Active Traffic Monitoring for Heterogeneous Environments

Hélder Veiga, Teresa Pinho, José Luis Oliveira, Rui Valadas,
Paulo Salvador, and António Nogueira

University of Aveiro/Institute of Telecommunications - Campus Santiago, Aveiro, Portugal
{jlo, rv}@det.ua.pt, {hveiga, salvador, nogueira}@av.it.pt

Abstract. The traffic management of IP networks faces increasing challenges, due to the occurrence of sudden and deep traffic variations in the network, which can be mainly attributed to the large diversity of supported applications and services, to the drastic differences in user behaviors, and to the complexity of traffic generation and control mechanisms. In this context, active traffic measurements are particularly important since they allow characterizing essential aspects of network operations, namely the quality of service measured in terms of packet delays and losses.

The main goal of the work presented in this paper is the performance characterization of operational networks consisting in heterogeneous environments including both wired and wireless LANs, using active measurements. We propose a measurement methodology and its corresponding measurement platform. The measurement methodology is based on the One-Way Active Measurement Protocol (OWAMP), a recent proposal from the Internet2 and IETF IPPM groups for measuring delays and losses in a single direction. The measurement platform was implemented, tested and conveniently validated in different network scenarios.

Keywords: Network management, traffic monitoring, active measurement, OWAMP.

1 Introduction

The relevance of traffic monitoring in the global management of IP networks has been growing due to the recent acknowledgment that sudden and deep traffic variations demand for frequent traffic measurements. This peculiar behavior of network traffic can be mainly attributed to the combination of different factors, like the great diversity of supported applications and services, different user's behaviors and the coexistence of different mechanisms for traffic generation and control.

Traffic monitoring systems can be classified in active and passive ones [1], [2], [3]. Passive systems simply perform the analysis of the traffic that flows through the network, without changing it. Usually, they are used to identify the type of protocols involved and to measure one or more characteristics of the traffic that flows through the measurement point, like the average rate, the mean packet size or the duration of the TCP connections. Nowadays, there are several passive monitoring systems, like for example NeTraMet [4] and NetFlow [5]. Active systems insert traffic directly into the network. Usually, they are intended to provide network performance statistics between two distinct measurement

P. Lorenz and P. Dini (Eds.): ICN 2005, LNCS 3420, pp. 603–610, 2005.

points, like for example mean packet delay and packet loss ratio. Those statistics can be one-way statistics, when they refer to a single direction of traffic flow, and round-trip statistics, when they refer to traffic that flows in both directions. Active systems require the synchronization of the involved measurement points, using for example GPS (Global Positioning System) or NTP (Network Time Protocol).

The IETF IPPM (IP Performance Metrics) group established in the last few years a set of recommendations in order to assure that measurement results obtained from different implementations are comparable, namely regarding measurements of one-way packet delays and losses [6], [7]. However, these recommendations do not address the interoperability of the measurement elements, that is, the possibility of having traffic senders and receivers that belong to different administrative domains and are developed by different entities. OWAMP is a proposal for a one-way active measurement protocol that intends to solve this problem [8].

In this work, we intend to perform a set of active measurements in a real operational network consisting in a heterogeneous environment that includes both wired and wireless LANs. Thus, instead of using available tools (like PING, for example), some of them with a limited scope of applications, we have decided to implement a complete measurement platform (freely available at `http://www.av.it.pt/JOWAMP/`). In order to guarantee its compliance with other available platforms, its measurement methodology is based on the OWAMP protocol.

The paper is structured in the following way: section 2 describes the architecture and the operational details of the OWAMP protocol, that forms the basis of the implemented solution; section 3 presents the details of the implemented solution; section 4 presents the active measurements experiments, and their corresponding scenarios, that we want to carry out in this work; section 5 presents and discusses the results obtained from its application to the defined measurement scenarios and, finally, section 6 presents the main conclusions.

2 One-Way Active Measurement Protocol

The One-Way Active Measurement Protocol (OWAMP) is a recent proposal from the Internet2 group, developed under the scope of the End-to-End Performance Initiative project [9], [10], for performing active measurements in a single direction. This proposal is also promoted by the IETF IPPM work group [8].

