Impact of Internet on Business Activities in Serbia and Worldwide

Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-600-605

PERFORMANCE EVALUATION OF WPA2 SECURITY PROTOCOL IN MODERN WIRELESS NETWORKS

Dejan Tepšić, Mladen Veinović, Dejan Uljarević
Singudunum University, Serbia

Abstract:
This paper evaluates performance impact of WPA2 security protocol on various operating systems in modern wireless networks. For the purpose of experiments IEEE 802.11n wireless network platform was deployed. Metrics of throughput and jitter were obtained during the generation of TCP and UDP data flows in different security scenarios. Experimental results showed that IPv4 operating systems achieve higher throughput values than IPv6 systems under the same conditions within the IEEE 802.11n wireless network. Results further indicate that WPA2 security protocol reduces value of throughput and increases jitter in wireless networks.

Key words:
WPA2,
security protocol,
wireless network,
802.11n,
operating system,
throughput,
jitter.

INTRODUCTION

Wireless networks provide mobility and accessibility beyond traditional wired networks. While mobility is an undoubted advantage of wireless networks, improved productivity and flexibility in allocation of clients are also important advantages of wireless networks. Security risks in wireless networks are numerously higher than those in wired networks, given the nature of wireless radio waves which are transmitted on a shared wireless medium.

In addition to safety, performance is another major problem of wireless networks. The objective of this research is to understand and quantify the relationship between security and performance in IEEE 802.11n wireless networks. To conduct this study experiments were performed in a wireless network environment. WPA2 security protocol was used to encrypt TCP and UDP traffic for different packet sizes on IPv4 and IPv6 operating systems. In order to quantify and compare the impact of WPA2 security protocol, experiments were conducted also for the scenario when encryption is not used (open system). Data obtained in these experiments quantifies and compares the relationship of performance, such as throughput and jitter.

IEEE 802.11n [1] is the latest wireless standard that defines the design of wireless network equipment. New standard provides a number of enhancements and features, among which are increased data rates, quality of service, optimization of distance between wireless devices, reliability, network management and improved security. With addition of multiple-input multiple-output (MIMO) technology, IEEE 802.11n wireless networks theoretically supports data rates up to 600 Mb/s, with a maximum radius of covered area up to 250 meters. This proves that IEEE 802.11n wireless standard achieved substantial increase of throughput and area coverage with wireless network signals compared to its predecessors, IEEE 802.11a/b/g.

With the growth of the Internet and its increasing globalization, current Internet Protocol version 4 (IPv4) will soon run out of available IP addresses. Internet Engineering Task Force (IETF) has developed a new version of Internet Protocol version 6 (IPv6). IPv6 greatly expands the IP address space from 2^{32} to 2^{128} addresses. IPv6 delivers additional features that are missing in Internet Protocol version 4, such as automatic configuration, more accurate selection of quality of services, new security features and compatibility with 3G mobile technology. Improvements within the IPv6 protocol entered a negative effect on performance of wireless network devices, due to the fact that the size of IPv6 packet header is doubled. The minimum size of IPv4 packet header is 20 bytes [2], while within the IPv6 protocol this value is 40 bytes. Given that the transition from IPv4 to IPv6 protocol is inevitable, it is necessary to consider the difference of performance between IPv4 and IPv6 systems.

At the time of this research Windows operating systems have had an absolute majority of market share among operating systems. Currently among them the most relevant is Microsoft Windows 8 64-bit operating system. Although their percentage is far lower, Linux operating systems are constantly evolving and becoming more popular. For purposes of this study created is wireless network platform for network performance evaluation of different operating systems in IEEE 802.11n wireless network protected with WPA2 security protocol. Analyzed operating systems are 64-bit Windows 8 Professional and Linux Ubuntu Desktop version 13.04.

LITERATURE REVIEW

The main focus of this research is need for stronger security and better performance of operating systems in IEEE 802.11n wireless networks. The relationship between these two factors has to be studied. Existing works in this field have partly described this [3]-[6].

