International Journal of Engineering Innovation & Research
Volume 5, Issue 1, ISSN: 2277 – 5668

Ensuring Secure Info-Communication Networks Based on the Special Filtering Mode

Sherzod Rajaboevich Gulomov
sherzod.gulomov@rambler.ru
Gulnora Sabirovna Rakhmanova
g.rahmonova.tuit@mail.ru
Bobur Elmurodovich Boymurodov
boburboymurodov@gmail.com

***Abstract* – In this article was developed a method for calculating the invariant characteristics of traffics for a special filtering mode with two physical interfaces and parametric conditions of implement the special filtering mode through virtual connections. Offered a model of a virtual TCP connection to the physical network, allowing ensure *H* (exponent Hurst) to input and output Firewall and performing the estimate of the accuracy of a special filtering for defining the intensity of the packet and performance of Firewall, analyzed conditions of implementation of the Firewalls in special filtering mode and also considered using Firewall to implement special filtering mode on the basis session controls and mirroring traffic.**

***Keywords* – Special filtering mode, Exponent Hurst, Queuing system, Mirroring traffic.**

I. Introduction

Nowadays computers, networks, the Internet has become an integral part of our daily life. Our fast-growing, rich world of technology with each passing day becomes more and more dependent on computer technology and networking. However, this relationship did not emerge suddenly. Every year the financing of computer technologies increased significantly and it is not surprising that these technologies have penetrated almost all spheres of human activity. At the dawn of the development of computer technology, most people could not imagine how widely these technologies will be used in the near future. That is probably why many people do not dare to give a lot of time and effort to develop what, in the end, could prove to be an ordinary fun. Compared to the requirements of the modern labor market the number of people working at the time in the field of computer technology, was negligible. People who work in this close community were familiar and trusted each other. In addition, it allowed only a select community who are trustworthy. Thus, that time security problem in the field of computer technology practically absent.

II. The Way of Calculation of the Invariant Characteristics for a Special Filtering Mode

Under implementing packet traffic filtering factor limiting the performance of the Firewall is system performance packet processing operating according to the filter rules. To evaluate the performance of the network is commonly used parameter bits/s. When processed by the Firewall packet traffic this option is not applicable. For example, a network device that handles 2000 byte packets at a speed of 100 Mbit/s can be handled packet size of 50 bytes at a speed of 10 Mbit/s. If the first case handle having approximately 8000 packets, in the second case, the traffic is around 32,000 packets per second that is four times larger [1]. Therefore the description of the intensity of the input and output flow necessary use the integral characteristic performance Firewall, which measured in number of packets per unit time calculated for fixed-size packets.

III. Settings Firewalls to Implement Special Filtering Mode

Setting the Firewall in a special filtering mode can be represented as a buffer (see Fig.1). In Fig.1 the following notation: M – the checksum intensity of the processing of all TCP connections (packet/s), $\rho = \lambda / M$ – utilization, q – buffer size (number of packets), C – number of TCP connections, the time existence of which allows us to estimate parameters H, H_{in} and H_{out} – the exponent Hurst at the input and output Firewall for allowed TCP connections, λ_i – intensity of input flow for the i – th allowed TCP connections, q_i – buffer size allocated for the i – th TCP connection and m_i – intensity of the i – th TCP connection.

IV. Parametric Conditions Special Filtering Mode

Under considering data communication in the transport layer of model OSI, the interaction between the source and the receiver data realizes via virtual connection [2]. Although the physical network through which the interaction may consist of a plurality of intermediate nodes: routers, switches, et al. equipment, also and Firewall and have a certain value of the Hurst exponent H (see Fig.2). From the experimental data it is known that the value for global network the value H aggregate flow is in the range $0.6 \div 0.8$.

If setting Firewall filtering rules allow packets from the source to the receiver, then this virtual connection will be characterized by some exponent Hurst H.

