International Journal of Computing Academic Research (IJCAR)
ISSN 2305-9184 Volume 3, Number 6(December 2014), pp. 131-137
© MEACSE Publications
http://www.meacse.org/ijcar

Measuring the Impact of Security Protocols for Bandwidth

Milos Orgon and Lubomir Fackovec

Department of Telecommunication, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology, Bratislava, Slovakia

Abstract

This paper will assess the impact of the use of security protocols for bandwidth in wireless networks [1,2,3]. Two scenarios were created – one without network operation quality impairment, and the other one with additionally impaired operation quality by means of software tools IxChariot and NetDisturb, which artificially undermined the operation of the network by generating of delay, jitter, limited bandwidth, packet loss rate increases, the generation of duplicate packets and modifying packets transmitted, etc.

Keywords: Wireless networks, bandwidth, security protocols, transfer rate.

Introduction

Examination of the impact of security protocols on the transfer rate was carried out in laboratory conditions at the Institute of Telecommunications of FEI STU in Bratislava. For the test we used a PC with Windows XP (32-bit version) with installed software tool designed to simulate application-generated data stream IxChariot. The second PC had an installed software emulator NetDisturb with two network adapters. In both scenarios another notebook (running Windows 7 - 32-bit version) was used. The notebook was connected to a wireless network through an access point on the router Cisco WRVS4400N - EU.

IxChariot can be characterized as a test tool for simulating the real-life application under the conditions of a real load by generating additional data streams. It also enables the testing of security protocols. It allows testing of both wired and wireless networks. It consists of IxChariot console with a graphical interface, which is used to run simulations and evaluate their results. Through the endpoints (Performance Endpoints) it is possible to generate the use and collect data, which are used to evaluate the simulation. These end points must be placed upon at least two of the terminal devices (creating communication pair), so that the simulation can take place [4,5].

The two terminal devices are set up using IP addresses in the software tool of the IxChariot console. In our case it was the IP address of the computer used to generate traffic and at which this application was lodged. The other endpoint consisted of a notebook connected to the wireless network. During the testing, the network protocol TCP was set up and used for all simulations HTTP text script, which describes the behaviour of endpoints. The script can be set up choosing from a wide variety of scripts for testing: FTP, DNS or applications such as Citrix, LDAP, database servers or voice signalising, and many others [4,5].

NetDisturb is a network software emulator that can artificially reduce the quality of network operation by degrading network traffic by the means of generating different delays and jitters, it also allows limiting bandwidth, increasing packet loss, generating duplicates of packet flows, modifying transmitted packets and the like. Furthermore, it also allows impairing streams over IP networks and therefore studying the behaviour of applications, devices and services in a networked environment exposed to disturbance. NetDisturb is inserted between two Ethernet segments acting as a bridge and operates bi-directional packet transfer on Ethernet, FastEthernet and GigabitEthernet [6,7].

The NetDisturb network emulator is built at the client-server architecture and uses the HTTP protocol and XML (Extensible Markup Language) format for the exchange of packets between client and server. Two configurations are possible: either the server and the client are located at the same computer (local governance), either the server and the client are placed at different computers (remote management). NetDisturber supports protocols IPv4 and IPv6.

The role of software tool NetDisturb is to manage, disrupt and in other ways harm packet streams. For the operation of this instrument two NIC cards are required. Each of them has an interface A and B and, for each direction A → B and B →A, 16 flows can be defined, and at the same time a depreciation of transfer can be set up for each flow, such as loss or duplication of packets, generation of delays and the like [6,7].

Principles of operation of the software tool NetDisturb is as follows. Depending on the predefined streams, the incoming packet is controlled, whether it meets the criteria of set packet flow filters. In the event that the packet satisfies the flow filter, it is identified whether the packet should be lost or duplicated and / or delayed and / or damaged. In the event that it does not match any of the filters, the specific flow is considered to be unfiltered. Each packet received on the interface is analyzed by filters in order from 1 to 16, before it is assigned as an unfiltered stream [6,7].

Scenarios of measuring the impact of protocols on bandwidth

In the scenario of measuring the impact of protocols on bandwidth without operation impairment, was tested the impact of security protocols on the transfer rate without degradation of data transfer. Despite of the fact that the measurement was performed in the laboratory, laboratory conditions were not fully met, because nearby the measuring workplace were located other wireless networks affecting the testing. Fig. 1 provides an overview of wireless networks that were in range of the testing workplace and the figure also shows the availability of each channel. After the auto-occupation of the channel No. 6 by an access point, this setting was changed to the working channel No. 9-2452 GHz (network CISCOSB) to take advantage of the less overwhelmed part of the band.

