A research on the impact of encryption algorithms on the quality of VPN tunnels' transmission

Dariusz Strzęciwilk[1,*], *Krzysztof* Ptaszek[2], *Paweł* Hoser[1] and *Izabella* Antoniku[1]

[1]Department of Applied Informatics, University of Life Sciences, Nowoursynowska Street 159, 02-787 Warsaw, Poland
[2]Central Anti-Corruption Bureau, al. Ujazdowskie 9, 00-583 Warsaw, Poland

Abstract. The following article presents the results on the impact of encryption algorithms and the cryptographic hash function on the QoS (*Quality of Service*) transmission in a computer network. A network model supporting data encryption using the AES algorithm and the MD5 and SHA hash functions used in VPN tunnels was designed and tested. The influence of different data length on the quality of transmission in a secured network was studied. The measurements and tests of networks were performed according to two methodologies ITU-T Y.1564 and RFC 2544. The impact of the data encryption mechanism on bandwidth, data loss and maximum delays was examined. The secured network tests were performed with different combinations of encryption algorithms and hash functions of the VPN tunnel in the ESP (*Encapsulating Security Payload*) transport mode.

1 Introduction

The Quality of Service as well as network security and information transfer are among the most important challenges emerging during the design and maintenance of modern computer networks and the next-genaration networks [1, 2]. Guaranteeing adequate quality of service is of particular importance in case of real-time applications such as Voice over IP [3] and video - IPTV [4]. The quality of services can be understood as the network's capability of providing a particular service in a better or special way for a group of users or applications, at the expense of other users and applications. Guaranteeing proper quality of service is of big importance in case of real-time applications [5]. These services are particularly sensitive

* Corresponding author: dariusz_strzeciwilk@sggw.pl

to delay and require perfect bandwidth [6]. For this reason, they must have a higher priority and require special management in the network, in comparison with other services and applications, such as e-mail or HTTP traffic. The aim is to provide the desired QoS packages for the entire route from the sender to the recipient, which has been the subject of research for many years [7-9]. The second, but also important, is the issue regarding security of modern computer networks. One of the commonly used methods of increasing network and transmission security is the use of VPN (*Virtual Private Networks*), which is an alternative solution to traditional WAN (*Wide Area Network*) of service providers. VPNs allow you to create private, virtual network connections, so-called tunnels through an unsecured external network - such as public Internet network. However, due to the fact that communication takes place through an unsecured network, there are two problems: no guarantee that the information sent is secured or whether the network is exposed to external attacks. For this reason, adequate protection of the communication channel and access to the internal network should be of great concern, which is why various solutions are sought, such as secured IPSec (*Internet Protocol Security*) tunnels, the use of hardware or software firewalls and systems for detecting and preventing intrusions and attacks on the network. Due to the variety and level of network security advancement as well as data transfer methods, there is a question of how the network security can affect the quality of services available. Thus, the aim of the following research is to examine the impact of network security on the quality of service, using one of the leading Cisco Systems network equipment. A network has been designed and tested that can serve as backbone of a corporate network. The network built is based on Cisco routers and ASA 5510 (*Adaptive Security Appliance*) firewalls, using QoS technology and OSPF (*Open Shortest Path Protocol*). The designed and configured network underwent transmission quality tests using the EXFO FTB-860 measuring platform, which supports the RFC 2544 [10] and ITU-T Y.1564 measurement methodology [11]. Although security is the main priority, the performance of VPN must also be considered. This paper presented how performance of VPN affected by choosing different encryption algorithms used by VPN devices.

