IP Packaging Filtering in Computer Networks Using Artificial Intelligence in the Regulatory Authority of Electronic and Communications Kosovo

Kastriot Dermaku[1], Liridon Hoti[1], Selami Klaiqi[1], and Hifoblina Dermaku[2]
[1] University of Kadri Zeka, Gjilan, Kosovo
[2] University of Academy Tempulli, Prishtina, Kosovo
Email: {kastriot.dermaku, liridon.hoti, selami.klaiqi}@uni-gjilan.net, hiflobina.obertinca@gmail.com

***Abstract*—**The security of our data is one of the most important challenges, and it is one of the things we must be careful about what we display on the Internet. For the security of this data, computer and cyber networking experts use different methods to prevent these attacks, prevention is done by Firewall techniques, and then by Router where both of these cases are quite popular nowadays today, however, another innovation is that filtering can also be done through Artificial Intelligence. In this paper, research has been done on the application of Artificial Intelligence methods such as those of deep learning on IP packages through Artificial Intelligence where specifically the method of Support Vector Machine with the training of a model through a simulated input corpus, using MATLAB software. From the results of the research by Artificial Intelligence, the source address, destination address, port number, protocol and package size were used as filters. All the practical work was done in over 350 different IP addresses, where 175 IPs were used for algorithm training, as well as 175 IPs were used for testing by combining them with filtering attributes, where in the end the filtering accuracy gained is quite high (83%).

***Index Terms*—**Firewall, filter, matlab, internet protocol, artificial intelligence

I. Introduction

Artificial Intelligence during its development, in addition to other fields, also found application in the field of Computer Networks in filtering IP packets. Considering the importance of packet filtering, where by filtering we can totally save our network from any possible attack which may come towards the network. Packet filtering works in such a way that it makes stops and allows different packets to enter or not into our network. This is done through IP addresses where it determines which IP addresses should be allowed and which are not (source and destination), then it can be done through Ports, through Protocol etc.

But although the security for such filtering is quite complex, the possibility has also become the possibility for packet filtering to be done through Artificial Intelligence or to be assisted by IA, where nowadays we have the incorporation of packet filtering using Artificial Intelligence.

The working methodology used during the analysis and research is in practical work within the institution of the Regulatory Authority for Electronic Communications (Republic of Kosovo) where we will see how to filter packets in computer networks using Artificial Intelligence. We will use the MATLAB software, where the training of the algorithm will be done, so that after it has the values that need to be filtered, and which values are created manually, then the algorithm itself will learn and do the detection of IP addresses of which are not secure to access the network. This will be represented by a manually created database.

II. Internet Security and Firewall

Given that nowadays the use of the Internet is extremely high, then the need for security has increased significantly as we have many types of threats and attacks that occur nowadays ranging from the simplest to obtaining credentials for a social network, to the point of blocking credit cards and stealing money from users' bank accounts. These threats and attacks are usually carried out by a virus which spreads on the Internet by malicious people and reaches the end users. Attacks can be of different types and divided into different categories.

Having network security is one of the biggest demands nowadays in the world of technology, as many attacks occur, many personal data is stolen by strangers, and many institutions and companies can even go bankrupt due to insecurity of the network [1].

A. IP Address

IP is one of the main protocols of the TCP / IP model. It is in the form of an IP datagram, where all TCP, UDP, ICMP and IGMP data travel across the network. IP is connection less and an insecure protocol.

It is insecure in that it does not guarantee that the IP datagram will be sent to the destination or not, very easily the data can fail while traveling through the internet (lost), this happens when the IP datagram sees some errors in the destination or in the hosts intermediate (as the packet travels online to the destination), and if this happens, the sender will receive a warning message that the packet has not reached its destination [2].

Manuscript received September 1, 2021; revised January 20, 2022.
doi:10.12720/jcm.17.2.134-142

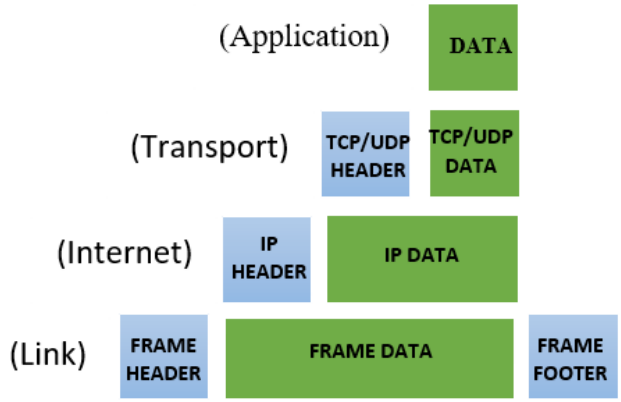


Fig. 1. TCP / IP [3], [4]

A very important point to explain here is how data is packaged across the TCP / IP model. If we analyze the figure carefully, then we will see that:

- The application layer (the fourth layer of the TCP / IP model, is the layer that holds the data), and then sends this data to the Transport layer.
- Then the Transport layer (the third layer of the TCP / IP model), places the header at the beginning of the packet and then sends the complete packet (TCP-header + app-data) to the IP layer [5].