Near the workplace were also found other sources of interference out of our control - microwave ovens, electrical machinery and equipment, which could have affected the measurement. The shown utilization of channel (Fig. 1) can cause problems in communication - collisions and decrease of transfer rate may occur, particularly when the same channel is occupied by several networks at the same time.

During the testing, functions of the access points associated with affecting the quality of service QoS were disabled. Working mode was set to 802.11b/g/n standard mixed.

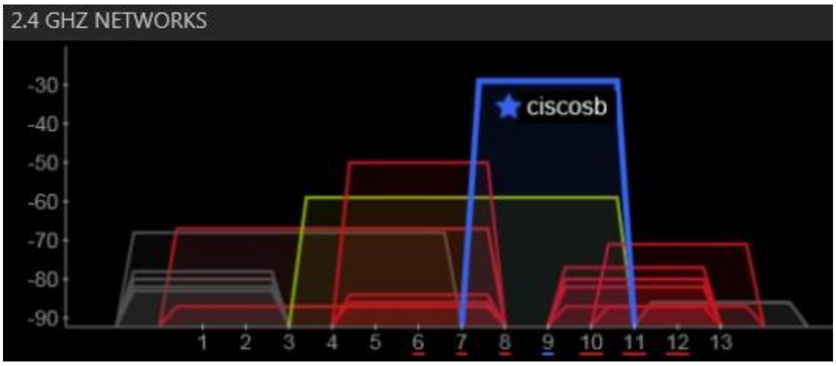


Fig . 1 Occurrence of wireless networks within range of the measuring workplace

The topology of the testing facility is illustrated by Fig. 2. In both scenarios the same connection was used, data traffic passes through the instrument NetDisturb without damage. The computer on which this tool was located, had two network cards. A notebook was placed at a distance of one meter from the AP without obstacles.

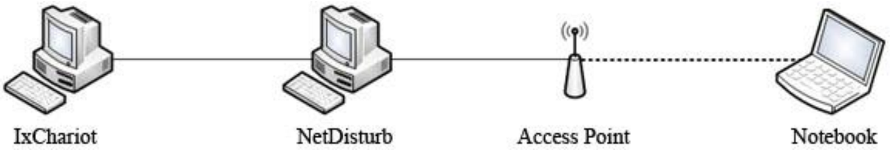


Fig . 2 The testing facility

During the testing, the IP address on the computer IxChariot was set up as a gateway for notebook and vice versa. Thus, both computers were connected via an access point. On the computer on which the tool NetDisturb was installed, no network address was set up, but all services were disabled. On the notebook, it was necessary to allow network discovery to allow other computes to recognize it in the network.