2 QoS Model

Along with applications requiring different levels of service quality, various QoS models are available, i.e. ways or strategies according to which the QoS mechanisms designed and implemented within the network. At the current stage of research done by IETF concerning QoS, two architectures have been defined in IP networks, which enable the division of traffic into classes with differentiated quality of services. The first class is Integrated Services (*IntServ*) as described in RFC 1633 [12], and the second class is the Differentated Services (*DiffServ*) described in RFC 2475 [13]. These structures allow for extension of the default Best Effort (BE) model [14] currently applied via the Internet. BE is the default model used in computer networks, which neither does it require package delivery nor configuration. It does not use any QoS mechanisms, but all traffic in the network is treated identically - on the principle of FIFO (*First In, First Out*). This means that packets are sent by a given network device in the order they arrive, regardless of traffic type or priority. In this model, packages are delivered to the destination without guaranteed bandwidth, packets transfer latency, jitter and packet loss at a given level. For this reason, it can only be used by applications not susceptible to latency and not requiring guaranteed bandwidth. The service classes of the IntServ model support all types of applications for which the Guaranteed Service is intended, but they relate to the reservation of resources and scalability problems in backbone networks. For this purpose, the RSVP (*Resource Reservation Protocol*) protocol [15] is used, which deals with a large signaling overhead required for information transfer on reservation

parameters and dedicated processor resources for handling packets from a given reservation stream. The Int-Serv model provides a guaranteed bandwidth, however it has low scalability, resulting from a large number of reservations, which is caused by a lack of free bandwidth of network. The scalability problem found in the IntServ model has been eliminated in the DiffServ architecture, which provides the most extensive and appealing solution for QoS support in current IP networks. An important advantage of this model is also the fact that it does not require any signaling protocol. The 8-bit ToS (*Type of Service*) field in the IP packet header (Fig. 1) is used to label the packets, which depending on the value assigns the packet to a specific traffic class - the service type. The DS field value associated with DSCP (DS codepoint) is the label used to classify packages in the DiffServ architecture.

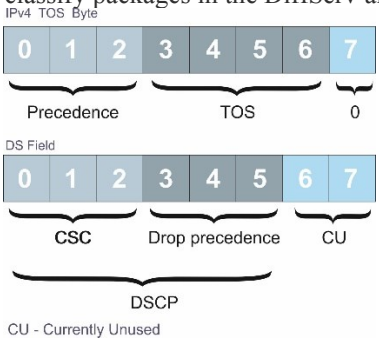

Fig. 1. ToS and DSCP fields

3 IPSec policy components

IPSec is a standard developed by the IETF (*Internet Engineering Task Force*) as a set of protocols and methods that defines configuration of a VPN using the IP protocol. It has been described in RFC documents - among others 2402, 2406, 4301 [16, 17]. The overall IPSec implementation is guided by "*Security Architecture for the Internet Protocol*" RFC 2401[18]. It is not limited to specific security algorithms, encryption, authentication or key exchange, but it is an open standard based on existing algorithms and protocols, in order to implement encryption, authentication and key exchange. The protection offered by IPSec to certain traffic is based on requirements defined by security policy rules defined and maintained by the system administrator [19]. IPSec is a collection of protocols and algorithms used to protect IP packets at layer 3. IPSec consists of five blocks:

- first block - represents the IPSec protocol. You can choose between ESP (*Encapsulating Security Payload*) or AH (*Authentication Header*),
- the second represents encryption algorithms to ensure confidentiality of transmitted data. This can be, for example, DES (*Data Encryption Standard*), 3DES (*Triple DES*), AES (*Advanced Encryption Standard*) or SEAL (*Software-Optimized Encryption Algorithm*),
- the third block represents the algorithms used for ensuring data integrity - the choice is MD5 (*Message Digest 5*) or SHA (*Secure Hash Algorithm*),
- the fourth represents the methods for selecting a shared key used for authentication. It can be PSK (*Pre-shared Keys*) or using a digital signature using the RSA algorithm (from the names of the creators - *Ron Rivest, Adi Shamir, Leonard Adleman*),
- the last block represents DH (*Diffie-Hellman*) key exchange algorithms. There are so-called DH1, DH2, DH5 and DH7.

IPSec defines two modes. It's worth to remember that the IPSec header follows the IP header because it is reference by an IP Protocol number. When IPSec headers are just interested into

an IP Packet after the IP header (transport mode). In this mode, the original header is exposed and unprotected. The second mode is known as tunnel mode. In this mode an external IP header is created and the IP addresses are replaced with the tunnel endpoints (Fig. 2).

