Packet Flow Analysis Through NS2 Model

[1]Rakesh Poonia, [2]Devendra Gahlot
[1,2]Assistant Professor
[1,2]Department of Computer Application,
Govt. Engineering College Bikaner,
Karni Nagar Industrial Area, Bikaner (Raj)
[1]rakesh.ecb98@gmail.com, [2]devendragahlot@gmail.com

Abstract

Safety measure is a necessary instruct to resolve the practical exertion in the researches of computer networks. Attacks on networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not. NS2 and OPNET are best network simulation tools, which provide very powerful simulation functions for network protocols. As the huge use of internet increases day by day so as safety anxiety is also elevate day by day in excess ofthe internet.In this paper we discuss the network security and its related threats and also study the types ofprotocols and few issues related to protocols in computer networks. We also simulate the model of nodeswired network scenario, its packet flow rate analysis through TCP protocol using NS2 as a simulator.

Keywords- Simulation, Security attacks, TCP/IP& NS2

1. Introduction

There exist some outstanding network simulation tools in the computer network research area, such as NS2 and OPNET, which provide very powerful simulation functions for network protocols, and through which it is very convenient to create the running environment for various protocols and it is very easy to display the protocol behaviour visually. Nevertheless these simulation tools are very hard to install and utilize. At present they are used by computer network researchers to study, extend and develop new protocols. Through this system, the students not only can leave out the difficulty to learn the network simulation software NS2, but also can make use of its powerful simulation functions to carry out network simulation researches, and consequently understand the complex behaviour of network protocols more comprehensively.

2. NS2 Outline

Network simulation is a kind of technology that simulates the net-work behavior through mathematical modeling and statistical analysis method and then obtains the specific parameters

which reflect the characteristics of the network. NS2 is one of the most famous network simulation software which was developed by LBNL network research group at UC Berkeley in the USA. It is primarily useful for simulating local and wide area networks, no matter what are wired or wireless networks. It has great value for network researchers, especially for the designers of new network protocols.

NS2 is an object-oriented, discrete event driven network simulation tool. One main component of NS2 is the event scheduler. An event in NS2 is a packet ID that is unique for a packet with scheduled time and the pointer to an object that handles the event. In NS2, an event scheduler keeps track of simulation time and fires all the events in the event queue scheduled for the current time by invoking appropriate network components, which usually are the ones who issued the events, and let them do the appropriate action associated with packet pointed by the event. Network components communicate with one the other passing packet; however this does not consume actual simulation time. All the network components that need to spend some simulation time handling a packet use the event scheduler by issuing an event for the packet and waiting for the event to be fired to itself before doing further action handling the packet. The other use of an event scheduler is timer. Timers use event schedulers in a similar manner that delay does. The only difference is that timer measures a time value associated with a packet and does an appropriate action related to that packet after a certain time goes by, and does not simulate a delay.

NS2 is designed to simulate variety of IP networks. It covers a very large number of applications, network types, network elements and traffic models which are called simulated objects. It implements network protocols such as TCP and UDP, traffic source behaviour such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Dijkstra, and more. NS2 also implements multicasting and some of the MAC layer protocols for LAN simulations. Besides, NS2 supports the simulation of various new technologies such as GRPS, mobile IPv6, RSRV, MPLS and Ah Hoc networks..

NS2 simulator is based on two languages: an object oriented simulator, written in C++, and aOTcl (an object oriented extension of Tcl), used to execute user's command scripts. For efficiency rea-son, NS2 separates the data path implementation from control path implementations. In order to reduce packet and event pro-cessing time, the event scheduler and the basic network compo-nent objects in the data path are written and compiled using C++. These compiled objects are made available to the OTcl interpreter through an OTcl linkage that creates a matching OTcl object for each of the C++ objects and makes the control functions and con-figurable variables specified by the C++ object act

as member functions and member variables of the corresponding OTcl object. In this way, the controls of the C++ objects are given to OTcl. It is also possible to add member functions and variables to a C++ linked OTcl object. The objects in C++ that do not need to be con-trolled in a simulation or internally used by the other object do not need to be linked to OTcl. Likewise, an object can be entirely implemented in OTcl.