B. *Firewall*

Firewall is a device that protects computer network resources by blocking unauthorized access by unauthorized users, and allowing only authorized or authorized communication to take place. A firewall is commonly used to protect private Internet-connected networks, especially intranets. All traffic entering or leaving the intranet passes through this Firewall, which first checks each traffic packet to meet security criteria and then decides which packet to allow passing through the intranet [6].

Firewall technology has evolved over time to support options such as:

- Control of services - determines which of the Internet services can be accessed from inside as well as from outside. The firewall can make traffic filtering appear based on the source IP, destination or port number, and it can also have a proxy server that receives and interprets each service before it passes through the intranet.
- Direction control - determines the direction of some requests for access to services and allows them to flow through the firewall.
- User control - controls users who request access to certain services. This mode is usually configured as local to internal computers, but also if we have users from outside the network then the incoming network configuration is done.
- Behavior control - controls how services will be used. For example, firewall can filter email addresses to stop spam emails.

So, while the firewall is used to filter computer networks, it also has some drawbacks or limitations such as:

- The firewall cannot protect the network from attacks that pass through the firewall.
- Firewall can't protect the network against attacks that occur within the organization.
- Laptop, Telephone or other smart device may, during its stay in a network outside the company, pick up the infection and then spread it inside the company without its knowledge.

III. Packet Filtering

Packet filtering is a firewall technique that it uses to control network packets by monitoring packets leaving and entering the network and enabling these IP packets to then pass through the network or even i stop, based on the source IP address and destination address, protocol and port. Packet filtering is one of the many techniques for implementing a secure network.

The internal network of the Electronic Communications Regulatory Authority is not very segmented, so we do not use a very sophisticated firewall to isolate one network from another. But nevertheless it is very preferable to become a kind of internal network security from the outside world of internet. Packet filtering is one of the techniques we use to secure the network and is done in the third layer (network).

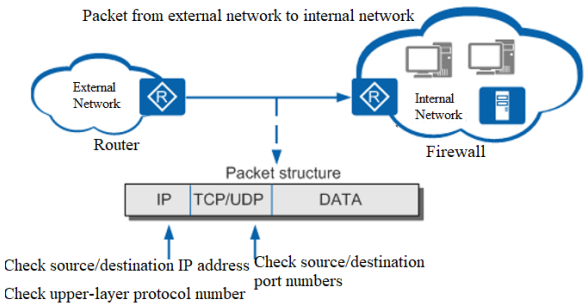


Fig. 2. IP packet filtering [7]

But one thing to know is that packet filtering is not a very sophisticated network security technique like the proxy firewall technique [8]. Since the proxy filters the message in the application layer, which is why this filtering method is often known as the application firewall, where it acts as a gateway between the internal network and the Internet, not allowing unauthorized access to leave the network. or even the opposite.

A. *Filtering Packages at the Regulatory Authority of Electronic and Communications*

Filtering of packages in the Electronic Communications Regulatory Authority is done through the configurations which occur in the network of this institution by the network administrator. The configurations are made in such a way that it is known that IP X cannot communicate with IP Y, and this case can be as follows.

```
Extended IP access list 101
    10 permit icmp 172.20.2.0  0.0.0.255  172.20.36.0  0.0.1.255
    20 permit icmp 172.20.2.0  0.0.0.255  172.20.68.0  0.0.1.255
    30 permit icmp 172.20.2.0  0.0.0.255  172.20.6.0   0.0.1.255
    40 permit icmp 172.20.2.0  0.0.0.255  host 192.168.200.200
    50 permit icmp 172.20.2.0  0.0.0.255  80.80.160.36  0.0.0.3
    60 deny icmp 172.20.2.0  0.0.0.255  any
    70 permit ip any (240 match(es))
```

Fig. 3. Creating ACL in the electronic regulator and communications

The figure above shows the configuration of stops for certain IPs:

- The first line shows that the access list is extended, we have two types of implementation of extended and standard access lists. Standard access lists usually use only the source address. These ACLs typically disable or enable all network protocols. Used in numbers from 1-99 and 1300-1999. So, their configuration is done in the following way:

```
Router(config)#access-list 20 ?
  deny Specify packets to reject
  permit Specify packets to forward
  remark Access list entry comment
```

Fig. 4. Standard ACL configuration

So, it is given the access list number and then it chooses whether we want to stop or allow an entire network to communicate with our network.

Then we have the extended access list type where the configuration of these is the same except that they use both the source and destination address. In this type of ACL we can specify which IP will be banned and which will be allowed. Enhanced ACLs are distinguished by the number given to them which can be from 100-199 and 2000-2699.

