UDC 004.738.5.057:004.94

J.N. DAVIES[*], P. COMERFORD[*], V. GROUT[*], M.V. VEROVKO[**], S.S. STASIUK[**]

COMPARISON OF NETWORK SIMULATORS IN IP NETWORKS

[*]Creative and Applied Research for the Digital Society (CARDS), Glyndŵr University, Wrexham, Ukraine
[**]Chernihiv National University of Technology, Chernihiv, Ukraine

Анотація. *При проведенні досліджень у галузі комп'ютерних мереж широкого розповсюдження набуло використання симуляторів для створення мережі для дослідження. Завдання вибору симулятора, що є найбільш придатним для конкретних досліджень, є досить складним, оскільки існує велика кількість мережевих симуляторів, що мають високі стандарти якості та пройшли перевірку часом. Завдання вибору симулятора також ускладнюється необхідністю усвідомлення достовірності отриманих результатів. У даній статті представлено дослідження симуляторів мереж Ns-2, Ns-3, Opnet, PacketTracer, Gns3 та Matlab. Порівняння роботи симуляторів проводилося на основі продуктивності IP-мереж із налаштованим захистом. Для отримання справедливих висновків результати роботи симуляторів порівнювались із результатами реальних фізичних мереж.*
Ключові слова: *симулятори мережі, емулятори мережі, ns-2, ns-3, Opnet, gns-3, Matlab, IP-мережа, захист.*

Аннотация. *При проведении исследований в области компьютерных сетей широкое распространение получило использование симуляторов для создания сети для исследований. Задача выбора симулятора, наиболее подходящего для конкретных исследований, является достаточно сложной, поскольку существует большое количество сетевых симуляторов, которые имеют высокие стандарты качества и прошли проверку временем. Задача выбора симулятора также осложняется необходимостью осознания достоверности полученных результатов. В данной статье представлено исследование симуляторов сетей Ns-2, Ns-3, Opnet, PacketTracer, Gns3 и Matlab. Сравнение работы симуляторов проводилось на основе производительности IP-сетей с настройками защиты. Для получения справедливых выводов результаты работы симуляторов сравнивались с результатами реальных физических сетей.*
Ключевые слова: *симуляторы сети, эмуляторы сети, ns-2, ns-3, Opnet, gns-3, Matlab, IP-сеть, защита.*

Abstract. *Under conducting the researches in the field of Computer Networksusage of simulators for network creation became widespread. The task of choosing a simulator that is most appropriate for specific researches is quite difficult because there are a large number of network simulators with high quality standards and have passed the test of time. The task of choosing simulator became more complicated because of necessity of awareness of obtained results. This paper presents the study of Ns-2, Ns-3, Opnet, Packet Tracer, Gns3 and Matlab networks simulators. Comparison of simulators was conducted on the base of efficiency of IP networks with security settings. To receive realistic conclusions the results of simulators performance have been compared with the results of real physical networks.*
Keywords: *network Simulators, network emulators, ns-2, ns-3, Opnet, gns-3, Matlab, IP networks, security.*

1. Introduction

Due to the influence of the Internet IP networks dominate all types of communication. The size and complexity of networks has greatly increased recently due to ubiquity of the Internet. This is required to cater for the large increase in bandwidth intensive applications such as VoIP and video streaming and to fulfil the need for enhanced security [1]. One of the major problems associated with network design is being able to predict what the effect of changes is on the network.

ISSN 1028-9763. Математичні машини і системи, 2014, № 4

To this end a series of tools have been built to address this issue. It would be ideal if the network could be duplicated since this would give very precise answers. Unfortunately because of the amount of equipment and hence cost involved in this it is not practical, so tools like network emulators and simulators are used. This leads to the question how accurate are the results obtained from these compared to a real network which is the purpose of this paper.

It is very important to identify the requirements of the research when selecting a tool since some tools are better in certain areas than others. Often the tools are not interchangeable between these functional areas. However where they are interchangeable it is expected that similar results should be obtained.

The particular area of interest for this research work was network performance in an IP network with multiple routing protocols across several domains and with security implemented inline with a policy. A part of the investigation of particular interest is the delays experienced by packets as they transverse a network.