The OWAMP architecture, shown in figure 1, is based on two inter-dependent protocols, the OWAMP-Control and the OWAMP-Test, that can guarantee a complete isolation between client entities and server entities. The OWAMP-Control protocol runs over TCP and is used to begin and control measurement sessions and to receive their results. At the beginning of each session, there is a negotiation about the sender and receiver addresses, the port numbers that both terminals will use to send and receive test packets, the instant of the session beginning, the session duration, the packets size and the mean interval between two consecutive sent packets (it can follow an exponential distribution, for example).

The OWAMP-Test runs over UDP and is used to exchange test packets between sender and receiver. These packets include a Timestamp field that contains the time

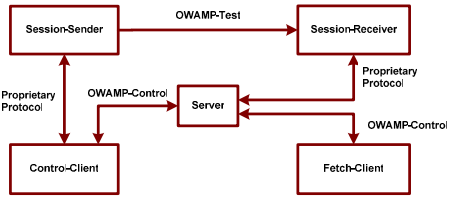

Fig. 1. OWAMP architecture

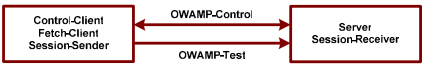

Fig. 2. OWAMP simplified architecture

instant of packet emission. Besides, packets also indicate if the sender is synchronized with some exterior system (using GPS or NTP) and each packet also includes a Sequence Number.

OWAMP supports test packets with service differentiation: DSCP (Differentiated Services Codepoint), PHB ID (Per Hop Behavior Identification Code) or Best-effort. Additionally, OWAMP supports some extra facilities like cypher and authentication for the test and control traffic, intermediary elements called Servers that operate as proxies between measurement points and the exchange of seeds for the generation of random variables that are used in the definition of transmitted test flows. The OWAMP specification also allows the use of proprietary protocols (that can be monolithic or distributed programming interfaces) in all connections that do not compromise interoperability.

The OWAMP architecture includes the following elements:

- Session-Sender: the sender of the test packets;
- Session-Receiver: the receiver of the test packets;
- Server: the entity that is responsible for the global management of the system; it can configure the two terminal elements of the testing network and receive the results of a test session;
- Control-Client: a terminal system that programs demands for test sessions, triggers the beginning of a session set and can also finish one or all ongoing sessions;
- Fetch-Client: a terminal system that triggers the demands for results of test sessions that have already ended or are still running.

A network element can carry out several logical functions at the same time. For example, we can have only two network elements (figure 2): one is carrying out the functions corresponding to a Control-Client, a Fetch-Client and a Session-Sender and the other one is carrying out the functions corresponding to a Server and a Session-Receiver.

3 J-OWAMP: A System Based on OWAMP

In order to create an innovator platform for active measurements, that can also represent a basis for the development and test of new algorithms and models, we built a system designated by J-OWAMP (that stands for Java implementation of OWAMP) that corresponds to the analogous of the OWAMP model. The developed system corresponds

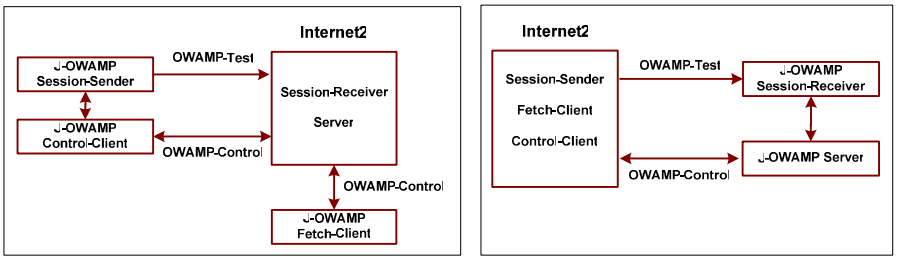

Fig. 3. Configuration of the compliance tests

to the OWAMP most general architecture, depicted in figure 1, allowing the definition of only one client and one server in the network (possibly installed in machines with the highest processing capacity) and the installation of senders and receivers in any machine of the network, which leads to a lower processing impact. In this way, the network manager can perform tests all over the network controlled from a single machine, which is not possible in the simplified scenario of figure 2.

Structure and Implementation - The J-OWAMP system was developed in Java because this language presents a set of favorable characteristics, like semantic simplicity, portability and a set of classes that greatly simplify the construction of distributed applications.