Their configuration is:

```
Router (config)#access-list 190 permit ?
  ahp Authentication Header Protocol
  eigrp Cisco's EIGRP Routing Protocol
  esp Encapsulation Security Payload
  gre Cisco's GRE Tunneling
  icmp Internet Control Message Protocol
  ip Any Internet Protocol
  ospf OSPF Routing Protocol
  tcp Transmission Control Protocol
  udp User Datagram Protocol
```

Fig. 5. Protocol selection for ACL

Set the extended ACL number which in this case is 190, then select the option whether we want to stop or allow it and the next step is to select the protocol we want to allow / stop and in this case I have chosen the ICMP protocol. Then select the source from where we want to make this stop / permission and then the destination where it will be banned / allowed to communicate and finally what message will be displayed at the source address it wants to communicate which can be:

echo, echo-reply, host-unreachable, net-unreachable, port-unreachable, protocol-unreachable, ttl-exceeded and unreachable:

Router(config)#access-list 190 deny icmp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 host-unreachable

Then we configure a packet filter where we will stop the ping to be impossible from the network 192.168.10.0 with subnet mask 255.255.255.0 not to communicate with the network 192.168.20.0 with subnet mask 255.255.255.0 using as notification message "host - unreachable ", from the network in the following figure.

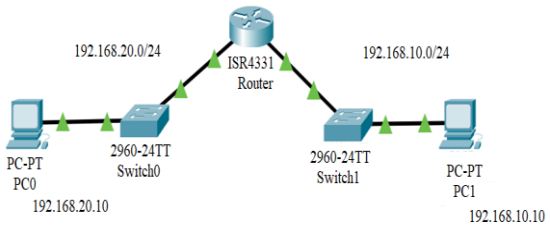


Fig. 6. Network for creating ACL

```
C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.20.10: bytes=32 time=1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time=32ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 32ms, Average = 8ms
```

Fig. 7. Ping before ACL configuration

From the figure above we have ping when ACL is not yet configured, everything works normally with the communication between the two networks.