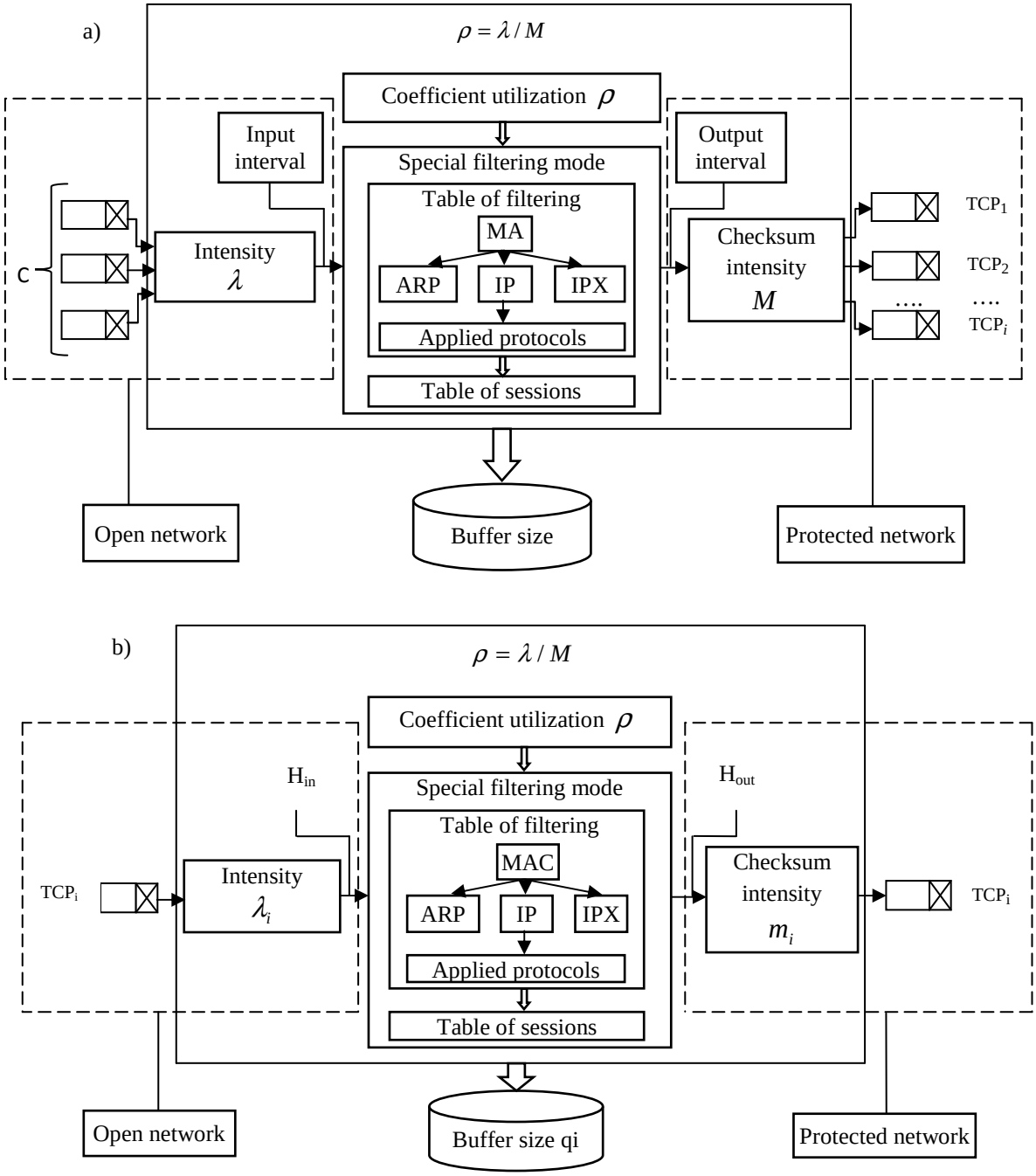

Fig.1. Architecture Firewall with two physical interfaces: a - general flow, b - a single TCP

Special filtering mode will provide consistent H in input and output Firewall for this model of virtual connection.

V. Procedures and Conditions for Implementation of a Special Filtering Mode

Under processing the input fractal process network device by coefficient utilization p and use the Hurst exponent H there is a level buffer size q which [3]does not happen to be dropping packets and the exponent Hurst H on the input and output Firewall remains unchanged. In queuing system, taking into account the fractal properties of network processes, there are increased demands to the buffer, therefore to calculate its size using the ratio, obtained with the diffusion approximation of the input stream applications. This relationship is as follows:

$$q = \frac{p^{1/2(1-H)}}{(1-p)^{H/(1-H)}}, \quad (1)$$

where q – buffer size, p – utilization, H – exponent Hurst.