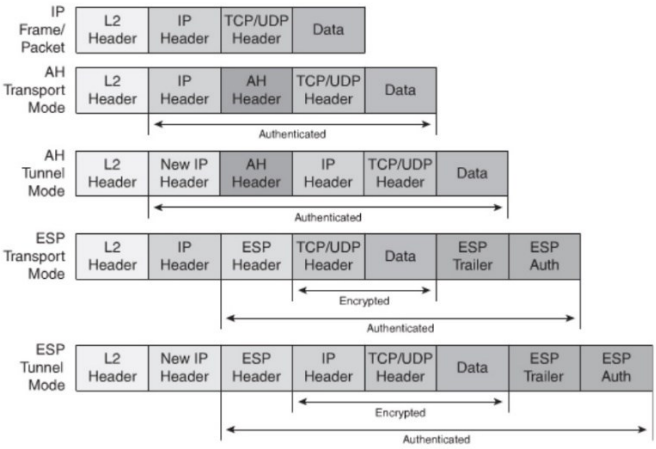

Fig. 2. IPSec header

Confidentiality of data sent in the VPN is ensured by encryption. The level of security depends on the key length of the encryption algorithm. The most commonly used algorithms are:

- DES - fast, symmetrical algorithm using a 56-bit key,
- 3DES - a higher cryptographically DES variant, it uses 3 independent 56-bit keys for each subsequent 64-bit data block, thus providing a much higher level of security,
- AES - symmetric algorithm, safer and more efficient than 3DES. It offers 3 key lengths: 128, 192 and 256 bits,
- SEAL - a symmetric stream algorithm using a 160-bit key.

DES currently does not provide high level of security required in some applications, however, you can artificially increase the length of the key by encrypting the data with the DES (3DES) algorithm. AES was created as a successor of DES at the request of NIST (*National Institute of Standards and Technology*). The AES cipher can operate on a variable length block using variable length keys. The specification allows the use of 128, 192 or 256-bit blocks, encrypted with 128, 192 or 256-bit keys, where all 9 combinations are allowed. The encryption process takes place in N rounds, where N depends on the key length, for a 16-byte key it is 10 rounds, for 24-bytes it is 12 rounds, and for 32-bytes it is 14 rounds. In each round (except for the last one) four transformations are performed successively, with three substitutions and one permutation among them:

- Subbytes - byte substitution using the S-box,
- ShiftRows - simple permutation,
- MixColumns - substitution using arithmetic over $GF(2^8)$,
- AddRoundKey - adding a symmetric (XOR) part of the key to the block.

The encryption and decryption process starts with the AddRoundKey operation, followed by nine four-stage rounds and the tenth three-stage round. The structure of the four-stage round is shown in Fig. 3.

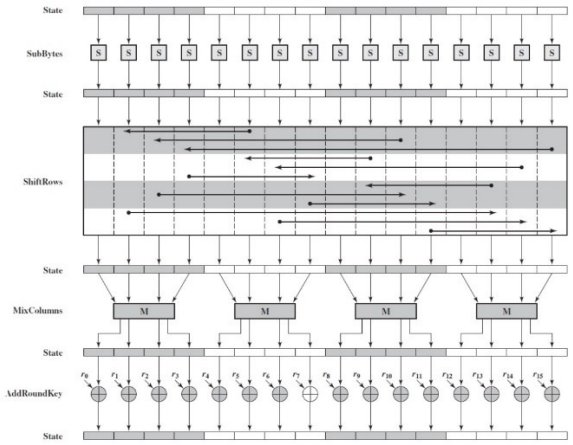

Fig. 3. The course of a single round encryption in the AES algorithm [22].