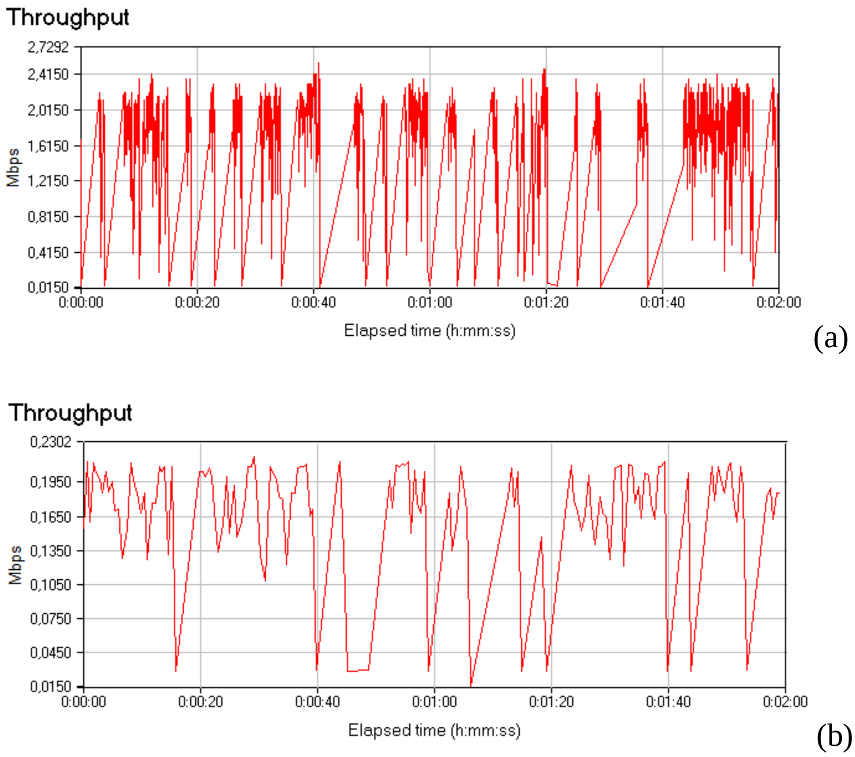


Fig. 3 Throughput of an unsecured network a) with non-imparied operation b) with impaired operation

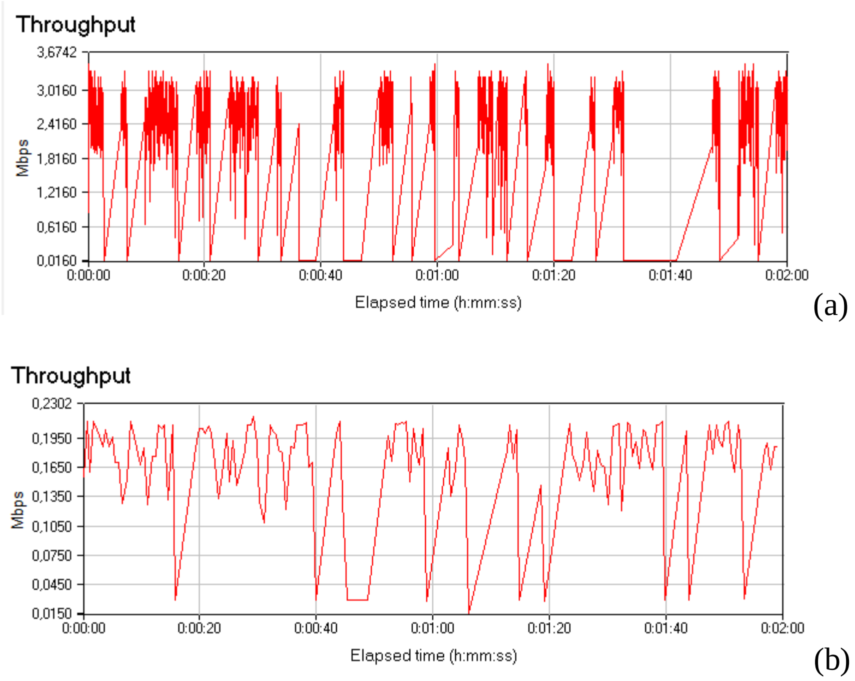


Fig. 4 Network throughput when using WEP security a) with non-imparied operation b) with impaired operation

