UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

JÉFERSON CAMPOS NOBRE

Decentralized Detection of Violations of Service Level Agreements using Peer-to-Peer Technology

Thesis presented in partial fulfillment
of the requirements for the degree of
Doctor of Computer Science

Advisor: Lisandro Zambenedetti Granville

Porto Alegre
July 2016

CIP – CATALOGING-IN-PUBLICATION

Nobre, Jéferson Campos

Decentralized Detection of Violations of Service Level Agreements using Peer-to-Peer Technology / Jéferson Campos Nobre. – Porto Alegre: PPGC da UFRGS, 2016.

175 f.: il.

Thesis (Ph.D.) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação, Porto Alegre, BR–RS, 2016. Advisor: Lisandro Zambenedetti Granville.

I. Granville, Lisandro Zambenedetti. II. Título.

“The secret of happiness is: find something more important than you are and dedicate your life to it.”

— Daniel Dennett

ACKNOWLEDGMENT

I would like to thank to my mother Maria for the support during all my life, for encouraging me on my projects (even in the most difficult moments), and for always teaching me how to be a good person;

To my dear Maíra, I would like to thank for all the love, affection, understanding, companionship, and patience;

To my Ph.D. Advisor, Professor Lisandro Zambenedetti Granville, I would like to thank for all the collaboration, wisdom, friendship, and the valuable lessons which contribute to my professional and personal development;

I also would like to thank to the Professors Luciano Paschoal Gaspary, Liane Margarida Rockenbach Tarouco, Marinho Pilla Barcellos, Alberto Egon Schaeffer Filho, and Juergen Rochol from the Computer Networks Group (UFRGS) for all the lessons, experiences, and opportunities;

To all colleges from the Computer Networks Group (UFRGS), I would like to thank for the support, experiences, technical and philosophical discussions, and brotherhood.

To Cisco Systems, I would like to thank for the great opportunity of doing my sandwich Ph.D in one of the most important network equipment vendors;

I would like to thank the Institute of Informatics of the Federal University of Rio Grande do Sul for the infrastructure provided for the graduate students;

Finally, I also would like to thank the Brazilian Funding Agencies, CAPES and CNPq, for the financial support during my Ph.D. and sandwich Ph.D.

CONTENTS

LIST OF ABBREVIATIONS AND ACRONYMS

AgS	Aggregation Service
ALR	Application Layer Routing
AN	Ambient Network
ANM	Autonomic Network Management
ANIMA	Autonomic Networking Integrated Model and Approach
ANOVA	Analysis of Variance
API	Application Programming Interface
AS	Autonomous System
CBR	Case-Based Reasoning
CNP	Contract Net Protocol
DC	Data Center
DHT	Distributed Hash Table
DITA	Distributed IP Traffic Analysis
DMTF	Distributed Management Task Force
DNA	Distributed Network Agent
DNM	Distributed Network Management
FCAPS	Fault, Configuration, Accounting, Performance, Security
I-D	Internet-Draft
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ILP	Integer Linear Program
IP	Internet Protocol
IPSLA	Internet Protocol Service Level Agreement
IPFIX	IP Flow Information eXport

IPPM	IP Performance Metrics
IRTF	Internet Research Task Force
ITU-T	International Telecommunication Union - Telecommunication standardization sector of ITU
JXTA	Juxtapose
LEISURE	Load-EqualIzed meaSUREment
LLM	Lower Level Manager
LMAP	Large-Scale Measurement of Broadband Performance
LP	Linear Programming
MA	Mobile Agent
MA	Measurement Agents
MAS	Multi-Agent System
MbD	Management by Delegation
MIB	Management Information Base
MILP	Mixed Integer Linear Programming
MINLP	Mixed-Integer Non-Linear program
M-Lab	Measurement Lab
MLM	Middle Level Manager
MMPR	Measurement-aware Monitor Placement and Routing
NE	Network Element
NMRG	Network Management Research Group
NMS	Network Management System
NSQM	Network and Service Quality Measurement
OAM	Operations, Administration, and Maintenance
OSI	Open System Interconnect
OWAMP	One-Way Active Measurement Protocol

P2P	Peer-to-Peer
P2PBNM	P2P-Based Network Management
PBNM	Policy Based Network Management
PDN	Policy Decision Node
PDP	Policy Decision Point
PEP	Policy Enforcement Point
perfSONAR	PERFormance Service Oriented Network monitoring ARchitecture
PMT	Policy Management Tool
POP	Point of Presence
PoP	Peers of Peers
PRISM	PRecision-Integrated Scalable Monitoring
QoS	Quality of Service
RELOAD	REsource LOcation And Discovery
RFC	Request For Comments
RPM	Real-time Performance Monitoring
RTFM	Realtime Traffic Flow Measurement
SATOs	Service-aware Adaptive Transport Overlays
SLA	Service Level Agreement
SLO	Service Level Objective
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SMC	Self-Managed Cell
SPAND	Shared Passive Network Performance Discovery
SPoF	Single Point of Failure
TCP	Transmission Control Protocol
TLM	Top Level Manager

TNM	Telecommunications Management Network
ToS	Type of Service
TWAMP	Two-Way Active Measurement Protocol
UFRGS	Universidade Federal do Rio Grande do Sul
VoIP	Voice over Internet Protocol
SDIMS	Scalable Distributed Information Management System
SLA	Service Level Agreement
SLO	Service Level Objective
YAF	Yet Another Flowmeter
WG	Working Group

LIST OF TABLES

LIST OF FIGURES

LIST OF ALGORITHMS

ABSTRACT

Critical networked services established between service provider and customers are expected to operate respecting Service Level Agreements (SLAs). An interesting possibility to monitor such SLAs is using active measurement mechanisms. However, these mechanisms are expensive in terms of network devices resource consumption and also increase the network load because of the injected traffic. In addition, if the number of SLA violations in a given time is higher than the number of available measurement sessions (common place in large and complex network infrastructures), certainly some violations will be missed. The current best practice, the observation of just a subset of network destinations driven by human administrators expertise, is error prone, does not scale well, and is ineffective on dynamic network conditions. This practice can lead to SLA violations being missed, which invariably affect the performance of several applications. In the present thesis, we advocated the use of Peer-to-Peer (P2P) technology to improve the detection of SLA violations. Such use is described using principles to control active measurement mechanisms. These principles are accomplished through strategies to activate measurement sessions. In this context, the major contributions of this thesis are: i) An approach to improve the detection of SLA violations through the steering of the activation of active measurement sessions using local and remote past service level measurement results and resource utilization constraints; ii) The concept of destination rank as an approach to autonomically prioritize destinations for the activation of active measurement sessions using destination scores; iii) The concept of correlated peers to enable the autonomic provisioning of a P2P measurement overlay for the exchange of relevant active measurement results; iv) The concept of virtual measurement sessions to enable the sharing of measurement results among correlated peers in order to save network devices resources and to improve SLA monitoring coverage; v) The definition of decentralized strategies to steer the activation of active measurement sessions using P2P principles. The method used on the investigation started with the execution of literature reviews on the network-wide control of measurement mechanisms and the employment of P2P technology on network management. After that, the proposed principles to control active measurement mechanisms and the strategies to activate measurement sessions were described. Finally, experiments were performed to evaluate the performance as well as to highlight properties of such principles and strategies. The findings showed properties which improve the detection of SLA violations in terms of the number of detected violations and the adaptiv-

ity to network dynamics. We expect that such findings can lead to better SLA monitoring tools and methods.

Keywords: Network management. P2P. P2P-Based Network Management. SLA. Active measurement. Autonomic management.

1 INTRODUCTION

Computer network infrastructures have been improving dramatically in terms of size, capacity, and accessibility in the last years. The communication requirements of distributed services and applications running on top of these infrastructures have become increasingly strict too. Performance problems caused by violations of these requirements usually present significant financial loss to organizations and end users. As a consequence, service level requirements of critical networked services have become a critical concern of network operators.

The requirements for the operation of critical networked services are usually described in Service Level Agreements (SLAs), established between service providers and customers. These agreements are contracts, either legally bound or informal, that clearly depict such requirements to ensure that they are consistently met in a given period. The enforcement of SLAs is performed through the use of rewards and penalties, which consider the result of the agreed service levels as received by the customer. The description of several characteristics of such levels must be included in a SLA.

Service Level Objectives (SLOs) are one of the most important terms of a SLA. SLOs are descriptions of required service levels that should be sustained by the provider with respect to the SLA parameters. One of these parameters is the location where the service is provided. In this context, SLOs (and a SLA as whole) can be considered regarding either one single site or across multiple locations. For example, the maximum latency that should be experimented in the interconnection of different branches of an enterprise by a service provider is a possible network-wide SLO. Since SLOs must be specified in terms of defined values, it is vital that such values be measured and controlled.

Network service levels need to be constantly monitored to ensure that network-related SLOs are being met. If these levels are below than the objectives agreed on the SLA, costly penalties would usually incur on the network service provider. In addition, SLA monitoring allows the remediation of violating service levels. In this context, solutions that help network administrators to monitor and troubleshoot the underlying communication infrastructure are crucial. To that end, network measurements must take place.

The use of network measurement mechanisms is an effective technique for monitoring SLOs. The detection of SLA violations is based on the identification of deviations from the contracted SLOs. Today, this detection is usually realized through either active or passive measurement techniques. In passive measurement, network conditions are said

to be checked in a non intrusive way because no monitoring traffic is created by the measurement process itself. Passive measurements are realized, for example, inside network devices when they observe the passing traffic flows. Active measurements, on the other hand, are intrusive because they inject synthetic traffic into the network to measure the network performance.

Active measurements usually offer better accuracy and privacy than passive ones. Furthermore, active measurement mechanisms are able to detect end-to-end network performance problems in a fine-grained way. As a result, active is preferred over passive measurement for SLA monitoring. The Cisco Service Level Assurance Protocol (CHIBA et al., 2013), One-Way Active Measurement Protocol (OWAMP) (SHALUNOV et al., 2006), and Two-Way Active Measurement Protocol (TWAMP) (HEDAYAT et al., 2008) are examples of protocols employed on active measurement mechanisms. Several logical entities compose the architecture of active measurement mechanisms. These entities are usually grouped in two main roles: sender, a network element which is the initiator of a measurement message exchange, and responder, a network element that responds to a measurement message (CHIBA et al., 2013). Senders and responders are commonly known as measurement probes.

Measurement probes must be hosted and measurement sessions must be activated inside network devices to compute the current network performance in active measurement mechanisms. Thus, to deliver the end-to-end network metrics, it is necessary to have a measurement session activated on the local device (the sender) and on the remote device at the network destination (the responder). However, the activation of such sessions is expensive in terms of resource consumption, *e.g.*, CPU cycle and memory footprint required by measurement sessions inside network devices, and the network load, due to the injected traffic. Both the required resources and traffic generated by the measurement sessions are a function of the number of measured network destinations, *i.e.*, with more destinations the larger will be the resources and the traffic generated to deploy the sessions. Despite the required computational resources and additional traffic, the impact of having SLA violations is usually much higher than that one caused by the resource consumption of active measurement mechanisms.

There is an inherent trade-off between attempting to maximize SLA coverage over network destinations and minimizing resource consumption concerning the utilization of active measurement mechanisms to detect SLA violations. Intuitively, two extreme strategies can be described to cover a network infrastructure using active measurement

mechanisms: maximum coverage, increasing the number of activated sessions without considering resource consumption and possibly leading to network devices exhaustion; and minimum resource consumption, decreasing network coverage and, probably, missing SLA violations. An effective activation of measurement sessions should balance these strategies. To have a better monitoring coverage, it is necessary to activate more sessions, which consequently increases consumed resources. On the other hand, enabling the observation of just a small subset of all network flows can lead to an insufficient coverage. Thus, it is crucial to find the sweet spot considering each network infrastructure.

The current usual practice on the employment of active measurement mechanisms is to distribute the available measurement sessions along the network relying entirely on the operator's expertise to infer which would be the best locations to activate such sessions. This is done through several steps. First, it is necessary to collect traffic information in order to grasp the traffic matrix. Then, the operator uses this information to infer which are the best destinations for the measurement sessions. After that, the operator activates sessions on the chosen subset of destinations considering the available resources (*i.e.*, number of available sessions). This practice, however, does not scale well because it is still labor intensive and error-prone for the operator to compute which sessions should be activated given the set of critical flows (*i.e.*, SLA-related flows) that needs to be measured. Even worse, this practice completely fails in networks whose critical flows are too short in time and dynamic in terms of traversing network paths, like in modern cloud environments. That is so because fast reactions are necessary to reconfigure the sessions and operators are not just enough in computing and activating the new set of sessions required every time the network traffic pattern changes. Finally, the current active measurements practice usually covers only a fraction of the network flows that should be observed, which invariably leads to the damaging consequence of undetected SLA violations.

The activation of active measurement sessions is normally controlled by management software. This software can be either hosted in a centralized party (*i.e.*, a management station) or embedded inside network devices. In fact, to embed management software in devices is an usual approach taken by network equipment vendors to control the resource consumption of active measurement mechanisms. This is specially done to avoid exhaustion due to configuration errors and lack of experience from human administrators. However, this approach do not enhance the active measurement capabilities in important terms, such as scalability and efficiency. For example, the number of measured network destinations (and, consequently, detected SLA violations) is still bounded by the

number of activated sessions. Thus, if the number of SLA violations is greater than the number of activated sessions, only a fraction of the violations would be observed. Also, the activation control of measurement sessions only takes the devices into consideration individually, thus, devices cannot share resources and knowledge about the networking infrastructures in order to promote a network-wide control of measurement sessions. Up to today, few investigations have been carried out in the control of active measurement mechanisms for the detection of SLA violations, despite the financial losses related to resource consumption on network devices and undetected SLA violations.

In this thesis, we investigate the benefits of the employment of Peer-to-Peer (P2P) technology to control the network-wide activation of measurement sessions. It is possible to embed such technology in network devices since their level of programmability have increased substantially. P2P technology can provide the foundations for increasing the intelligence applied in active measurement solutions through the introduction of an embedded P2P management overlay. This overlay controls the decision making process of determining which measurement sessions must be activated/deactivated to cope with the network dynamics.

The remainder of this chapter is organized as follows. In Section 1.1, the goal, research questions, and approach employed in the thesis are presented. In Section 1.2, the contributions are summarized. The scope and limitations are described in Section 1.3. Finally, the outline of the thesis is detailed in Section 1.4.

1.1 Goal, Approach, and Research Questions

The goal of the present thesis is to investigate the decentralized detection of SLA violations using active measurement mechanisms in order to propose an approach to improve this detection. The general approach employed consists in to analyze how these mechanisms are employed, considering the human administrators and the mechanisms *per se*, and to learn which are the shortcomings of the current best practice. The idea is to capture the common sense of human administrators in order to develop techniques that allow the network devices themselves better detect SLA violations. To accomplish this, we propose a fundamental research question and a research hypothesis:

- **Fundamental Research Question:** How to improve the network-wide detection of SLA violations in terms of the number of detected violations and the adaptivity to

changes in network conditions?

- **Research Hypothesis:** The detection of SLA violations can be improved through the use of Peer-to-Peer (P2P) technology to steer autonomically the activation of active measurement mechanisms.

