Middle-East Journal of Scientific Research 10 (1): 39-44, 2011
ISSN 1990-9233

Modeling and Simulation Firewall Using Colored Petri Net

[1]Behnam Barzegar and [2]Homayun Motameni

[1]Department of Computer Engineering, Nowshahr Branch, Islamic Azad University, Nowshahr, Iran
[2]Department of Computer Engineering, Sari Branch, Islamic Azad University, Sari, Iran

Abstract: In this paper the methodology of firewalled LAN models construction in the form of Colored Petri Net is introduced and model the ACL (Access Control List) in firewalls as the first form of defense for the simulation and analysis of the model the Design/CPN Tools is used The components of the model are Firewall, Switch, Hub, Server and Workstation.

Key words: Firewall · Simulation · ACL · Access Control List · CPN · Petri Net · Lan

INTRODUCTION

Data communications networks have become an infrastructure resource for businesses corporations, government agencies and academic institutions. Computer networking, however, is not without risks as Howard [1] illustrates in his analysis of over 4000 security incidents on the Internet between 1989 and 1995.

Firewall technology is one mechanism to protect against network based attack methods. A balanced approach to network protection draws from several other fields, such as physical security, personnel security, operations security, communication security and social mechanisms [2].

Classically, firewall technology has been applied to TCP/IP (transmission control protocol, internet protocol, internetworks. Firewalls are used to guard and isolate connected segments of internetworks. "Inside" network domains are protected against "outside" untrusted networks, or parts of network are protected against other parts. Various architectures for firewalls have been published and built, such as filtering routers, or application level proxy services. In this paper a packet filtering firewall with ACL (Access control List) models by Colored Petri net.

Coloured Petri Net (CPN) is a tool by which validation of discrete-event systems are studied and modeled. CPNs are used to analyze and obtain significant and useful information from the structure and dynamic performance of the modeled system. Coloured Petri Nets mainly focus on synchronization, concurrency and asynchronous events [3].

The graphic features of CPNs specify the applicability and visualization of the modeled system. Furthermore, synchronous and asynchronous events present their prioritized relations and structural adaptive effects. The main difference between CPNs and Petri Nets (PN) is that in CPNs the elements are separable but in PNs they are not. Coloured indicates the elements specific feature. The relation between CPNs and ordinary PNs is analogous to high level programming languages to an assembly code (Low level programming language).

Theoretically, CPNs have precise computational power but practically since high level programming languages have better structural specifications, they have greater modeling power.

CPN's drawback is its non-adaptivity [4] therefore it is not possible to access the previous information available in CPNs. If there is more than one transition activated then each transition can be considered as the next shot. This Coloured Petri Net's characteristic indicates that since several events occur concurrently and event incidences are not similar, then when events occur they do not change by time and this phenomenon is in contrast with the real and dynamic world. Simulation would be similar to execution of the main program.

Coloured Petri Nets: The coloured petri net is a language for modeling and evaluating of system that co-processing connection and synchronization play the main rule in it. This language is a complex of petri net with ML programming language [3, 5].

Corresponding Author: Behnam Barzegar, Department of Computer Engineering, Nowshahr Branch, Islamic Azad University, Nowshahr, Iran.

CPN model is an executive model system that shows position of a system and incidents which cause change in position of system.

CPN Tools is also a suitable tool for editing, modeling, analysis of space of position and analysis of operation of CPN models. graph of Petri net is a method for showing of structure of Petri nets that two shapes are in them.

These places and transitions connect to each other by arcs. when an arc connects from a transition to a place, it means, the place will be the exit of the mentioned transition and if an arc be drawn from a place to a transition, it means, that place will be entrance of the mentioned transition. For description of Petri net action, tokens add to this graph, too.

It causes, concept of position be defined in this graph. Number of these tokens in the whole graph and manner of their distribution among places, determines the position of Petri net, which called it a petri net marking.
A formal definition of CPN is as follows [3]:

A Coloured PN (CPN) is a 6-tuple CPN $(P,T,C, I^{-}, I^{+},M_0)$

Where:

- P = {p1, p2,..., pn} denotes a finite and non-empty set of places,
- T = {t1, t2,..., tm} denotes a finite and non-empty set of transitions, PnT =Ø,
- C is a colour function that assigns a finite and non-empty set of colors to each place and a finite and non-empty set of modes to each transition.
- I^{-} and I^{+} denote the backward and forward incidence functions defined by P×T, such that $I^{-}(p,t),I^{+}(p,t) \in [C(t) \rightarrow C(p)MS], v(p,t) \in P \times T^{2}$.
- Mo denotes a function defined on P, describing the initial marking such that Mo (p) ∈ C(p)MS.