Another important function of IPSec is data integrity. To ensure the integrity of data during transmission, the HMAC (*Hashed Message Authentication Code*) algorithm is used. Its job is to perform calculations by the device responsible for sending hash values based on the message and the secret key by attaching it to the sent message. Then the receiving device calculates the hash of the received message and compares it with the received one. If the values are equal, then the integrity of the data is preserved. Otherwise, the content of the message changes during transmission and is rejected. Currently, two HMAC algorithms are used:

- messages of any length using 128-bit shared secret key and results in 128-bit hash messages,
- HMAC-SHA-1 - calculates the hash of messages of any length using a 160-bit shared secret key, the calculated hash has 160 bits,
- HMAC-SHA-1 is stronger in cryptographic terms and it is recommended for networks that require a higher level of security.

4 The results of research and discussion

In order to perform tests, two networks were designed - unsecured (as a reference level) and secured one (with different parameters of VPN tunnel). The physical topologies of the networks used are shown in Fig. 4.

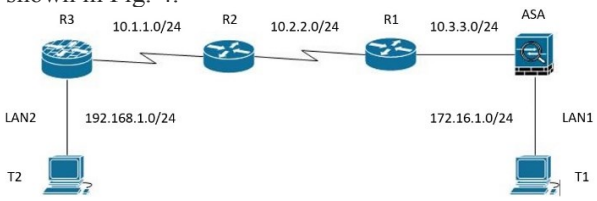

Fig. 4. Topology of the research network

Both networks were implemented using Cisco technology. Cisco 2801 routers with operating system versions IOS 12.4 (13r) T and Cisco 2811 with IOS 12.4 (13r) T (R3). In addition, the Cisco ASA 5510 firewall with operating system 9.1 (2) (ASA), network research and tests were carried out using EXFO FTB-860 *NetBlazer* testers.In the unsecured network, only

the basic configuration of all devices was carried out as well as the OSPF routing protocol and NAT address translation on R1 and R3 routers were configured. In the secured network, in addition to the configuration mentioned earlier, the IOS firewall was implemented to R3 router and Intrusion Prevention System (IPS) to guard the network. In addition, in the LAN1 network, a software ASA firewall was used. A site-to-site tunnel IPsec VPN was configured between LAN1 and LAN2 (with different combinations of encryption algorithms and hash functions), while the function of VPN gateways is performed by ASA firewall and R3 router. Traffic in both networks was generated by network testers. These generators were also used to measure QoS parameters in networks. Network tests were carried out according to the RFC 2544 [20] methodology and ITU-T Y.1564 [11], also known as EtherSam. Tests according to RFC 2544 were carried out for frames with 7 sizes defined in the standard - 64, 128, 256, 512, 1024, 1280 and 1518 bytes, while the measured QoS parameters were the following:

- bandwidth,
- frame loss,
- maximum latency (from the moment of sending from the source, until the receiving device collects the frame).

According to the EtherSam methodology tests were performed simultaneously for 3 different services, i.e. types of network traffic, generated at speeds of 3 Mb/s (service-1), 5 Mb/s (service-2) and 2 Mb/s (service-3) and frames about randomly generated size. The secured network tests were performed with the following combinations of encryption algorithms and hash functions used in the IPSec. VPN tunnel in the ESP transport mode. In both test methodologies, network traffic with a total speed of 10 Mb/s was generated from the testers - at the entrance. As a result of the conducted tests, it was found that network bandwidth for frame 64 - 512 bytes increases with the size of the frame, and after reaching the value of 512 bytes remains at a similar level. The exception is a 1518-byte frame in a secured network, where one can observe a significant increase in bandwidth. The measured bandwidth values of frames of different sizes and different encryption algorithms and hash functions are shown in Fig. 5.