The structure of the system is based on two levels: Messages and Entities. At the Messages level, we developed a set of classes corresponding to each one of the data packets that are exchanged in the OWAMP protocol. A particular class, Packet, is the basis for all messages (derived classes). At the Entities level, a set of classes was developed in order to implement the five elements of the OWAMP architecture: Client, Server, Session-Sender, Session-Receiver and Fetch-Client.

Compliance Tests - In order to guarantee the compliance of the developed system with the OWAMP proposal, we have performed a set of tests involving an implementation (for a UNIX platform) developed by the Internet2 group and publicly available in [9]. The tests were carried out in the private IT-Aveiro network using, in a first experiment, the J-OWAMP modules as the client, monitor and sender modules and using the Internet2 modules as server and receiver modules and, in a second experiment, the J-OWAMP and Internet2 modules in the reverse order (figure 3).

The communication between the J-OWAMP modules (developed in Java language) and the Internet2 modules (developed in C language) was correctly established, in both directions. Using the Ethereal traffic analyzer, we have verified that the control messages and the test packets are correctly exchanged, as specified in the protocol.

4 Measurement Scenarios

Before carrying out active traffic measurements in a real network involving an heterogeneous environment, we have first established a laboratorial measurement setup to test the developed measurement solution in a more controllable environment.

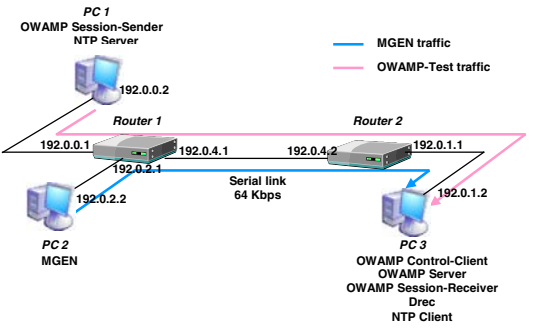

Fig. 4. Network corresponding to the first measurement scenario

Laboratorial Setup - The laboratorial measurement setup is illustrated in figure 4. Routers 1 and 2 are connected through a serial link configured with a transmission capacity of 64 Kb/s and three networks are configured with the following structure: network 192.0.0.0, that contains PC1 running the OWAMP sender; network 192.0.2.0, that contains PC2 running the traffic generator MGEN and network 192.0.1.0 that contains PC3 where we have previously installed the OWAMP client, server and receiver elements as well as a receiver (Drec) of the traffic generated by the MGEN application running on PC2. The service discipline for all queues belonging to the serial interfaces of routers 1 and 2 is FIFO. PCs 1 and 3 are synchronized via NTP.

Using this scenario, we want to measure and study the packet delays that occur in the queuing system of Router 1 as a function of the traffic load in the serial link between Routers 1 and 2. In this way, we have configured the MGEN application to generate traffic according to a Poisson distribution and send it to PC3 (using the serial link). Using the sender installed in PC1 and the receiver installed in PC3 we were able to measure the packet delay values that occurred in the queue of the Router 1 serial interface, for different values of the traffic load. Arrows represented in figure 4 show the directions that are followed by (i) the traffic generated by MGEN and (ii) the test packets generated by the J-OWAMP measurement system.

University of Aveiro (UA) Wireless Network - The network corresponding to this scenario is illustrated in figure 5. In order to evaluate the performance of accessing the UA wireless network from the students' residences, a set of measurements were conducted between a PC located at the laboratory of Institute of Telecommunications (IT), named Lab PC, and another one located at a students' residence of the University campus, named Residence PC. We measured and studied the traffic that flows between the Residence and the Lab PCs, in both directions. The client, server and receiver were installed in the PC that receives the test packets and the sender was installed in the PC responsible for sending the packets. Both PCs are synchronized via NTP. Since Internet access from the student's residences is performed through the UA network, traffic in the downstream direction includes mainly the downloads that are made from the Internet to the residences.