But after we have configured the ACL when we try to pin the same IP, then we will have the following message:.

```
C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fig. 8. Certification ACL for ping stop

But, this is not the end of the configuration after that we will have to set the interface input, in which interface we will put this ACL, to show the incoming Router that if we have request from the network 192.168.10.0 for communicate with our network 192.168.20.0 be stopped immediately. Such configuration is done as follows:

In the Electronic Communications Regulatory Authority, the configuration will be made in the Gigabit Ethernet Interface 0/0/0, i.e. at the entrance of the network:

Router(config-if) #ip access-group 190 in

B. Filtering Packages with Wireshark

In the Wireshark filter display method it shows us packet filters and tells us in detail what kind of packets they are, their protocol and source and destination addresses. So, in itself there are some parameters that we can look at from this filtering method. Through the Wireshark tool in the network of the Electronic Communications Regulatory Authority and we will see the following:

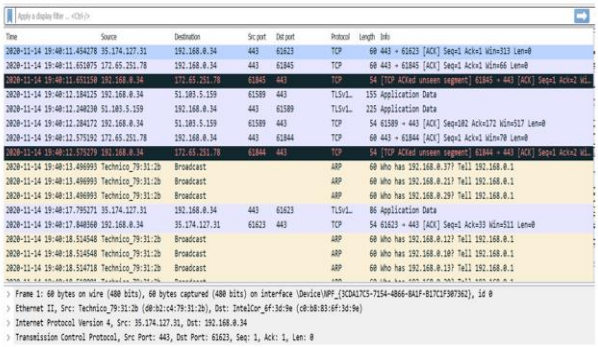
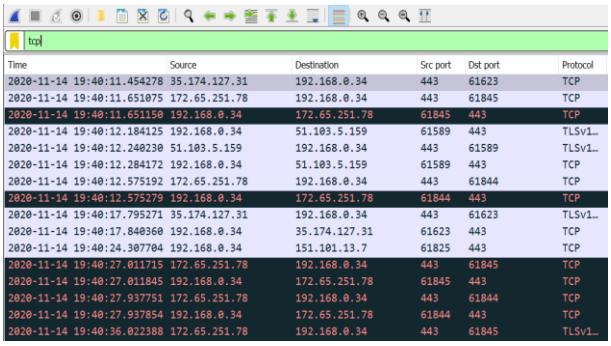


Fig. 9. Wireshark Filtering

From the figure above we see that we have many packages that enter our network, for example we have in the first row a packet which is destined for the IP address 192.168.0.34 from the source address: 35.174.127.31 which is an IP address and Amazon.com. Then, it also shows the source port 443 (HTTPS) and the destination port 61623 and the protocol which is being used which is TCP and other additional information.

To filter packets if we want only those packets that contain the TCP protocol to be displayed to us then this is done in the search window that is to apply a display filter and enter TCP as shown in the following:



tcp

Time	Source	Destination	Src port	Dst port	Protocol
2020-11-14 19:40:11.454278	35.174.127.31	192.168.0.34	443	61623	TCP
2020-11-14 19:40:11.651075	172.65.251.78	192.168.0.34	443	61845	TCP
2020-11-14 19:40:11.651150	192.168.0.34	172.65.251.78	61845	443	TCP
2020-11-14 19:40:12.184125	192.168.0.34	51.103.5.159	61589	443	TLSv1…
2020-11-14 19:40:12.240230	51.103.5.159	192.168.0.34	443	61589	TLSv1…
2020-11-14 19:40:12.284172	192.168.0.34	51.103.5.159	61589	443	TCP
2020-11-14 19:40:12.575192	172.65.251.78	192.168.0.34	443	61844	TCP
2020-11-14 19:40:12.575279	192.168.0.34	172.65.251.78	61844	443	TCP
2020-11-14 19:40:17.795271	35.174.127.31	192.168.0.34	443	61623	TLSv1…
2020-11-14 19:40:17.840360	192.168.0.34	35.174.127.31	61623	443	TCP
2020-11-14 19:40:24.307704	192.168.0.34	151.101.13.7	61825	443	TCP
2020-11-14 19:40:27.011715	172.65.251.78	192.168.0.34	443	61845	TCP
2020-11-14 19:40:27.011845	192.168.0.34	172.65.251.78	61845	443	TCP
2020-11-14 19:40:27.937751	172.65.251.78	192.168.0.34	443	61844	TCP
2020-11-14 19:40:27.937854	192.168.0.34	172.65.251.78	61844	443	TCP
2020-11-14 19:40:36.022388	172.65.251.78	192.168.0.34	443	61845	TLSv1…

Fig. 10. TCP Filtering

We can see that the Frame how the encapsulation is done, when this package has reached our network, then the number and frame length, then in Ethernet, Internet protocol and Transmission Control Protocol there is much more necessary information about this package.

After opening this presentation, we will be given the opportunity to do various filters as follows [9]:

- Filtering traffic from only one IP address e.g., IP address 172.16.0.4 is done as follows:
  host 172.16.0.4
- Filter traffic from a range of IP addresses or for a range of IP addresses:
  host 172.16.0.1/24 or host 172.16.0.1 mask 255.255.255.0
- Filter packets from a range of IP addresses:
  scr net 172.16.0.5/24
- Filter packets for a range of ip addresses
  dst net 172.16.0.5/24 apo dst net 172.16.0.5 mask 255.255.255.0
- Single DNS port filtering 53
  port 53
- Filter the entire network but not ARP and DNS
  port not 53 and not arp

