agent programmable modelling environment with a wide range of applications in different areas that makes it very useful for students. But it is not specialized in computer networks modelling and analysis like Riverbed Modeler and Cisco Packet Tracer.

The similarity between Riverbed Modeler and Cisco Packet Tracer is the possibility to simulate the complete network by connecting real types network devices and components. The main advantage of Riverbed Modeler compared to Cisco Packet Tracer is the possibility for directly simulating the impact of cyberattacks on different computer networks. For this reason the author has preferred Riverbed Modeler Academic Edition 17.5 to make the part of this research related to modelling the TCC and a cyberattack on it.

The research can be continued using the professional traffic modelling software Aimsun 8.0 after a logical assumption that the servers or services stop responding to client requests as a result of the simulated DoS-attack and this affects the Traffic Signal Control System. In this paper the focus is on strengthening the protection through a firewall insertion in order to reduce the probability of infection and respectively traffic changes under the impact of a DoS-atack to be prevented. Disturbances in normal signalling of traffic lights are observed after the server has stopped working due to the communication between the server and the signal controllers of the traffic lights [7]. Using reliable protections in TCC should help to support the normal traffic flows without increasing time delay and mean queues observed under the impact of successful cyberattacks.

The research of Prof. J. Alex Halderman from the University of Michigan in the field of computer security can be used in support of the claims about the course and consequences of cyberattacks on an urban ATS. In this study, the team led by Prof. Halderman concludes that the vulnerabilities they discovered in the infrastructure are not a fault of any one device or design choice, but rather show a systemic lack of security consciousness, which is expressed in: unencrypted radio signals; use usernames and passwords by default; a debug port that is easy to be attacked; using an older version of the installed software [8].

The author's reference model (M_{Ref}) of TCC has a typical network configuration including 3 workstations, 3 servers and a switch connected in a linear bus network. It has been developed in Riverbed Modeler Academic Edition 17.5 using built-in protections simulated by specific settings. The model is subjected to the impact of a DoS-attack that causes such an intensive traffic (flooding) that the processing of the requests is impeded [9].

The author has chosen to work with a firewall type *ethernet2_slip8_firewall_adv,* which is a specially programmed router. A screenshot of the model is shown in Fig. 3.

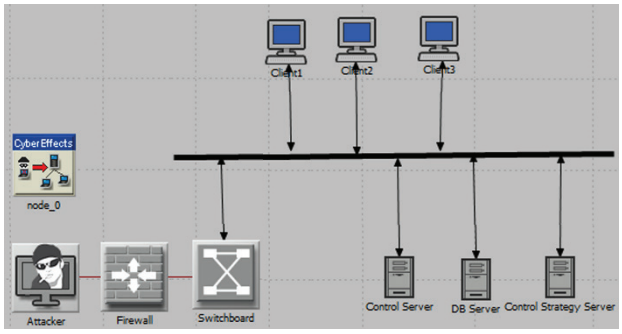

Fig. 3. The model of TCC with a firewall insertion under the impact of a DoS-attack.

The duration of this simulation is 30 s and is divided into six equal intervals of 5 s. Table 1 contains simulation results from 10 scenarios.

In the current research, the method used for verification of the model is based on the reaction time that represents a time interval between the beginning of an action and beginning of the corresponding response. The research is made for 10 consecutive scenarios. This method has been preferred by the author, because it demonstrates one of the great advantages of simulation modelling. It provides an opportunity the research to be done entirely in a virtual environment in order to save financial resources for realization in a physical environment using a hardware prototype. Therefore, the simulation results can be accepted as sufficiently reliable and at this stage it is not required to be compared with results of other analogous studies.

The comparative diagrams in Figures 4, 5 and 6 show in which second of running the simulation are registered peak levels of T_S and T_R, respectively with built-in protections and a firewall. The dark blue chart shows T_R without a firewall, while the red one shows T_R with a firewall. The green chart shows T_S without a firewall, while the light blue one shows T_S with a firewall.

Table 1. Peak levels of "traffic sent" ($T_{S,\max}$) and "traffic received" ($T_{R,\max}$), depending on the inter arrival time (T) for the model under the impact of a DoS-attack respectively without and with a firewall.