The Fundamental Research Question focuses on the network-wide detection of SLA violations by providing an investigation on its current shortcomings (and their causes) and how this detection can be improved. We explicitly aim at two factors that can enable this improvement: the number of detected violations and adaptivity to changes in network conditions. These factors are directly related to the actual best practice and its drawbacks. Besides that, the relevance of this question is highlighted considering the effect of undetected SLA violations and the cost of resource consumption on network devices.

We hypothesize that employing P2P technology it is possible to improve the network-wide detection of SLA violations through an autonomically steering of active measurement mechanisms. This hypothesis comes from the results found on the investigation of several initiatives regarding P2P-Based Network Management (P2PBNM) and distributed network-wide control for measurement mechanisms. To carry out this employment, we propose and evaluate P2P concepts and algorithms.

Different distribution approaches for network management have been studied for many years. Such approaches are usually grouped in three classes: centralized, hierarchical, and distributed ones. P2PBNM can be classified as a distributed approach since the management logic is performed across management nodes in a decentralized fashion. Thus, the alternatives to that would be either the centralization of such logic in a management station or the delegation of management tasks in a hierarchical approach. Centralized management is not considered in our study since it does not provide the necessary adaptivity to deal with large network infrastructures considering active measurement mechanisms. In this context, hierarchical control does not suit our purposes either since it also lacks such adaptivity. Besides that, the interfaces for the full control of active measurement mechanisms are usually provided only locally on the devices which also hampers the use of centralized and hierarchical approaches in the context of this thesis.

Besides the fundamental research question addressed in this thesis, we describe additional research questions. Such questions highlight several properties of our research hypothesis.

- **Research Question 1**: Which aspects of the detection of SLA violations can be

improved using P2P technology?

In Research Question 1, we focus in aspects of the employment of P2P technology on the network-wide detection of SLA violations. In fact, with respect to the fundamental question, the number of detected violation and approach adaptivity are already emphasized. However, other aspects in respect to the measurement coverage could be also improved regarding the use of this technology. For example, it is important to assure that each destination is measured frequently, even if its measurement results are not close to violate SLAs. Besides that, resources constraints can be also used in order to enable an efficient operation of network devices.

Our fundamental hypothesis highlights an autonomic steering of the activation of active measurement sessions in order to detect SLA violations. In this context, it is interesting that P2P technology can be used to include human expertise and heuristics employed to determine which sessions should be activated in a given time. Therefore, we concentrate our attention on the common sense used by network administrators when using active measurement mechanisms for SLA monitoring. It is important to clarify that we do not claim that every human intervention would be avoided through the use of P2P technology, but that it could be greatly reduced for the operation of active measurement mechanisms on the detection of SLA violations.

- **Research Question 2**: Which characteristics of the use of P2P technology in network management can be successfully deployed on the steering of active measurement mechanisms?

Some authors state that P2P technology present three fundamental properties: high degree of decentralization, self-organization, and multiple administrative domains (RODRIGUES; DRUSCHEL, 2010). Peers implement both client and server functionality and, require little (or no manual) configuration to maintain the system after peers introduction. This can increase the scalability and fault-tolerance of distributed systems. Besides that, P2P technology can deal with current Internet idiosyncrasies much more effectively since they are are conceived taking Internet peculiarities explicitly in mind. For example, peers can be owned and controlled by different organizations or individuals. P2P systems have shown success at providing sophisticated communication services to support applications as diverse as audio and videoconferencing (*e.g.*, Skype) and file sharing (*e.g.*, BitTorrent), among others.

The use of P2P technology in network management inherits fundamental properties from general use of this technology and combine them with Distributed Network Management (DNM) (GRANVILLE et al., 2005). We studied the background on P2PBNM systems in order to identify which characteristics of these systems can be successfully deployed on the steering of active measurement mechanisms. P2P technology enables the incorporation of management code which can be used to deploy innovative management services into the managed network. Besides that, it is possible to federate the network devices in a flexible and multi-domain way using P2PBNM.

- **Research Question 3**: What are the impacts on using P2P technology to steer active measurement mechanisms?

Active measurement mechanisms need to be carefully deployed in order to save devices resources. In this context, approaches to control active measurement mechanisms must also take into considerations the resources necessary to implement the own control. Some costs are usually associated with P2P technology, such as the cost of bootstrapping a network device with a minimal peer and the minimal traffic generated to maintain the P2P overlay. Thus, the use of P2P technology to steer active measurement mechanisms may have impacts on the network devices and in the network infrastructure as a whole.

The employment of P2P technology in the execution of management tasks usually implies in additional costs. Such costs are related with the maintenance of the P2P management overlay and the intrinsic distribution of management functions. For example, the resource consumption in terms of bandwidth usage and deployment time of management services over a P2P overlay can be significant. Thus, the use of P2P technology to steer active measurement mechanisms to steer should have a better impact on the resource consumption of these mechanisms than the necessary resources for the support of such technology itself.

- **Research Question 4**: How to decide whether different nodes are management peers considering the employment of P2P technology on the control of active measurement mechanisms?

P2P management overlays can be used to exchange management information among network devices. Thus, the provisioning of such overlays must take into account which nodes should be considered management peers in terms of the information they can exchange. In this context, it is necessary to define which network devices produce management information relevant to each other. This can be done through the selection of

network devices that present similar features.

Several characteristics of network devices can be used to identify which devices have similar features. One of these features is service level performance considering a specific destination. Results produced by active measurement mechanisms are an indicator of this performance. Since these results are obtained by different devices within a network infrastructure, each device can compare its own results with remote ones in order to look for similarities. Similar network devices can be autonomically grouped in order to enable joint management tasks.

- **Research Question 5**: What are the conditions to enable the sharing of active measurement results among peer nodes?

In Research Question 5, we focus in analyzing the condition to enable the sharing of active measurement results among nodes. Network administrators employ different strategies to maximize the coverage of a network infrastructure regarding the number of detected SLA violations. However, even considering a naïve attempt of maximum coverage, the number of measurements that a device can perform is still bounded by the available resources, *i.e.*, the number of measurement sessions which a device can actually activate given their resource consumption. Besides that, the administrators usually aim at saving resources from network devices for main network functions, such as switching and routing. We aim to capture one of the behaviors commonly employed by network administrators, the sharing of active measurement results. Several factors can be taken into consideration by the network administrator to define which results can be shared by specific network devices.

The evaluation of the sharing of active measurement results must consider the relevance of using remote results. For example, it is important to define which network devices are prone to share results, considering their own capabilities, the quality constraints, and the available resources. We consider a scenario of several network devices which probe several destinations where those devices can share results considering an overlay network. In this context, SLA violations and their related management decisions may use partially available information and virtual management data models.

1.2 Contributions

The present thesis is to present, to the best of our knowledge, the first proposal of the employment of P2P technology to control the network-wide activation of active measurement sessions. Our investigation proceeded as follows. First, we surveyed the state of the art of the network-wide control of measurement mechanisms and P2PBNM. After that, verifying the current best practice regarding such activation, we analyze which characteristics of this practice can be autonomically supported by the network devices themselves and how to provide new features that can help human administrators in the detection of SLA violations in a network infrastructure. The main contributions of this thesis are:

- An approach to improve the detection of SLA violations through the steering of the activation of active measurement sessions using local and remote past service level measurement results and resource utilization constraints;
- The concept of destination rank as an approach to autonomically prioritize destinations for the activation of active measurement sessions using destination scores;
- The concept of correlated peers to enable the autonomic provisioning of a P2P management overlay for the exchange of relevant active measurement results;
- The concept of virtual measurement sessions to enable the sharing of measurement results among correlated peers in order to save network devices resources and to improve SLA monitoring coverage;
- The definition of decentralized strategies to steer the activation of active measurement sessions using P2P principles.

The contributions provided in this thesis aims at helping network administrators in their tasks related to the detection of SLA violations. Besides that, it is possible to use the produced concepts, definitions, and approaches to better develop SLA management tools and practices.

1.3 Scope and Limitations

We propose the use of P2P technology to control the network-wide activation of measurement sessions considering the detection of SLA violations. Our approach for this use considers some assumptions. These assumptions help to define the scope and

limitations for the present work.

The present thesis is aimed at the control of active measurement mechanisms. Thus, we consider the presence of an underlying active measurement infrastructure. Such infrastructure is composed of senders and responders which are known as measurement probes. We assume that every probe in the infrastructure is able of both initiate and respond synthetic traffic for the production of performance metrics. The active measurement infrastructure permits end-to-end SLA monitoring and deviations from SLOs (*i.e.*, detection of SLA violations) can be identified by single network devices.

The approach for the employment of P2P technology on the network-wide control of the activation of measurement sessions considers features commonly presented by widely known active measurement mechanisms, such as TWAMP and IPSLA. In this context, the chosen mechanism does not need any modification to be controlled by the approach described in this thesis. Besides that, it is assumed that there is an open interface for the activation of measurement sessions in the network devices which support the active measurement mechanism themselves.

The activation of measurement sessions is one of the necessary steps to perform SLA monitoring. In this context, we do not claim to address the whole SLA monitoring process. For example, even considering an optimal measurement session activation, it would be necessary an approach to integrate the monitoring data in order to produce SLA violation information in the form of reports. In any case, since the activation of measurement sessions is a critical step in SLA monitoring process, an improvement in this step impacts the process as a whole.

Security issues are considered orthogonal to the present proposed solution. Thus, the description of the principles and strategies employed to use of P2P technology on the network-wide activation of measurement sessions do not consider security properties, such as privacy and authenticity. However, we are aware that the proposed solution has security implications and we pose possibilities to overcome these implications as future work.

1.4 Thesis Outline

The structure of this thesis was defined to address the fundamental research question and how our hypothesis is tailored to cover it. Besides that, the additional research questions are used to highlight different aspects of our research hypothesis. Following

this structure, we describe the following chapters. Each of one of such chapters has a different emphasis on the investigation.

In Chapter 2 - Network-Wide Control of Measurement Mechanisms, we present a review on the initiatives to provide a network-wide control for measurement mechanisms. First, we highlight the fundamental concepts behind such mechanisms. After that, we describe and classify several approaches to support a network-wide control for measurement mechanisms. Finally, a discussion of current challenges and future research trends regarding such control is presented.

In Chapter 3 - P2P-Based Network Management, we cover the employment of P2P technology on network management since this technology is involved in our research hypothesis. Initially, we review some general concepts about P2P technology and DNM approaches. In addition, we present an overview of the current research scenario regarding the employment of P2P-Based Network Management (P2PBNM). Furthermore, we discuss the current challenges and future research trends on P2PBNM.

In Chapter 4 - Principles to Steer Autonomically the Activation of Active Measurement Session, we provide the description of principles and their associated concepts proposed to employ P2P technology on the control of the active measurement mechanisms. At first, we present the utilization of past service level measurement results to prioritize destination which are likely to violate the SLA. After that, the concept of correlated peers as an approach to provision the P2P management overlay is explained. Finally, we present the concept of virtual measurements to enable the sharing of active measurement results in order to optimize resource consumption.

In Chapter 5 - Strategies to Activate Active Measurement Sessions using P2P Technology, we depict the use of destination ranks and measurement session activation strategies in order to deploy a P2P control for active measurement mechanisms. First, we describe the concept of destination ranks and scores which are used to prioritize network destinations considering the measurement sessions. Then, we present several measurement session activation strategies which differ regarding the employed information sources and the level of collaboration among peers.

In Chapter 6 - Evaluation, we investigate the quantitative performance of the measurement session activation strategies considering simulation experiments. Initially, we describe the implemented code for the execution of such experiments. After that, we depict the experimental setup, including the selected topologies and simulation setup parameters used to evaluate the proposed strategies. Finally, results produced on the execution

of the simulation experiments are presented.

In Chapter 7 - Conclusion, we finalize this thesis, by providing conclusions as well as the guidelines for the next steps. At first, we present the main contributions of this thesis in the light of the research questions. In addition, we discuss the future work along with potential topics to be explored.

2 NEWTORK-WIDE CONTROL OF MEASUREMENT MECHANISMS

The deployment of measurement mechanisms consumes resources which could be useful for primary network functions (*e.g.*, routing and switching). Besides that, the operation of these mechanisms also requires valuable human resources since their configuration is usually a complex process based on experience and knowledge of the network administrators. In this context, approaches to help such administrators and to decrease resource consumption concerning measurement mechanisms are of paramount importance. Some approaches aim at single devices, *e.g.*, sampling packets when observing flows at a network device and setting thresholds to trigger the injection of a specific test traffic, but network-wide approaches can provide a larger impact, *e.g.*, coordinating the activation of measurement sessions to enable a better monitoring coverage.

In this chapter, we present a literature review of the current efforts on network-wide approaches to control measurement mechanisms. To the best of our knowledge, a survey of such approaches has not been provided so far. Moreover, we describe criteria which can be used to analyze and compare the reviewed efforts. In this context, this chapter provide an integrated perspective of the network-wide approaches to control measurement mechanisms and insights into the rationale for their deployment and applicability.

The remainder of this chapter is organized as follows. First, an overview of active and passive measurement mechanisms is presented. Then, the method employed to perform the literature review is described. After that, the initiatives on the network-wide control of measurement mechanisms are presented. Then, such initiatives are depicted in respect to their intrusiveness, distribution aspects, and application areas. After that, a discussion of current challenges and future research trends is shown. Finally, some final remarks are presented.

2.1 Measurement Mechanisms

Measurement mechanisms are some of the most important tools deployed by network administrators. These measurements can be used in different contexts, such as pre-deployment validation and measurement of in-band live network performance characteristics, and by several applications, such as intrusion detection and lawful interception. Measurements can be performed considering end-to-end paths, individual segments or

even domains in a network infrastructure. Finally, information from different layers of the OSI model can be collected, *e.g.*, messages exchange due to specific application protocols.

Results from measurement mechanisms encompass several network metrics, which are a (mostly) quantitative way to verify particular network behaviors. Some of the most important metrics are produced as a measure of time needed for the data to travel between two measurement points; one-way or two-way (round-trip) delay are measurements of such time, and jitter is the variation in arrival times for packets. Some metrics are directly related to network traffic, such as network capacity, network utilization, and throughput. Finally, the number of packets which are dropped is known as packet loss and the number of packets which are duplicated is known as packet duplication. These basic metrics can be also used to produce more specific network metrics. For example, jitter data can be decomposed into positive and negative egress jitter, positive and negative ingress jitter, and positive and negative round-trip jitter. Such metrics can be used to provide an approximation of the characteristics experienced by live traffic in the network.

Several mechanisms can be used to enable network measurements. In general, these mechanisms are divided considering the injection of measurement traffic by the mechanisms themselves. This leads to two kinds: passive measurement mechanisms and active measurement mechanisms. Passive measurement is realized, for example, inside network devices through the use of packet sniffers. On the other hand, active measurement is deployed through measurement probes hosted along the network which inject synthetic traffic and compute the current network performance.

In this section, we first cover some passive measurement mechanisms and their main concepts. After that, most prominent active measurement mechanisms are presented. For the sake of simplicity, we will focus on the mechanisms from the Internet Engineering Task Force (IETF) and leading networking equipment vendors. Finally, we describe a background on the control of measurement mechanisms.