2.1 Main Description

First and primary, NS2 is an object-oriented, discrete event driven network simulator which was originally developed at University of California-Berkely. The programming it uses is C++ and OTcl (Tcl script language with Object-oriented extensions developed at MIT). The usage of these two programming language has its reason. The biggest reason is due to the internal characteristics of these two languages. C++ is efficient to implement a design but it is not very easy to be visual and graphically shown. It's not easy to modify and assembly different components and to change different parameters without a very visual and easy-to-use descriptive language. Moreover, f or efficiency reason, NS2 separates control path implementations from the data path implementation. The event scheduler and the basic network component objects in the data path are written and compiled using C++ to reduce packet and event processing time. OTcl happens to have the feature that C++ lacks. So the combination of these two languages proves to be very effective. C++ is used to implement the detailed protocol and OTcl is used for users to control the simulation scenario and schedule the events. A simplified user's view of NS2 is shown in figure 2. The OTcl script is used to initiate the event scheduler, set up the network topology, and tell traffic source when to start and stop sending packets through event scheduler. The scenes can be changed easily by programming in the OTcl script. When a user wants to make a new network object, he can either write the new object or assemble a compound object from the existing object library, and plumb the data path through the object. This plumbing makes NS2 very powerful.

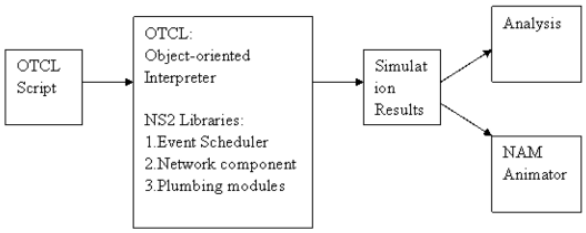

Figure1: Simplified User's View o f NS2

Another characteristic of NS2 is the event scheduler. In NS2, the event scheduler keeps track of reproduction time and liberates all the proceedings in the occasion queue by invoking appropriate network components. All the network components use the event scheduler by issuing an event for the packet and waiting for the event to be released before doing further action on the packet.

3. STUDY OF PROTOCOLS

Different types of protocols used on the each layer of TCP/IP model which helps in communication fromone network to more networks and also accommodating to communicating with other layer protocols.

1. Physical/ Data link layer: Data is transmit by wire or cables called asETHERNET or as well as concerned with addressing the data from one network node to other, forthis linking ETHERNET Cables are used. There isnumerous type of ETHERNET cables are Forexample: 10BASE5, co-axial, twisted cable etc.

2. Network layer: It tells how to route the packet on network for this purpose IPprotocol used to route the packet from source node to destination node. The protocols are IP.IPXused at this layer.

3. Transport layer: To transport the routed packet that comes from the Network layer by meansof protocols as TCP, UDP.

4. Application layer: Application layer used to show the data to the end user. There are so many protocols used at this layer for the end user through whom they can recognize the data inuser clear form so the protocols used at this layer are HTTP, SMTP, DNS etc.

4. THREATS ON NETWORK SECURITY

There are so many threats on network which will harm the safety of user on the network we mentionfew of them below in this:

Intrusion Attack: There are so many users on the network who use the internet and needsecurity on their network but when any illegal person or dishonestuser achieves access on thenetwork to use the data of that user.

Spoofing Attack: When the illegal user access authorized information at transport layer bychanging the source IP packet. These illegal users change the private information of theauthorized user due to this the authorized user will obtainmisshapen information.

Protocol based Attacks: Communication protocols are the medium with the help of whichdata or information is transferred or retrieve on the computer network. There are so many attacksas discussed in next section come under this attack.

Denial-of-service Attack: DOS is a type of attack through which the network become weakand DDOS is distributed in the whole network and the appearance of the DDOS is present in thecore architecture of internet [13] It is of two type[14]:

Ping of death

SYN attack

Application level Attack: Application level is called as user level where user gets so manyprotocols which help them to retrieve the information from sender but attack is also generated atthis level in form of malicious node Trojan on the HTTP etc.

Logon Attack: Due to safety and solitudereason logon policy is expand on the network butthere are so many hackers who hack the secret word and username of the authorized user.

Attack on address: Address are of two types MAC address and physical address when someunauthorized user stole the information by accessing the address of source and destination. There are so many researchers who researched the so many methods to detect the attacks orthreats.