Firewall: A firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communication to pass.

One form of defense for every network connected to the internet is Access Control List. These lists reside on routers or firewalls and determine which machines (that is, which IP addresses) can use the sub network and in what directions.

Model of LAN: LAN is a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings.

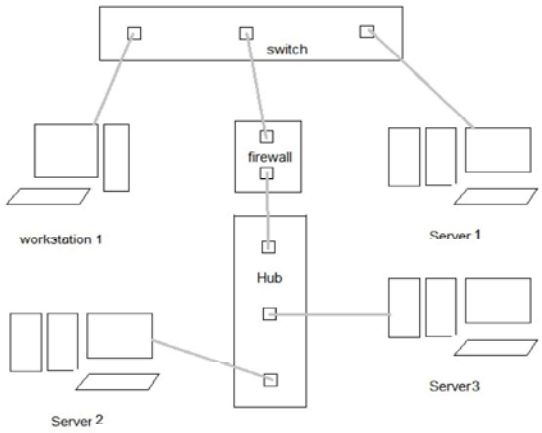

Fig. 1: Model of LAN

However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN).

Most LANs connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions.

Figure1 shown a model of sample LAN we used in this paper. the elements of the model are sub models of: Firewall, Switch, Hub, Server and Workstation. In this sample LAN, workstation is used to produce traffic in network and send request to the servers. switch navigate network traffic to the right port and avoid packet collision.

Firewall analyse input/output packets and filter unauthorized packets by rules exist in Access Control List.hub get the firewall output packets and deliver them to server2 and server3. Servers response to the incoming packets by sending 2 response packet to sender's address.Server2 and server3 are protected by ACL firewall and server1 operate in network without any protection.

Model of Firewall: The modeled firewall shown in Figure 2 is a full duplex ACL firewall. Packets come to firewall from in places and firewall control unit, control packets Source IP and Destination IP and mark them as a authorized or unauthorized packet based on ACL rules by checking ACL place.

In the next step Block Packet transition block the unauthorized packets and Pass transition fire to send out authorized packets if there is any authorized marked packet exist in firewall buffers.