When using different tools it is important to understand the terminology used e.g. node. Having said this it should still be possible to compare results for the same network. Additionally this paper compares the results with the results from a physically built real network.

The best definition found to define a network emulator is "to imitate the function of (another system), that allows the imitating system to accept the same data, execute the same programs, and achieve the same results as the imitated system and that for a network simulator is a representation of a problem, situation, etc., in mathematical terms, especially using a computer" [2].

Some tools that have been investigated fall into the category of emulators e.g. Cisco Packet Tracer. These are excellent tools for use in a teaching environment or for creating configurations for real networks but are incapable of producing reliable performance results for research purposes. So these have been omitted from this investigation.

Having investigated the simulators most commonly used in the submission of IEEE papers it has been decided to consider ns-2 Matlab and Opnet [3–4]. Additionally it was felt advantageous to include gns-3 an Open System simulator. Results obtained from running identical models in the simulators were compared the results obtained from a real network made up from Cisco routers.

Models chosen for this comparison were for a very simple network containing one IP routing device and measuring the delay for single ICMP packets across the device. Since this is the basic component of a network then comparing the simulator results with a real network will give some indication of the accuracy of the results when the network is scaled up. Following on from this the research work applies the same process to a far more complex network which is found in a typical IP network. Conclusions show the difficulty in producing the models as well as comparing the results.

2. Related work

The credibility of network simulator results has been an ongoing research topic for many years since the inception of computer-based network simulators.

An early study of simulation credibility is provided by Pawlikowski, which provides an overview of network simulation publications [5]. It provides a discussion on the issues which affect the credibility of simulation results, with the guidelines to help mitigate this. It was found that in many cases, an insufficient level of credibility was provided by simulation results. Recommendations included the need for repeatability in experiments and the capability to provide a faithful representation of original system functionality detailed information regarding random number generation and simulator type.

Heidemann provides best practices for simulation and model validation on the effects of scaling on it [6]. Some of the practices recommended in the study include a comparison of simu-

lation results with other representations such as laboratory experiments. In addition, it is recommended that the state of the simulation is examined as fully as possible, aided by visualization tools to detect possible invalid behaviour. Finally, the approaches for scaling simulations to large number of nodes are discussed such as parallelism using clusters and abstraction.

Lucio discussed network simulator suitability using experimental results from OPNET modeler and ns-2 [7]. In addition, results from an equivalent real network were gathered for comparison purposes. The experiment used constant bit rate (CBR) traffic and file transfer protocol (FTP) file transfers for each simulator. Despite reasonably accurate results with CBR traffic, FTP results with ns-2 lacked accuracy. This was attributed to the simplified model used for packet forwarding. However, it was found that OPNET gave more accurate results after fine tuning simulation parameters.

Jansen and McGregorperform simulation testing using real-world network stacks from open source operating systems such as Linux and FreeBSD [8]. Ns-2 and ns-3 have support for the network simulation cradle which allow such functionality. Experimental results showed that ns-2s TCP implementation did not match observed behaviour from any real network. Results from experiments using real-world network stacks did however produce results very close to a real network. It was also found that using real-world network stacks impaired simulation performance but not excessively so. In addition, it requires minimal change to simulation scripts which makes it viable to quickly replace the protocol implementation with its more accurate real network equivalent.

Rathod compared 3 network simulators: ns-2, OPNET and QualNet against a simple real network with results which were found to significantly differ from a real network, this was due to the blocking behavior of socket calls on a real network which could not be replicated via simulation [9]. Additionally, it was noted that realistic results required significant time in configuring simulation properties, several recommendations were provided for improving confidence in results.

Weigle, 2006 discusses the use of heavy tailed distributions in network simulations for modelling Internet traffic such as HTTP [10]. The improper usage of random number generators was found to lead to a high variability in simulation results. A number of approaches were proposed to deal with this problem.

Weingartner Carries out a performance and scalability comparison using ns-2, OMNet++, ns-3, SimPy and JiST/SWANS [11]. Findings reveal that only ns-2, OMNet++, ns-3, and JiST were capable of scaling to very large networks. Ns-3 was considered to show best overall performance and was recommended as a platform for developing new simulation models.