In [3], studied is the effect of WPA2 security protocol in IEEE 802.11n wireless network on bandwidth and round trip time for different operating systems. Experimental results showed a decrease in value of TCP bandwidth on Windows 7 and Linux Fedora operating systems for both IPv4 and IPv6 protocols when WPA2 security protocol is used.

In [4], quantified is the effect of security techniques in IEEE 802.11n wireless network on Windows XP, Windows Vista and Windows Server 2008 operating systems. The main contribution was to explore the impact of WPA2 security protocol on throughput of different Windows operating systems. The results showed a decrease in throughput for both IPv4 and IPv6 systems when WPA2 security protocol is enabled. Also, it showed that IPv4 protocol achieves less reduction in throughput than IPv6.

In [5], presented are results of performance comparison of IEEE 802.11n encryption methods on four operating systems, for both TCP and UDP traffic. This research has shown that operating systems perform differently within IEEE 802.11n wireless network and its encryption algorithms. It is also shown that WPA2 behaves significantly differently to the other encryption methods.

In [6], authors presented results on the performance of IEEE 802.11n using open system (no security) and WPA2 security for Windows XP and Windows 7 operating systems. WPA2 security results in lower TCP throughput than open system for both IPv4 and IPv6 systems. For both open system and WPA2 security IPv4 provides higher bandwidth than IPv6.

WIRELESS NETWORK PLATFORM

Wireless network platform used in this study (Fig. 1) [7] consists of TP-Link wireless access point (WAP) and two identical Toshiba laptop computers with wireless network adapters. IEEE 802.11n protocol is fully supported by all of the devices which are used in the experiments.

Technical specifications of used wireless network devices and software:

- TP-Link WAP with the following characteristics [8]:
  - Model: TL-WR941ND supports IEEE 802.11b/g/n standards.
  - It has 13 radio channels in the range of 2.4 GHz with maximum data transfer speeds up to 300 Mb/s in the case when IEEE 802.11n standard is used.
  - Supports WEP with a key length of 64, 128 and 152 bits, WPA-TKIP and WPA2-AES security protocols.
  - WPA2-AES protocol is processed within hardware on wireless access point.
  - Supported authentication methods are open system, system with a shared key and 802.1X authentication.
- Toshiba laptop computers with wireless network adapter:
  - Model: Toshiba Satellite C655-S5208 [9] with Intel ® Core ™ i3 processor and Atheros AR9285 IEEE 802.11b/g/n wireless network adapter.
  - Operating system: Microsoft Windows 8 Professional 64-bit, Linux Ubuntu Desktop 13.04 64-bit.
  - Software used: JPerf, software for generating TCP and UDP network traffic at different data transfer speeds for IPv4 and IPv6 systems.

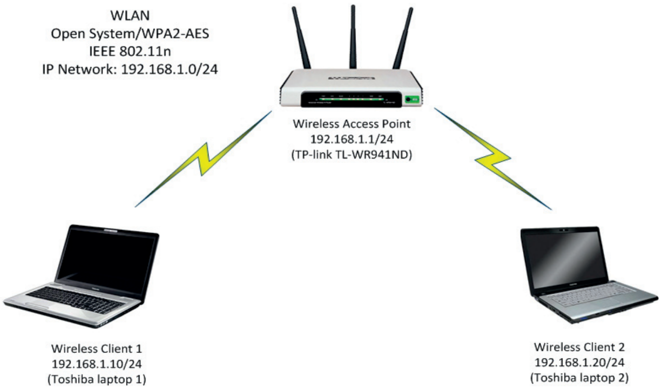

Fig. 1. Wireless network platform.

SECURITY SCENARIOS

The experiments were carried out in wireless network environment for various security scenarios and traffic flows:

- Without security protocol (open system): in this scenario clients communicate over WAP without any authentication and encryption of traffic. The results are used as a reference for comparison with scenario where WPA2 security protocol is used.