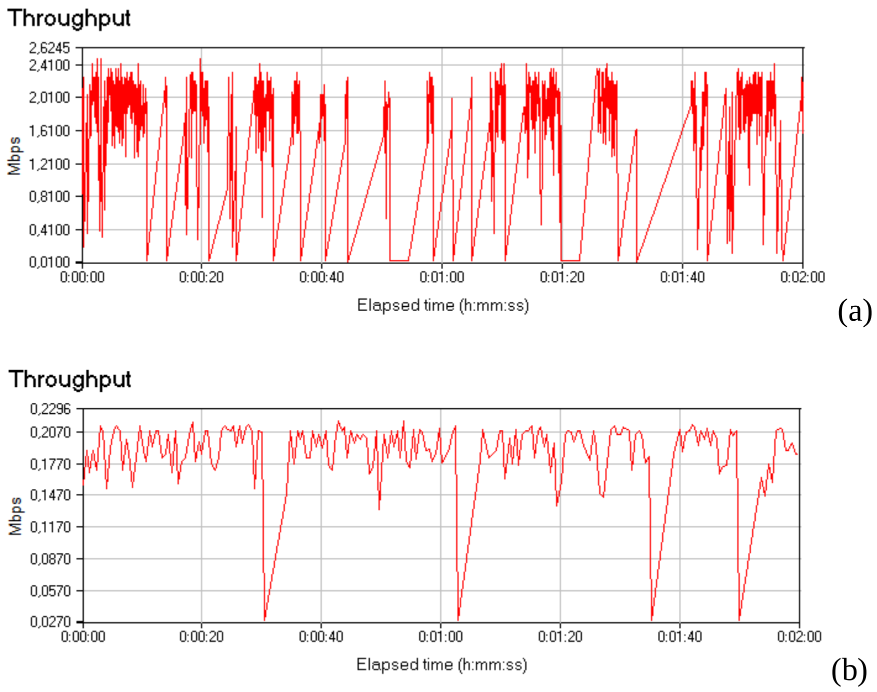


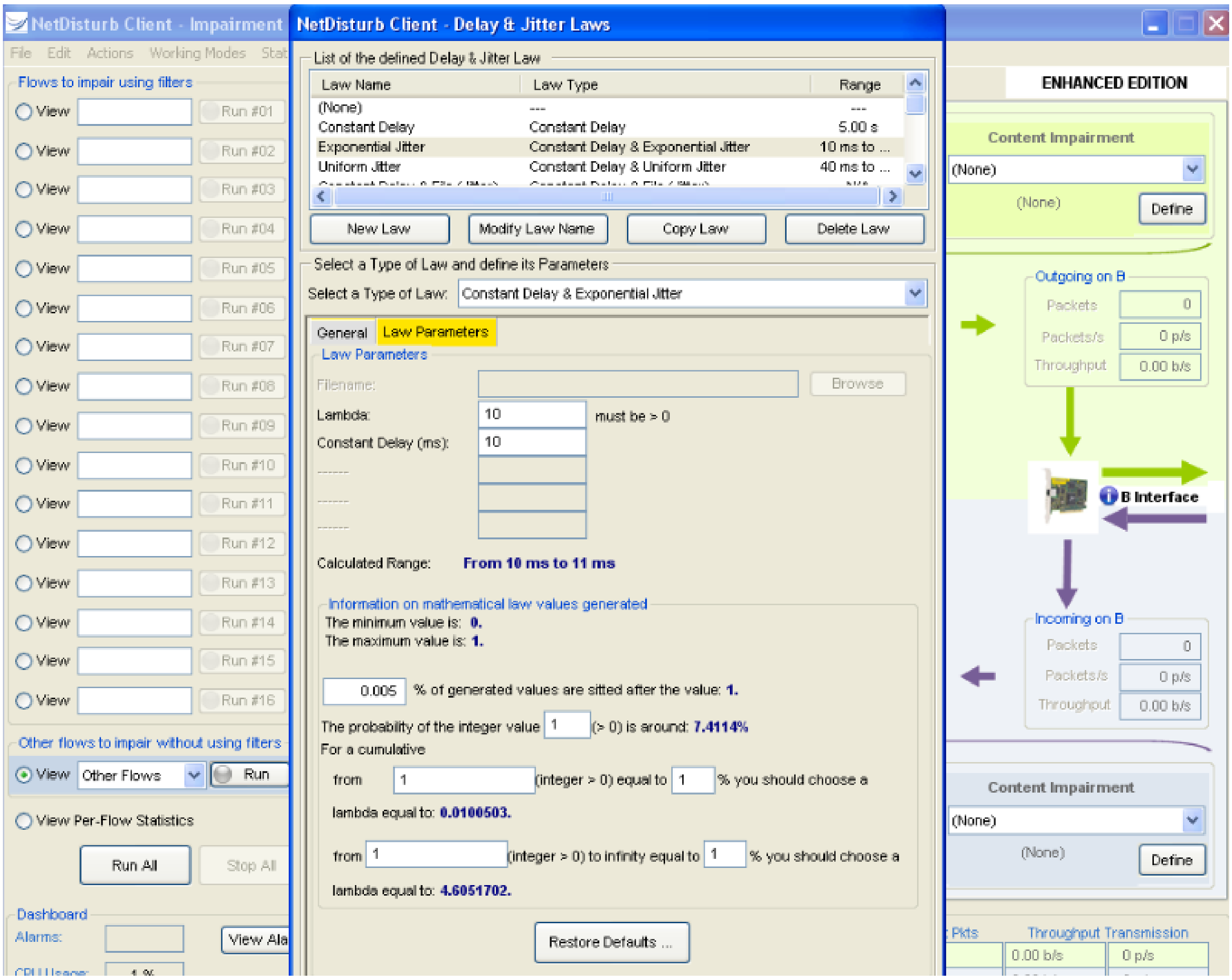
Fig. 5 Network throughput when using WPA- Personal a) with non-impaired operation b) with impaired operation

While implementing the first scenario, three tests were performed without network operation impairment, whereby each test lasted two minutes. The obtained values are shown in Table. 1 and the related graphs with non-impaired operation are shown in Fig. 3a, Fig. 4a, and Fig. 6a.