Perrone discuss the automation of computer network simulators [12]. Several automation tools were produced to mitigate the risk of unrealistic simulation results due to scripting errors, poor use of random number generators and parameter selection. The authors claim that such tools can improve manageability of large-scale simulations and provide more credible and consistent results.

Rahman provides a detailed comparison of the most common network simulation tools with the aim to equip researchers with the knowledge to choose the most suitable simulator for their requirements [13]. The authors use a number of criteria such as supported network models, platform and stored data format in order to aid the selection process.

Font provides a guide for developers wishing to create brand-new models for network simulation [14]. A comparison of the architecture and design of ns-2 and ns-3 was undertaken and several advantages of ns-3 such as complete use of C++ and strict adherence to software engineering practices are discussed. Ns-3 is recommended as a viable alternative for the development of new networking models.

3. Methodology

3.1. Simulators

Ns-2 is the most popular simulator used in the production of papers because it is Open System freely available with many contributors in the research community. However development for it has stagnated and it is now showing its age now being gradually replaced by the upgraded version ns-3. Since the basis of this comparison is IP networks and ns-2 is not particularly strong in this area it was decided to use ns-3 instead since the support for IP networks is far more advanced. For example, ns-2 does not offer full IPv4 or IPv6 support which is included in ns-3. Ns-3 also provides improved handling of multiple network interfaces and is aligned to be a more faithful representation of a real computer using a sockets-like API. Another major advantage of ns-3 is that there is a consistent programming language used throughout c++.

Opnet is a commercial product but educational licenses are freely available on condition that the research work is fed back into the suppliers. Opnet is very user friendly and handles IP networks and protocols very well. Configuration can be carried out either as a gui with pull down lists or using the command line. Most commercially available equipment is supported with their many options. Results can be obtained in many formats, the most popular being graphical.

The graphical network simulator (gns3) is based on Dynamips which allows Cisco and Juniper router configurations to be tested out. Additionally it has support for wireshark which means that similar test to those carried out on the real network could be carried out. Files saved by passing ICMP packets can be saved in a format that allowed them to be analyzed in the same way s the real network.

Matlab is a commercial product utilized in many academic areas e.g. maths, physics, engineering and computer networks. Again educational licenses are available. Since this tool has its origins in math and engineering it is a good tool for computing results for mathematical models of the network under consideration. This is a very flexible tool but does not have good support for IP networks.

3.2. Scenarios

Two scenarios were setup to do the comparison. Due to the diversity of the simulators it was felt that the scenarios should reflect the research area of interest as opposed to undertaking an in depth analysis of all functionality and features of each simulator. The particular area of interest was network performance in an IP network with multiple routing protocols across several domains and with security implemented inline with a policy.

3.3. Simulation parameters

When conducting the simulations it was necessary to produce a simulation which was as faithful to a real network as possible. When using OPNET, the same Cisco router models (2600) were used with the same 100 Mbps links. For ns-3, a script was created using the topology helpers with a speed of 100 Mbps and a channel delay of 2 ms.

4. Investigations

4.1. Basic IP network

The obvious place to start doing comparisons is by creating the simplest network and observing the results. This allows a baseline figure for delays across a single device to be obtained. The most basic IP network that has been considered is a simple network with one routing device. Simple ICMP packets were passed through the model and the real network to obtain the results. Figure 1 shows the topology of the used basic network.

4.1.1. Real basic IP network

Chosen basic network was configured in a laboratory using Cisco router and in second case with Linux configured router (machine running Fedora). ICMP packets were passed through the network; the packets were captured in Wireshark and then analyzed to provide the results.