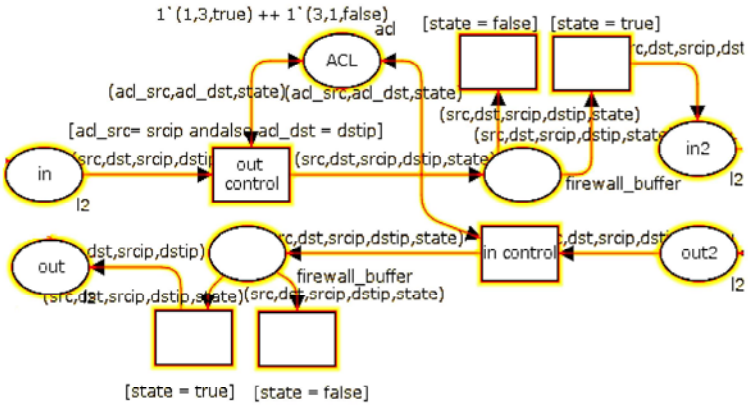

Fig. 2: Model of Firewall

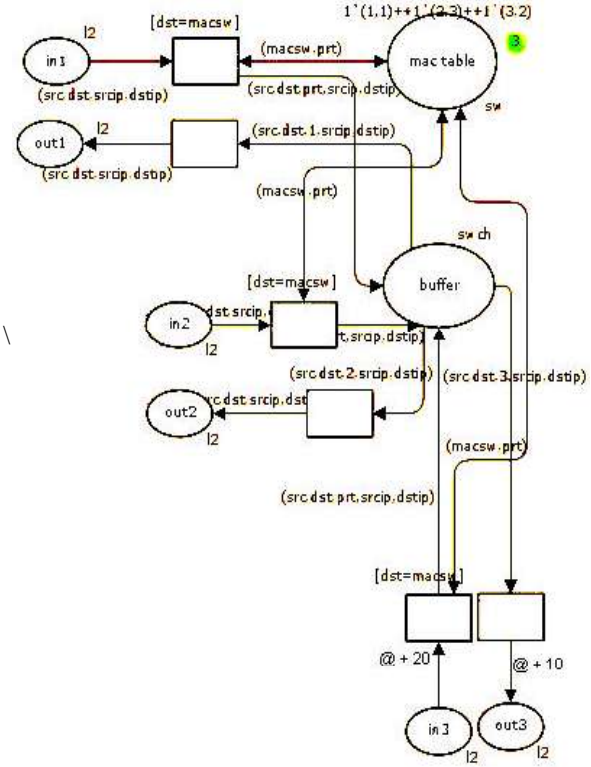

Fig. 3: Model of Switch

State field represent authorized (state = true) and unauthorized (state = false) packets in firewall.

Model of Switch: To construct the model for a network switch we shall consider separate input and output frame buffers for each port and a common buffer of the switched frames. A model of the switch presented in Figure 3. Hosts disposition according to Figure 1 was used for the testing of the model.

MAC address of the host is represented by the integer number. Moreover, content of the frame is not considered. Data type l2 describes the frames of the network, data type sw represents the switching table records and data type swch describes the switched frames waiting for output buffer allocation.

Places PortX In and PortX Out represent input and output buffers of port X accordingly.

Place mac table models the switching table; each token in this place represents the record of the switching table. Place Buffer corresponds to the switched frames' buffer.

Transitions InX model the processing of input frames.

The frame is extracted from the input buffer only in cases where the switching table contains a record with an address that equals the destination address of the frame; during the frame displacement the target port number is stored in the buffer.

Transitions OutX model the displacement of switched frames to output ports' buffers. Fixed time delays are assigned to the operations of the switching and the writing of the frame to the output buffer.

Model of Hub: To distribute packets in a small LAN it is common to use hubs and in this work hub is used to deliver firewall output packets to servers (Server2 and Server3) and servers (Server2 and Server3) responses to firewall's input port. Hubs repeats all incoming data to all outgoing ports except sender's port because the operate in the first layer of network and they have not MAC Table to save addresses. InX transition fires when at least one packet exist in InX place and it send 2 packets (each for one port) with the same information as incoming packet to the hub's buffer. OutX transition send packets to OutX place (Port). Figure 4 shows a Hub model.

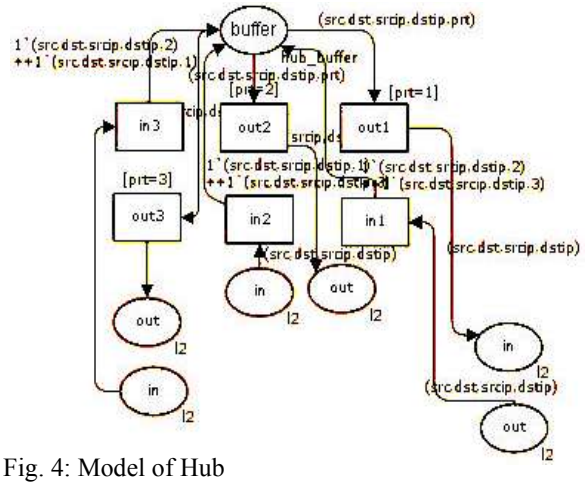

Fig. 4: Model of Hub

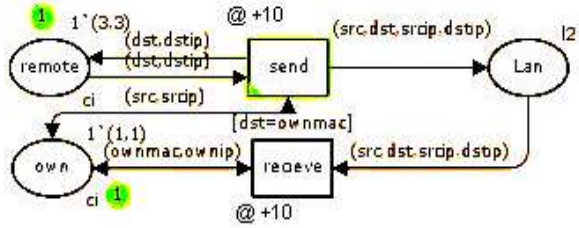

Fig. 5: Model of Workstation

Model of Server and Workstation: To investigate the frames' flow transmitting through the local area network and to estimate the network response time it is necessary to supply the model constructed with the models of terminal devices attached to the network. The general model assembling may be provided by means of union (fusion) of places.