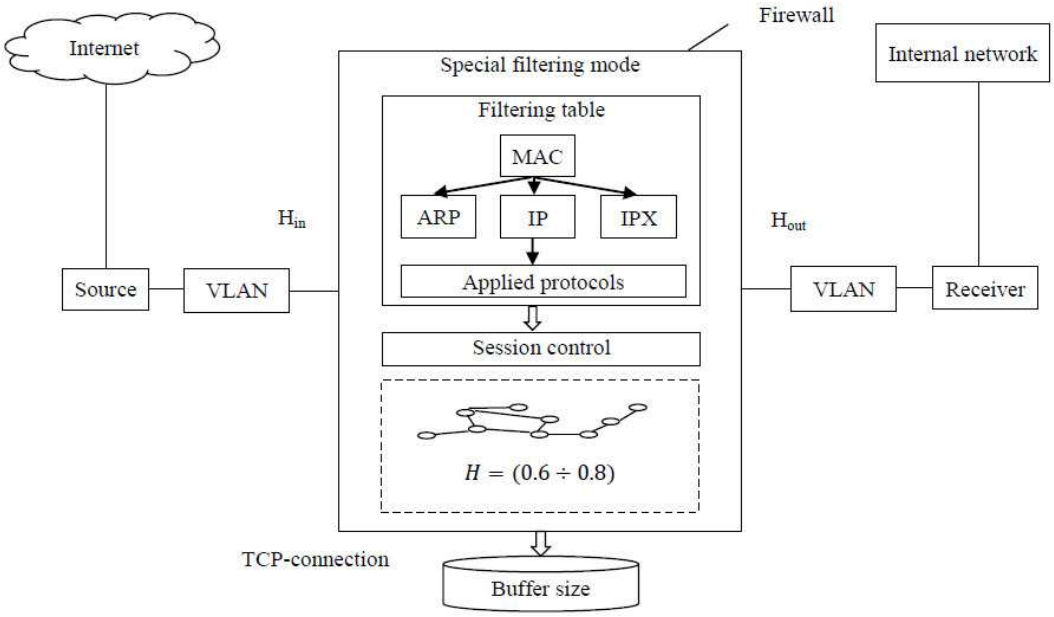

Fig.2. Displaying model of virtual connection to a physical network connection

Given that traffic handled by the Firewall, is a set of packets from a variety of transport connection, the above method of calculating the buffer size offers to apply for individual transport connections, allowed to pass through the Firewall.

When H is large (based on research findings H is in the range 0.6-0.8) increase in the coefficient p requires a much larger capacity buffer (see Fig.3and Table 1).

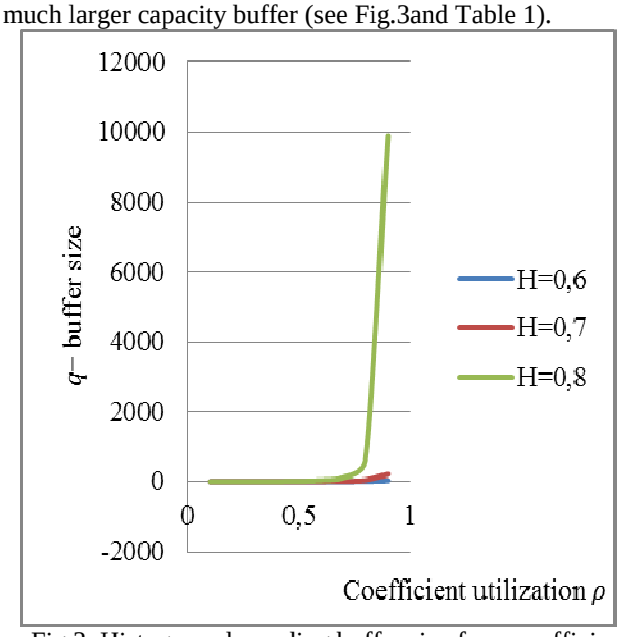

Fig.3. Histogram depending buffer size from coefficient utilization

Table 1. Depending buffer size from coefficient utilization

Coefficient utilization p	Exponent Hurstunder $H = 0,6$	Exponent Hurstunder $H = 0,7$	Exponent Hurstunder $H = 0,8$
0,1	0,738986	0,905248	1,210682
0,2	1,01291	1,322141	2,078467
0,3	1,342076	1,918696	3,692495
0,4	1,791369	2,87049	7,040459
0,5	2,462289	4,542018	14,92853
0,6	3,568948	7,856867	37,1172
0,7	5,666798	15,73313	119,131
0,8	10,69235	41,34219	611,208
0,9	30,96338992	212,0653481	9895,192582