2.1.1 Passive Measurement Mechanisms

In passive measurement, network conditions are said to be checked in a non intrusive way because no monitoring traffic is created by the measurement process itself. Passive measurement data can be used for a variety of purposes. Considering the FCAPS model, there are applications on Fault Management (*e.g.*, abnormal traffic behavior), Con-

figuration Management (*e.g.*, capacity planning), Accounting Management (*e.g.*, Internet Service Provider billing), Performance Management (*e.g.*, bandwidth monitoring), and Security Management (*e.g.*, flow-based Intrusion Detection Systems). Passive measurement is realized, for example, inside network devices when they observe the passing traffic flows.

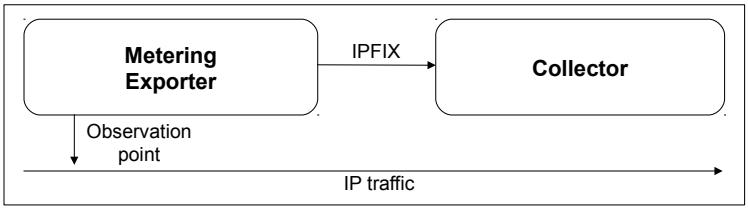
Flows can be defined as unidirectional sequences of packets that pass through a network device which are grouped according to some common properties. These properties can consider several packets fields, such as source/destination IP address and port number, layer three protocol type, Type of Service (ToS), and size (aggregated number of bytes). Besides that, other information, such as source/destination Autonomous System (AS), and input/output interfaces can also be used to define flows. It is necessary uniformity in the representation of flow data and the means of communicating such data from the network elements to corresponding collection points (CLAISE, 2008). There are several protocols used to enable flow data producing and exchange.

sFlow (PHAAL; PANCHEN; MCKEE, 2001) provides continuous traffic monitoring for high speed networks through traffic flows. The sFlow design specifically addresses issues associated with accurately monitoring network traffic using sampling techniques. The sFlow monitoring system consists of sFlow agents and a central data collector, *i.e.*, a sFlow analyzer. The sFlow agent, which can be embedded in a network device or implemented as a stand alone probe, captures traffic statistics from the device which it is monitoring. sFlow datagrams are used to immediately forward the sampled traffic statistics to a sFlow analyzer for processing.

The IETF Realtime Traffic Flow Measurement (RTFM) Working Group released several documents describing a method for the specification of real-time traffic flows within a network (BROWNLEE; MILLS; RUTH, 1999). This method is composed of a hierarchy of devices (meters, meter readers, and managers) for measuring the specified flows and configuration and collecting mechanisms. RTFM provides high time resolution for flow first- and last-packet times. Counters for long-duration flows may be read at intervals determined by a manager. The RTFM meter is designed to do as much data reduction work as possible, which minimizes the amount of processing needed to read the traffic data and produce reports. At least, one meter reader is needed to collect the measured data from the meters, and a single manager is needed to control the meters and meter readers (BROWNLEE, 1999).

Cisco NetFlow (CLAISE, 2004) is a widely deployed protocol used to provide

Figure 2.1: IPFIX Logical Model.



Source: by author (2015).

access to IP flow information from data networks. NetFlow architecture is based on two types of components: metering exporters, able to collect and transmit flows, and collectors, which receive such flows and save them for further processing. NetFlow is a push protocol, *i.e.*, each exporter will periodically send NetFlow messages to configured collectors without any interaction by the collector. Currently, the most widespread protocol version is NetFlow v5, which is the *de facto* standard to exchange flow records. The NetFlow v5 record format contains source/destination address, source/destination port, protocol number, start/end timestamp, packet and byte count, TCP flags, type of service, input/output network interface, next hop address, source/destination Autonomous System (AS) number, and source/destination prefix mask. In order to overcome format restrictions, a flexible record format was defined in the NetFlow v9 through the use of record templates. Although NetFlow protocol is a proprietary solution developed by Cisco, v9 is described in the RFC 3954 (CLAISE, 2004).

The IETF IP Flow Information eXport (IPFIX) Working Group has released several documents describing a protocol, based on the version 9 of NetFlow (CLAISE, 2008). Some enhancements in different domains (*e.g.*, congestion-aware transport protocol and built-in security) were incorporated in the IPFIX protocol. Besides that, IPFIX adopts an improved use of templates through more precisely defined record items and measurable values. Unlike NetFlow, IPFIX requires Stream Control Transport Protocol (SCTP) to transport data. The use of SCTP provides a reliable transport and prevents congestion. Figure 2.1 shows the IPFIX logical model (which is based on the NetFlow logical model) as an example of passive measurement models. In such model, metering exporters hosted in network elements (*e.g.*, routers and switches) gather flow data and export IPFIX records to configured receivers, *i.e.*, collectors (or collecting points).

2.1.2 Active Measurement Mechanisms

Active measurement mechanisms are an important tool to monitor Service Level Objectives (SLO) and the health of a network as a whole. Such mechanisms inject synthetic traffic into specific network paths to measure the network performance in terms of, for example, delay, loss, jitter, and packet/frame loss. A well-defined injection of such traffic is usually called a measurement session. Active measurement mechanisms can be employed in different contexts, such as pre-deployment service validation and live network-wide SLA monitoring.

Active measurements are performed either one-way or two-way (*i.e.*, round-trip). One-way measurements allow more informative measurements since it is usually easier to isolate asymmetric effects on specific parts of a network. However, high-precision one-way measurements require good time sources, such as Global Positioning System (GPS). Two-way measurements, which are common in IP networks, employ time stamps applied at the echo destination to achieve better accuracy, thus, they do not require synchronization between local and remote clocks. However, it is difficult to isolate the direction in which performance issues are experienced using round-trip measurements.

The generation of synthetic traffic and its computation to provide measurements results is usually performed by an architecture comprised of two hosts with specific roles, a sender and a responder, also collectively known as (active) measurement probes. The exchange of packets between probes is usually defined by two inter-related protocols: a control protocol, used to initiate and control measurement sessions and to fetch their result, and a test protocol, used to send single measurement packets along the network path under test. Measurement support at the responder end may be limited to a simple echo function. There are several protocols used to enable active measurement.

Juniper Networks presents Real-time Performance Monitoring (RPM)[1] to enable the configuration of active probes in order to track and monitor traffic across the network for the investigation of performance problems. The RPM is a service running as a Junos operating system process which is used on the Juniper routing engine. RPM can be described as having a client (source) that sends out probe queries and a server (destination) that responds such queries. During a measurement session, the client device sends a packet to a remote server, which in turn returns the packet with an acknowledgement to the sender.

[1] Real-Time Performance Monitoring on Juniper Networks Devices - http://www.juniper.net/us/en/local/pdf/app-notes/3500145-en.pdf

The main use for RPM is performance monitoring on layers three and 4 and it can also generate traps on configured thresholds.

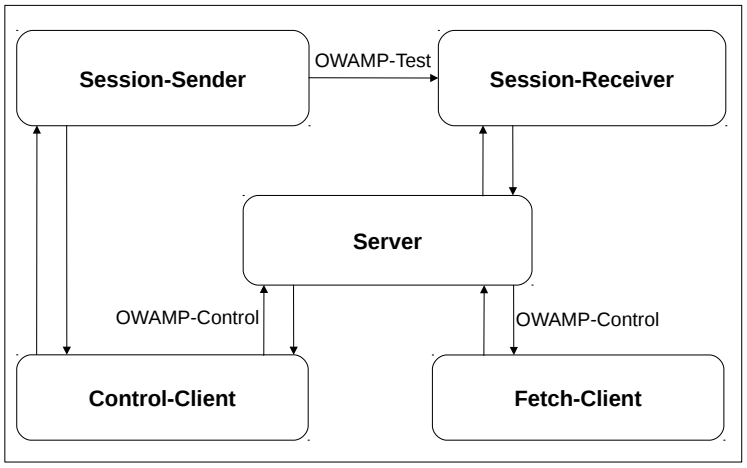
Cisco Systems defines the Service Level Assurance (SLA) protocol (also known as IPSLA) which is described in an IETF informational RFC (CHIBA et al., 2013). This widely deployed protocol measures service levels related to data link and network layers as well it emulates characteristics of different applications, both considering one-way and two-way metrics. The IPSLA logical model consists essentially of a sender and a responder, *i.e.*, measurement probes. The protocol consists of two distinct phases: the control phase and the measurement phase. The control phase forms the base protocol, which establishes the identity of the sender and provides information for the measurement phase. The measurement phase is comprised of a sequence of measurement-request and measurement-response messages (test messages).

The IETF IP Performance Metrics (IPPM) Working Group has proposed open active measurement mechanisms that allow the exchange of packets to produce one-way and two-way metrics. These mechanisms are called, respectively, One-Way Active Measurement Protocol (OWAMP) (SHALUNOV et al., 2006) and Two-Way Active Measurement Protocol (TWAMP) (HEDAYAT et al., 2008). The O/TWAMP mechanisms consist of two inter-related protocols: a control protocol, used to initiate and control measurement sessions and fetch their result, and a test protocol, used to send single measurement packets along the Internet path under test. Control protocol is performed by the control-client (requests, starts, and ends test sessions) and server (manages test sessions); and the test control is the executed by the sender (sending endpoint) and session-receiver/reflector (receiving endpoint). Besides that, TWAMP has a special mode, called TWAMP-light, which eliminates the need for the TWAMP-Control protocol, and assumes that the Session-Reflector is configured and simply reflects the incoming packets back to the controller while copying the necessary information and generating sequence number and timestamp values. The first part of the Figure 2.2 (*a*) shows the logical model used on O/TWAMP. The different logical roles can be played on different hosts, but some of these roles can be also played by the same host as shown in the second part of the Figure 2.2 (*b*).

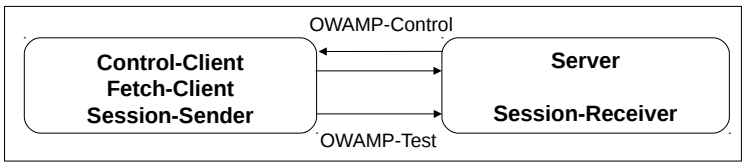
2.1.3 Control of Measurement Mechanisms

Measurement mechanisms enable performance monitoring features in order to assess and analyze network efficiency. However, there is an inherent human and compu-

Figure 2.2: O/TWAMP Logical Model.



(a) Roles Distributed on Different Hosts



(b) Roles Integrated on Two Hosts

Source: by author (2015).

tational cost related to the deployment of measurement probes and their continuously operation, *i.e.*, the management of measurement sessions. Human resources are necessary to compute and configure the set of probes to bootstrap the measurement process as well as to respond to network changes. Besides that, it is necessary to save network equipment resources, which are required for routing and switching. In this context, solutions to control measurement mechanisms are vital.

Measurement mechanisms are expensive in terms of the consumed computational resources. For example, in flow table processing (present in some passive mechanisms), probes calculate hash values of each packet arriving to update the flow table and this must be done at the transmission line rate, which requires high-speed (and high-cost) memory for such processing (KAMIYAMA; MORI; KAWAHARA, 2013). In active mechanisms, resource consumption has also an impact on the hosting devices. In this context, even active measurement protocol descriptions usually include advices on configuration parameters to limit the use of computational resources (SHALUNOV et al., 2006). The cost

of measurement mechanisms is strongly related with the size and complexity of network infrastructures. However, such cost also limits the monitoring target to be just some of the network destinations. Thus, it is usually not possible to monitor all network flows. In some settings, even dedicated routers (also known as "shadow routers") are deployed only to handle measurement mechanisms.

Different approaches can be used to control measurement mechanisms. The simplest approach is to consider only the single-device case, *e.g.*, flow sampling control on the context of an individual device. On the other hand, the network-wide case considers multiple devices, *e.g.*, positioning of measurement probes in devices across a network infrastructure. It is important to clarify that the term "network-wide" control does not mean that every (or even the majority of) network device in the infrastructure be under such control, but that several devices can be controlled in an integrated approach.

Network-wide control of measurement mechanisms can help network operators to understand better the global network behavior of an infrastructure. Given the fast-changing network environments, single probes could not be capable of accomplishing measurement tasks in an accurate way. Thus, probes can be placed anywhere on the network and collect information from different infrastructure portions at the same time. Moreover, probes across the network produce distributed management information which could be used to improve management tasks. In this context, a network-wide control of measurements among multiple distributed probes can further improve measurement tasks.

2.2 Method for the Literature Review

In the present thesis, we are interested in network-wide approaches to control measurement mechanisms since these approaches are more related to the decentralized detection of SLA violations. We performed a literature review (considering the author's best knowledge) of the current efforts on network-wide approaches to control measurement mechanisms. To the best of our knowledge, a survey of such approaches has not been provided so far. Work carried out on single devices is already addressed in the literature (*e.g.*, sampling for passive measurements (DUFFIELD, 2004)) and, hence, is out of the scope. Besides that, the initiatives included in this review must describe some form of evaluation of their own proposals (experiments, case studies, etc). The method employed for the literature review is based on the one proposed by Magdaleno, Werner and Araujo (2012).

The remaining of the section presents the method used in the present survey. First, the objectives and the review questions are described. After that, two main phases are proposed to gather, evaluate, and analyze the literature concerning network-wide approaches to control measurement mechanisms: the planning and execution phases.

2.2.1 Objectives and Review questions

The objectives of the literature review are the characterization of the state of the art regarding the network-wide control of measurement mechanisms approaches and exploration of future works on such approaches. Thus, in order to achieve these objectives, this review aims to answer the following review questions:

- What are the intrusiveness level of measurement mechanisms controlled by network-wide approaches?
- What are the distribution paradigms used by network-wide approaches to control measurement mechanisms?
- What are the application areas for network-wide approaches to control measurement mechanisms?
- What are the opportunities and challenges in network-wide approaches to control measurement mechanisms?

We provide more details about the challenges related to these features in the future research directions section (Section 2.7). In the following, we briefly describe the features we focus on this literature review.

Network measurements can be classified in respect to their intrusiveness. In simple terms, such mechanisms can be either passive or active. Besides that, there are hybrid mechanisms, which integrate both active and passive mechanisms. Therefore, this classification can be also extended to network-wide approaches which control the mechanisms themselves. Some of the surveyed initiatives rely on actual mechanisms (*e.g.*, Cisco Systems NetFlow and IETF IPFIX) and others on simulated mechanisms deployed just for research purposes.

Different distribution paradigms can be used by network-wide approaches which control measurement mechanisms. The first alternative is the use of centralization to support the control logic and data. On the other hand, distributed approaches makes it possible to avoid some pitfalls of centralized systems, such the existence of a Single

Point of Failure (SPoF). Distribution features can be exploited not only to provide fault tolerance, but also to improve load balancing, for example. Regarding our review, we do not found hierarchical approaches.

The network-wide control of measurement mechanisms can aim at different application areas. In the literature review, we find 5 main areas: resource consumption, measurement accuracy, fault localization, monitoring coverage, and topology discovery. In particular, several initiatives address more that one area since it is difficult to effectively separate some application areas. In this context, we focus at the features explicitly stated as the main ones by the authors.

2.2.2 Planning Phase

The planning phase of the present literature review explores the defined objectives and review questions about network-wide approaches to control measurement mechanisms to produce search keywords and inclusion and exclusion criteria. The definition of such keywords and criteria was performed through the analysis of a set of papers obtained from an initial review (considering the authors' best knowledge). The keywords were selected to explore contrasting features of network-wide approaches to control measurements mechanisms. After that, the review questions were answered regarding the papers in order to extract relevant information.