On the peculiarity of the traffic's form we shall separate workstations and servers. For an accepted degree of elaboration, we shall consider the periodically repeated requests of the workstations to the servers with the random uniform distributed delays.

On reply to accepted request the server sends a few packets to the address of the requested workstation. The number of packets sent and the time delays are the uniform distributed random values.

A model of workstation is represented in Figure 5. Place LAN models the segment of the local area network that the workstation is attached to.

The workstation listens to the network by means of a transition Receive that receives frames with the destination address that equals the own address of the workstation saved in the place Own. The processing of received frames is represented by the simple absorption of them.

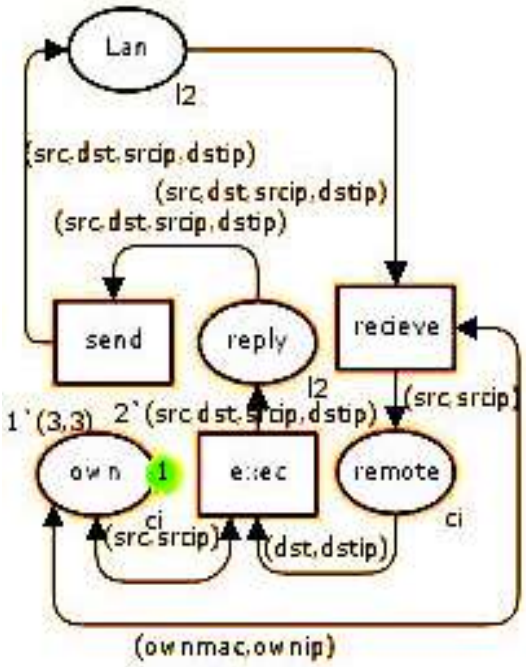

Fig. 6: Model of Server

The workstation sends periodic requests to the server by means of transition Send. The servers' addresses are held in the place Remote. The sending of the frame is implemented only if the LAN segment is free.

It operates by checking of the place LAN for the lack of tokens. In such a manner we may interact with a few servers holding their addresses in the place Remote.

A model of the server is represented in Figure 6. The listening of the network is similar to the model of the workstation but is distinct in that the frame's source address is held in the place Remote. Transition Exec models the execution of the workstation's request by the server. As a result of the execution request the server generates a random number of the response frames that are held in the place Reply.

Then these frames are transmitted into the network by the transition Send. The assembly of the general local area network model is implemented by the union of the places LAN of workstations and servers for each of the segments. The model of the switch is attached to the models of segments by means of additional transitions ReceiveX and SendX accepting frames into the input buffer and transmitting frames from the output buffer accordingly for each switch port.