- WPA2-AES: in this scenario the most processor demanding encryption algorithm is used, Advanced Encryption Standard (AES). Experiments were carried out for the key length of 256 bits.

In described experiments TCP and UDP traffic flows are generated. UDP traffic represents voice and video packets which are transmitted over computer networks, while TCP traffic represents standard network traffic, such as HTTP, FTP and others. Distinguishing between these two types of traffic is crucial for understanding the results of experiments. UDP traffic flow allows us to determine the maximum throughput of wireless networks, because it has no mechanism for checking the receipt of sent packets.

Traffic was generated and received with JPerf software tool installed on each wireless client. JPerf is a free software tool with a graphical interface from which parameters are set to generate a TCP or UDP traffic flow on IPv4 and IPv6 systems. It consists of server component that runs on a wireless client which sends packets, and client component that runs on a wireless client that receives the packets. Simply, by changing the settings on each wireless client traffic can be generated in the opposite direction.

Initially, on both laptops was installed Microsoft Windows 8 Professional 64-bit operating system. On operating system were not installed any additional software, except the JPerf. Wireless devices were initially configured to work without a security protocol (open system) and complete measurements are made. Then, on all wireless network devices was configured WPA2 security protocol and identical performance measurements were performed. After that, on laptops was changed operating system on 64-bit Linux Ubuntu Desktop version 13.04, and identical experimental measurements were repeated for both scenarios.

TP-Link TL-WR941ND wireless access point for wireless channel width value has an option of 20 and 40 MHz. To achieve the maximum throughput of wireless channel, value for channel width is set on 40 MHz. Generally, greater width of wireless channel enables higher transmission speeds.

During the generation of traffic UDP window size was set to 8 KB, and TCP window size was set to the value of 64 KB. These values were chosen in order to ensure optimal data transfer speeds during the experiments.

Given that the entire communication was established wirelessly, distance between wireless access point and wireless clients is fixed at about 5 meters in order to maintain optimum power of wireless signals.

MEASUREMENT PROCEDURES

Transport flows in different experiments were generated using JPerf software package. Following rules were used during data collection:

- To make a wireless network environment stabilized, first two measurements were discarded.
- Each experiment was performed at least five times for the reliability of data.
- Measurements are recorded only when the results from two different attempts were similar at least ninety percent.
- For each experiment the mean value of all readings was calculated by computer.

Performance of wireless networks measured in experiments are throughput (number of bits transmitted per unit time) and jitter (variation in the time between packets arriving at destination) [10]. These characteristics of wireless networks provides a clear insight into their network performance, since they show the rate at which data is transferred from one to another wireless client, as well as the time fluctuations between the received packets.

EXPERIMENTAL RESULTS

When conducting the experiments TCP and UDP packets were generated and sent from one wireless client to another wireless client over wireless access point on IEEE 802.11n wireless network. Packet size was increased gradually in the range from 256 up to 1460 bytes. Values of throughput and jitter were recorded during execution of experiments. Identical experiments were performed for both IPv4 and IPv6 protocols on two operating systems, Windows 8 and Linux Ubuntu. WPA2 security protocol with AES encryption algorithm was analyzed, and identical experiments were carried out for open system when none of the security protocols were used.

Average Value of Throughput for TCP Protocol

Proportionally with increasing the size of packets to be transmitted increases the value of throughput for TCP protocol, but with varying degrees of growth depending on the selected operating system and whether the WPA2 security protocol is used.

For the system without encryption (open system) (Fig. 2) Windows 8 and Linux Ubuntu operating systems show different TCP throughput values for IPv4 and IPv6 protocols, but it is evident that there are similarities in their performance. IPv4 exceeds IPv6 on both operating systems, and values of throughput increases with the size of packets transmitted over the wireless network. The maximum difference between Windows 8 and Linux Ubuntu operating system is observed in the transfer of packets size of 1280 bytes for both IPv4 and IPv6 protocols, where Windows 8 operating system has about 5 Mb/s less throughput value. The best result for IPv4 protocol achieves Linux Ubuntu operating system with maximum throughput of 48.8 Mb/s.