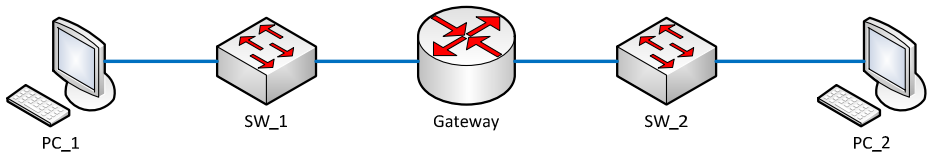

Fig. 1. Basic network topology

4.1.2. Models of basic IP network

Ns-3. One of the major benefits of using ns-3 is the research community that can help reduce the work involved in setting up the simulator and creating models. Modelling IP networks using ns-3 is a great improvement on ns-2 due to the availability of Topology Helpers. This allows the connecting of network devices to nodes, the assigning IP addresses etc. to be carried very easily. Additionally there is a GUI available called ns-3-generator that is intended to speed up the creation of large networks. This model had to be modified before it could be used to pass the required traffic. Traffic was created using the UDP Echo Server Helper which enabled ICMP packets to be sent across the network. The capturing of the data and analysis of the packets was carried out using the link to Wireshark.

Opnet. Due to the structure and design of Opnet it was relatively easy to create models of network infrastructures. It was also easy to set up traffic models. However these traffic models did not necessary create exactly the traffic as required which is probably due to one of the main uses of the simulator to be able to create large volumes of traffic. Forcing the simulator to transmit a small number of single packets was easy to configure but were not transmitted as expected.

Gns-3. The results of the simulation have high similarity to the physical Cisco network.

MatLab. Since a router is a specialized computer a basic equation can be defined by including parameters for the hardware (D_h), the operating system (D_{os}), the application configuration (D_a) and Services (D_s). The model can be described by the equation Router Delay $(D_r) = D_h + D_{os} + D_a + D_{s\ (ref)}$. This can be modelled in Matlab relatively easily however the problem being what functions or values should be used for the calculation. This model would rely on taking values from measurement made on the real network.

4.2. Basic IP network with security

Similar test were carried out to the network but this time Access Control Lists (ACLs) were enabled.

4.2.1. Real basic IP network with security

It was and easy process to configure security by way of adding ACLs to the real Cisco network. A similar process was used to configure security using Iptables on the Linux machine. ICMP packets were used for the testing and Wireshark used to capture and analyze the delays.

4.2.2. Models of basic IP network with security

Ns-3. Ns-3 at present does not have a standard script that can be used to take account of internal delays within nodes. However there are mechanisms in place that could be used to implement this by writing c++ code. A mechanism for handling IPSec which is an interface between TCP and the IP layer it appears could be exploited to do this. Due to the time constraints this was not attempted.

Opnet. There are many models available in Opnet for routers dependent on manufacturer, model number and features enabled. For these tests the Cisco 2600 router, which was the device used in the real network measurements, was used for the Opnet model. Device does have the possibility to configure forwarding rates etc. This is easy to change but it does not help in understanding what values to use. Due to the inconsistency in the traffic flows highlighted earlier then this was not attempted.

Gns-3. The configuration of ACL was performed easily and results of the simulation have high similarity to the physical Cisco network.

Matlab. Earlier work has shown that the equation used previously needs to be modified to include the ACL delays.So functions reflecting the introduced type of ACL (Dta) used and the number of rules in an ACL Dnr and the protocol delayD_p. The equation now becomes Router *Delay* $(D_r) = D_h + D_{os} + D_a + D_s + D_{ta} + D_{nr} + D_p$. Again the functions or values for these parameters have to be obtained from measurements of a real network.

4.3. Results for Basic IP network

The results for basic network are presented in table 1. Table 1 contains a summary of the results for the delay across routers and shows the % difference to the values measured in the real network.

Table 1. Summary of Router Delays for Simulations against Real Networks

	No Security	With Security	%
Real Network (Cisco)	150mSecs	320mSecs	0% : 0%
Real Network (Linux)	70 mSecs	90 mSecs	-53% : -72%
Ns-3	4380 mSecs	N/A	2820% : N/A
Opnet	600 mSecs	N/A	300% - N/A

When comparing the results obtained from a real network using Cisco equipment with that of a real network using a Linux machine, considerable discrepancies were observed. For the Linux network, delays were ~50% less than the equivalent Cisco network; this was exacerbated with the addition of security. This discrepancy could be attributed to underlying hardware architecture of the Linux machine however it would be beneficial to repeat the tests a number of times using both a basic network and a more complex IP network consisting of several nodes.