The keywords used on search process are *active measurement*, *passive measurement*, *IPSLA*, *OWAMP*, *TWAMP*, *NetFlow*, *IPFIX*, and *probe placement*. Alternative spellings and synonyms for these keywords are also considered, *e.g.*, *active measurement* and *active monitoring*. Besides that, similiar measurement mechanisms (*e.g.*, NetFlow and sFlow) from the ones used on control papers and other related initiatives are also included. Effective search strategies use operators "AND" and "OR" along the keywords. The operator "AND" dramatically narrows the search and selects most relevant papers (*i.e.*, the ones that contain all of the terms). However, operator "OR" makes the searches highly sensitive, in spite of yielding a high number of hits.

Inclusion and exclusion criteria were defined to adjust and calibrate the survey focus. We aimed at network-wide approaches to control measurement mechanisms as our review topic. These criteria is used to delineate the final set of papers regarding this topic. The inclusion criteria is basically the mention of at least one of the keywords in the title, the abstract or keyword fields. On the other hand, we also defined exclusion criteria in

order to omit papers with content which is not relevant for the present review. We were not interested on works that address only the "single-device" case, *e.g.*, IPSLA/Flow sampling on the context of an individual switch, and the works primarily focused in frameworks to produce measurement federations. Besides that, the included works must describe some approach to evaluate their own proposals (experiments, case studies, etc).

2.2.3 Execution Phase

This section describes in more detail how the selection process of the present review was performed. Initially, keywords are used to collect possibly relevant papers on the survey topic. In a second step, the set of collected papers is processed to find and eliminate duplicates. After that, titles and abstracts were read to apply the exclusion criteria. Papers that do not adapt within the scope of this survey were excluded. Finally, with the complete list of relevant papers, information concerning the review questions is extracted.

The execution phase of the review explores queries about the survey topic on the following digital libraries: Institute of Electrical and Electronics Engineers (IEEE) Xplore Library, Association for Computing Machinery (ACM) Digital Library, Elsevier ScienceDirect, Springer SpringerLink, USENIX Online Library and Index, and arXiv e-Print Archive. We assumed that the digital libraries are reliable since the papers went under peer review, which can serve as a quality filter. The papers selected in the performed queries were the candidates ones to be included in the survey.

The candidate papers were retrieved and they were organized in a list to allow duplicate elimination and to apply the exclusion criteria. A final validation is performed by two different persons and the output is the final set of papers. After that, this set is confronted with the review questions in order to extract the main characteristics of network-wide approaches to control measurement mechanisms. Such characteristics were then used to produce an integrated perspective of the research area.

2.3 Surveyed Initiatives

The objectives of the present literature review are the characterization of the state of the art of the network-wide approaches to control measurement mechanisms. Thus, the

complete list of relevant initiatives considering the selected keywords and inclusion and exclusion criteria are classified using the proposed review questions.

In Table 2.1, we provide the classification of the surveyed initiatives according to the review questions. It is important to emphasize that an initiative may address more than one feature in each question. Then, we describe such initiatives.

Table 2.1: Summary of the Network-Wide Approaches to Control Measurement Mechanisms.

Proposal	References	Intrusiveness	Distribution	Application
cSamp	(SEKAR et al., 2008)	Passive	Centralized	Resource Consumption, Monitoring Coverage
DECON	(PIETRO et al., 2010)	Passive	Distributed	Resource Consumption, Monitoring Coverage
Cantieni et al. (2006)	(CANTIENI et al., 2006)	Passive	Centralized	Resource Consumption, Monitoring Accuracy
Lassoued et al. (2011)	(LASSOUED et al., 2011)	Passive	Centralized	Resource Consumption, Monitoring Accuracy
CMON	(ZANG; NUCCI, 2009)	Passive	Centralized	Resource Consumption, Monitoring Coverage
Kamiyama, Mori and Kawahara (2013)	(KAMIYAMA; MORI; KAWAHARA, 2013)	Passive	Distributed	Resource Consumption, Monitoring Coverage
MMPR	(HUANG et al., 2012)	Passive	Centralized	Resource Consumption
LEISURE	(CHANG et al., 2015)	Passive	Centralized	Resource Consumption
Suh et al. (2006)	(SUH et al., 2006)	Passive	Centralized	Resource Consumption, Monitoring Coverage
SPAND	(SESHAN; STEMM; KATZ, 1997)	Passive	Distributed	Monitoring Accuracy
SLAm	(BARFORD et al., 2009)	Active	Centralized	Fault Localization
NetQuest	(SONG; QIU; ZHANG, 2006)	Active	Centralized	Monitoring Accuracy
Patil, Kinger and Pathak (2013)	(PATIL; KINGER; PATHAK, 2013)	Active	Centralized	Fault Localization
Gangam and Fahmy (2011)	(GANGAM; FAHMY, 2011)	Active	Centralized	Monitoring Accuracy
Wren	(ZANGRILLI; LOWEKAMP, 2003)	Hybrid	Distributed	Resource Consumption
NSQM	(RACZ; DONNI; STILLER, 2010)	Hybrid	Distributed	Resource Consumption
Chaudet et al. (2005)	(CHAUDET et al., 2005)	Hybrid	Centralized	Resource Consumption, Monitoring Coverage
Eriksson, Barford and Nowak (2008)	(ERIKSSON; BARFORD; NOWAK, 2008)	Hybrid	Centralized	Topology Discovery

Source: by author (2015).

cSamp. Sekar et al. (2008) proposed cSamp (Coordinated Sampling), a centralized optimization engine for the network-wide control of flow monitoring. The main features of cSamp are the use of flow sampling steering, hash-based packet selection, and a centralized engine for distributing responsibilities across routers. Such distribution is performed through the dissemination of routing manifests within an IPFIX-enabled Autonomous System (AS). The effort requires modifications in the measurement mechanisms. The authors claim that cSamp can provide greater monitoring coverage and an improved use of router resources.

DECON. Pietro et al. (2010) proposed DECON, a decentralized coordination system aimed at assigning monitoring probes. Authors claim that DECON scales up to large numbers of flows without requiring network topology information, traffic matrices and packet marking. DECON achieves a high degree of measurement coverage using a detached P2P overlay, even when faced with short-lived flows. The authors describe a monitoring probe prototype to form the overlay using commodity hardware.

Cantieni et al. (2006). A formulation of the probe placement problem was proposed by Cantieni et al. (2006). Besides that, the authors also propose an optimal algorithm to solve such problem given a network where all links can be monitored. In addition, it is described a performance study considering measurement session activation and sampling rate for specific measurement task in terms of accuracy and resource consumption. Finally, the authors discuss methods to deploy the proposed solution in real backbone networks.

Lassoued et al. (2011). A network-wide cognitive monitoring system is proposed by Lassoued et al. (2011). Such system employs an adaptive centralized architecture that provides visibility over an entire network. Given a measurement task and a constraint on the volume of collected information, this architecture drives the sampling rates on the interfaces of measurement probes to achieve maximum possible accuracy and adaptivity to changes in network traffic conditions.

CMON. Zang and Nucci (2009) investigated the problem of deploying measurement probes in a network with optimized coverage and cost. The authors proposed solutions to enable a significant monitoring coverage using a major portion of traffic instead of the entire traffic. This is done to save resources while at the same time giving administrators enough insight to their network. The proposed solutions are based either on NetFlow or in new measurement mechanism called CMON.

Kamiyama, Mori and Kawahara (2013). Kamiyama, Mori and Kawahara (2013)

proposed a method to enable autonomous load balancing for measurement probes. In this method, such probes are required to select the measurement destinations to maximize the number of flows monitored in the network, while maintaining a balanced load. In order to control autonomously the load balancing, probes exchange their load information with adjacent probes.

MMPR. Huang et al. (2012) proposed MMPR (Measurement-aware Monitor Placement and Routing), a framework that jointly optimizes probe placement and dynamic routing strategy to achieve maximum measurement utility. This is done through several heuristic algorithms. The authors claim that their heuristic solutions can achieve measurement gains that are quite close to the optimal solutions, while reducing the computation time.

LEISURE. Chang et al. (2015) proposed LEISURE (Load-EqualIzed meaSUREment), a centralized optimization framework for load-balancing network measurement workloads across distributed monitors. This framework supports coordinated measurements in order to perform in-depth per-flow measurements, *e.g.*, detailed payload analysis. The authors claim that such coordination can provide a more complete view of network behavior. Besides that, different load-balancing objectives are considered.

Suh et al. (2006). Suh et al. (2006) studied the problem of where to place measurement probes and their sampling rate within a network. The authors proposed greedy heuristics considering minimum cost and maximum coverage problems under various constraints. The proposed solution is employed to show that there is a trade-off between cost and coverage, and that a small number of measurement probes is often enough to monitor most of the traffic in network.

SPAND. Seshan, Stemm and Katz (1997) proposed Shared Passive Network Performance Discovery (SPAND), a system that determines network characteristics by making shared passive measurements from a collection of hosts. The authors employed such measurement in order to replace the use of individual active ones while maintaining the accuracy, specially to avoid the injection of synthetic traffic. Besides that, SPAND can be used to address the use of redundant network probes by nearby hosts

SLAm. Barford et al. (2009) proposed a framework for detecting and localizing performance anomalies based on using an active probe-enabled measurement infrastructure deployed on the periphery of a network. The authors aim at full coverage through decomposing end-to-end paths. After this decomposition, paths are selected in which probes will be configured. This framework assumes a centralized controller for path se-

lection.

NetQuest. Song, Qiu and Zhang (2006) propose NetQuest, a flexible framework for large scale network measurement. NetQuest uses bayesian experimental design to select active measurements that maximize the amount of information collected about the network path properties. Besides that, the authors apply network inference techniques to reconstruct the properties of interest based on the partial and indirect measurements. Several design requirements are supported, such as better resolution to certain parts of the network and joint design for supporting multiple users who are interested in different parts of the network.

Patil, Kinger and Pathak (2013). Patil, Kinger and Pathak (2013) presented an approach for minimal measurement probe selection for fault localization purposes. The authors claim that the utilization of smaller probe sets reduces computational resources required to localize faults within a network infrastructure. Besides that, the proposed algorithms also decrease the deployment cost of measurement probes on nodes and the activation of measurement sessions.

Gangam and Fahmy (2011). Gangam and Fahmy (2011) modeled the measurement interference problem and showed how to schedule measurement tasks to reduce interference and hence increase measurement accuracy. The authors defined such problem considering that two active measurements are said to interfere when the injected packets of one measurement session are viewed as network traffic by the other which may lead to faulty measurement data. Besides that, the authors claim that shared measurement services offer key advantages over conventional ad-hoc techniques for network monitoring.

Wren. Zangrilli and Lowekamp (2003) developed a bandwidth monitoring tool as part of the Wren network measurement system in order to decrease the measurement traffic on the network. The authors combine active and passive monitoring techniques to reduce the need for intrusive measurements. This is done by passively obtaining measurements from existing application traffic whenever possible, instead of actively probing the network. When there is less traffic on the network, active measurements are used since the intrusiveness of active measurement sessions is bearable.

NSQM. Racz, Donni and Stiller (2010) proposed the Network and Service Quality Measurement (NSQM) architecture, which integrates network- and service-specific measurements and can configure dynamically measurement probes to setup network-wide measurements in an automated manner. NSQM integrates both active and passive mea-

surements and supports a fine-grained selection of traffic to be measured in order to reduce the amount of collected and processed measurement data. Besides that, NSQM supports the correlation of measurement data from multiple locations.

Chaudet et al. (2005). Chaudet et al. (2005) studied the problem of assigning measurement probes for passive and active measurement mechanisms in order to minimize the overhead in terms of human and computational resources. The authors presented a combinatorial view of such problem from which it is derived complexity and approximability results. Besides that, the minimization of the number of measurement probes and the definition of optimal locations is performed regarding monitoring coverage goals.

Eriksson, Barford and Nowak (2008). Eriksson, Barford and Nowak (2008) described a methodology for inferring network structures from measurement data. The authors describe algorithms that enable traffic sources that share network paths to be clustered accurately and topological structure to be inferred accurately with only a small number of active measurement session. Besides that, it is characterized the degree to which missing information can be recovered from passive measurements to further enhances the accuracy of the inferred topologies.

In the following sections, the presented initiatives are classified in order to produce an integrated perspective of such initiatives. The classification is performed regarding the review questions. After that, opportunities and challenges in network-wide approaches to control measurement mechanisms are described.

2.4 Network-Wide Control of Measurement Mechanisms with Different Levels of Intrusiveness

Network measurements can be performed through different levels of intrusiveness. As described in Section 2.1, such mechanisms can be classified in active or passive considering the traffic they inject in the network. Although both mechanisms use measurement probes to deliver network metrics, their control has several differences in spite of some similarities. These differences arise from the peculiarities of each kind of measurement mechanism, *e.g.*, the measurement entities and their relationship. Besides that, some control approaches aim at integrating active and passive measurement mechanisms for specific reasons and goals.

In this section, we describe initiatives on the network-wide control of measurement mechanisms with different levels of intrusiveness. First, the control of passive ones

is described. After that, the steering of active measurements mechanisms is illustrated. Finally, control approaches that mix active and passive measurement mechanisms are presented. In Table 2.2, we provide the specific measurement mechanisms controlled by such initiatives.

Table 2.2: Summary of the Measurement Mechanisms Controlled by Network-Wide Approaches.

Proposal	Measurement Mechanisms
cSamp	IPFIX
DECON	NetFlow
Cantieni et al. (2006)	NetFlow
Lassoued et al. (2011)	NetFlow
CMON	NetFlow
Kamiyama, Mori and Kawahara (2013)	IPFIX
MMPR	Simulated Passive Mechanism
LEISURE	Simulated Passive Mechanism
Suh et al. (2006)	Simulated Passive Mechanism
SPAND	Simulated Passive Mechanism
SLAm	Implemented Active Mechanism
NetQuest	Implemented Active Mechanism
Patil, Kinger and Pathak (2013)	Simulated Passive Mechanism
Gangam and Fahmy (2011)	Simulated Active Mechanism
Wren	Implemented Hybrid Mechanism
NSQM	IPFIX, OWAMP
Chaudet et al. (2005)	Simulated Hybrid Mechanism
Eriksson, Barford and Nowak (2008)	Simulated Hybrid Mechanism

Source: by author (2015).

2.4.1 Control of Passive Measurement Mechanisms

Passive measurement mechanisms do not inject additional traffic that can influence actual network traffic. This non-intrusive nature is one of the most appealing feature of such mechanisms. Therefore, it is expected that the control of passive measurement mechanisms not be intrusive along with other characteristics. Several different mechanisms are used to passively collect data from network infrastructures, as shown in Section 2.1.1.

As one of the most used passive measurement mechanisms, Cisco NetFlow is the most chosen one regarding initiatives to investigate network-wide control. Cantieni et al. (2006) formulated the placement problem (also known as location problem) of NetFlow

probes (also called monitors or metering exporters) as well as their sampling rate in order to achieve a given measurement task. Lassoued et al. (2011) tackled a similar problem, but with an emphasis in the maximum possible accuracy and adaptivity to changes in network traffic conditions. Also, Pietro et al. (2010) proposed DECON aimed at the scalable placement of NetFlow probes. Finally, CMON was developed to achieve a given network traffic coverage ratio through probe placement too (ZANG; NUCCI, 2009).