When WPA2 security protocol with AES encryption algorithm is enabled (Fig. 3) both operating systems experienced a decrease in the value of TCP throughput. The decline is noticeable in both IPv4 and IPv6 protocols ranging from 5 to 7 % for most of the TCP packet sizes compared to the open system. On Windows 8 operating system the biggest difference between the open system and scenario where WPA2 security protocol is enabled evident is for TCP packet size of 1460 bytes. On Linux Ubuntu operating system the maximum difference is noticeable for packet size of 256 bytes for both IPv4 and IPv6 protocols. Value of TCP throughput on IPv4 protocol exceeds IPv6 for all packet sizes on both operating systems. The biggest difference between IPv4 and IPv6 protocol is noticeable for packet size of 1024 bytes on Windows 8 operating system and has a value of 1.6 Mb/s.

Obviously, Linux Ubuntu for both IPv4 and IPv6 protocols gives significantly better results than Windows 8 operating system, regardless of whether the wireless network uses WPA2 security protocol.

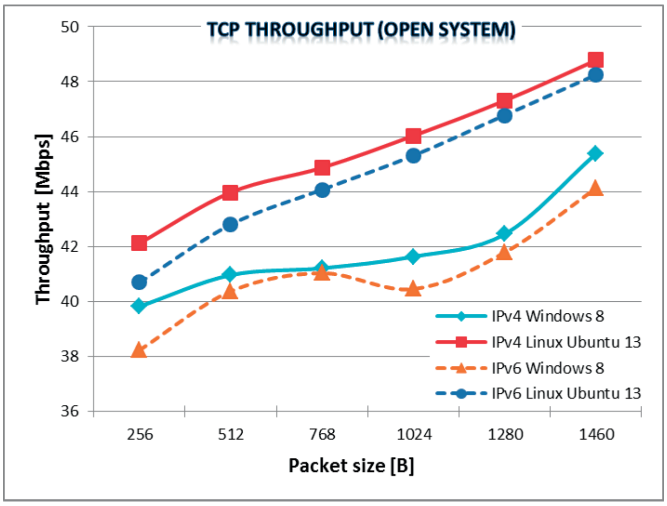

Fig. 2. Average value of TCP throughput of operating systems for open system.

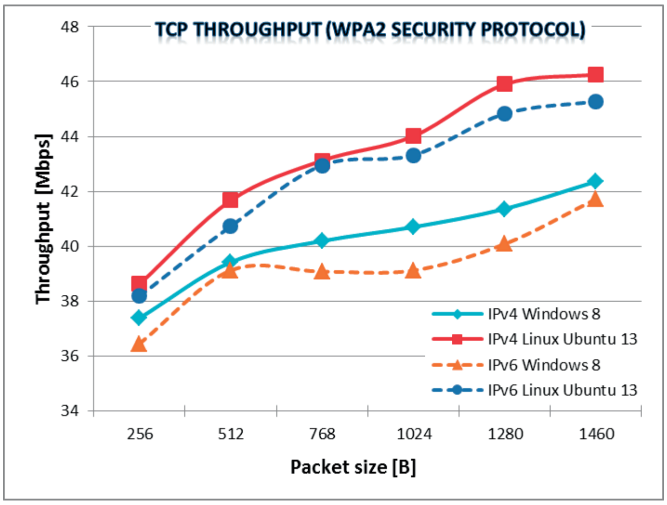

Fig. 3. Average value of TCP throughput of operating systems with WPA2 security protocol enabled.

Average Value of Throughput for UDP Protocol

The value of throughput for UDP traffic reaches 118 Mb/s which is twice the value of TCP traffic. Increasing size of transmitted packets increases throughput for both operating systems.