VI. Estimation of Accuracy for Performing the Special Filtering Mode

For the permissible values of the parameters Firewall m_i and q_i need from the expression (1) to obtain depending exponent Hurst H for different values λ_i – intensity, q_i – buffer sizes and m_i – performance (see Fig.4). Figure 4 on the following notation: λ_i – load intensity of i – th TCP connection in relation to the capacity of the physical channel, m_i – processing performance of i – th TCP connection in Firewall, q_i – buffer size in packets allocated to the i – th connection. By plotting the exponent Hurst H at different λ_i, q_i and m_i defined ranges of values of m and q for i – th allowed TCP connections. In particular, for the case of network interfaces Firewall 100 Mbit/s, the special filtering mode will be provided

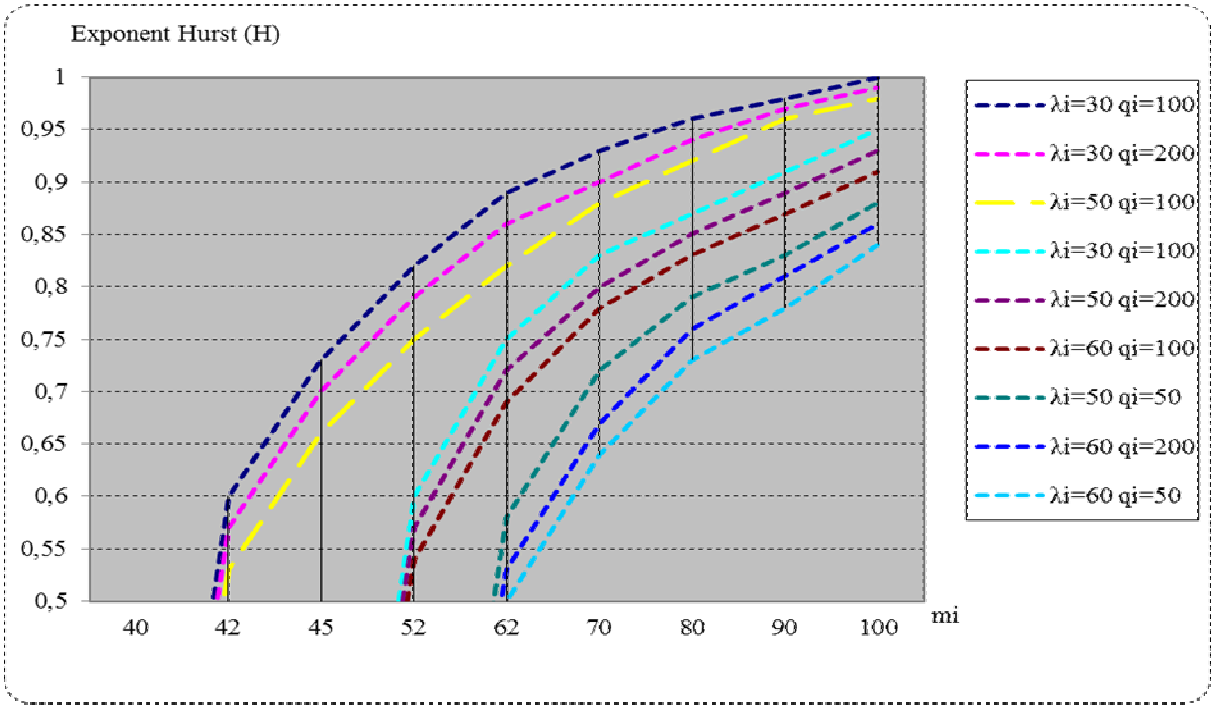

Fig.4. The dependence *H* from parameters settings of the Firewall

Figure 5 is presented selection of parameters Firewall with considering the proposed model.
Firewall: $H_{in} = H_{out}$ under q = 50 – 200 packets and m = 14000 – 16000 packets/s

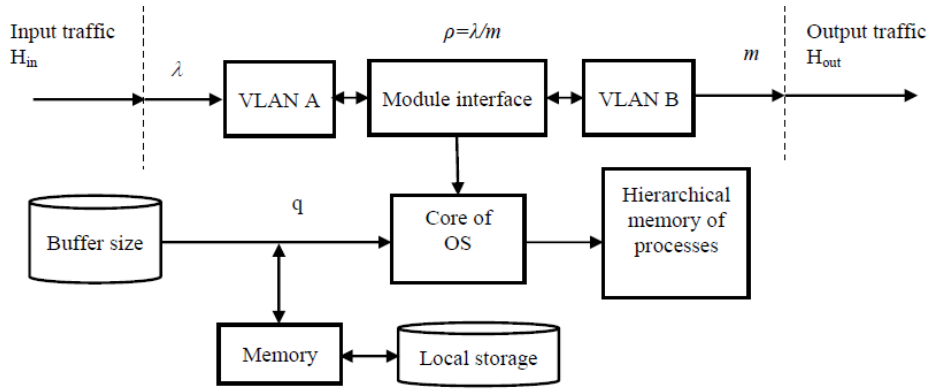

Fig.5. Firewall with proposed model

VII. Conditions Implementation the Special Filtering Mode

The packets are transmitted to the network card and stored in the buffer. When the buffer is filled, the card generates an interrupt and the network card driver copies the data from the buffer card (mbufs) in core memory.