These are just a few examples of catch filtering, but the extended list of these filters can be found by reference [10].

IV. Statement of the Problem

While we have a lot of cyber-attacks it has been seen very important that filters be raised to a higher level than they have been so far, attacks which directly affect the security level of the Electronic Communications Regulatory Authority. So seeing these network threats, we have done analysis and scientific research about the use of artificial intelligence in filtering IP packets, thus we will manage to make our networks more secure, critical data will be protected and the possibility of attacks will be more difficult.

V. Results

Based on what we have talked throughout this paper, we will present some results worked in practice. We will filter packets in MATLAB by training the back-propagation algorithm which algorithm is mostly used in multi-layer neural networks since it is known that in AI filtering, we have three main layers (input layer, hidden layer and output layer), that based on the data we have, i.e., from IP addresses, port, protocol to be filtered based on these attributes.

We present a part of the network within the Electronic Communications Regulatory Authority and how the filtering will be done.

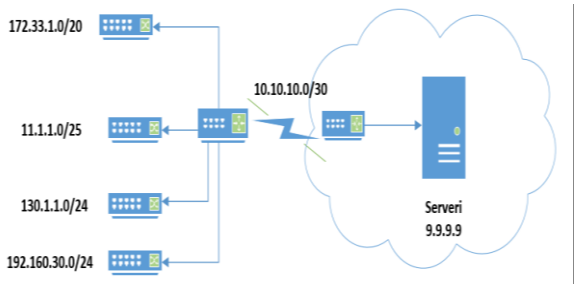


Fig. 11. Network layout

Based on the figure above, the filtering will be done by the Router which is located on the Internet connected to the Server. From the nets on the right that are; 172.33.1.0, 11.1.1.0, 130.1.1.0 and 192.160.30.0 will make various

requests to the server, and from these requests we will filter the packets.

Filtering will be done based on port number, protocol, packet size as well as source addresses.

TABLE I. PROTOCOLS USED IN THE REGULATORY AUTHORITY OF ELECTRONIC AND COMMUNICATIONS

Protocol	Port Number	Matlab-Reference Number
TCP	n/a	1
UDP	n/a	2
Telnet	23	3
HTTP	80	4
ICMP	7	5
REMOTE	3389	6
SSH	22	7

Scenario 1, filtering rules:

So, the filters will be done based on this protocol, and will do the following:

a) Network 172.33.1.0/20, if you do not want to access REMOTE on the Server will be banned here, also do not stop here also Telnet and SSH.

b) Network 11.1.1.0/25, if you have requested to REMOTE on the Server you will be banned here, also for Telnet and SSH.

c) Network 130.1.1./24, also REMOTE do here stop for Server, and Telnet and SSH.

d) Network 192.160.30.0/24, do here to stop the requests you requested in Port 80 on the Server, so you can't access the websites.

Also the other protocols we have for our example which are ICMP, TCP and UDP make it permissible for all networks.

A. Submission in Packet Tracer

We filter packets on the network side in the Electronic Communications Authority, using the Packet Tracer software tool.

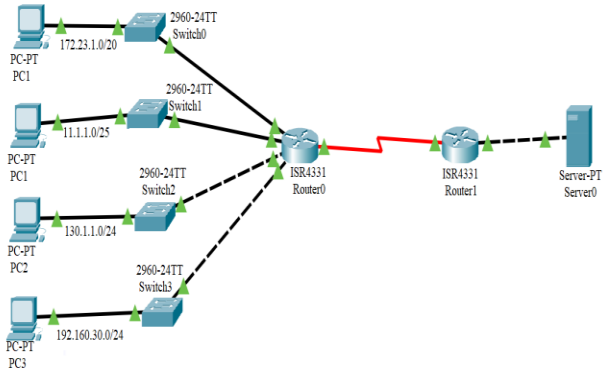


Fig. 12. Appearance in the tracer packet

From the network above, we will do the filtering as I mentioned that stops and permissions will be done.

First of all, in order to make this filtering as efficient as possible, everything must be released, and the ip addresses must be well configured for traffic exchange. Between the two routers we have placed the network 10.10.10.0/30 since we are dealing with only two IP addresses.

Now that everything is in order and communication can take place between all the devices, we start and create stops by accessing lists.

For the first network which is 172.33.1.0/20, we will stop Telnet, SSH and Remote, and this is done by accessing the extended lists:

Access-list 101 deny tcp 172.33.1.0 0.0.15.255 9.9.9.9 255.255.255.255 eq 23

where:

Access-list 101 - is the access list number

Deny stop command

TCP - protocols

172.33.1.0 - Source IP address

0.0.15.255 - Wildcard mask

9.9.9.9 - Destination IP address

255.255.255.255 - Wildcard mask

Eq 23 - Protocol port number

From the above command we understand that, for the network 172.33.1.0, telnet should be disabled, where in eq we can also write the port number, for the host 9.9.9.9.

Below we will make the stops for Remote (3389 - Port) and for SSH (22 - Port):