IPFIX is the IETF standard for passive measurements. Some initiatives on the network-wide control of measurement mechanisms considered this standard, notably using the YAF (Yet Another Flowmeter) (INACIO; TRAMMELL, 2010) as the measurement probe. cSamp (Coordinated Sampling) (SEKAR et al., 2008) provides flow sampling steering, hash-based packet selection, and the distribution of responsibilities across routers with the dissemination of routing manifests for IPFIX-enabled Autonomous System (AS). Kamiyama, Mori and Kawahara (2013) proposed an autonomous load balancing method to maximize the number of monitored IPFIX flows in the entire network.

The network-wide control use of passive measurement mechanisms can be also investigated using implementations developed just for research reasons or simulated mechanisms. MMPR (Measurement-aware Monitor Placement and Routing) (HUANG et al., 2012) and LEISURE (Load-EqualIzed meaSUREment) (CHANG et al., 2015) used simulation experiments for evaluating solutions for probe placement and load balancing across distributed probes, respectively. Suh et al. (2006) also used such experiments to evaluate solutions for probe placement and sampling rate considering minimum cost and maximum coverage. SPAND (Shared Passive Network Performance Discovery) also employed simulation, but in order to determine accurately network characteristics (SESHAN; STEMM; KATZ, 1997).

The network-wide control of passive measurement mechanisms can use the advantages of collecting flows from different measurement probes. One of this advantages is to present a similar level of accuracy found on active measurements, but without the intrusiveness. Besides that, it is feasible to evaluate such control using real management data since there are a significant number of publicly available flow datasets. Computer networking consortia such as Internet2[2] are a common source for these datasets.

[2]Internet2 - http://www.internet2.edu/

2.4.2 Control of Active Measurement Mechanisms

Active measurement mechanisms inject synthetic traffic in the network in order to produce the current end-to-end network performance. However, the traffic injection consumes computational and network resources, thus it should be controlled. Several different intrusive mechanisms are used to deliver network metrics, as shown in Section 2.1.2.

Some researches initiatives developed an active measurement mechanisms to evaluate network-wide control characteristics. Barford et al. (2009) proposed a framework for identifying and localizing network-wide performance anomalies using SLAm (SLA monitor) as the active measurement mechanism. SLAm was developed in the context of other works from the same authors (SOMMERS et al., 2007). NetQuest is a framework to select active measurements that maximize the amount of information gained about the network path properties from active measurement sessions (SONG; QIU; ZHANG, 2006). NetQuest employs its own active mechanism to produce network metrics.

Simulated active measurement mechanisms can be utilized to perform experiments regarding their network-wide control. Patil, Kinger and Pathak (2013) presented an approach for fault localization which aims at minimal probe selection. The authors used simulation to evaluate such approach. Gangam and Fahmy (2011) proposed a model for the measurement interference problem and a solution to schedule measurement tasks avoiding such interference. The very nature of interference experiments influences the choice of an evaluation through simulation experiments.

It is interesting to note the lack of research initiatives which use Cisco IPSLA and IETF TWAMP. One reason that could explain that is the shortage of readily available implementations. There are just partial TWAMP implementations publicly available. In the case of IPSLA, just the Cisco own proprietary implementation is obtainable. Anyway, this situation can change with the IPSLA protocol disclosure through an IETF RFC (CHIBA et al., 2013). Furthermore, active measurement datasets are not readily available, thus, it is difficult to perform evaluations considering real network infrastructures.

2.4.3 Control of Passive and Active Measurement Mechanisms

The network-wide control of measurement mechanisms can consider both active and passive ones. Combining such mechanisms could be used to achieve different goals.

For example, a hybrid control could reduce the need for intrusive (*i.e.*, active) measurements without sacrificing the accuracy of the measurement results (ZANGRILLI; LOWEKAMP, 2003).

Hybrid network-wide control can be deployed to decrease resource consumption. Zangrilli and Lowekamp (2003) proposed Wren bandwidth monitoring tool which aims reducing the mean measurement burden on the network by using passive measurements when an application is running and active measurements when none are running. Network and Service Quality Measurement (NSQM) integrates passive and active measurements mechanisms (IPFIX and OWAMP, respectively) in order to reduce the amount of measurement data to be collected and processed (RACZ; DONNI; STILLER, 2010). Chaudet et al. (2005) also tackled resource issues through the minimization of the number of probes, both active and passive, and finding optimal strategic locations for such probes.

The network-wide control of passive and active measurement mechanisms can be deployed for other goals besides resource consumption. Eriksson, Barford and Nowak (2008) described a methodology for inferring network structure from passive and active measurements which can recover from missing information on the measurements.

Passive and active measurement mechanisms have different characteristics and produce network performance data with particularly properties. For example, extremely detailed view of the network performance could be inferred using both mechanisms. Thus, as a general rule, it would be good to combine their desirable features. However, it possible to say that hybrid network-wide control is less investigated that the control of each kind of mechanism separately. One possible reason for that is the difficulty to integrate different data and configuration models from passive and active measurement mechanisms.

2.5 Distribution Aspects of the Control of Measurement Mechanisms

The control of measurement mechanisms does not necessarily follow the distribution features of the mechanisms themselves. Despite the fact that there is not an widely accepted taxonomy which defines and characterizes distribution aspects of network management models, network management researchers usually consider distribution aspects which bring, at least, centralized and distributed (or decentralized) models (*e.g.*, (PAVLOU, 2007) (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2006) (MARTIN-FLATIN; ZNATY; HABAUX, 1999) (LEINWAND; CONDROY, 1996). Besides being

effectively accepted in network management literature, both models are important in the present work because they present relevant characteristics considering the control of measurement mechanisms.

Several characteristics can be used to classify the control of measurement mechanisms considering distribution aspects. For example, the use of the number of managed elements and the system scalability is a common classification approach (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2006). In the the present work, we do not employ a specific taxonomy neither propose a new one, but we use a simplified taxonomy considering only centralized and distributed control. The main aspect used for our classification is where the majority of the control logic is performed.

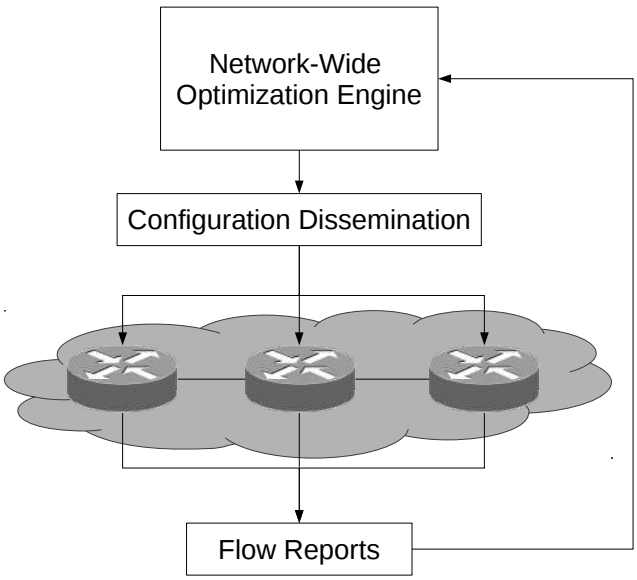
In this section, we describe the distribution models which are used to deliver network-wide approaches to control measurement mechanisms. The presented models are centralized control and distributed control.

2.5.1 Centralized Control of Measurement Mechanisms

The use of a centralized approach to control measurement mechanisms is usually easier to implement and has a simplified architecture. In Figure 2.3, we present a model of a centralized control. This seems to be the most common distribution model. In such control, passive or active measurement probes are connected to the management station which performs the control logic. The management station configures such probes, besides running management applications (*e.g.*, traffic engineering). Measurement probes, which are usually hosted in network devices, are limited to collect data and send, either synchronously or asynchronously, measurement results.

A common approach for the network-wide control of measurement mechanisms is to employ a centralized optimization framework. In fact, it is possible to argue that this is the most used approach considering the literature. For example, several linear and integer programming formulation are used: MILP (Mixed Integer Linear Programming) to optimize the probe placement (HUANG et al., 2012), the load balance of network measurement workloads (CHANG et al., 2015), and the number of required probes (CHAUDET et al., 2005); Integer Linear Program (ILP) to optimize the number of probes required to cover a major portion of network traffic (ZANG; NUCCI, 2009); Mixed-Integer Non-Linear program (MINLP) to optimize probe placement and packet sampling (SUH et al., 2006); and Linear Programming (LP) to perform probe placement, flow sampling and

Figure 2.3: Centralized Control of Measurement Mechanisms Model.



Source: Adapted from Sekar et al. (2008).

hash-based packet selection (SEKAR et al., 2008). Most of these works stated that the problem formulations are NP-hard, thus, several heuristic algorithms to approximate the optimal solution are proposed and evaluated.

Some solutions employed in centralized controllers of measurement mechanisms are outside the spectrum of linear and integer programming. For example: clustering techniques considering traffic sources to infer network infrastructure from measurements (ERIKSSON; BARFORD; NOWAK, 2008); bayesian experimental design to select measurements that maximize the amount of information gained about the network path properties (SONG; QIU; ZHANG, 2006); Lagrange multipliers to formulate which probes should be activated and which sampling rate should be set on these probes in order to achieve a given measurement task (CANTIENI et al., 2006); and cognitive monitoring to drive the sampling rates on the interfaces of network devices in order to achieve the maximum possible accuracy (LASSOUED et al., 2011). Besides that, *ad hoc* centralized techniques are also used: to schedule measurement tasks for interference reduction (GANGAM; FAHMY, 2011); to detect and localize performance anomalies (BARFORD et al., 2009); and to define a minimal probe selection for fault localization (PATIL; KINGER; PATHAK, 2013).

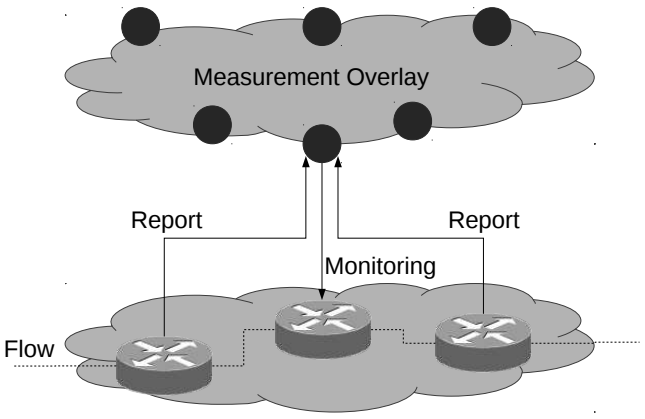
The use of a centralized control could reduce management complexity and operating costs. However, centralized management approaches, despite being wide spread, have

several limitations on current network environments (PRAS et al., 2007). One of these limitations is related to scalability since an increase in the number of managed network devices turns out to increase proportionally the computational load and network traffic required on the management station. Centralization also can lead to fault-tolerance issues because the management station is a Single Point of Failure (SPoF) within the network management system.

2.5.2 Distributed Control of Measurement Mechanisms

The control of measurement mechanisms can be performed in a distributed fashion. In Figure 2.4, we present a model of a distributed control. Distribution features can be employed to improve the control task in respect to scalability, flexibility, and robustness (MARTIN-FLATIN; ZNATY; HABAUX, 1999). In any case, there is a close relationship between the network infrastructure and the way the control system can be organized. The size and/or complexity of the network infrastructures can require the use of specific Distributed Network Management (DNM) technologies to help the network-wide distributed control. Besides that, the measurement data distribution can be performed in different ways.

Figure 2.4: Distributed Control of Measurement Mechanisms Model.



Source: Adapted from Pietro et al. (2010).

P2P technology can be employed to control measurement mechanisms. This technology is known to be successful regarding the support of different kind of applications. For example, DECON (PIETRO et al., 2010) employs a detached P2P coordination sys-

tem aimed at assigning monitoring probes on network devices. The authors claim that it could scale up to large numbers of flows without requiring network topology information, traffic matrices and packet marking. Considering grid environments, Zangrilli and Lowekamp (2003) proposed a bandwidth monitoring tool to adapt measurement mechanisms to changing network conditions and to make efficient use of grid resources.

Measurements sharing can be employed to organize the control system and to feed the control process itself. For example, SPAND (SESHAN; STEMM; KATZ, 1997) uses shared measurements from a collection of network devices to increase the accuracy and timeliness of predictions from passive mechanisms, thus avoiding the use of active measurements. Regarding the determination of link-specific performance problems, NSQM (RACZ; DONNI; STILLER, 2010) supports the correlation of measurement data from multiple locations, enabling the localization of faulty links. Besides that, NSQM can use measurement data correlation to control the aggregation level used by the measurement probes. Finally, Kamiyama, Mori and Kawahara (2013) proposed an autonomous load balancing method where probes exchange information on probe load only with adjacent probes. Thus, probes must select the monitoring targets while maintaining a balanced load among them.

Distribution features can be employed to overcome some limitations of the centralized control of measurement mechanisms (*e.g.*, scalability). Besides that, such distribution can add flexibility in the control tasks, for example, through the sharing of measurements among network devices. However, it is necessary to consider intrinsic costs needed to support a distributed management system, such as an intrinsic traffic consumption related to the communication of the management entities (*i.e.*, the ones that perform the control logic).

2.6 Application Areas of Initiatives on the Network-Wide Control of Measurement Mechanisms

The network-wide control of measurement mechanisms can be employed in several different application areas. Such areas can be used to group applications that aim to achieve similar goals. As mentioned in Section 2.1, network measurements are essential for assessing different management tasks. In this context, the process of data collection from network infrastructures can be controlled regarding these tasks. For example, the measurement mechanisms can be steered to locate faults. Despite the fact that several

network-wide control initiatives addressed more than one application area, it is feasible to describe these initiatives in respect to their main features.