Once a packet is transmitted to the mbuf, the execution of all further operations carried out with the packets does not depend on its size, as analyzed only its title. If packet missed necessary, then packet will be sent the network traffic, which will extract it from the mbuf and pass the line. Most of these operations have a relatively high cost per one packet, but a very low cost on the basis of packet size.

Therefore, the processing of a large packet is only slightly more expensive than processing a small packet.

Some limitations imposed by hardware tools. For example, machine grade x86-64 not treated with more than 15000 interrupts per second, regardless of the processor speed, which is caused by the limitations architecture[4]. Some network adapter generates one interrupt for each packet. Consequently, the unit will drop packets when their amount exceeds about 15000 packets per second.

Other maps, for example, more expensive gigabit have large internal buffer, which allows them to connect multiple packets in a single interrupt. Therefore, the

selection of hardware tools may impose some limitations on performance.

In the Ethernet environment, the maximum transmission block size that can be transmitted or received adapter is 1538 bytes, which comprises:

- start of frame 8 bytes;
- Ethernet header 14 bytes;
- data up to 1500 bytes;
- checksum 4 bytes;
- packet interval 12 bytes.

The controller is able to send and receive Ethernet frames:

- for 1 Gbit/s - every 12.3 microseconds or about 81.000 frames per second (1.000.000.000 / 1538/8 ~ 81000);
- for 100 Mbit/s - every 123 microseconds or about 8100 frames per second (100.000.000 / 1538/8 ~ 8100).

During normal operation not all network packets have a full size, because their actual number may be much greater importance. Packet processing for such speed requires considerable efficiency, therefore from performance the physical layer performance depends not only the speed of the transmission network, but also the state of the whole system [5].

The work of the network interface can be divided into two stages-this transmit/receive packets and place them in the buffers.

Both of these processes are interrelated - before the packet is sent to the network, first it is placed in the buffer of the network card, in the case receive of packet from the network, contrariwise. Traffic allocates buffers in physical memory, where the network card stores newly packets.

To determine the size of the allocated memory is used, as a rule, two parameters - the number of buffers (one buffer - one packet), which are defined in the configuration of the network card, and the maximum transmission segment (Maximum Transfer Unit MTU).

The last parameter is used driver to determine, the amount of memory which necessary pick out under one buffer. If the MTU is not used, it may happen that the allocated buffer is less than that received packet, or is greater than the allocated memory [6-7].

For example, some network adapters for MTU 1500 allocate 2048 bytes. It is getting, if set the number of buffers in 5000 for incoming packets, the driver will allocate about 10 MB of memory.

VIII. Using Firewall to Implement Special Filtering Mode

To filter traffic of operation Firewall in special filtering mode uses session controls and mirroring traffic. Under traffic filtering Firewall treats each packet independently of the data link, network and transport layers. When managing the sessions Firewall further check packets for compliance with the current state of the session to which the packet belongs.

Control sessions permits (see Fig.6):