```
Router# show access-list 101
Extended IP access list 101
  deny tcp 172.33.0.0  0.0.15.255  eq telnet host 9.9.9.9
  deny tcp 172.33.0.0  0.0.15.255  eq 3389 any
  deny tcp 172.33.0.0  0.0.15.255  eq 22 any
```

Fig. 13. Prohibitions for Telnet, SSH and REMOTE

So with these commands we will make the network stop for all three of these protocols in the direction of the network 9.9.9.9.

In the same access list, we will make the network stops 11.1.1.0/25 and 130.1.1.0/24 for these three protocols:

```
Router show access-list 101
Extended IP access list 101
  deny tcp 11.1.1.0  0.0.0.127  any eq telnet
  deny tcp 11.1.1.0  0.0.0.127  any eq 22
  deny tcp 11.1.1.0  0.0.0.127  any eq 3389
  deny tcp 130.1.1.0  0.0.0.255  any eq 3389
  deny tcp 130.1.1.0  0.0.0.255  any eq 22
  deny tcp 130.1.1.0  0.0.0.255  any eq telnet
  deny tcp 172.33.0.0  0.0.15.255 any eq 3389
  deny tcp 172.33.0.0  0.0.15.255 any eq 22
  deny tcp 172.33.0.0  0.0.15.255 any eq telnet
  deny tcp 192.160.30.0  0.0.0.255 any eq www
  permit tcp any any
```

Fig. 14. Stop for three networks

Now in the following we will make the network stop 192.160.30.0/24 to not allow access to Port 80:

Router(config)#access-list 101 deny tcp 192.160.30.0 0.0.0.255 9.9.9.9 255.255.255.255 eq 80

Fig. 15. Stop Port 80

And after we have made the configurations for the necessary stops, then at the end of this access list a command should be marked which is:

```
Router show access-list 101
Extended IP access list 101
  deny tcp 11.1.1.0  0.0.0.127  any eq telnet
  deny tcp 11.1.1.0  0.0.0.127  any eq 22
  deny tcp 11.1.1.0  0.0.0.127  any eq 3389
  deny tcp 130.1.1.0  0.0.0.255  any eq 3389
  deny tcp 130.1.1.0  0.0.0.255  any eq 22
  deny tcp 130.1.1.0  0.0.0.255  any eq telnet
  deny tcp 172.33.0.0  0.0.15.255 any eq 3389
  deny tcp 172.33.0.0  0.0.15.255 any eq 22
  deny tcp 172.33.0.0  0.0.15.255 any eq telnet
  deny tcp 192.160.30.0  0.0.0.255 any eq www
  permit tcp any any
```

Fig. 16. Complete access list

Once we are done with the access list, we have to put the same in the interface of Router1, which will also be the Packet Filter in the interface that 0/1/0 respectively at the entrance of the network.

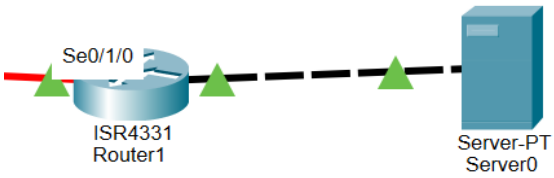


Fig. 17. Network filtering at the interface 0/1/0

B. Submission to MATLAB

We will present the same network in MATLAB, where it will be done through Artificial Intelligence where the device itself will learn which should be allowed and which should not, by first entering the data for our network. We will work with the Supervised Machine Learning method, and with seven dimensions.

Dataset, is a collection of data which is treated as a single value by computers. This means that we can have multiple separate data which can be used to train an algorithm to find predictions within this data.

Building a dataset requires three main steps:

1. The collection should be done from the data of some revenues which we will train to get the results. Usually the revenue can be in three forms: open source data, from the internet and we can generate data ourselves (which in our case we created the network ourselves).

2. Preprocess is a principle in data science that everyone should adhere to, starting with whether the data we are using has been used. If not, then we need to keep in mind that this data may be bad or flawed, if so, then we need to do even more to get a better result.

3. Since we have provided that the data is clean and ready for processing, we must be sure that this data will be understood by computer equipment in order to be processed, which must be in the form of binary numbers [10].

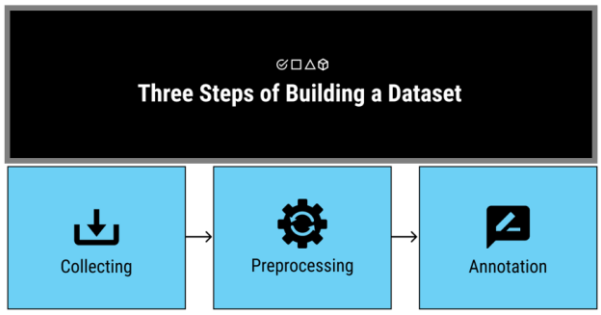


Fig. 18. Steps for creating a dataset [10]

The data is created manually, a database is created with IP addresses, with the protocol number, with the protocol that was used, the package size as well as the filter fields with 0 and 1.

TABLE II. DATA TABLE IN THE REGULATORY AUTHORITY OF ELECTRONIC AND COMMUNICATIONS

Number	Source_1	Source_2	Source_3	Source_4	Destination_1	Destination_2	Destination_3	Destination_4	Port_Number	Protocol	Packet_Size	Allow/Deny
1	11	1	1	56	9	9	9	9	23	3	120	0
2	11	1	1	125	9	9	9	9	80	4	150	1
3	130	1	1	198	9	9	9	9	25	1	200	1
4	192	160	30	211	9	9	9	9	22	5	1900	0
5	11	1	1	56	9	9	9	9	80	2	100	1
6	11	1	1	22	9	9	9	9	3389	6	200	0
7	11	1	1	93	9	9	9	9	80	4	201	1
8	192	160	30	222	9	9	9	9	80	4	189	1
9	130	1	1	125	9	9	9	9	80	4	89	1
10	130	1	1	250	9	9	9	9	23	3	500	0
11	11	1	1	120	9	9	9	9	7	5	45	1
12	172	33	1	25	9	9	9	9	7	5	30	1
13	11	1	1	33	9	9	9	9	7	5	23	1
14	172	33	1	210	9	9	9	9	23	3	88	0
15	130	1	1	111	9	9	9	9	80	4	22	1
16	192	160	30	55	9	9	9	9	7	5	450	0
17	172	33	1	30	9	9	9	9	7	5	55	1
18	172	33	1	50	9	9	9	9	80	1	40	1
19	192	160	30	125	9	9	9	9	80	1	28	1
20	11	1	1	85	9	9	9	9	7	5	50	1
21	11	1	1	35	9	9	9	9	22	3	1509	0
22	11	1	1	120	9	9	9	9	80	4	29	1

Given that for data processing the numbers must be decimal then the IP addresses are divided by four columns for the source address, and also for the destination address:

TABLE III. SUBMISSION IN THE REGULATORY AUTHORITY OF ELECTRONIC AND COMMUNICATIONS

Source_1	Source_2	Source_3	Source_4	Destination_1	Destination_2	Destination_3	Destination_4
11	1	1	56	9	9	9	9
11	1	1	125	9	9	9	9
130	1	1	198	9	9	9	9

where in Source_1, is the first octet of the source IP address, Source_2 is the second octet and so on. The same goes for the destination IP address.

After that, the port number and the protocol that was used are presented.

TABLE IV. PORT NUMBER AND PROTOCOL

Port_Number	Protocol
23	3
80	4
25	1
22	5
80	2
3389	6
80	4
80	4

Since the computer does not understand the data in the form of text, we have marked the protocols with decimal numbers from 1-7 which are as follows:

1- TCP; 2- UDP; 3- Telnet; 4- HTTP; 5- ICMP; 6- Remote; 7- SSH

Now that we have created the databases with the data we want, then on this data we will train an algorithm using MATLAB, to do packet filtering as we have set the rules [11].

C. Algorithm Training in MATLAB

Algorithm training will be done with the commands:

dataip = [ip1 ip2 ip3 ip4 port packetsize protocol]

With this command we specify which data will be used to filter packets.

groups - Variable with 0 and 1-sha, where 0 means ip address should be filtered, while 1 ip address should not be filtered.

The following command randomly divides the dataset for training and testing.

[train, test] = crossvalind ('holdOut', group);

cp = classperf (group);

The following command trains the support vector machine with the training set which was created in the previous code:

svmStruct = svmtrain (dataip (train, :), groups (train));

After that we test the model with test set:

classes = svmclassify (svmStruct, dataip (test, :));

And finally we do the training performance calculation, where it turns out that the classification accuracy is 0.8391 or 83%.

classperf (cp, classes, test);

cp.CorrectRate

ans = 0.8391 - Percentage of performance. The project has been for 350 Records.

The training of the algorithm was done with the method of SVM 7 dimensional, where the data which we have created manually (see appendix 1), were read by this algorithm to do packet filtering according to scenario 1. The training of the algorithm was done by receive the manually created database of 350 IP addresses for training and testing [train, test] where the allocation was done randomly:

- 175 IP addresses were used for algorithm training, where these IP addresses were routinely generated from the created database where each of the IP addresses was trained one by one to make the training as accurate as possible, and
- The other 175 IP addresses were used for algorithm testing where the accuracy was 83% (0.83%).

Seeing the accuracy which was quite high, then from the 175 IP addresses that were used for testing it turns out that out of: 175 IP addresses 145 of them were properly filtered.

175/100 * 83% = 145

From the obtained result we can conclude that the filtering of IP packets, using Artificial Intelligence, and based on the source address, port number, protocol and packet size is possible with a very high accuracy and that it can be used in computer networks.

VI. Conclusion

Nowadays, the security of the Internet and the networks of various institutions as well as in the Electronic Communications Regulatory Authority in Kosovo is a very big challenge but also a point in which we must be very careful and pay close attention. network security as this can affect their bankruptcy, as it is known that nowadays we have many different cyber-attacks.