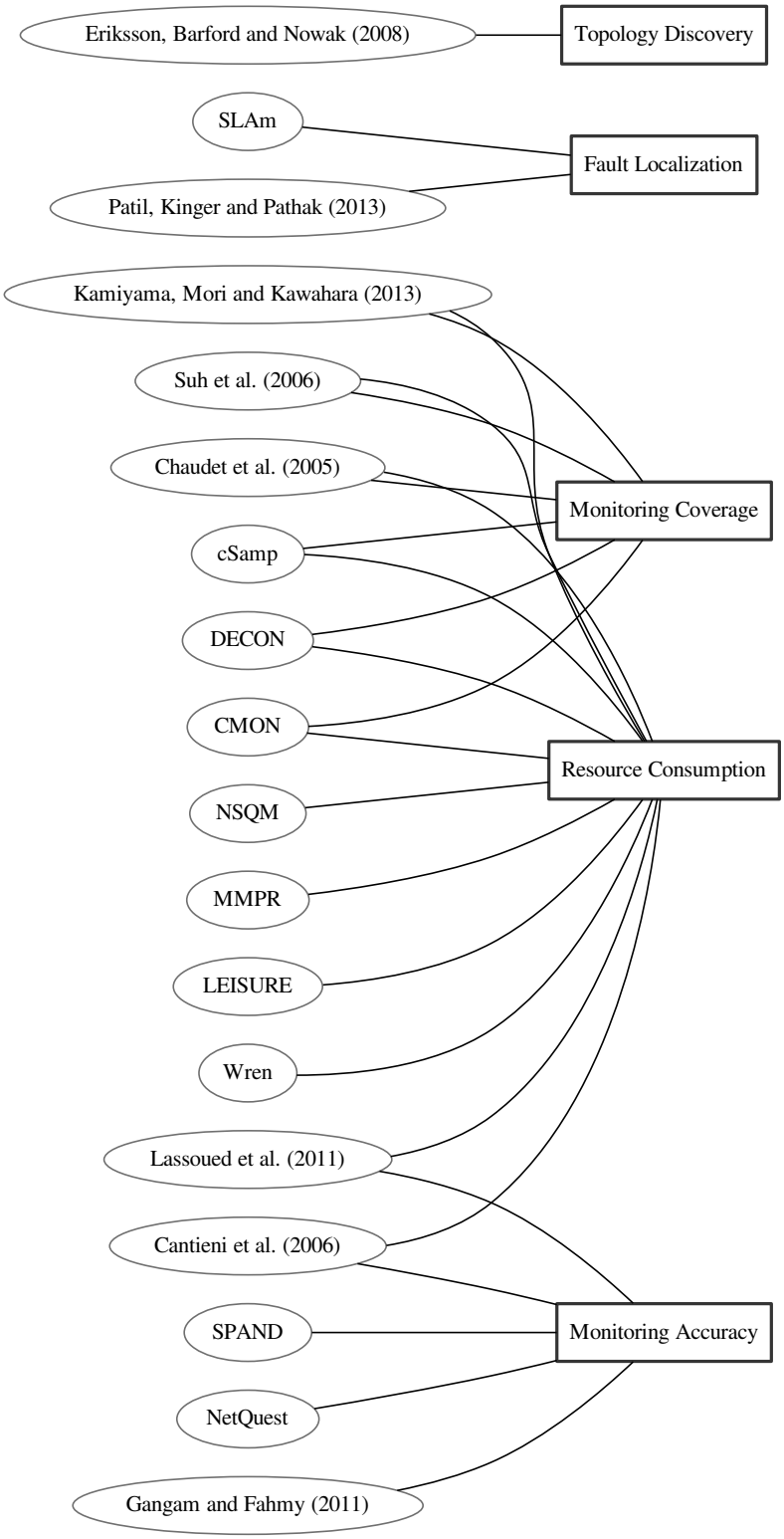
In this section, we describe initiatives on the network-wide control of measurement mechanisms in respect to the application area. In Figure 2.5, we present the classification of such initiatives. It is important to emphasize that a initiative may address more than one area. Then, we describe in more detail each application area. Initially, the applications which have the resource consumption as the main area are presented. After that, the steering of measurements mechanisms for monitoring accuracy purposes is represented. Then, applications that perform fault localization are illustrated. Subsequently, applications that focus at monitoring coverage are presented. Finally, the utilization of network-wide control of of measurement mechanisms for topology discovery is described.

2.6.1 Resource Consumption

One of the most common application area for the network-wide control of measurement mechanisms is resource consumption. Since these mechanisms, both active and passive, are expensive in terms of the consumed resources, approaches to decrease deployment and operation costs are appealing. For example, the measurement mechanism control can reduce the number of the deployed probes or even the intrusiveness of the mechanism itself.

The utilization of optimization frameworks is a common approach to control the resource consumption of measurement mechanisms through measurement probe placement and load balancing. In the present review, cSamp (SEKAR et al., 2008), DECON (PIETRO et al., 2010), LEISURE (CHANG et al., 2015), Chaudet et al. (2005), and Patil, Kinger and Pathak (2013) use such frameworks. The employment of heuristic algorithms is present in some initiatives, such as Suh et al. (2006) and MMPR (HUANG et al., 2012). Finally, the correlation of different measurements is specially employed in hybrid (active and passive) approaches, *e.g.*, NSQM (RACZ; DONNI; STILLER, 2010) and Zangrilli and Lowekamp (2003), in order to choose a less intrusive mechanism when it is feasible.

Figure 2.5: Classification of Network-Wide Control of Measurement Mechanisms in Respect to Application Area.



Source: by author (2015).

2.6.2 Monitoring Accuracy

Measurement mechanisms should provide accurate characterizations of network infrastructures. In this context, single measurement sessions usually result in less accuracy than using more redundant probing for network investigations. Thus, a network-wide control can effectively help to collect information from network portions aiming at monitoring accuracy. On the other hand, such control can avoid measurement mechanism to perform several sessions concurrently (possibly from different network administrators) which can interfere in each other.

The location of measurement probes affect monitoring accuracy. Thus, some initiatives try to address that through the formulation of the placement problem (also known as location problem), such as, Cantieni et al. (2006) and Lassoued et al. (2011). SPAND employs information sharing between probes to increase measurement accuracy (SESHAN; STEMM; KATZ, 1997). NetQuest selects active measurement sessions that maximize the amount of information gained about the network path properties (SONG; QIU; ZHANG, 2006). Finally, Gangam and Fahmy (2011) proposed a solution to schedule measurement tasks avoiding in order to avoid measurement interference.

2.6.3 Fault Localization

Network measurements are essential for identifying and locating network problems. In this context, fault diagnosis is usually the first step on fault management. Therefore, quick detection is essential to recover the network from faults since it provides the necessary information for network remediation. The network-wide control of measurement mechanisms for fault localization usually involves the selection of a measurement probe set and their placement. Besides that, the behavior of such mechanisms can be shaped to adapt to faulty conditions.

Fault localization can be performed through the injection of synthetic traffic to monitor the network and collecting this traffic to perform diagnostics. In this context, active measurement mechanisms are the prime choice for fault localization. Patil, Kinger and Pathak (2013) presented an approach for fault localization which aims at minimal multi-path selection. Barford et al. (2009) proposed a framework for identifying and localizing network-wide service level performance anomalies through the unification of the results from different measurement sessions.

2.6.4 Monitoring Coverage

Monitoring coverage is one of the main concerns of network administrators when deploying measurement mechanisms. This coverage is usually considered in terms of time, geography, and applications (*i.e.*, traffic characteristics). In this context, network-wide control can be employed to increase the fraction of flows being probed in the network infrastructure. For example, such control can coordinate the activation of measurement sessions by different nodes to enable a better monitoring coverage.

Several initiatives presented in the present literature review have an emphasis to achieve network-wide monitoring coverage goals while respecting (and possibly decreasing) resource consumption. This is usually done addressing the placement problem and packet sampling. cSamp (SEKAR et al., 2008), DECON (PIETRO et al., 2010), Suh et al. (2006), Chaudet et al. (2005), CMON (ZANG; NUCCI, 2009), and Kamiyama, Mori and Kawahara (2013) are examples of such initiatives.

2.6.5 Topology Discovery

The network-wide control of measurement mechanisms can be used to perform topology discovery. Understanding the network infrastructure through empirical measurements is important for different network management tasks, such as traffic engineering and troubleshooting (ERIKSSON; BARFORD; NOWAK, 2008). However, there is an inherent trade-off between the number and the information carried by measurement sessions and the information about the topology that can be collected by such sessions.

The utilization of a network-wide control of measurement mechanisms offers the possibility to perform topology discovery with less resource consumption and more accuracy than employing these mechanisms in *ad hoc* manner. Eriksson, Barford and Nowak (2008) described a methodology for inferring network structure from passive and active measurements which can recover from missing information on such measurements.

2.7 Trends and Analysis of the Future of Network-Wide Control of Measurement Mechanisms

Measurement mechanisms are one of the most important tools employed by human administrators. Regarding network management tasks, such mechanisms are used on several contexts and for different ends. However, there are limitations on such use, specially considering the required computational and human resources. This is particularly true considering the increasing complexity of computer networks. Thus, it is important to investigate approaches to improve the control of measurement mechanisms as well as their use on network infrastructures.

As the survey described in this chapter illustrates, there are several initiatives on the control of measurement mechanisms. In this context, the mechanisms themselves should include technical mechanisms to limit the use of network capacity and memory (e.g, OWAMP (SHALUNOV et al., 2006)). Besides that, some control approaches aim at single devices, *e.g.*, setting the default configuration on the resource use limits to low values. We chose to focus on only on network-wide approaches since they can provide a larger impact on the network infrastructure as whole. It is possible to say that there is substantial interest in the network-wide control of measurement mechanisms, thus we explore in this section some of the research areas which could potentially attract more attention. Examples of these areas are the architecture and relationship of test and control protocols, measurement federations, and approaches to deploy large-scale measurements.

Some measurement mechanism consist of inter-related protocols, usually a control protocol (used to initiate, start, and stop test sessions) and a test protocol used to exchange test packets (as an example, TWAMP-Control and TWAMP-Test (HEDAYAT et al., 2008)). Besides that, the roles that composed the architecture of such mechanisms can be deployed in different nodes (as an example, the metering exporter and the collector in case of IPFIX (CLAISE, 2008)). The relationship of these protocols and localization of roles could be exploited in a network-wide control of measurement mechanisms. For example, such network-wide control could be employed to support load balancing as well as fault-tolerance features. Also, resource control techniques can be implemented considering the different entities. For example, memory consumed by an unauthenticated OWAMP-Test session should be reclaimed after the OWAMP-Control connection that initiated the session is closed (SHALUNOV et al., 2006).

Explicit measurement federations could help network operators to troubleshoot

perceived abnormalities as well as improve network middleware regarding faults and performance issues. This can be done to assure SLAs aimed at end users. For example, the PERFormance Service Oriented Network monitoring ARchitecture (perfSONAR)[3], SamKnows[4], Grenouille[5], and Measurement Lab (M-Lab)[6]. Measurement federations employ several monitoring and diagnosing tools using an integrated interface and information base. However, there is a lack of algorithms to provide an effective network-wide control of such tools in these federations. Besides that, novel approaches are needed to foster wider adoption of explicit measurement federations.

The IETF chartered the Large-Scale Measurement of Broadband Performance (LMAP) Working Group (WG) in order to standardize the LMAP measurement system for performance measurements of broadband access devices, such as, for example, home and enterprise edge routers, personal computers, mobile devices, and set top box. The WG should specify an information model, the associated data models, and select/extend one or more protocols for secure control and report of Measurement Agents (MAs). So far, there are only RFC on LMAP, concerning use cases (LINSNER et al., 2015). Thus, most of the WG documents are Internet-Drafts (I-Ds), which can be significantly changed before standardization. In any case, several important features in the context of a network-wide control are currently considered out of scope by the LMAP WG, such as discovering and provisioning the MAs, a management protocol to bootstrap the MAs in measurement devices, deciding the set of measurements to run, and the coordination and information sharing on the MAs.

2.8 Final Remarks

Network monitoring is becoming more important nowadays because of the number of critical services which are supported in the network infrastructures. In order to uncover network behavior, it is necessary to employ both active and passive measurement mechanisms. However, there are several challenges concerning such mechanisms, such as those related to their scalability, performance, and robustness. In this context, the development of applications for the control of such mechanisms keeps advancing.

The control of measurement mechanisms can be either network-wide or aimed at

[3]perfSONAR - http://www.perfsonar.net/
[4]SamKnows - http://www.samknows.com/
[5]Grenouille Project - http://www.grenouille.com/
[6]M-Lab - http://www.measurementlab.net/

single devices. In the present literature review, we focused at network-wide since in order to reveal global network behavior is usually necessary to go beyond single measurement sessions. The network-wide control of measurement mechanisms can be deployed for different levels of intrusiveness, distribution approaches, and application areas. In spite of the availability of several solutions for such control, the problem formulation considered by the the research initiatives is usually NP-hard and the parameters are dynamic.

In summary, an efficient network-wide control of measurement mechanisms is still a difficult tasks in spite of the new research advances. Members of the Network Management Research Group (NMRG) of the Internet Research Task Force (IRTF) highlighted some research challenges to be investigated on future network and services management (GRANVILLE; FESTOR, 2012). Among these challenges, large-scale network-wide measurements, network-wide configuration, and autonomic management were reported. In this context, NRMG organized a workshop on large-scale network measurements (BAJPAI; SCHÖNWÄLDER, 2014). Thus, it is possible to say that, considering the present survey, improvements in the network-wide control of measurement mechanisms are valuable and desired achievements.

3 P2P-BASED NETWORK MANAGEMENT

Network management has become an important discipline, with several solutions being proposed to tackle the increasing management demands. Such solutions, for example, historically addressed the delegation of management tasks (*e.g.*, Management by Delegation - MbD (GOLDSZMIDT; YEMINI, 1995)), support for high-level management goals (*e.g.*, Policy-Based Network Management - PBNM (SLOMAN, 1994)), more proper support for configuration management (*e.g.*, NETCONF (ENNS M. BJORKLUND, 2011)), and self-*-based automation and optimization of management tasks (*e.g.*, autonomic network management (SAMAAN; KARMOUCH, 2009)). In addition to these solutions, the employment of Peer-to-Peer (P2P) technology is also a possibility to further improve network management.

A P2P-Based Network Management (P2PBNM) system creates a management overlay over the managed network. In such an overlay, peers have a double role: besides acting as regular peers they also perform management tasks (GRANVILLE et al., 2005). P2PBNM holds the promise of incorporating key features of P2P technology into network management systems, such as high distributed processing and support for collaborative work. In addition, P2P technology deal with Internet's idiosyncrasies (*e.g.*, broken network-layer end-to-end communication as the result of intermediate boxes like firewalls and NAT) more effectively in comparison with traditional network management technologies, since the latter have not been conceived taking current Internet's peculiarities in mind, while P2P systems emerged already operating considering the current Internet patched architecture.

In the first moment, P2PBNM investigations carried out by the research community addressed aspects related to decentralized management, including, for example, load balance of management peers (PANISSON et al., 2006) and self-organization of management overlays (BINZENHÖFER et al., 2006). Afterwards, novel initiatives investigated the integration of P2PBNM with other management approaches like autonomic management (MARQUEZAN et al., 2008), cooperative management (MELCHIORS et al., 2011), and model-driven architectures (FALLON et al., 2007). Finally, complementary research efforts investigated other P2PBNM related aspects, such as consistency maintenance of states of management data (NOBRE; GRANVILLE, 2010). Since P2PBNM has received a significant attention from the research community, it is relevant to have literature review of the key P2PBNM research efforts, surveying the different initiatives carried out in the

last years

This chapter is organized as follows. First, we present an overview of P2P technology and P2PBNM concepts. Second, we discuss the method employed to perform the literature review. After that, the surveyed initiatives are highlighted and a comparison between such initiatives is described. Then, a discussion of current challenges and future research trends is presented. Finally, this chapter is closed with concluding remarks.

3.1 Background

In this section, we present the state-of-the-art on P2P technology and Peer-to-Peer (P2P)-Based Network Management (P2PBNM) concepts. P2P technology constructs application specific overlay networks, usually running over the Internet as the underlay. In these overlays, resources distributed in several peers are used in order to implement applications (*e.g.*, file sharing). This technology has been used to support diverse applications and services (*e.g.*, file sharing, instant messaging, VoIP, collaborative work), often with varying conceptual definitions. In this section, we clarify the context and concepts behind the use of P2P technology, in addition of presenting an overview of P2PBNM concepts.