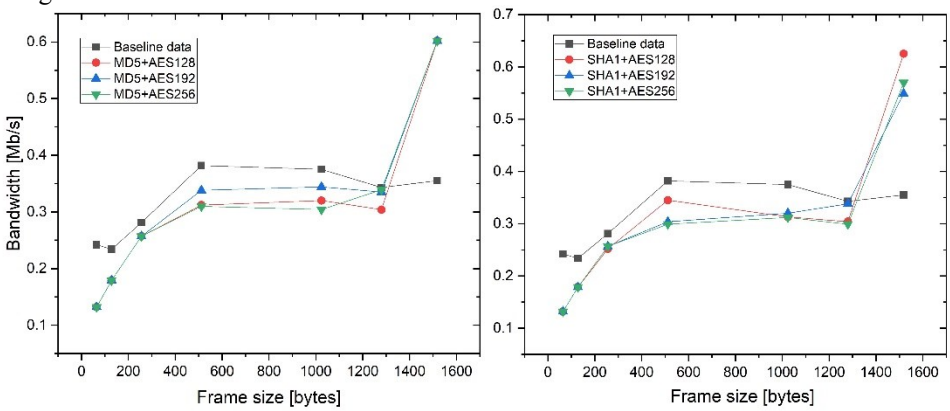

Fig. 5. Network bandwidth values for different frame sizes and AES algorithms as well as MD5 and SHA hash functions

The resulting latency values for frames in the range of 64 to 512 bytes increase with the increase of the frame size, and after reaching the value of 512 they remain at a similar level, except for a 1518 byte frame in a secure network for which the latency value is more than doubled (Fig. 6). In addition, the test showed that the values of network capacity measured for individual services are the highest for unsecured networks, however the secured network remains at a similar level regardless of the security method. The obtained jitter values for

different services are the smallest in case of unsecured network, while for the secured network there are slight fluctuations of values (Fig. 7).