For open system (Fig. 4) Windows 8 and Linux Ubuntu show different values of UDP throughput for IPv4 and IPv6 protocols. It is evident that IPv4 exceeds IPv6 protocol on both operating systems, and that the size of throughput increases with the size of transmitted packets. The maximum difference between Windows 8 and Linux Ubuntu operating systems is observed in the transfer of packet size of 1280 bytes for IPv4 protocol, where Windows 8 operating system has 6 Mb/s less value of throughput than competitor. For IPv6 the biggest difference is achieved when transferring UDP packet size of 1024 bytes, where Linux Ubuntu has 5.7 Mb/s greater value of throughput.

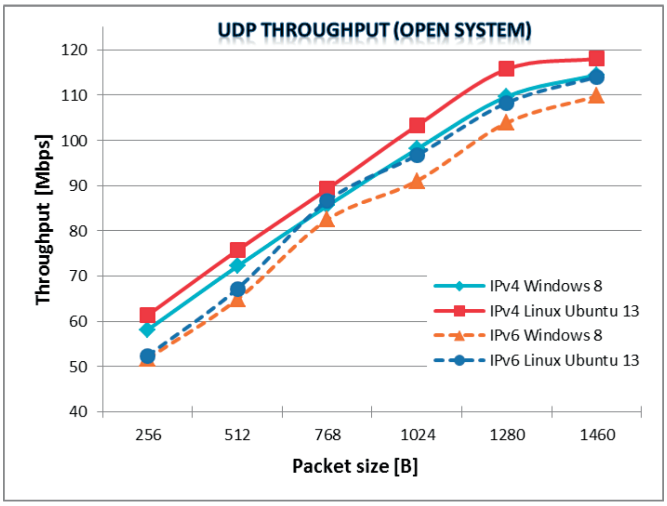

Fig. 4. Average value of UDP throughput of operating systems for open system.

WPA2 security protocol with AES encryption algorithm (Fig. 5) has similar impact on throughput reduction for both operating systems. Due to use of WPA2 security protocol both operating systems achieve up to 22 % lower results compared to the case when not using encryption. The biggest difference between IPv4 and IPv6 protocols is conspicuous for packet size of 1460 bytes on Windows 8 operating system and has a value of 7.8 Mb/s.

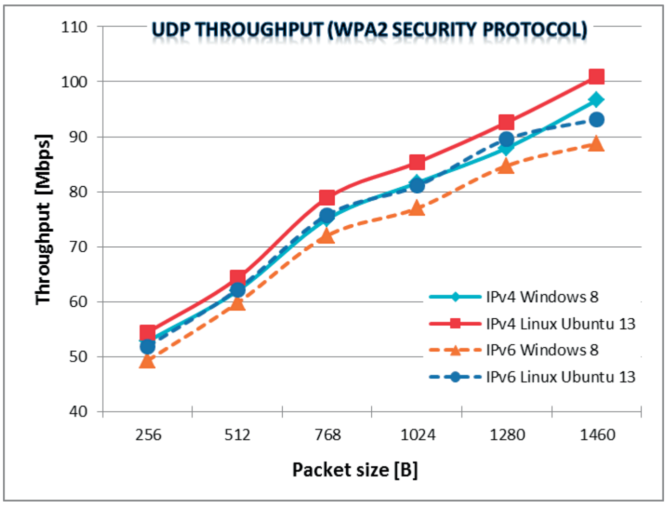

Fig. 5. Average value of UDP throughput of operating systems with WPA2 security protocol enabled.

Similar to the TCP protocol, also for the UDP protocol Linux Ubuntu operating system achieves higher values of throughput compared to the Windows 8 operating system for both IPv4 and IPv6 protocols, regardless of whether the wireless network is using WPA2 security protocol.

Average Value of Jitter for UDP Protocol

When comparing network performance of systems based on IPv4 and IPv6 protocols in addition to the size of throughput it is necessary to consider other metrics. The time it takes that operating system reacts to incoming packets equally affects the overall performance evaluation of a system. Jitter is the variation in packet delay over time. The average value of jitter for UDP packets transmitted in a variety of security scenarios is presented in Fig. 6.