3.1.1 P2P Technology in a Nutshell

The term "Peer-to-Peer" (P2P) can be applied to several and distinct contexts. Usually, in the computer science literature, P2P is followed by words like system, application, infrastructure, overlay, and network. Androutsellis-Theotokis and Spinellis (2004) stated that *"it is fair to say that there is not a general agreement on what 'is' and what 'is not' peer-to-peer"*, attributing such a lack of agreement to the fact that systems or applications are labeled "P2P" not because of their internal behavior, but because of their external appearance. Rodrigues and Druschel (2010) reviewed P2P technology and stated three fundamental properties: i) high degree of decentralization, since peers implement both client and server functionality; ii) self-organization, thus, little (or no manual) configuration is needed to maintain the system after peers' introduction; and iii) multiple administrative domains, *i.e.*, peers can be owned and controlled by different organizations or individuals.

P2P is employed in different contexts, associated with different levels of abstrac-

tion, and interpreted in distinct manners. Despite the fuzzy definitions and terminologies associated with P2P technology, Androutsellis-Theotokis and Spinellis (2004) grouped the use of such technology into P2P infrastructures and P2P applications. They define these groups considering only one kind of application, the P2P content distribution, which was the most popular and developed technology at the time their work was published. However, over the years, other types of P2P technology emerged. We argue that it is possible to analyze and regroup use of such technology at this moment, for example, into P2P infrastructures, P2P infrastructures for specific applications, and P2P applications. Examples related to each one of these groups are presented below.

P2P infrastructures. Infrastructures employed to deliver underlying conditions and services for applications. Examples include: routing and location (LI; JIN, 2014), reputation (JAVANMARDI et al., 2014), topology management (PAPADAKIS et al., 2009), performance (XIE; MIN; DAI, 2009), connectivity (JIMENEZ; OSMANI; KNUTSSON, 2009), and security (SAINI; CHATURVEDI; YADAV, 2014). Some well-known works related to P2P infrastructure are JXTA (GONG, 2001), Pastry (BJUREFORS; LARZON; GOLD, 2004), and Chord (STOICA et al., 2003).

P2P infrastructures for specific applications. This group is comprised of uses of P2P technology that present a very tight relationship between the P2P infrastructure and the application running on top of it. Examples are multiplayer games (GAUTHIERDICKEY; RITZDORF, 2014), workflow (ZHANG et al., 2015), Voice over IP (VoIP) (AGUIRRE; ALVAREZ; ZAMORA, 2015), and multimedia (MEGIAS, 2015).

P2P applications. Applications that make use of P2P infrastructures. Examples of current popular P2P applications are: file sharing (LU; WANG; LI, 2015), P2P television (P2PTV) (TRAVERSO et al., 2014), and databases (AGHAMAHMOODI; RANKOOHI; AGHAMAHMOODI, 2014).

Androutsellis-Theotokis and Spinellis (ANDROUTSELLIS-THEOTOKIS; SPINELLIS, 2004) also classified P2P applications into five categories based on the purposes associated with the applications. A look at the recent literature shows that the definition of those categories is still relevant and meaningful, and because of that we review them below.

Communication and collaboration. These applications usually focus on providing direct communication among peers (*e.g.*, instant messaging applications such as

Google Hangouts (GOOGLE, 2015)). The possibility of direct communication can enable collaborative behaviors.

Distributed computing. In this category, it is possible to find applications that need to compute massive tasks. In order to accomplish that, such applications break down the tasks into smaller ones and distribute them among the available peers of the P2P infrastructure (*e.g.*, Seti@Home (KORPELA et al., 2001)).

Internet service support. This group is composed of applications that use P2P infrastructures to provide services such as: videoconferencing and telecommunication (*e.g.*, Skype (BONFIGLIO et al., 2007)), Web portals (*e.g.*, Osiris (OSIRIS, 2015)), and streaming (SUN et al., 2014).

Database systems. The applications of this group are able to use the P2P infrastructure as a database system, instead of a traditional central repository (EBRAHIMI; RANKOOHI, 2014).

Content distribution. This is the most popular category of application. In this context, files are spread along the P2P infrastructure and can be accessed through file sharing or content distribution application (*e.g.*, BitTorrent (COHEN, 2015)).

Some of the major contributions from the P2P research community are related to the variety of applications that can be developed exploiting $i)$ the features introduced by P2P infrastructure (*e.g.*, scalability, robustness, and reliability), and $ii)$ the design concepts behind the P2P applications (*e.g.*, distributed algorithms, collaboration on executing tasks, sharing information, decentralized decision-making). Encouraged by the features and design concepts introduced by P2P technology, the network management community started to explore this technology on their solutions.

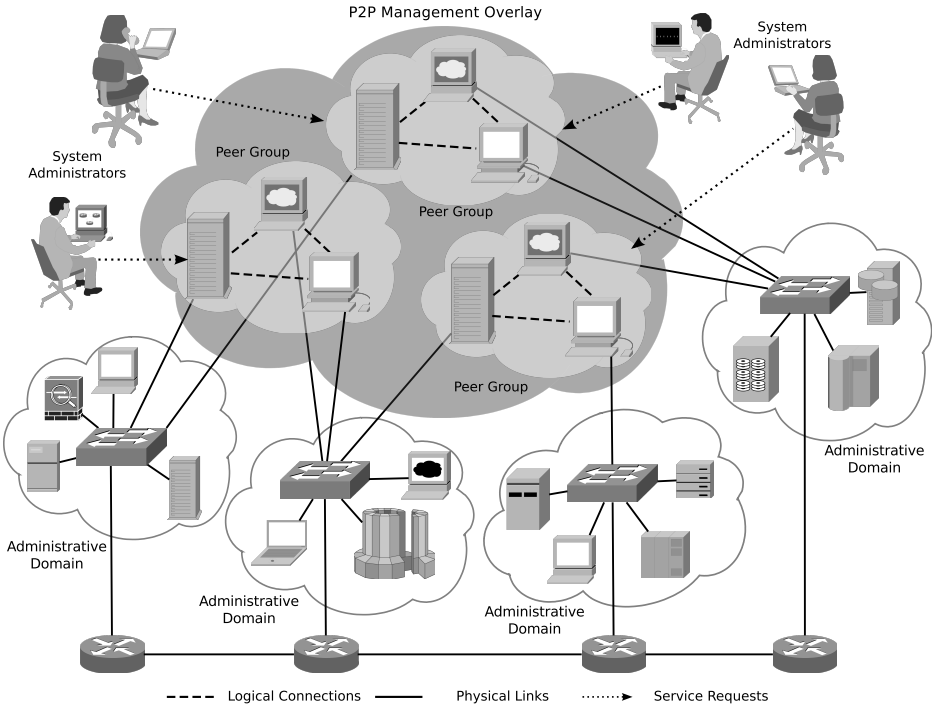
3.1.2 Peer-to-Peer (P2P)-Based Network Management Concepts

There is substantial research on models that address the structure of interactions required to execute network management tasks. In these models, various forms of decentralization (*i.e.*, distribution) are used to produce, access and store management data. In the traditional centralized model, a single management station typically controls the whole managed infrastructure. Scalability issues of the centralized model motivated intense research on Distributed Network Management (DNM) alternatives. Some work that has emerged in the management literature classified the various flavors of DNM solutions.

A possible approach to decentralize the execution of management tasks is to employ P2P technology. Such technology is known to be successful regarding the support of different kind of applications. Therefore, it is plausible to infer that P2P technology could also succeed for DNM.

Several investigations use the abstraction of a P2PBNM model to explain how P2P technology is employed to perform management tasks. One of these investigations was conducted by Granville et al. (2005) in which P2PBNM is described as an extension of Management by Delegation (MbD) model (GOLDSZMIDT; YEMINI, 1995). In MbD, managers delegate the execution of tasks to Mid-Level Managers (MLMs) located closer to agents (*e.g.*, transferring management scripts), which reduces network bandwidth consumption and decentralizes the execution of management tasks. The authors merge the services introduced by P2P technology with the MbD model in order to define a P2PBNM model. The Figure 3.1 presents a general view of P2PBNM model proposed by Granville et al. (2005). The authors also use their P2PBNM model to highlight some possibilities of P2PBNM: human-based cooperative management, improved connectivity for message exchange, and management tasks load balancing.

Figure 3.1: P2P-Based Network Management (P2PBNM) model



Source: by author (2015).

Figure 3.1 presents a P2P overlay in which resources are used to perform management tasks. The choice of protocols used to build a P2P management overlays differs

significantly among P2PBNM research initiatives and prototypes. Some initiatives reuse well-established P2P protocols in order to exploit the properties of these protocols, which were already described in the literature. For example, the *Cyclon* protocol (VOULGARIS; GAVIDIA; STEEN, 2005) is used on management overlays (DUARTE et al., 2011). Besides that, this reuse eases the development of P2PBNM system since the focus can remain on the management tasks. On the other hand, some initiatives (WUHIB et al., 2009) build a P2P protocol from the scratch focusing only on the required features/properties to make the management overlay operational. A P2P protocol designed specifically for DNM needs does not bring "compulsory" overheads needed to address requirements of general purpose P2P systems. Therefore, the P2PBNM system efficiency can be increased.

The approach to distribute management tasks also varies in P2PBNM investigations. One possibility is the utilization of a Service-Oriented Architecture (SOA) (JONES, 2005). When using SOA, management peers perform management tasks through management services (PANISSON et al., 2006). In this context, the result of these services is the execution of a management task. In general, these services are requested by system administrators (as shown in Figure 3.1) or automation procedures (which can be hosted either inside the peers themselves or even in a centralized party). The software portion that is responsible to deliver management services is usually known as a *management component*. These components vary largely; *e.g.*, from simple monitoring probes to complex autonomic policies interpreters.

The power of P2P systems as well as their features and properties is intrinsically related to the approach used by peers to communicate. P2PBNM systems usually employ some form of peer aggregation instead of using a flat overlay for message exchange. Figure 3.1 highlights the concept of peer groups which are groups of peers that share one or more properties, *e.g.*, provided management services. Peer groups can support several desirable properties. For example, when aligned with replication of management components among different peers, peer groups can provide improved fault-tolerance and load balancing (PANISSON et al., 2006). Besides that, peer groups can be also used to decrease the number of exchanged management messages (NOBRE; GRANVILLE, 2010). Some investigations also exploit the concept of epidemic communications to aggregate management information in a P2P approach, specially in monitoring tasks (WUHIB et al., 2009) (WUHIB; STADLER, 2011).

P2P technology may be a valuable tool to enable inter-domain distributed management (FIORESE; SIMõES; BOAVIDA, 2009). P2PBNM systems usually use Application

Layer Routing (ALR) as their main message passing resource and ALR adapts more easily to administrative domains boundaries. In this context, logical connections among the peers are mapped into physical links. In Figure 3.1, we illustrate a scenario where participating peers (of peer groups) spread over different administrative domains; logical connections among peers are represented by dashed lines. Management entities in traditional management rely on the IP routing to communicate with one another, thus, if the default route is unavailable alternative routes cannot be selected. Furthermore, boundary boxes (*e.g.*, circuit gateways, packet filters) break the network layer logic. The use of ALR can overcome network layer issues or, at least, optimize connectivity using information from the network layer (RIMAC et al., 2010).

In the following sections, several initiatives of P2P-Based (or, at least, -Enabled) network management are presented. These initiatives are mapped and grouped in order to produce a consistent overview of the employment of P2P technology in network management research scenario.

3.2 Method for the Literature Review

The management of computer networks is concerned with the control of various network components in order to reach a desired system state. Given the solutions that have been presented along the years in the network management literature, it is clear that the materialization of DNM can be accomplished following different approaches and technologies. In the present work, we performed a literature review (considering the author's best knowledge) of the current efforts on the employment of P2P technology on network management. To the best of our knowledge, a survey of such approaches has not been provided so far. The method employed for the literature review is based on the one proposed by Magdaleno, Werner and Araujo (2012).

The remaining of the section presents the method used in the present survey. First, the objectives and the review questions are described. After that, two main phases are proposed to gather, evaluate, and analyze the literature concerning the employment of P2P technology on network management: the planning and execution phases.

3.2.1 Objectives and Review questions

The objectives of the literature review are the characterization of the state of the art regarding P2PBNM approaches and exploration of future works on such approaches. Thus, in order to achieve these objectives, this review aims to answer the following review questions:

- What functional network management areas can be tackled by P2P technology?
- What network management approaches can be deployed using P2P technology?
- What management methods can be employed using P2P technology?
- What are the opportunities and challenges for the employment of P2P technology in network management?

We provide more details about the challenges related to these features in the future research directions section (Section 3.7). In the following, we briefly describe the features we focus on this literature review.

The employment of P2P technology can be realized for management tasks related to different functional areas. In simple terms, considering the FCAPS model, such tasks can be classified as on Fault Management, Configuration Management, Accounting Management, Performance Management, and Security Management. In particular, several P2PBNM initiatives address more that one area since it is usually difficult to effectively classify management tasks in strictly separated functions areas. In this context, we focus at the areas explicitly stated as the main addressed ones by the authors.

Different management approaches can be used by P2PBNM. *A priori*, one can argue that P2PBNM is an example of Distributed Network Management (DNM). However, it is feasible that some form of centralization be used for specific processes in a P2PBNM system (*e.g.*, storage of management data). Besides that, P2P technology can be used either in an *ad hoc* manner or in addition to concepts and entities found on well established DNM models, such as Policy-based Network Management (PBNM). Finally, there are approaches related with the automatization of management tasks, such as autonomic and self management, and pro-active management.

P2PBNM initiatives can use different management methods to perform their tasks. Some methods can use intrinsic properties of P2P technology to enhance the applicability of the methods themselves. In the literature review, we find 11 main methods: control theories; optimization theories; economic theories; machine learning and genetic algorithms;

logics; probabilistic, stochastic processes, queuing theory; simulation; experimental approach; design; monitoring & measurements; data mining and (big) data analytics.

3.2.2 Planning Phase

The planning phase of the present literature review explores the defined objectives and review questions about the employment of P2P technology in network management to produce search keywords and inclusion and exclusion criteria. The definition of such keywords and criteria was performed considering, as an initial review, the meta-analysis of literature reviews performed in the context of three M.Sc dissertations and two Ph.D thesis on different aspects of P2PBNM. After that, the review questions were answered regarding the papers in order to extract relevant information.

The keywords used on search process are *P2P* and *network management*. The set of papers which was retrieved using these keywords was significant. In any case, such papers still needed to surpass the exclusion criteria. Furthermore, we also studied the initiatives referenced by this set of papers and the ones that reference them in order to finish the definition of the search keywords.

Inclusion and exclusion criteria were defined to adjust and calibrate the survey focus. We aim at the employment of P2P technology in network management as our review topic. These criteria is used to delineate the final set of papers regarding this topic. The inclusion criteria is basically the mention of at least one of the keywords in the keyword fields. On the other hand, we also defined exclusion criteria in order to omit papers with content which is not relevant for the present review. We were not interested on works that address the management of P2P technology, *e.g.*, controlling the network traffic load due to P2P applications in an infrastructure. Finally, the included works must describe some approach to evaluate their own proposals (experiments, case studies, etc).

3.2.3 Execution Phase

This section describes in more detail how the selection process of the present review was performed. Initially, keywords were used to collect possibly relevant papers on the survey topic. In a second step, the set of collected papers was processed to find and eliminate duplicates. After that, titles and abstracts were read to apply the exclusion crite-

ria. Papers that did not adapt within the scope of this survey were excluded. Finally, with the complete list of relevant documents, information concerning the research questions was extracted.