5. The Demonstration System

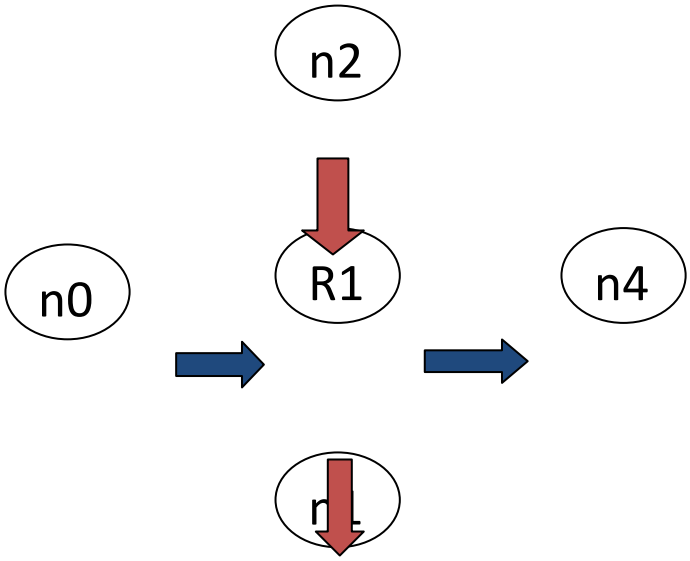

Figure 2: Model of Wired TCP Network

These are the four parameters of the exponential traffic through which traffic is generated onsource nodes and this traffic in form of packets send to router node R1 at that time due tocongestion window

or the packet rate the some data is fall down through the router node R1 andpackets which are not fallen down are send to destination node n4.

6. Outcome Analysis When Packets Are Drop Down Through Router

Below figures shows that packets comes from three sources n0, n1, n2 that are transmitted to thedestination n4 which is in hexagonal shape and packets are drop down at the routernode called n3 which is in square shape. TCP mediator is formed at three sources and exponential traffic is attached to the mediator but at that time rate parameter value is in mb so that packets would drop down at router node.

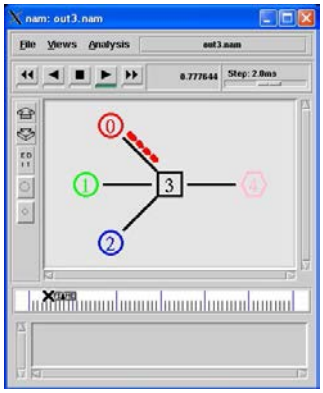

Figure 3: Packets send from source n0 to destination n4 through n3

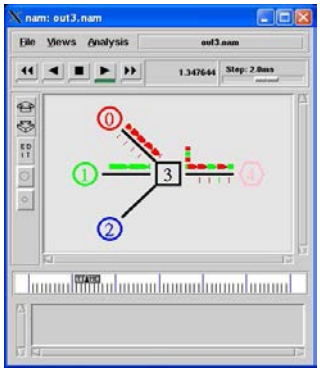

Figure 4: Packets send from source n1 to destination n4 through n3

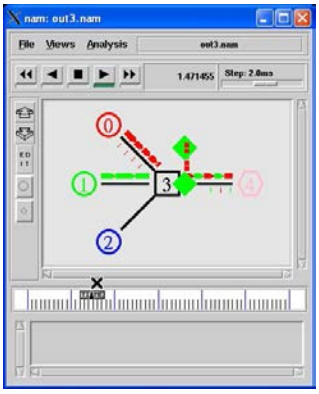

Figure 5: Few packets source n1 drop down at n3

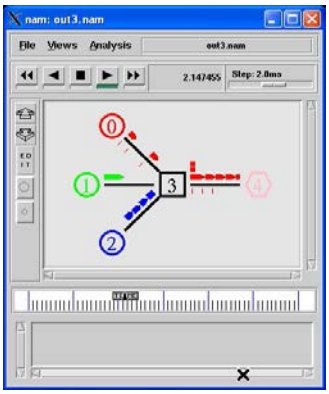

Figure 6: Packets send from source n2 to destination n4 through n3

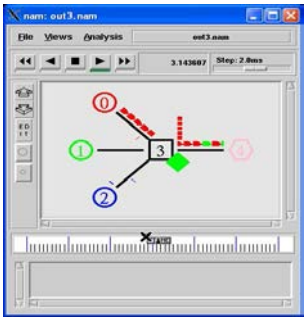

Figure 7: Packets would drop out when rate is in mb at n3

7. Outcome analysis when packets are not drop down through router

In this segment there is no packet would drop down at router node due to rate parameter is in K of exponential traffic as shown below:

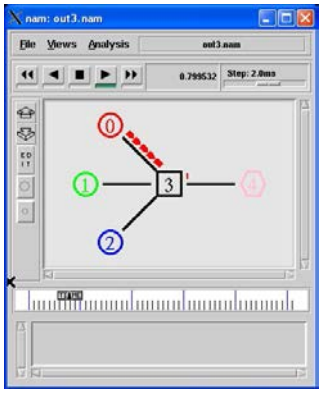

Figure 8: Packets send from source n0 to destination n4 through n3

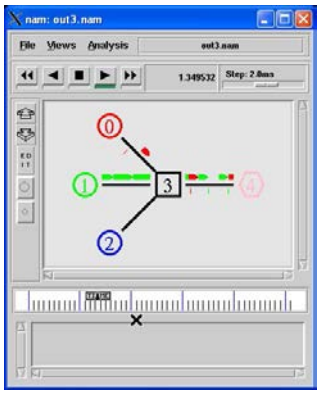

Figure 9: Packets send from source n1 to destination n4 through n3

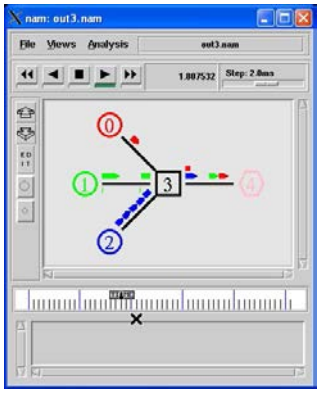

Figure 10: Packets send from source n1 to destination n4 through n3

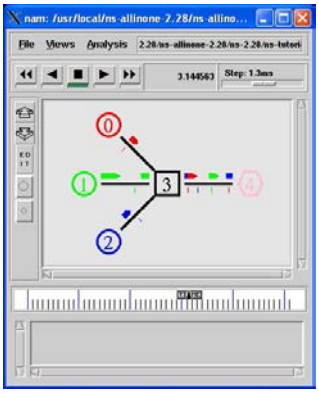

Figure 11: Packets would not drop out when rate is in K at n3

8. Conclusion

As the huge use of internet increases day by day so as safety anxiety is also elevate day by day in excess ofthe internet. Wehave analyzed the security threats of network faces and presented mean to model these attacks in Network Simulator-2. In this paper we discuss the network, its scenario and also it'spertaining to issues. We also talk about the types of attack which affects the network so that results will the unintended user access the authorized data by different methods as discussed. We also revise the types ofprotocols used on each layer of TCP/IP model and its associated issues by means of which data ishacked or alter by unauthorized user by illegal way from sender side, at the router side or even atdestination by attacking on the number of protocols used at each layer.

References:

[1] Y. Wang, G. Attebury, et al. "A survey of security issues in wireless sensor networks." Computer Science and Engineering.Vol.8, no. 2. 2006.

[2] E. Shi and A. Perrig, "Designing Secure Sensor Networks," Wireless Commun.Mag.,vol. 11, no. 6, pp. 38–43, Dec. 2004.

[3] N. Gura, A. Patel, et al. "Comparing elliptic curve cryptography and RSA on 8-bit CPUs."Cryptographic Hardware and Embedded Systems-CHES 2004, pp 925-943, 2004.

[4] M. Razzaque., S.Ahmad Salehi. Security and Privacy in Vehicular Ad- Hoc Networks: Survey and the Road Ahead. Wireless Networks and Security, Springer: 107-132, 2013.

[5] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, no. 5, pp. 521–34, Sept. 2002.

[6] H. Du, X. Hu, et al. "Energy efficient routing and scheduling for realtime data aggregation in WSNs." Computer communications.Vol.29, no. 17.3527-3535, 2006.

[7] X. Hung, et al. “An Energy-Efficient Secure Routing and Key Management Scheme for Mobile Sinks in Wireless Sensor Networks Using Deployment Knowledge,” Sensors,
Vol 8. 2008, 7753-7782

[8] L. Jialiang, Valois, F.; Dohler, M.; Min-You Wu; "Optimized Data Aggregation in WSNs Using Adaptive ARMA," Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference on pp.115-120, 18-25 July 2010.

[9] S. Zhu et al., “An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks,” Proc. IEEE Symp. Security and Privacy, Oakland, CA, pp. 259–71, May 2004.

[10] J. Ben-Othman, and B. Yahya. "Energy efficient and QoS based routing protocol for wireless sensor networks." Journal of Parallel and Distributed Computing 70(8), 849-857 2010.

[11] D.W. Carman, P.S. Krus, and B.J. Matt, “Constraints and approaches for distributed sensor network security”, Technical Report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, 2000.

[12] R. E. Shannon, “Introduction to the art and science of simulation,” in Proc. of the 30th conference on winter simulation (WSC’98), 1989

[13] http://ns2tutor.weebly.com/ns2-in-windows.html

[14] http://www.cs.berkeley.edu/~dawnsong/papers/sybil.pdf

[15]http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=44318 60

[16]http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.403.6592&rep=rep1&type=pdf

[17] http://ijaiem.org/Volume2Issue2/IJAIEM-2013-02-06-005.pdf

[18] http://sourceforge.net/projects/nsnam/files/

[19]http://www.ipcsit.com/vol35/003-CNCS2012-N010.pdf