Comparing the results obtained on different operating systems one can see that both operating systems generate relatively low values of jitter for both IPv4 and IPv6 protocols in the case when wireless network does not use encryption (open system). For both operating systems UDP jitter values are less than 3 ms.

On the contrary, in presence of WPA2 security protocol with AES encryption algorithm high values of jitter are achieved on both operating systems. This negative tendency is especially pronounced for IPv6 protocol. The distribution of jitter values for different operating systems reaches extremes for different sizes of transmitted packets. Overall, it was observed that Windows 8 achieves the highest value of jitter for IPv6 protocol. With increasing size of packets values of jitter on Windows 8 operating system significantly increases and reaches maximum of 21.4 ms for IPv6 protocol and size of transmitted packets of 1280 bytes. UDP jitter values for IPv4 protocol are more moderate than on IPv6 protocol, which can be rewritten to the increased size of packet headers in IPv6.

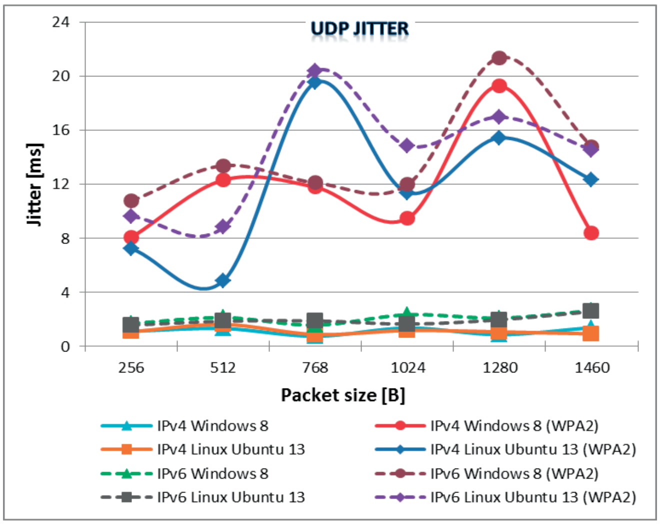

Fig. 6. Average value of UDP jitter of operating systems.

DISCUSSION AND INTERPRETATION OF EXPERIMENTAL RESULTS

The obtained results revealed the following:

- When using WPA2 security protocol headers of encrypted packets increase by 16 bytes, which increases the total size of packets to be transmitted over a wireless network. Increasing the size of packets to be transmitted over a wireless network has a negative effect on the performance of operating systems.
- There is a degradation of the average value of throughput when WPA2 security protocol is used on wireless network. The measurement results unambiguously show that Linux Ubuntu achieves greater throughput than Windows 8 operating system for IPv4 and IPv6 protocols. The maximum difference between Windows 8 and Linux Ubuntu operating systems was notable for TCP and UDP packet size of 1280 bytes for both IPv4 and IPv6 protocols, where Linux Ubuntu achieved 4.5 Mb/s higher throughput value.
- The results show that IEEE 802.11n wireless network enables maximum throughput of 49 Mb/s for TCP protocol, and 118 Mb/s for UDP protocol in the case when both wireless clients were associated to a wireless access point. This is much less than the theoretical maximum value of throughput which for TP-Link TL-WR941ND wireless access point is 300 Mb/s.
- There is a substantial increase in jitter value during transfer of UDP packets through IEEE 802.11n wireless network protected with WPA2 security protocol. Increase in jitter value with increasing packet sizes that are transmitted is the result of the depreciation costs arising from the greater size of the packets, and thus the greater amount of time required for packet transmission.
- Results of experiments show that IPv4 protocol achieves higher value of throughput for TCP and UDP traffic flows than on IPv6 protocol for any packet size on both Windows 8 and Linux Ubuntu operating systems, regardless of whether the wireless network uses WPA2 security protocol.