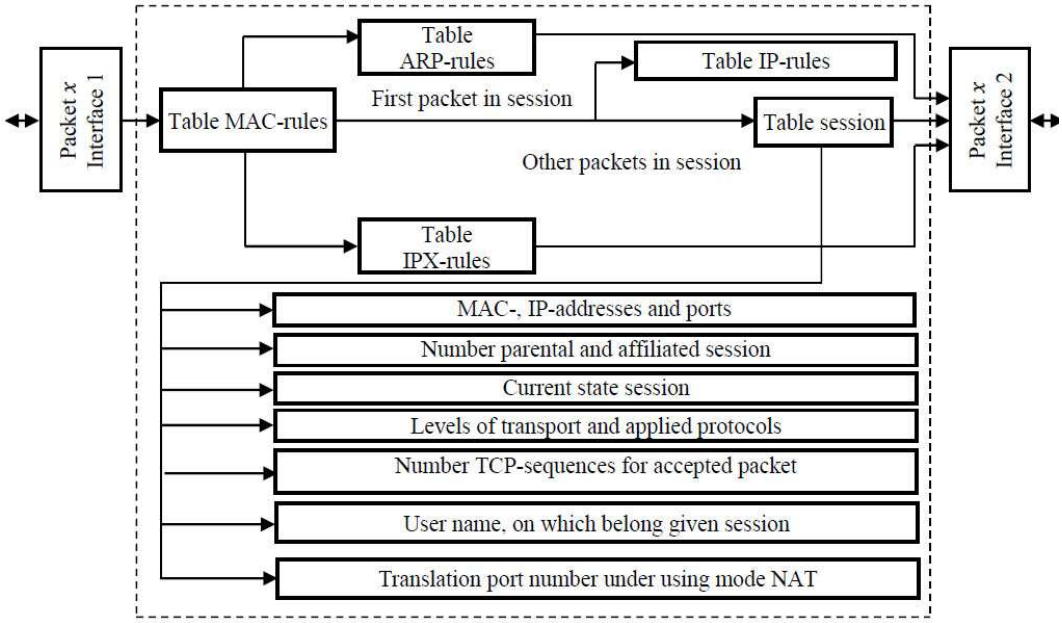

Fig.6. Structure of the monitoring sessions

- monitoring of progress of the virtual TCP-connection: each packet is checked against the context of the session. At the same time control: header flags TCP: for the different states of the virtual TCP connection identified a possible set of flags; sequence numbers and acknowledgments header TCP: for each packet sequence number is checked - it should lie in the so-called "window of the receiver" TCP; constant parameters of the TCP session;
- stroke control packet exchange on protocol UDP: each packet is checked against the context of the session. This is controlled by the immutability of UDP-session settings (IP-address and port number) [8];
- control of the course of exchange ICMP-messages

"echo request" and "echo reply": each packet is checked against the context of the session. Thus monitored parameters unchanged ICMP-session (IP-addresses, types message and ICMP requests);

- control data application protocols

The ability to use the mode of address translation:

- blocking attacks related to the improper installation of flags and sequence numbers protocol TCP;
- automatic opening of client ports required for the current session;
- caching of information when a part derived from the external network of information temporarily stored in the local memory, which saves time and consumed traffic on subsequent calls to the same information;
- address translation, allowing the use of external communications for the computers on the LAN is only one IP-address - the address of the firewall, internal network addresses can be anything.

Under this bandwidth the Firewall increases, due to the fact that a full check to all filter rules is subject to only the first packet of the session and all other packets open session only checked for compliance with the state vector of the session (see Fig.7 and Table 2).