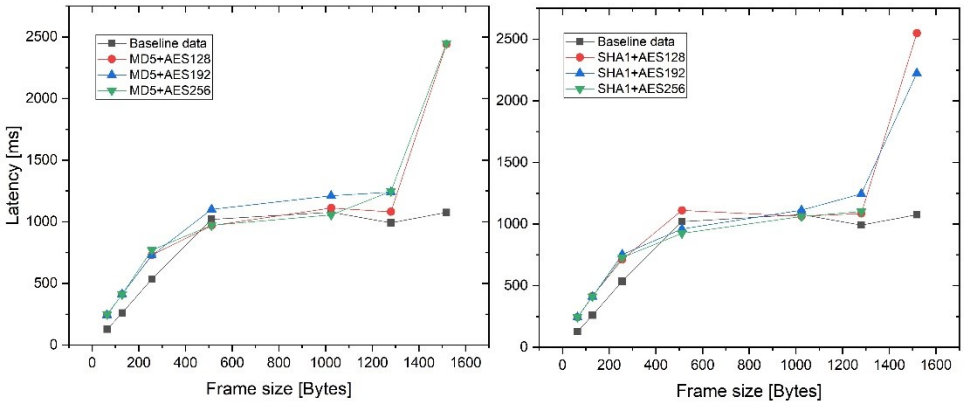

Fig. 6. Latency values [ms] obtained for various network and service protections

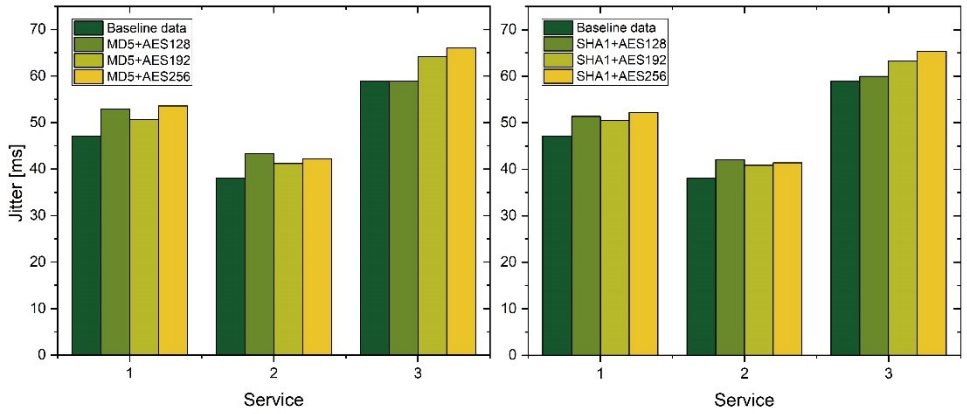

Fig. 7. Jitter values [ms] obtained for various network and service protections

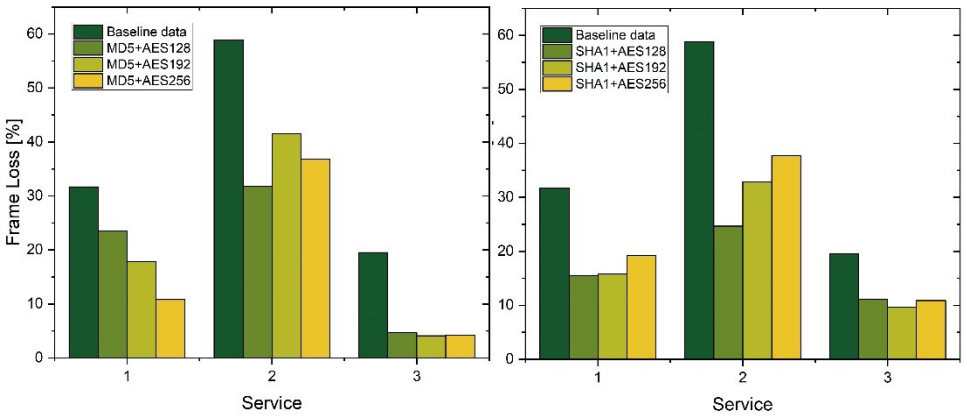

Fig. 8. Percentage of frame loss for various network and service security

The measured frame loss for individual services are the highest for unsecured networks, while for the secured network a clear measured parameter dispersion is noticed (Fig. 8). The analysis of test results according to the RFC 2544 methodology showed that the rise in frame size increases throughput and latency, while the number of frame loss decreases. In case of bandwidth, this is due to the fact that additional bytes are added to each transmitted Ethernet frame - a preamble and a frame interval. The mentioned information overhead causes that the actual network bandwidth decreases, which is much more visible for frames with a smaller payload, because a large part of the transmitted bytes are additional bytes not belonging to stored area. For large frames, additional bytes absorb less bandwidth, as the frame payload is larger. Comparing the obtained bandwidth values of unsecured networks with a secured network, one can observe that the bandwidth of the secured network is smaller. This is due to the encapsulation of IP packets transmitted in the IPSec VPN tunnel. As a result of ESP encapsulation, additional bytes are added to the original packet - ESP header, training sequence, authentication bytes and a new IP address. This is typical for smaller frames. In case of larger frames, the difference between the unsecured and secured network bandwidth is almost unnoticeable due to the large frame payload. It can be concluded that the effect of choosing the AES key length and the hash function is not perceived. Analyzing the results on the key length dependency for the AES algorithm, it can be stated that key length does not have a significant impact on the measured parameters. In AES, depending on the key length used - 128, 192 or 256 bits, the numbers of cipher rounds in the algorithm change, with the value of 10, 12 and 14 respectively, making a small difference in AES speed for various keys. Analyzing the impact of the hash function used, it can also be said that its choice has an nonmeasurable effect on the obtained values of QoS parameters. In addition, the small differences in measured parameters for different algorithms and key lengths used in the tunnel are certainly influenced by hardware support for algorithms implemented in Cisco devices. Tests made in accordance with ITU-T Y.1564, confirm the results obtained for RFC 2544. For all measured parameters common to both methodologies, analogous relations are seen. For all services, the bandwidth values are lower in respect to the secured network, similar with latency - it is greater for secured network. It can be noticed, however, that latencies measured according to ITU-T Y.1564 are much higher, which is due to the fact that they were measured from the moment the frame was sent until the return frame was received by the tester and not one-way like in case RFC 2544. The only parameter, not measured according to RFC 2544 - average jitter, is also lower for all services of unsecured networks. The reason for this is the introduction of additional jitter by means of firewalls and IPS implemented in the secured network. When analyzing the results of the EtherSam tests it is difficult to notice, similarly to the RFC 2544 tests, the dependency of the measured parameter values on the level of security, thus the encryption algorithm, key length or cryptographic hash function used.