While the packet filtering was previously done only by devices such as Firewall or Router where through the access lists various permissions and prohibitions of devices have been made, where in itself this has sufficient security but, still it can still at some point fall and various attackers deport to the network and damage data. But to make this more difficult network administrators also use different methods which constitute an extremely high level of data protection as the attacker has to deport to two network security devices until he reaches the point where he wants.

But in addition to this filtering which is also known as traditional filtering, today technology has advanced and great developments have been made in the field of Artificial Intelligence, where a use of it was also found in filtering IP packets in computer networks. Filtering of computer packages through Artificial Intelligence is possible.

From this paper we conclude that packet filtering speed is a very big advantage as it is always the same regardless of how many packets will be filtered and can be used in solving communication control problems in networks computer.

The dataip function is used in this paper. Such a function is usable for reasons of suitable range of range (from 0 to 1). The dataip function is identical to the sigmoid which is a mathematical function characterized by the S-shaped curve.

We presented the case of how a simple application for a seller's route from one point to another all the calculations were done, all the values were collected and in the end the trusted route was chosen.

It is concluded that this can be achieved since in this paper is analyzed a database with 350 IP addresses for filtering, where here are specified: source IP address, destination IP address, port number and packet size as attributes for filtering. Where then the algorithm which is trained based on these attributes has also done the filtering of IP packets. The algorithm training was done in MATLAB software using the Support Vector Machine (SVM) method, which algorithm from the created data

corpus will take the data for filtering, where then the algorithm will automatically detect that which IP addresses should be allowed and which not. The training of the algorithm is done with IP addresses received in a regular way with 50% of the addresses, while the other 50% will be taken for testing the algorithm where it turns out that the accuracy is 83% (or 0.83%), which accuracy is quite above and from this we can conclude that packet filtering based on attributes such as: source address, port number, protocol and packet size is quite accurate and that it can be used for filtering on computer networks.

APPENDIX 1

Appendix 1 presents the database, it is created manually.

Nr- Serial number

S_1- The first octet of the source address

S_2- Second octet of source address

S_3- The third octet of the source address

S_4- Fourth octet of source address

D_1- The first octet of the destination address

D_2- Second octet of destination address

D_3- The third octet of the destination address

D_4- Fourth octet of destination address

Port_Nr- Port number

Pro – Protocol

P_S –Pocketsize

L/N – Allow / Stopped

The destination address is the same for everyone, 9.9.9.9 so it is the network where we made the access lists (filtering rules).

The practical work was done on over 350 different IP addresses, where 175 IPs were used for algorithm training, as well as 175 IPs were used for testing by combining them with attributes for filtering. Due to the large number of rows, we are only giving the initial 5 IPs and the last 5 IPs.

No	*S_1*	*S_2*	*S_3*	*S_4*	*D_1*	*D_2*	*D_3*	*D_4*	*Port_No*	*Pro*	*P_S*	*L/N*
1	11	1	1	56	9	9	9	9	23	3	120	0
2	11	1	1	125	9	9	9	9	80	4	150	1
3	130	1	1	198	9	9	9	9	25	1	200	1
4	192	160	30	211	9	9	9	9	22	5	1900	0
5	11	1	1	56	9	9	9	9	80	2	100	1
…	…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…	…
346	11	1	1	100	9	9	9	9	80	4	12	1
347	192	160	30	70	9	9	9	9	80	4	55	0
348	11	1	1	9	9	9	9	9	7	5	80	1
349	192	160	30	8	9	9	9	9	23	3	10	1
350	11	1	1	100	9	9	9	9	7	5	1600	0

Conflict of Interest

We declare that this submitted work was carried without a conflict of interest.

Author Contributions

Kastriot Dermaku, profesor at Public University of Gjilan "Kadri Zeka", Computer Science Faculty. He finished Ph.D. degree in Organisation and Managment Information Process at the University of Library Studies and Information Technologies, Sofia, Bulgaria, in 2018, master deegre in Buissnes Informatics at South East European University -Skopje, North Macedonia in 2015 and bachelor deegre in Faculty of Engeeniering at Public University of Prishtina "Hasan Prishtina"-Prishtina, Kosovo in 2009.

Liridon Hoti received his Ph.D. degree in Information System and Technologies, Informatics and Computer Sciences from the University of Library Studies and Information Technologies, Sofia, Bulgaria, in 2021. He is a teacher at several Universities.

Selami Klaiqi, completed his Bachelor and Master studies in the field of Computer Science, also now has a PhD.c. at the University of Veliko Turnovo St Cyril and St. Methodius. Since 2009 he has been working in pre-university and university education in the subjects: Programming, Artificial Intelligence, Distributed Systems and other subjects in the field of Computer Science!

Hiflobina Dermaku, completed Bachelor deegre Faculty of Economics - Department of Management and Informatics, University of Prishtina, Prishtina ,Kosovo, in 2009, Master MA Managment, FAMA College - Prishtina ,Kosovo in 2019, also now has a PhD.c. at the University of Library Studies and Information Technologies, Sofia, Bulgaria.

This research is interests to all cooperating authors is to include network configurations and security, dynamic systems, systems modeling, optimization, control, GIS systems, etc.

References

[1] M. I. Buhari, M. H. Habaebi, and B. M. Ali, "Performance of Packet Filtering using Back Propagation Algorithm," in *Proc. 6th Annual Computer Security Applications Conference*, 2004, pp. 79-95.

[2] Cisco. IP Addressing: IPv4 Addressing Configuration Guide, Cisco IOS XE. Americans Headquarters: Cisco, 2015.

[3] G. Eason, B. Noble, *et al*., "Network security and types of attack in network," in *Proc. International Conference of Intelligent Computing, Communication & Convergence (ICCC-2015)*, Odisha, India: Procedia, Computer Science, 2015, pp. 503-506

[4] M. Haenlei and A. Kaplan, A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence, 2019.

[5] M. Hashem, A. Mohamed, and M. Wahib, Intelligent IP Packet Filtering., Suez Canal University, pp. 522-532.

[6] S. Ivenson. (2019) *packetpushers.net*. [Online]. Available: https://packetpushers.net/ip-fragmentation-in-detail/

[7] V. N. M. Dutt, "A multi-layer feed forward neural network approach for diagnosing diabetes," in *Proc.11th International Conference on Developments in eSystems Engineering (DeSE)*, Research Gate, 2018.

[8] I. Sydorenko. (2021). labelyourdata. [Online]. Available: https://labelyourdata.com/articles/what-is-dataset-in-machine-learning/

[9] K. Valentin and M. Maly, "Network firewall using artificial neural networks," Bratislava, Slovakia, 2013, pp. 1312-1327.

[10] A. Wool, Packet Filtering and Stateful Firewalls, 22.

[11] R. Raci, "IP packet filtering in computer network, artificial intellegence," 2021, pp. 71-79.