CONCLUSIONS

In this paper, impact of WPA2 security protocol on network performance of operating systems in modern IEEE 802.11n wireless networks was quantified. The results of performed experiments demonstrate active presence of WPA2 security protocol in IEEE 802.11n wireless networks, and the fact that encryption introduces a performance degradation of wireless networks. Values of throughput and jitter are attenuated relative to the scenario where security protocol is not used (open system). Performance degradation is more pronounced for IPv6 protocol due to the increased size of packet header than on the original IPv4 protocol.

Also, noticeable is the difference in performance between different operating systems. Experimental results showed that the performance of IPv4 and IPv6 protocols depends on the operating system on which they are implemented. Overall, Windows 8 achieved lower network performance than Linux Ubuntu 64-bit operating system.

Certainly, the results obtained in this paper should be taken with a dose of reserve due to the fact that the experiments are limited to the usage of single wireless access point and two wireless network clients. Wireless network infrastructure is created within closed space, so that interference present in atmospheric conditions and disruption that result from radiation from other wireless devices operating in close range of frequencies are not taken into account. For consistency of results obtained in different scenarios, wireless access point and clients are placed at fixed sites, and thereby the effect of mobility is not considered. Experimental wireless network platform used in this study represents an infrastructure wireless local area network, and therefore the results and conclusions may not be valid for ad hoc wireless networks.

Future Work

There are several research directions in this field. Future studies may examine impact of different security protocols and performance metrics on various operating systems. Extensive studies can be done by considering other wireless networks types which are used or will be used in the near future, and assess their performances using various metrics.

Acknowledgment

This work was supported by the Ministry of Education and Science of the Republic of Serbia through the projects TR32054 and ON174008.

REFERENCES

[1] IEEE Std. 802.11n-2009, IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 5: Enhancements for Higher Throughput, IEEE, New York, NY, USA, 2009.

[2] Z. Bojovic, Z. Peric, V. Delic, E. Secerov, M. Secujski, and V. Senk, "Comparative analysis of the performance of different codecs in a live VoIP network using SIP protocol," Electronics and Electrical Engineering Journal, vol. 117, no. 1, pp. 37-42, 2012.

[3] P. Li, S.S. Kolahi, M. Safdari, and M. Argawe, "Effect of WPA2 security on IEEE 802.11n bandwidth and round trip time in peer-peer wireless local area networks," Workshops of International Conference on Advanced Information Networking and Applications, pp. 777-782, 2011.

[4] S.S. Kolahi, Z. Qu, B.K. Soorty, and N. Chand, "The impact of security on the performance of IPv4 and IPv6 using 802.11n wireless LAN," 3rd International Conference on New Technologies, Mobility and Security, pp. 1-4, 2009.

[5] S. Narayan, T. Feng, X. Xu, and S. Ardham, "Impact of wireless IEEE 802.11n encryption methods on network performance of operating systems," 2nd International Conference on Emerging Trends in Engineering and Technology, pp. 1178-1183, 2009.

[6] S.S. Kolahi, P. Li, M. Argawe, and M. Safdari, "WPA2 security-bandwith trade-off in 802.11n peer-peer WLAN for IPv4 and IPv6 using Windows XP and Windows 7 operating systems," IEEE Symposium on Computers and Communications (ISCC), pp.575-579, 2012.

[7] D. Tepsic, and M. Veinovic, "Comparative analysis of UDP throughput on IPv4 and IPv6 operating systems in IEEE 802.11n wireless networks protected with WPA2 security protocol," 20th Telecommunications Forum (TELFOR), pp. 111-114, 2012.

[8] TP-Link, TL-WR941ND Datasheet, [Online]. Available: www.tp-link.com

[9] Toshiba, Toshiba Satellite C655-S5208 Product Specification, [Online]. Available: www.toshiba.com

[10] S. Paulikas, P. Sargautis, and V. Banevicius, "Impact of wireless channel parameters on quality of video streaming," Electronics and Electrical Engineering Journal, vol. 108, no. 2, pp. 27-30, 2011.