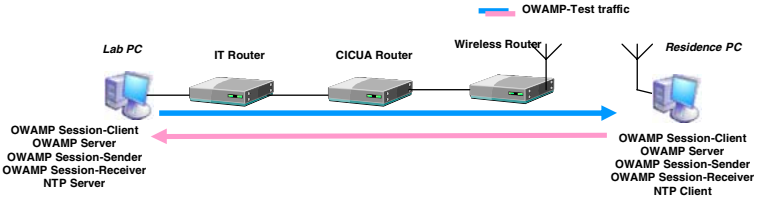

Fig. 5. Network corresponding to the second measurement scenario

All tests were performed in a 24 hours period. In each hour, sets of 10 tests (including both packet delay and loss) were performed, making a total of 240 tests. In each group, the tests beginning instants were separated by 2 minutes. All tests lasted for 1 minute and consisted in sending 60 packets of 14 bytes each, at an average rate of 1 packet/second. In order to conveniently characterize the packet average delay and packet loss ratio, we have calculated 90% confidence intervals based on the 10 average values obtained in each test belonging to a group of 10 tests.

5 Results

First Scenario - Figures 6 and 7 present the results corresponding to the packet delay and packet loss tests, respectively, that were carried out for the first scenario, for different rates of the MGEN generated traffic. From the analysis of the obtained results we can verify that, as expected, there is an increase in packet delays and losses with increasing network load: for network load values that are far from the maximum value supported by the serial link (64 Kb/s) there are no packet losses, however, packet loss values increase very fast as network load approaches the limit load supported by the serial link that connects both routers.

Second Scenario - For this scenario, the results of the average packet delay and packet loss ratio for the upstream direction are presented in figures 8 and 9, respectively,

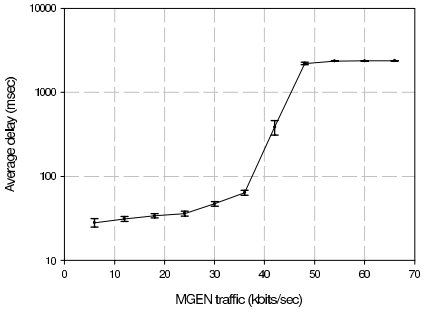

Fig. 6. Results of the first scenario: average packet delay versus MGEN generated traffic

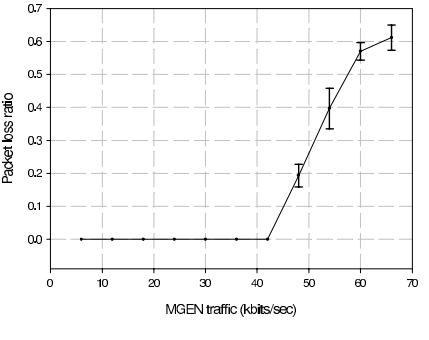

Fig. 7. Results of the first scenario: packet loss ratio versus MGEN generated traffic

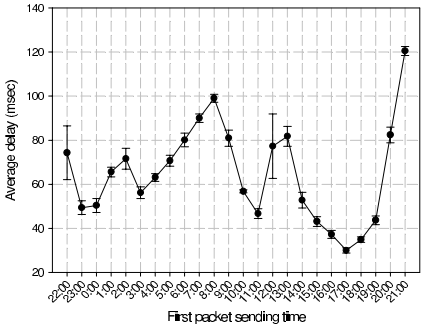

Fig. 8. Results of the second scenario, upstream direction: average packet delay versus first packet sending time

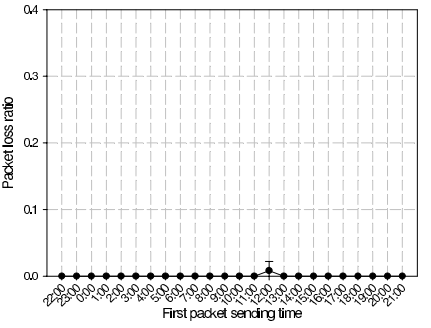

Fig. 9. Results of the second scenario, upstream direction: packet loss ratio versus first packet sending time

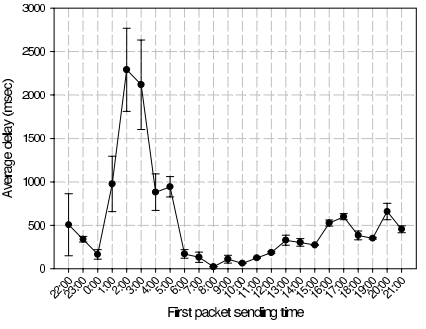

Fig. 10. Results of the second scenario, downstream direction: average packet delay versus first packet sending time