	Without a firewall		With a firewall	
T s	$T_{S,\max}$ pack/s	$T_{R,\max}$ pack/s	$T_{S,\max}$ pack/s	$T_{R,\max}$ pack/s
2	10	6,7	6,7	3,4
1	10	6,7	6,7	3,4
0,5	10	13,5	13,5	3,4
0,25	16,5	13,5	13,5	6,7
0,2	16,8	13,5	20	10
0,15	27	13,5	16,4	6,4
0,1	33,5	20	23	13
0,05	44	37	43	20
0,025	80	50	74,5	34,5
0,02	84	58	84	40

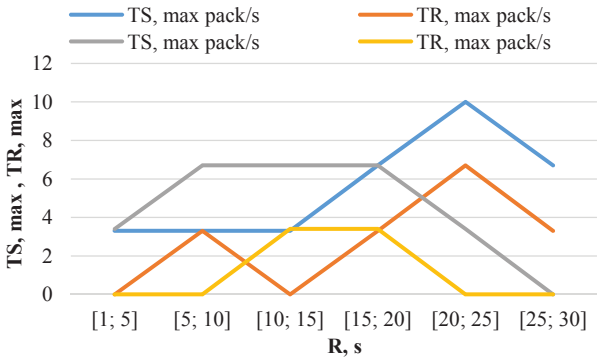

Fig. 4. $T_S = f(T)$ and $T_R = f(T)$ at $T = 2$ s.

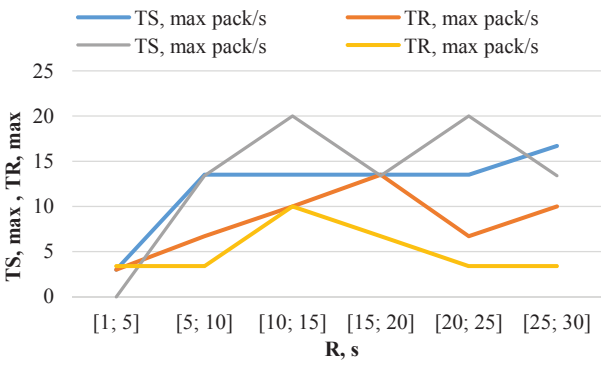

Fig. 5. $T_S = f(T)$ and $T_R = f(T)$ at $T = 0{,}2$ s.

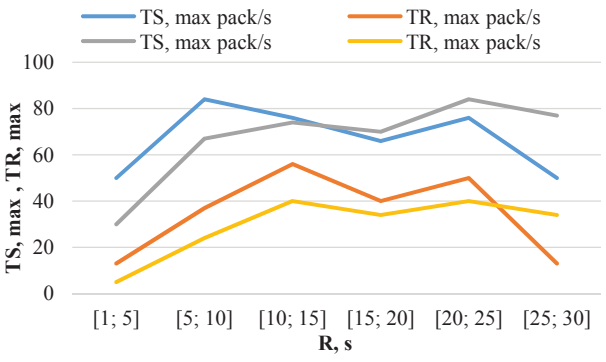

Fig. 6. $T_S = f(T)$ and $T_R = f(T)$ at $T = 0{,}02$ s.

Table 2, 3 and 4 contain the summary results of all three charts and show in which time intervals R in seconds are registered peak levels of T_S and T_R as functions of the selected three values of the inter arrival time T, respectively without and with a firewall.

Table 2. Peak levels of "traffic sent" ($T_{S,\max}$) and "traffic received" ($T_{R,\max}$) at $T = 2$ s.

	Without a firewall		With a firewall	
R s	$T_{S,\max}$ pack/s	$T_{R,\max}$ pack/s	$T_{S,\max}$ pack/s	$T_{R,\max}$ pack/s
[1; 5]	3,3	0	3,4	0
[5; 10]	3,3	3,3	6,7	0
[10; 15]	3,3	0	6,7	3,4
[15; 20]	6,7	3,3	6,7	3,4
[20; 25]	10	6,7	3,4	0
[25; 30]	6,7	3,3	0	0

Table 3. Peak levels of "traffic sent" ($T_{S,\max}$) and "traffic received" ($T_{R,\max}$) at $T = 0{,}2$ s.

	Without a firewall		With a firewall	
R s	$T_{S,\max}$ pack/s	$T_{R,\max}$ pack/s	$T_{S,\max}$ pack/s	$T_{R,\max}$ pack/s
[1; 5]	3	3	0	3,4
[5; 10]	13,5	6,7	13,4	3,4
[10; 15]	13,5	10	20	10
[15; 20]	13,5	13,5	13,4	6,7
[20; 25]	13,5	6,7	20	3,4
[25; 30]	16,7	10	13,4	3,4

Table 4. Peak levels of "traffic sent" ($T_{S,\max}$) and "traffic received" ($T_{R,\max}$) at $T = 0{,}02$ s.