While implementing the second scenario, three tests were carried out, each test took again two minutes, while the operation was impaired. The obtained values are also shown in Table. 1 and the related graphs with impaired operation are shown in Fig. 3b, Fig. 4b and Fig. 5b.The testing of the impact of the used security protocols on data transfer rate in network with impaired packet transfer by a network emulator NetDisturb was implemented in the same testing facility and under the same conditions as in the previous scenario. The working channel is the channel no. 9-2452 GHz (network CISCOSB) and the working mode is the 802.11b/g/n mixed. When performing measurements, the devices were connected to the same topology as in the precedent case (Fig. 2).

Table 1 The impact of the used security protocol on the transfer rate

Used security protocol	**Non-impaired vs. Impaired network operation**	**Transfer rate**	**Minimum transfer rate [Mbit/s]**	**Maximum transfer rate [Mbit/s]**	**Average response time [s]**	**Response time Min/Max [s]**
Unsecured network	Non-impaired net	0,671	0,017	2,537	0,015	0,004/0,620
	Impaired net	0,126	0,016	0,217	0,083	0,048/0,649
WEP	Non-impaired net	0,794	0,017	3,467	0,013	0,003/0,611
	Impaired net	0,126	0,016	0,217	0,083	0,048/0,649
WPA2 (AES)|	Non-impaired net	0,694	0,012	2,476	0,015	0,004/0,897
	Impaired net	0,172	0,029	0,217	0,060	0,048/0,362



NetDisturb Client - Delay & Jitter Laws

List of the defined Delay & Jitter Law

Law Name	Law Type	Range
(None)	---	---
Constant Delay	Constant Delay	5.00 s
Exponential Jitter	Constant Delay & Exponential Jitter	10 ms to ...
Uniform Jitter	Constant Delay & Uniform Jitter	40 ms to ...

Select a Type of Law and define its Parameters

Select a Type of Law: Constant Delay & Exponential Jitter

Law Parameters

Lambda: 10 must be > 0

Constant Delay (ms): 10

Calculated Range: From 10 ms to 11 ms

Information on mathematical law values generated

The minimum value is: 0.

The maximum value is: 1.

0.005 % of generated values are sitted after the value: 1.

The probability of the integer value 1 (> 0) is around: 7.4114%

For a cumulative

from 1 (integer > 0) equal to 1 % you should choose a lambda equal to: 0.0100503.

from 1 (integer > 0) to infinity equal to 1 % you should choose a lambda equal to: 4.6051702.

Fig. 6 Adjusting the constant delay and exponential jitter in the network emulator NetDisturb

Depreciation of the network operation was carried out through the network emulator NetDisturb by setting exponential constant delay and jitter. The setting up of the values of the network emulator is shown in Fig. 8. Constant delay was set up to 10 ms (this value can be set from 1 ms to 100 s**)**. Exponential jitter is calculated from the parameter lambda, while for purposes of this test the lambda value was not changed – remaining set up to the default value of 10. The value of exponential jitter is added to the constant delay, which affects bandwidth, as described below. The probability density function for the specified parameter lambda can be expressed by the following formula:

$$f(x;\lambda > 0) = \begin{cases} \lambda \cdot e^{-\lambda x} & ,x \geq 0 \\ 0 & ,x < 0 \end{cases} \tag{1}$$

The operation was influenced by setting the stream 1 on HTTP. We used a filter to drive delay for HTTP traffic in both directions A → B and B → A.

In the first test, no network security protocol was used. The average transfer rate with non-impaired operation was 0.671 Mbps, and respectively 0.126 Mbps with impaired operation (Table 1). The minimum transfer rate with non-impaired operation was 0.017 Mbps, and respectively 0.016 Mbps with impaired operation. The maximum transfer rate with the non-impaired operation was 2.537 Mbps, and respectively 0.217 Mbps with impaired operation.

In the second test, the security protocol WEP was used to ensure network security. The average transfer rate with the non-impaired operation was 0.794 Mbps, and respectively 0.126 Mbps with impaired operation. The minimum transfer rate with the non-impaired operation was 0.017 Mbps, and respectively 0.016 Mbps with impaired operation (both values are the same as in the previous case - without the use of a security protocol). The maximum transfer rate with the non-impaired operation was 3.467 Mbps (the highest of all measured values), and respectively 0.217 Mbps with impaired operation (same value as in the previous case - without the use of a security protocol). While comparing the values listed in Table 1, it appears that the maximum transfer rate is the highest.