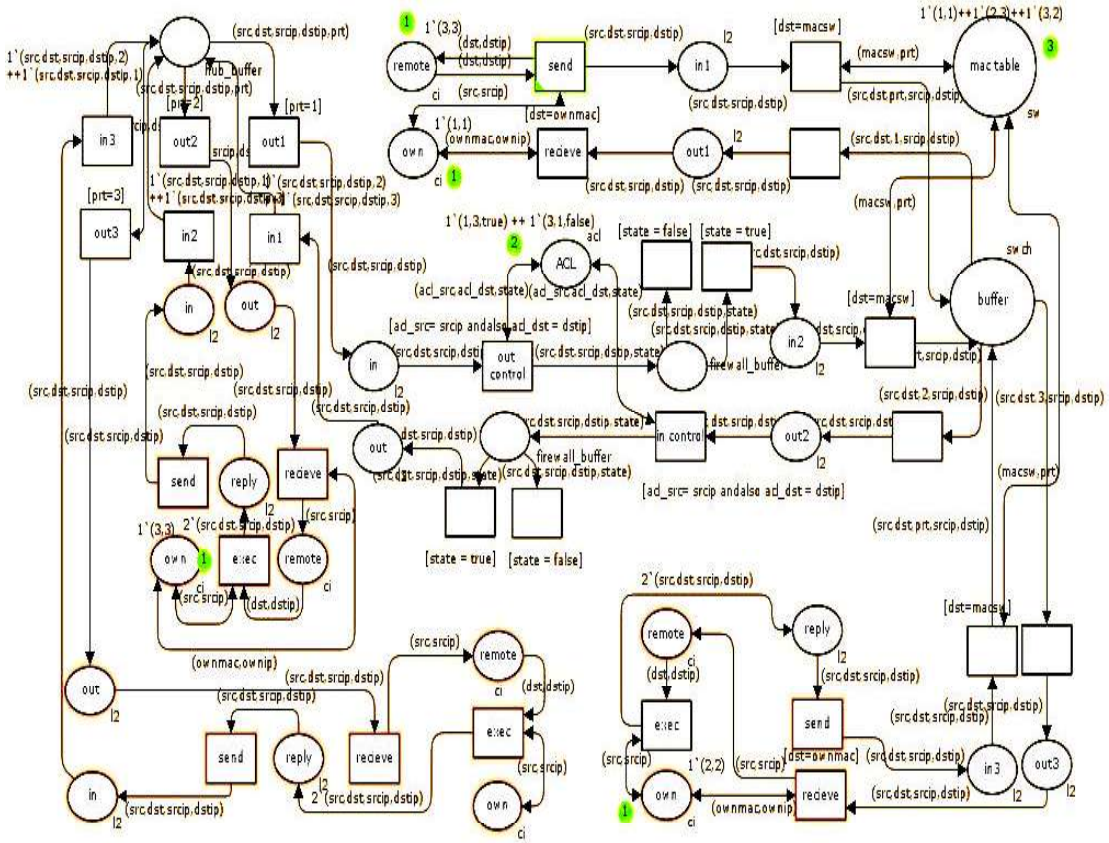

Fig. 7: Model of whole Network

```
color mac=INT;
color port=INT;
color ip=INT;
color l2=product mac * mac * ip * ip;
color sw=product mac * port;
color swch=product mac * mac * port * ip * ip;
color ci=product mac * ip;
color acl=product ip * ip * BOOL;
color firewall_buffer=product mac * mac * ip * ip * BOOL;
color hub_buffer=product product mac * mac * ip * ip * port;
var src, dst, macsw, ownmac:mac;
var prt:port;
var srcip,dstip,ownip, acl_src, acl_dst:ip;
var state:BOOL;
```

CONCLUSION

In the present work the technology of an ACL Firewall was studied.the sructure of ACL firewall, static MAC table Switches and Hubs was described and a simple model of workstation and server was shown.we saw firewall's Access Control List efficiency by model it in CPN.

As the future work it is good to simulate DMZ and other technologies in firewalls.

REFERENCES

1. Jensen, K., L. Michael Kristensen and L. Wells, 2007. Coloured Petri Nets and CPN Tools for modeling and validation of concurrent systems. International J. Software Tools Technology Transfer, pp: 213-254.
2. Asar, A., M. Zhou and R.J. Caudill, 2005. Making Petri Nets Adaptive: A Critical Review. IEEE Networking, Sensing and Control Proceedings, pp: 644-649.

3. Albert, K., K. Jensen and R. Shapiro, 1989. Design/CPN: A Tool Package Supporting the Use of Colored Nets. Petri Net Newsletter, pp: 22-35.
4. Elsaadany, A., M. Singhal and T. Lui Ming, 1995. Performance study of buffering within switches in local area networks. Proceedings of the Fourth International Conference on Computer Communications and Networks, pp: 451- 452.
5. Jensen, K., 1997. Colored Petri Nets—Basic Concepts, Analysis Methods and Practical Use. vols. 1-3, Springer-Verlag.
6. Hunt, R., 1999. Evolving technologies for new internet applications. IEEE Internet Computing, 5: 16-26.
7. Peterson, J., 1981. Petri Net Theory and the Modeling of Systems, Prentice Hall.
8. Rahul, V., 2002. LAN Switching, OHIO.
9. Zaitsev, D.A. and A.I. Sleptsov, 1997. State equations and equivalent transformations of timed Petri nets, Cybernet, 33: 659-672.
10. Gary, A. Donahue, 2007. Network Warrior. O'Reilly, 5.
11. Definition of Firewall, Check Point Resources.
12. Icove, D., K. Seger andW. VonStorch, 1995. Computer Crime. O'Reilley & Associates, Inc., Sebastopol, California.
13. Howard, J.D., 1997. An Analysis Of Security Incidents On The Internet 1989-1995. PhD thesis, Carnegie Mellon.