	Without a firewall		With a firewall	
R s	$T_{S,\max}$ pack/s	$T_{R,\max}$ pack/s	$T_{S,\max}$ pack/s	$T_{R,\max}$ pack/s
[1; 5]	50	13	30	5
[5; 10]	84	37	67	24
[10; 15]	76	56	74	40
[15; 20]	66	40	70	34
[20; 25]	76	50	84	40
[25; 30]	50	13	77	34

Summary evaluation

On the basis of the tabular and graphical results the author has come to the following conclusions. When a firewall is used the number of sent packets $T_{S,\max}$ is generally lower than the number of packets sent when built-in protections by vulnerability settings are used.

Before the time interval [25; 30], when the number of sent packets is less than 80, a better filtration of the packets sent is observed due to the firewall insertion as compared with the case of using only built-in device protections. In the last time interval, when the number of sent packets exceeds 80, there is a "saturation" which may be due to a limitation of the used type of a firewall.

It is also necessary to establish whether the packets themselves represent a threat or not. In case that certain packets threaten the system is necessary to improve the selected firewall model by replacing it with another model, or by integrating it with other means of protection.

In addition, when a firewall is used the cases of flooding are reduced to only one in the last time interval from all ten scenarios, while without the inserted means of enhanced protection the flooding starts in the time interval [20; 25] and it deepens in the last time interval [25; 30]. This means that a system denial can be observed in at least two of all 10 scenarios. If this should be presented with the probability of an adverse event, then when a firewall is used, this probability is equal to 10 %, but it is at least twice as much if there is not a firewall insertion.

Recommendation to enhance the protection used

One of the reliable solutions for analyzing the received packets are Intrusion Detection Systems (IDS), which evaluate each packet and assess whether it is a hazard or not. If a packet is defined as a source of a cyber threat, the system decides whether to ignore it completely, log it to be analyzed by the administrator or immediately alerts that such a packet has infiltrated the network.

The IDS can be placed in different locations in the network, as well as in the firewall itself. The advantage of placing it in the firewall is that many of the suspicious packets will be blocked at the entrance and potential cyber threats will be prevented. Besides, IDS control the firewall. An IP address of the network controller that monitors the traffic should not be set when configuring IDS to prevent a potential attacker from detecting the device. The aim is for the IDS sensor to be protected from network scans and attacks that it is trying to find. In this case the disadvantage is that the removal of the IP address causes problems for administrators to manage the process. The solution is to use two network interfaces, one of which is configured without IP and works as a sensor, and the other one is connected to a separate local area network that collects information and manages IDS devices [10].

5 Conclusion

This research is an example of applying simulation modelling for solving problems related to cybersecurity of critical transport infrastructure. There are possibilities for the study to be extended in order to improve the methods and means of protection using the simulation results.

It has been demonstrated that the negative impact of a cyber attack on the TCC can be reduced by using appropriate protection, but the wide variety of existing cyber threats requires that the means of protection are constantly tested, updated and improved. The demonstrated method proves that the use of a simulation environment is a very effective way to achieve that aim.

One of the directions in which the research can be expanded is an additional verification based on the margin of error by comparing the simulation results with measurements in a physical environment. In the present case, such study is not intended because the aim is to emphasize the advantages of simulation modelling itself.

References

1. Y. Ivanova, Military Journal, Sofia, 4, 113-126 (2015).
2. S. Jajodia, S. Noel, B. O'Berry, *Managing Cyber Threats: Issues, Approaches and Challenges*, Kluwer Academic Publisher, 248-250 (2005).
3. G. Weidman, No Starch Press Inc., San Francisco, 2-6 (2014).
4. E. Stoilov, *Department of Informatics at NBU*, Sofia, 21-28 (2010).
5. SANS Institute. *Honey Pots and Honey Nets - Security through Deception*, 1-5 (2003).
6. Riverbed Technology, *Riverbed Modeler: A Suite of Protocols and Technologies with a Sophisticated Development Environment*, San Francisco (2017).
7. Y. Ivanova, IJITS, issue 3, vol. 9, 117-142 (2017).
8. Y. Ivanova, IJITS, issue 2, vol. 9, 83-95 (2017).
9. B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek. & A. J. Halderman, *Green Lights Forever: Analyzing the Security of Traffic Infrastructure*, Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT '14) (2014).
10. E. Stoilov, *Department of Informatics at NBU*, Sofia, 32-36 (2011).