4.4. Complex IP network

When investigating the design of a complete network it is necessary to ensure all the configuration components are available. Figure 2 is a simplified diagram to show the actual route through the network. This scenario involves – setting IP addressing, Management and Security Policy, designing physical network including diagram, designing Wide Area Network requirements including backup routes, selecting and designing IP and AS Addressing, selecting and designing the required hardware and software, Designing issues associated with the internet and intranet servers, designing Routing protocol requirements, designing Management issues.

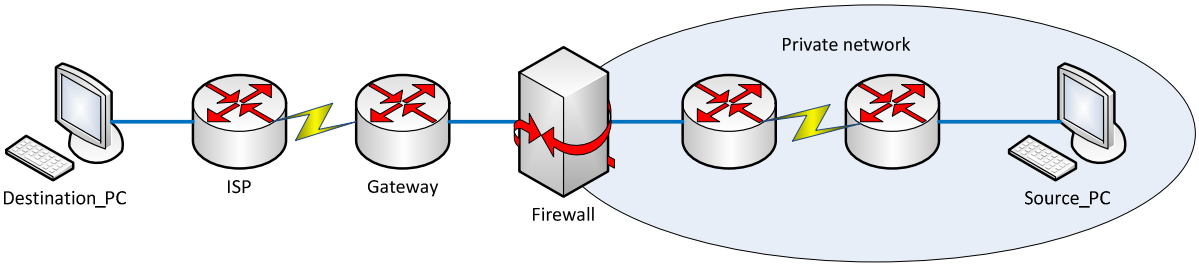

Fig. 2. Complex IP Network

Interior (OSPF) and exterior routing protocols (BGP) have been used to select the route. Additionally Network Address Translation (NAT) has been configured and links were installed to provide redundancy. Results were produced without a configuration in a firewall i.e. no security and then the further measurements were made with the firewall configure i.e. with security.

4.4.1. Real complex IP network

Complex network was configured in a laboratory using Cisco routers. An advanced configuration, produced in the laboratory, is about the limit in terms of size and complex that can be produced in this environment. Also creating controlled varying levels of traffic was not an easy task. Producing the same network in the Linux environment is not really a problem and should produce similar results to the real network taking into account the % differences. But this work was not carried out due to availability of equipment and time issues.

4.4.2. Models of complex IP network

Ns-3. Configuration of the ns-3 model for this network was carried out so that a comparison of the results could be gained.

Opnet. Creating the model for simulator was extremely easy and the ability to create all types of traffic was a distinct advantage however as discussed earlier the ability to control the traffic made it unsuitable for this comparison and hence no results were produced.

Gns3. Gns3 was also used with the configurations created for the real network and produced reliable results.

MatLab. The results of MatLab are similar to the real network, since the created model is mathematical.

4.4.3. Results for complex IP network

The results for complex network are presented in table 2. Table 2 contains a summary of the results for the delay across routers and shows the % difference to the values measured in the real network.

Table 2. Summary of Router Delays for Simulations against Real Networks

	No Security	With Security	%
Real Network (Cisco)	920msecs	1086msecs	18%
Ns-3	12049msecs	N/A	1200% – N/A
Gns-3	1073msecs	51574msecs	16% – 4600%

5. Conclusions

When starting a piece of research work it is necessary to understand the scope of the work to be carried out and to understand the amount of work needed to create models.

If the results required can be obtained using a small network with a limited amount of traffic then building this in the lab is the optimum solution. However as the network size and traffic size increases then simulators are clearly the approach to take. The results obtained by using simulators can be hit and miss since this work shows that large discrepancies can be observed.

It is not reasonable to assume that the simulators used are going to support exactly the area that is of interest and therefore it is likely that specialized code may well have to be written to support the work. Support of simulators by the research community is a definite advantage since it helps identify people working in the same area. It is essential to make sure that the simulator chosen has the ability to accept the code without having to do major rewrites.

The only sure way of guaranteeing that the results obtained reflect what is observed in real networks is to either use a mathematical model and implement it in Matlab or by creating an application.