5 The results of research and discussion

Information security is a trade-off between ease of use and convenience and restriction for protection from misuse. The conducted research and tests have shown that the use of network security methods offered by Cisco such as IPSec VPN, firewall or IPS causes slight deterioration of service parameter quality. For IPSec VPN, the deterioration of QoS parameters results from an additional information overhead - encapsulation of IP packets and the time needed for encryption, decryption and calculation of the hash function. However, as the results show, the differences in the obtained values for various combinations of VPN

tunnel algorithms are insignificant, which proves the high efficiency of Cisco technology. The quality parameters in the network are also influenced by the use of security systems that analyze packets continuously, i.e. firewalls and IPS systems, because the operation of these systems introduces additional latency and jitter to transmitted packets.

References

1. H. Tarasiuk, et al., The IPv6 QoS system implementation in virtual infrastructure, *Telecommunication Systems* **61.2**, 221-233, (2016)
2. G. Schollmeier, Ch. Winkler, Providing sustainable QoS in next-generation networks, *IEEE Communications Magazine* **42.6,** 102-107, (2004)
3. D. Strzęciwilk, Examination of Transmission Quality in the IP Multi-Protocol Label Switching Corporate Networks, International Journal of Electronics and Telecommunications. **58**(3), 267-272 (2012)
4. H. J. Kim, S. G. Choi, A study on a QoS/QoE correlation model for QoE evaluation on IPTV service, Advanced Communication Technology (ICACT), 2010 The 12th International Conference on. **vol. 2**. IEEE (2010)
5. D. Kyriazis, et al., A real-time service oriented infrastructure, *GSTF Journal on Computing (JoC)* **1.2** (2018)
6. W. Zuberek, D. Strzęciwilk, Modeling Quality of Service Techniques for Packet–Switched Networks**,** Dependability Engineering, ISBN 978-953-51-5592-8 (2018)
7. D. Strzęciwilk, W. M. Zuberek, Modeling and Performance Analysis of Priority Queuing Systems, *Computer Science On-line Conference*. Springer, Cham, pp 302-310 (2018)
8. J. Carmona-Murillo, et al., QoS in Next generation mobile networks: an analytical study, Resource management in mobile computing environments, Springer Int. Publishing. 25-41 (2014)
9. D. Strzęciwilk, W. M. Zuberek, Modeling and performance analysis of QoS data, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2016. International Society for Optics and Photonics (2016)
10. R. Bolla, R. Bruschi, RFC 2544 performance evaluation and internal measurements for a Linux based open router, *High Performance Switching and Routing, 2006 Workshop on*. IEEE (2006)
11. T. Diallo, M. Dorais, EtherSAM: The new standard in Ethernet service testing, *EXFO Applicartion Notes*, 4-6 (2001)
12. R. Braden, D. Clark, S. Shenker, *Integrated services in the internet architecture: an overview,* No. RFC 1633 (1994)
13. D. Grossman, New terminology and clarifications for diffserv, No. RFC 3260 (2002)
14. P. Gevros, et al., Congestion control mechanisms and the best effort service model, *IEEE network* **15.3**, 16-26 (2001)
15. L. Zhang, et al., Resource reservation protocol (RSVP)--Version 1 functional specification, *Resource* (1997)
16. S. Kent, R. Atkinson, RFC 2402, *IP Authentication Header* (1998)
17. S. Kent, K. Seo, *Security architecture for the internet protocol,* No. RFC 4301 (2005)
18. S. Kent, R. Atkinson, RFC 2401, Security architecture for the Internet Protocol, November (1998)
19. N. Doraswamy, D. Harkins, *IPSec: the new security standard for the Internet, intranets, and virtual private networks,* Prentice Hall Professional (2003)
20. S. Bradner, J. McQuaid, *Benchmarking methodology for network interconnect devices,* No. RFC 2544 (1999)
21. W. Stallings, *Cryptography and network security: principles and practice,* Pearson Education India (2003)