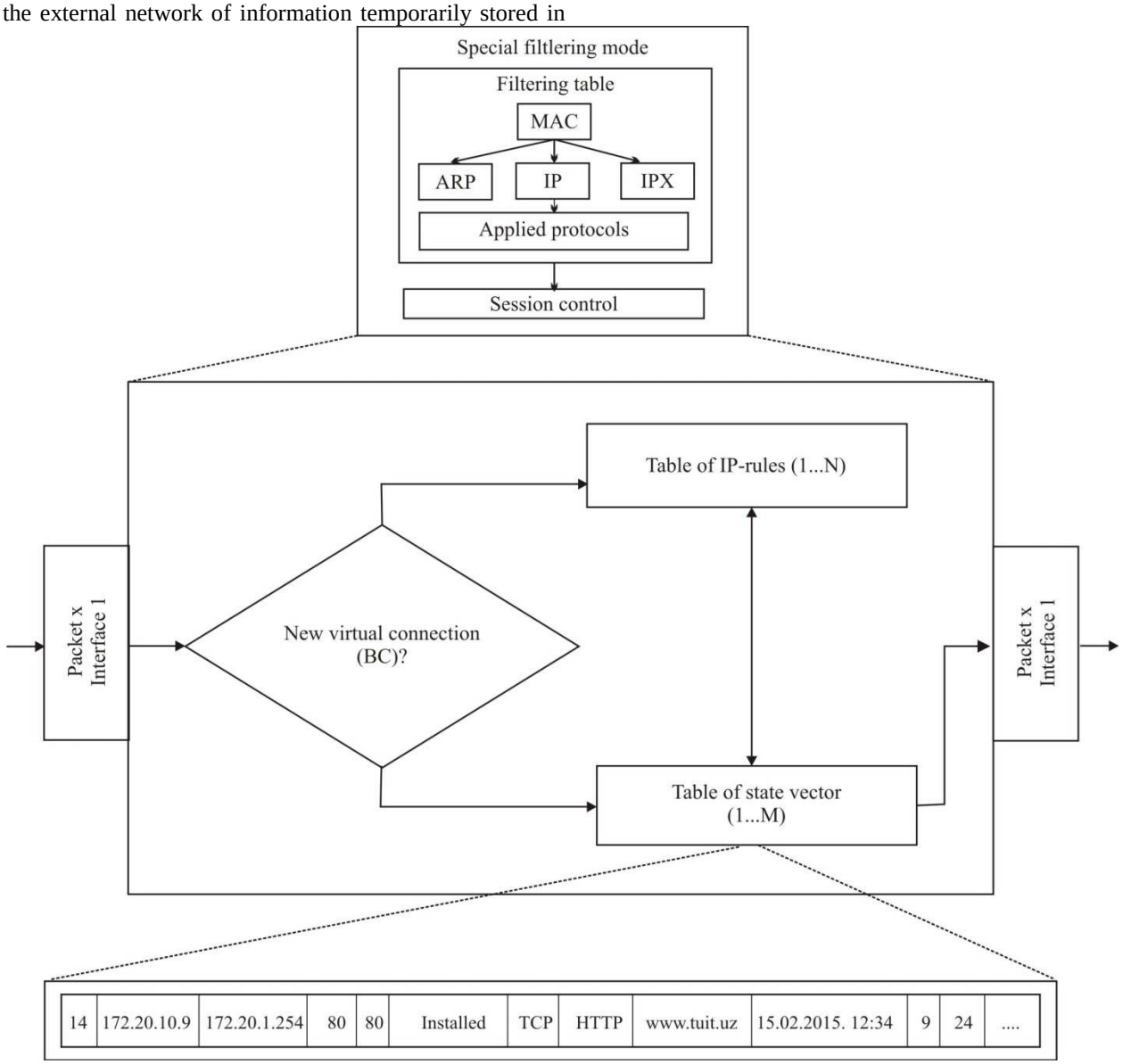

Fig.7. Operation architecture Firewall in a special mode traffic filtering

Table 2. Description of the state table (state vector)

Identification SV	14
IP- client address	172.20.10.9
IP-server address	172.20.1.254
Client port	80
Server port	80
State SV	Installed
Transport protocol	TCP
Applied protocol	HTTP
Inquired URL	www.tuit.uz
Time the beginning of SV	15.02.2015.12:34
Packets from client to server	22
Packets from server to client	31

IX. MIRRORING TRAFFIC

With mirroring traffic copies packets are forwarded to the specified interface Firewall regardless of the actions filter rules, which was processed packet [9-10].

This function can be useful when you need to keep track of all traffic passing through a filter interface additional analysis tools, such as intrusion detection system or a system of registration packets. Mirroring traffic includes three functions that are shown in Fig. 8.

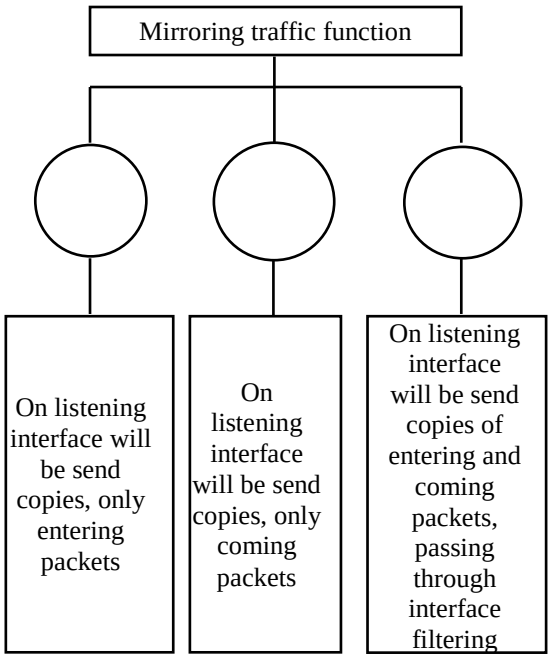

Fig.8. Scheme mirroring traffic function

Mirroring traffic function works in all special filtering modes (see Fig.9).In this mode the external network address translation (eth0) and internal (eth1) interfaces cannot act as a listener interface, on which send copies of packets.