The approach taken to compare the results obtained from the simulators is using Wireshark as the packet collector and analyzing the results obtained. This may not be the optimum approach for recording the times for some simulators and therefore each simulator should be investigated independently. It is envisage that a great improvement in the accuracy of results could be obtained by undertaking this work. Unfortunately this could take a substantial period of time.

A deeper investigation into each simulator of the support for internal delays experienced by routers should be undertaken. It would be desirable to develop a more complex mathematical model which is faithful in its behaviour to that found in real networks. This model could then be incorporated within existing simulators such as OPNET and ns-2/ns-3 to improve the credibility of simulation results. It is clear that the hooks are available in the simulators for this however the exploitation is not obvious.

REFERENCES

1. Troubleshooting chronic conditions in large IP networks / A. Mahimkar, J. Yates, Y. Zhang [et al.] // Proc. of the 2008 ACM CoNEXT Conference (CoNEXT '08). – ACM, NY, USA, 2008. – P. 1 – 12.
2. Free Dictionary Website [Електронний ресурс]. – Режим доступу:http://www. thefreedictionary.com.
3. Sarkar N.I. A Review of Simulation of Telecommunication Networks: Simulators, Classification, Comparison, Methodologies, and Recommendations / N.I. Sarkar, S.A. Halim // Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications. – 2011. – P. 10 – 17.
4. A comparison of TCP behaviour at high speeds using ns-2 and Linux / M. Bateman, S. Bhatti, G. Bigwood [et al.] // Proc. of the 11th communications and networking simulation symposium (CNS '08). – 2008. – P. 30 – 37.
5. Pawlikowski K. On credibility of simulation studies of telecommunication networks / K. Pawlikowski, H.-D.J. Jeong, J.S.R. Lee // IEEE Communications. – 2002. – Vol. 40, N 1. – P. 132 – 139.
6. Heidemann J. Expanding confidence in network simulation/ J. Heidemann, K. Mills, S. Kumar // IEEE Network Magazine. – 2001. – Vol. 15. – P. 58 – 63.
7. Opnet modeler and ns-2 – comparing the accuracy of network simulators for packet-level analysis using a network testbed / G.F. Lucio, M. Paredes-Farrera, E. Jammeh [et al.] // WSEAS Transactions on Computers. – 2003. – Vol. 2, N 3. – P. 700 – 707.
8. Jansen S. Simulation with Real World Network Stacks / S. Jansen, A. McGregor // Proc. of the 2005 Winter Simulation Conference. – Orlando, Florida, 2005. – December. – P. 2454 – 2463.
9. Rathod P. Bridging the gap between the reality and simulations: An Ethernet case Study / P. Rathod, S. Perur, R. Rangarajan // IEEE 9th International Conference on Information Technology (ICIT'06). – Bhubaneswar, Mumbai, India, 2006. – December. – P. 52 – 55.
10. Weigle M.C. Improving Confidence in Network Simulations / M.C. Weigle // WSC 06. Proc. of the Winter Simulation Conference. – 2006. – 3-6 December. – P. 2188 – 2194.

11. Weingartner E. A Performance Comparison of Recent Network Simulators / E. Weingartner, H. vom Lehn, K. Wehrle // ICC '09. IEEE International Conference on Communications. – 2009. – 14-18 June. – P. 1 – 5.
12. On the automation of computer network simulators/ L.F. Perrone, C. Cicconetti, G. Stea [et al.] // Proc. of the 2nd International Conference on Simulation Tools and Techniques (Simutools '09). – Rome, Italy, 2009. – P. 1 – 10.
13. Rahman M.A. Network modeling and simulation tools / M.A. Rahman, A. Pakstas, F.Z. Wang // Simulation Modelling Practice and Theory. –2009. –Vol. 17, Issue 6. – P. 1011 – 1031.
14. Architecture, design and source code comparison of ns-2 and ns-3 network simulators / J.L. Font, P. Inigo, M. Dominguez [et al.] // Proc. of the 2010 Spring Simulation Multiconference (SpringSim '10). – ACM, New York, NY, USA, 2010. – P. 1 – 8.

Стаття надійшла до редакції 02.10.2014