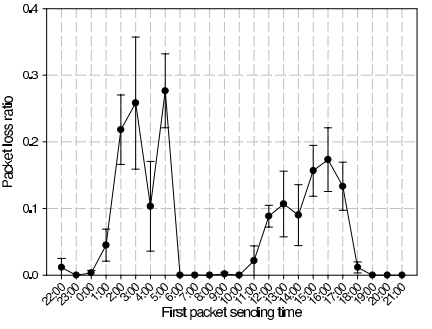

Fig. 11. Results of the second scenario, downstream direction: packet loss ratio versus first packet sending time

and the analogous results corresponding to the downstream direction are presented in figures 10 and 11, respectively. From the analysis of these results we can verify that delays corresponding to the upstream direction vary between approximately 30 and 120 milliseconds, being much smaller that the corresponding values for the downstream direction that vary between 20 and 2300 milliseconds. Packet losses are null in the upstream direction but have non zero values in the downstream direction. As expected, there is a direct relationship between packet delays and losses: higher packet delay values also correspond to higher packet loss values. In the performed tests, downstream traffic was much higher than upstream traffic, which is a typical result for these kind of scenarios. In the downstream direction, the highest delay and loss values were observed in the night and afternoon (between 2PM and 6PM) periods. These values can be attributed to the use of file sharing applications. In the night period, the utilization level of these applications is even higher, mainly from the students' residences. In the afternoon period,

the utilization of these applications is mainly performed from the library building, which is also covered by the wireless network.

6 Conclusions

Traffic monitoring through active measurements is having an increasing relevance in the IP networks management context, since it enables to directly monitor quality of service parameters, like for example average packet delay and packet loss ratio. The IETF IPPM group has recently proposed a protocol for conducting active traffic measurements in a single direction, the OWAMP (One-Way Active Measurement Protocol).

This paper presented a solution (based on the OWAMP protocol) for performing active measurements in a heterogeneous network, including its implementation, validation and some examples that allow a further exploration of the OWAMP protocol. The proposed system was developed in Java language, mainly due to its portability. Several compliance tests with the only known implementation (from the Internet2 group) were successfully conducted. The system was evaluated through a set of performed tests, conducted both in a laboratorial environment and in a real operational network. The obtained results show that the implemented system is a very useful active measurement tool that can be used for characterizing quality of service in IP networks.

Acknowledgments. This research was supported by Fundação para a Ciência e a Tecnologia, project POSI/42069/CPS/2001, and European Commission, Network of Excellence EuroNGI (Design and Engineering of the Next Generation Internet).

References

1. A.Pasztor, D.Veitch: High precision active probing for internet measurement. In: Proceedings of INET'2001. (2001)
2. Corral, J., Texier, G., Toutain, L.: End-to-end active measurement architecture in ip networks (saturne). In: Proceedings of Passive and Active Measurement Workshop PAM'03. (2003)
3. Grossglauser, M., Krishnamurthy, B.: Looking for science in the art of network measurement. In: Proceedings of IWDC Workshop. (2001)
4. NeTraMet home page: (http://www.auckland.ac.nz/net/netramet/)
5. White Paper - NetFlow Services and Applications: (http://www.cisco.com/warp/public/cc/pd /iosw/ioft/neflct/tech/napps_wp.htm)
6. Almes, G., Kalidindi, S., Zekauskas, M.: RFC 2679: A one-way delay metric for ippm (1999)
7. Almes, G., Kalidindi, S., Zekauskas, M.: RFC 2680: A one-way packet loss metric for ippm (1999)
8. Shalunov, S., Teitelbaum, B., Karp, A., andMatthew J. Zekauskas, J.W.B.: A one-way active measurement protocol (owamp), internet draft (2004)
9. Internet2 End-to-End Performance Initiative: (http://e2epi.internet2.edu)
10. Boyd, E.L., Boote, J.W., Shalunov, S., Zekauskas, M.J.: The internet2 e2e pipes project: An interoperable federation of measurement domains for performance debugging (2004)