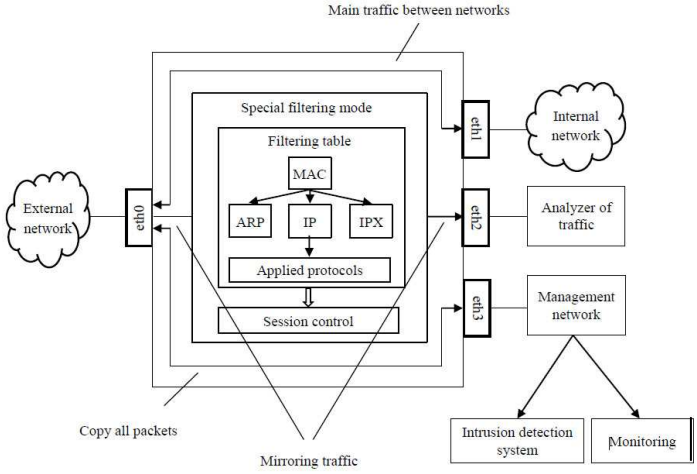

Fig.9. Structure research of mirroring traffic function

X. CONCLUSIONS

Overall, might highlight that the exponent Hurst H is an invariant characteristic to the scale of measurement, so his continued input and output of Firewall will be condition a special filtering mode. Developed model of the virtual TCP connection allows the identification of traffic parameters and influence to process of the fractal characteristics. Ranges of values are received under analysis of dependence of the exponent Hurst H, as a function of performance for different values of the buffer size and intensity. Researched mirroring traffic, which forwarded a copy of packets, continues to operate in the normal mode, send and receive packets regardless to each other.

REFERENCES

[1] Karimov M.M., Gulomov Sh.R. «Definitions policy access differentiations to IP networks on bases algebra of filtering rules». Кимёвий технология назорат ва бошқарув ISSN 1815-840 Халқаро илмий техникавий журнал 1/2014, ТДТУ.

[2] Sherzod Gulomov, Abduaziz Abdurakhmanov and Nurbek Nasrullaev. «Design Method and Monitoring Special Traffic Filtering under Developing «Electronic Government» International Journal of Emerging Technology & Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal), Volume 5, Issue 1, January 2015, India.

[3] Karimov M.M., Ganiev A.A., Gulomov Sh.R. «Models of network processes for describing operation of network protection tools». 4th International conference on application of information and communication technology and statistics in economy and education (ICAICTSEE – 2014) October 24 – 25th, 2014 University of National and World Economy Sofia, Bulgaria.

[4] Karimov M.M., Gulomov Sh.R., Yusupov B.K. «Approach development accelerate of process special traffic filtering». Journal of Computer and Communications, Vol.3 No.9, September 2015, PP. 68-82, USA.

[5] Karen Scarfone, Paul Hoffman, Guidelines on Firewalls and Firewall Policy, Recommendations of the NIST, September 2009.

[6] F. Schneider, J. Wallerich and A. Feldmann, “Packet capture in 10-gigabit Ethernet environments using contemporary commodity hardware”, (2007).

[7] Cristian Estan, Stefan Savage, George Varghese "Automated Measurement of High Volume Traffic" // ACM SIGCOMM Internet Measurement Workshop 2012.

[8] E. W. Fulp, "Optimization of Network Firewalls Policies using Directed Acyclic Graphs", IEEE Internet Management Conference, 2005.
[9] Ganiev A.A.,Gulomov Sh.R. «Mechanism prioritize packet traffic». 5th International conference on application of information and communication technology and statistics in economy and education (ICAICTSEE – 2015) November 13 – 14th, 2015 University of National and World Economy Sofia, Bulgaria.
[10] M. Christiansen, E. Fleury. Using IDDs for Packet Filtering. BRICS Report Series, RS-02-43, October 2010.

AUTHOR'S PROFILE

Rakhmonova Gulnora Sadirovna
Assistant professor.
was born September 19, 1963 year in Tashkent city, Republic of Uzbekistan. In 1985 graduated «Engineer economics» faculty of Tashkent Polytechnic Institute. Has more than 50 published scientific works in the form of articles, journals, theses and tutorials. Currently works of the department «Fiber optic lines and measurement systems» in Tashkent University of Information Technologies.

Gulomov Sherzod Rajaboevich
Assistant professor.
was born February 26, 1983 year in Shakhrisabz city, Republic of Uzbekistan. In 2009 graduated «Information technology» faculty of Tashkent University of Information Technologies. Has more than 70 published scientific works in the form of articles, journals, theses and tutorials. Currently works of the department «Information Security» in Tashkent University of Information Technologies.

Boymurodov Bobur Elmurodovich
Master degree.
was born June 22, 1987 year in Bukhara city, Republic of Uzbekistan. Has more than 10 published scientific works in the form of articles, journals, theses and tutorials. Currently works of the department «The system providing power» in Tashkent University of Information Technologies.