In the third test, the security protocol WPA2-Personal was used to ensure network security. The average transfer rate with the non-impaired operation was 0.694 Mbps, and respectively 0.172 Mbps with impaired operation. The minimum transfer rate with the non-impaired operation was 0.012 Mbps, and respectively 0.029 Mbps with impaired operation (both values are the same as in the previous case - without the use of a security protocol). The maximum transfer rate with the non-impaired operation was 2.476 Mbps (the highest of all measured values), and respectively 0.217 Mbps with impaired operation (the same value as in the first two cases). As it is also apparent from Table 1, the minimum transfer rate was the same as in the first two tests in with impaired operation.

As evidenced in the above Table 1, the differences between the achieved transfer rates are minimal. Although, based on the knowledge of the protocol frame structure, it was possible to predict the reduction of the transfer rate when using secure protocols. The former was confirmed, but only in a small extent - the difference of transfer rates was only minimal. However, the important finding is the following: a significant increase of security using security protocol WPA2 Personal instead of WEP was not reflected by an increased decrease of the transfer rate.

During the testing the assumption that the influence of a different frame structure would result into the reduction of the transfer rate was confirmed - by introducing artificial delay via the network emulator NetDisturb in both directions. The Tab. 1 shows a reduction in the average transfer rate of 0.5 Mbit / s under the impact of the operation impairment and that the maximum transfer rate dropped by more than 2.2 Mbps. The Effect of delay may be observed as well when comparing the instantaneous transfer rate shown in Fig. 3a, Fig. 4a and Fig. 5a (no degradation of service) with waveforms shown in Fig. 3b, Fig. 4b and Fig. 5b (which were measured when the network traffic network was deteriorated by the emulator NetDisturb). Measured flows of the instantaneous bit rate with operation impairment have significantly" less dense" course. Another factor should be taken into account - the relatively high availability of channels in the surrounding of the test facility (Fig. 3).

Conclusion

The aim of the contribution was to investigate the impact of using security protocols for bandwidth in wireless networks. For the network testing we used two scenarios – one without network operation quality impairment and the other with additionally impaired operation quality by means of software tools IxChariot and NetDisturb, which artificially devalued the network operation by generating traffic delay and delay variation, limited bandwidth, increased loss rates, generated duplicates of packet flows, modified transmitted packets and so on.

The wireless network tests led to the discovery of a negative impact of the impaired network operation (via a network emulator NetDisturb), which was expressed by the degradation of the instantaneous transfer rate. The reduced transfer rate was more significant particularly while using security protocols WEP, WPA2 compared to an unsecured network.

Acknowledgement

This article was created with the support of the Ministry of Education, Science, Research and Sport of the Slovak Republic within the Research and Development Operational Programme for the project "University Science Park of STU Bratislava", ITMS 26240220084, co-funded by the European Regional Development Fund and his article is a part of research activities conducted at Slovak University of Technology Bratislava, Faculty of Electrical Engineering and Information Technology, Institute of Telecommunications, within the scope of the project KEGA No. 039STU-4/2013 “Utilization of Web-based Training and Learning Systems at the Development of New Educational Programs in the Area of Optical Transmission Media”.

References

[1] Rita Pužmanová: Bezpečnost bezdrátové komunikace (Security of wireless communication), Brno, CP Books, 2005, ISBN 80-251-0791-4.

[2] Mandjid Nakhjiri, Mahsa Nakhjiri: AAA and network security for mobile Access, Chichester GB, John Wiley and Sons, 2005, ISBN 0-470-01194-7.

[3] Hakima Chaouchi, Maryline Laurent –Maknavicius: Wireless and Mobile Network Security, London GB, ISTE Ltd, 2009, ISBN 978-1-84821-117-9.

[4] IxChariot User Guide: Release 7.10 913-0949-04 Rev . and, IXIA 2011. pp.474 http://www.ixiacom.com.

[5] IxChariot™ Application Scripts, Release 6.20909-0397 Rev. A, December 2005

[6] Impairment Emulator Software for IP Networks (IPv4 & IPv6): User Guide. [online]. Plumbing, 2013, http://www.zti-telecom.com/User_GuidesN/NetDisturb_User _Guide_V6.0.pdf

[7] NetDisturb - IP Network Impairment Simulator Standard Edition - Software, http://www.omnicor.com/network_impairment_simulator_STD.aspx