The execution phase of the literature review explored queries about the survey topic in addition to the the initiatives found on the meta-analysis performed on literature reviews. Such queries were executed considering papers from 2010 to 2015 on network management conferences supported by the Institute of Electrical and Electronics Engineers (IEEE) and International Federation for Information Processing (IFIP): IEEE/IFIP Network Operations and Management Symposium (NOMS) and IEEE/IFIP International Symposium on Integrated Network Management (IM). Besides that, we also included initiatives from the International Conference on Network and Service Management (CNSM), which is recognized as the most competitive network management conference. In order to search for the P2PBNM initiatives on the proceedings of these conferences, we used the following digital libraries: IFIP Digital Library and IEEE Xplore Library. We assumed that the digital libraries are reliable and that selected papers went under peer review which served as a quality filter. The papers selected in the performed queries were the candidates ones to be included in the survey.

The candidate papers were retrieved and they were organized in a list to allow duplicate elimination and to apply the exclusion criteria. A final validation is performed by two different persons and the output is the final set of papers. After that, this set is confront with the research question in order to extract the main characteristics of the employment of P2P technology in network management.

3.3 Surveyed Initiatives

The objectives of the present literature review is the characterization of the state of the art of the employment of P2P technology in network management. Thus, the complete list of relevant initiatives considering the selected keywords and inclusion and exclusion criteria are classified using the proposed review questions.

In Table 3.1, we provide the classification of the surveyed initiatives according to the review questions. It is important to emphasize that an initiative may address more than one feature in each question. Then, we describe such initiatives.

ManP2P. Panisson et al. (2006) proposed ManP2P, a P2PBNM framework based on JXTA (GONG, 2001). This framework provides load balancing mechanisms for ma-

Table 3.1: Summary of the Intiatives on P2P-Based Network Management.

Proposal	References	Functional Areas	Management Approaches	Management Methods
ManP2P	(PANISSON et al., 2006), (DUARTE et al., 2011), (MELCHIORS et al., 2011)	Fault, Performance, Security	Policy-Based Network Management, Autonomic and Self-Management	Control Theories, Logics
DNA	(BINZENHÖFER et al., 2006)	Fault, Performance	Autonomic and Self-Management	Data Mining and Data Analytics
DECON	(PIETRO et al., 2010)	Performance	Distributed	Optimization Theories
Cartographer	(KRUPCZAK, 2015)	Fault	Distributed	Logics
G-GAP	(WUHIB et al., 2009)	Performance	Distributed	Probabilistic, Stochastic Processes, Queuing Theory
Ambient Networks Management	(SIMON et al., 2005), (KAMIENSKI et al., 2006), (MATHIEU et al., 2007)	Configuration	Policy-Based Network Management, Autonomic and Self-Management	Logics
SMC	(LUPU et al., 2008), (SCHAEFFER-FILHO; LUPU; SLOMAN, 2014)	Configuration	Policy-Based Network Management, Autonomic and Self-Management	Control Theories, Logics
Fallon et al. (2007)	(FALLON et al., 2007)	Configuration	Telecommunications Management Network	Control Theories
S^3	(YALAGANDULA et al., 2006), (BLANTON et al., 2012)	Performance	Distributed	Control Theories, Optimization Theories
PRISm	(JAIN et al., 2008)	Performance	Distributed	Probabilistic, Stochastic Processes, Queuing Theory
Idhaw et al. (2006)	(IDHAW et al., 2006)	Configuration	Policy-Based Network Management	Logics
Fiorese, Simões and Boavida (2009)	(FIORESE; SIMõES; BOAVIDA, 2009), (FIORESE; SIMOES; BOAVIDA, 2011)	Performance	Management by Delegation	Probabilistic, Stochastic Processes, Queuing Theory
DITA	(MORARIU; STILLER, 2011), (MORARIU; RACZ; STILLER, 2010), (MORARIU; STILLER, 2008)	Performance	Distributed	Data Mining and Data Analytics
Pattern-Based Management Programs	(LIM; STADLE, 2001)	Performance	Mobile Agents-Based Network Management	Control Theories
P2P-CBR	(TRAN; SCHÖNWÄLDER, 2007)	Fault	Autonomic and Self-Management	Machine Learning and Genetic Algorithms
Barshan, Fathy and Yousefi (2009)	(BARSHAN; FATHY; YOUSEFI, 2009)	Security	Management by Delegation	Probabilistic, Stochastic Processes, Queuing Theory
Nobre and Granville (2009)	(NOBRE; GRANVILLE, 2009), (NOBRE; GRANVILLE, 2010)	Fault, Configuration	Autonomic and Self-Management	Machine Learning and Genetic Algorithms, Probabilistic, Stochastic Processes, Queuing theory
Santos et al. (2008)	(SANTOS et al., 2008), (SANTOS et al., 2010)	Fault	Distributed	Probabilistic, Stochastic Processes, Queuing Theory
Mobi-G	(STINGL et al., 2014)	Performance	Distributed	Probabilistic, Stochastic Processes, Queuing Theory
Badis, Doyen and Khatoun (2015)	(BADIS; DOYEN; KHATOUN, 2015)	Security	Distributed	Probabilistic, Stochastic Processes, Queuing Theory
SMON	(GAO et al., 2010)	Configuration	Distributed	Probabilistic, Stochastic Processes, Queuing Theory

Source: by author (2015).

nagement applications through the use of peer groups and management applications are developed through management services. The framework supports a MbD infrastructure composed of Mid-Level Managers (MLMs), Top-Level Managers (TLMs), and agents. Melchiors et al. (2011) proposed a model that defines the ManP2P entities according to the different functions played by the management peers (*e.g.*, network administrator interface, managed resources control) and an architecture that integrates distributed functionalities such as publish-subscribe notification and distributed storage services. Finally, Duarte et al. (2011) proposed an extension to ManP2P (ManP2P-ng), which focus in materializing distributed self-healing features through the use of P2P management overlays and high-level descriptions called workplans.

Distributed Network Agent (DNA). Binzenhöfer et al. (2006) employed P2P overlays to address fault and performance management in a distributed and self-organized system that is based on DNAs (JUN et al., 2007). The distributed infrastructure is achieved by the employment of overlays formed by structured P2P networks using Distributed Hash Tables (DHTs) on top of the monitored network infrastrcuture. In this sense, groups of DNAs composing a DHT are able to communicate to exchange monitoring information and ask for other DNAs to execute tests in order to find eventual network failures.

DECON. Pietro et al. (2010) proposed a P2P coordination system aimed at assigning passive monitoring probes. DECON architecture makes assignment decisions about the match between monitoring probes and the set of flows they monitor. This architecture aims at increasing network coverage spreading the management load (due to monitoring probes) across different machines. This is done using a P2P overlay detached from the physical network. Authors claimed that DECON scales up to large numbers of flow records without requiring network topology information, traffic matrices, and packet marking.

Cartographer. Krupczak (2015) proposed an approach to collect and process management data without relying in a centralized repository. Cartographer agents self-organize into P2P management overlays in order to exchange management information, software updates, and events. Such agents play the roles of managers and agents (in the sense used in the manager-agent approach). In this context, Cartographer agents communicate with each other to poll and store data, run distributed decision-making algorithms, and self-propagate.

G-GAP. Wuhib et al. (2009) proposed a protocol in order to investigate the use of gossip for continuous P2P monitoring of network-wide aggregates under crash fail-

ures. Monitoring tasks are computed from local management variables using aggregates functions such as sum, max, and average. Authors claimed that G-GAP is robust against failures that are discontinuous in the sense that neighboring peers do not fail within a short period. Thus, G-GAP supports the correctly contributions from peers that have failed in order to generate its aggregates.

Ambient Networks Management. Simon et al. (2005) detailed the employment of a P2P approach to enable management composition for Ambient Networks (ANs) (BRUNNER et al., 2005). Kamienski et al. (2006) proposed a P2P infrastructure to provide a better support on the management of policies, keeping the same hierarchical concept behind the PBNM model. However, instead of using a single PDP, the authors replaced it using Policy Decision Nodes interconnected by a DHT network. Mathieu et al. (2007) proposed the employment of P2P technology in the self-management of contexts associated to the overlays of ANs through the definition of Service-aware Adaptive Transport Overlays (SATOs).

Self-Managed Cells (SMC). Lupu et al. (2008) proposed an architectural pattern for ubiquitous computing applications, aiming at different levels of scale. Each SMC is autonomous and uses policy-based techniques for driving adaptation decisions. In this context, each managed device is logically connected with only one SMC. Among different cross-SMC interactions, it is described P2P interactions and federations (SCHAEFFER-FILHO; LUPU; SLOMAN, 2014). SMC can be used for health monitoring applications, such as those related to body sensor networks.

Fallon et al. (2007). The authors proposed a P2P approach to autonomously form network management topologies in order to accomplish specific network management tasks (FALLON et al., 2007). Network Elements (NEs) are grouped into clusters and these clusters form P2P overlays that can be arranged hierarchically according to the requirements of the management task to be executed. The self-forming property is associated to the process of preparing the network management infrastructure. Based on parameters associated to the NEs, the clusters are formed, maintained, and self-optimized in the presence of environment changes.

S^3. Yalagandula et al. (2006) proposed S^3, a Scalable Sensing Service (thus, the "S^3" acronym), using concepts from SDIMS (Scalable Distributed Information Management System) (YALAGANDULA; DAHLIN, 2004) and Distributed Hash Tables (DHTs) algorithms. S^3 enables personalized sensing of the environment as dictated by applications. Such sensing is performed through the construction of network service overlays

composed by web service enabled sensor pods (BLANTON et al., 2012). These pods connect to a sensing information backplane which provides a substrate to aggregate the measured data.

PRecision-Integrated Scalable Monitoring (PRISm). Jain et al. (2008) proposed PRISm, a scalable monitoring service that makes imprecision an abstraction for its DHT-based aggregation service. PRISm introduces the notion of conditioned consistency that quantifies imprecision along a three-dimensional vector: arithmetic imprecision bounds numeric inaccuracy, temporal imprecision bounds update delays, and network imprecision bounds uncertainty due to network and node failures.

Idhaw et al. (2006). The authors proposed the utilization of P2P technology to improve policy distribution for an IP-based Airborne Network (IDHAW et al., 2006). In this context, Police Decision Points (PDPs) are implemented as peers of a P2P management overlay. The employment of P2P technology provides distributed services (*e.g.*, discovery mechanisms) and is able to handle specific characteristics of this network, such as highly dynamic topology and bandwidth limitations.

Fiorese, Simões and Boavida (2009). The authors focused their proposal on enhancing the connectivity among Mid-Level Managers (MLMs) and Top-Level Managers (TLMs), *i.e.*, peers that, reacting to human operator requests, communicate with other management entities to accomplish management tasks, by investigating the location issues of P2P infrastructures (FIORESE; SIMõES; BOAVIDA, 2009). The authors also presented a performance evaluation in the context of the Aggregation Service (AgS), which is a P2P overlay-tier to aggregate the services and service components maintained by service providers (FIORESE; SIMOES; BOAVIDA, 2011).

Distributed IP Traffic Analysis (DITA). Morariu and Stiller (2011) proposed DITA as an approach to leverage different bottlenecks of traffic analysis (*e.g.*, metering and exporting processes) using P2P technology. This is done through the distribution of IPFIX records to several management peers according to rules required by an analysis application. DITA is composed by two main mechanisms: Distributed Packet Capturing Architecture for High-Speed Network Links (DiCAP) (MORARIU; STILLER, 2008) and Scalable Real-time IP Flow Record Analysis (SCRIPT) (MORARIU; RACZ; STILLER, 2010). DITA management peers are organized in a Kademlia-based P2P overlay.

Pattern-Based Management Programs. Lim and Stadle (2001) proposed Pattern-Based Management Programs as a novel approach for distributed management. This approach is based on the methodical use of distributed control schemes for large-scale,

dynamic networks. Such programs can be viewed as mobile code distribution considering a P2P management overlay. In fact, most patterns interactions are intrinsic P2P. The authors claimed that the use of patterns makes easier to estimate the performance of management operations. Furthermore, these patterns could reduce the complexity of distributed management programs through the re-usability of key software components.

Tran and Schönwälder (2007). The authors outlined a distributed Case-Based Reasoning (CBR) system for fault management based on P2P technology (TRAN; SCHÖNWÄLDER, 2007). The goal of this work is to assist operators in finding solutions for faults using various online knowledge source and decentralized reasoning capabilities. The solution uses a self-organizing platform provided by a P2P management overlay. In this context, CBR engines propose fault-matching solutions using their local case databases and reasoning engines.

Barshan, Fathy and Yousefi (2009). The authors proposed a 3-tier hierarchical architecture, aiming at fault-tolerance features (BARSHAN; FATHY; YOUSEFI, 2009). The layers that built this architecture are composed by Low-Level Managers (LLMs), MLMs, and TLMs. Redundancy is used in each layer of the architecture to increase the availability and decrease the peers failure sensitivity concerning the P2P management overlay. This redundancy is implemented through the operation of some selected peers in different layers. In this context, peer groups are composed of peers of each layer.

Nobre and Granville (2009). The authors proposed the utilization of multi-agent truth maintenance features to bring consistency maintenance of the state of management data in P2P-based Autonomic Network Management (ANM) (NOBRE; GRANVILLE, 2009). This is done in order to avoid centralized management entities for state consistency. Besides that, the authors also address the consistency of policy states among autonomic management elements in general decentralized ANM (NOBRE; GRANVILLE, 2010).

Santos et al. (2008). The authors developed a notification service to be used in P2PBNM solutions (SANTOS et al., 2008). Such service is based on the publish/subscribe paradigm and implemented over a P2P management overlay that carry the notification messages using SOAP. The service uses MLMs to forward messages between a notification source and destination. Santos et al. (2010) also evaluated the impact of using presence services in P2PBNM to provide ways to deliver presence information to interested parties.

Mobi-G. Stingl et al. (2014) proposed an approach to exchange information through

flat gossiping and robust communication patterns. Mobi-G consists of a flexible protocol which relies on a time-based synchronization. Such protocol exploits the characteristics of wireless *ad hoc* communication and nodes mobility. Thus, Mobi-G can cope with constantly changing network topologies and operate even in sparsely populated networks to provide accurate results at minimum cost.

Badis, Doyen and Khatoun (2015). The authors presented an approach to enable a collaborative egress detection of DDoS attacks leveraged by a botcloud. Such approach employs trees structures maintained through a DHT. These structures enable a collaborative source based detection. The use of a P2P management overlay in a cloud environment is motivated by the need for a scalable infrastructure, the need to address the churn, and the resilience of the detection system due to the absence of any central point.

Self-Managed Overlay Network (SMON). Gao et al. (2010) proposed SMON to support self-management capability for the deployment and maintenance of the distributed application management system. This is important since the operation of the management system itself is one of the main issues of distributed management systems. SMON manages itself using an epidemic approach at runtime. SMON can automatically deploy itself in a set of machines and recovers failed peers securely. Besides that, SMON can also upgrade itself using new online versions.

In the following sections, the presented initiatives are classified in order to produce an integrated perspective of such initiatives. The classification is performed regarding the review questions. After that, opportunities and challenges in the employment of P2P technology in network management are described.

3.4 The Employment of P2P Technology on Management Functional Areas

Network management tasks can be classified considering the executed management functions. Clearly, there is a noticeable diversity on such functions, thus it is helpful to employ a model for this classification. The most accepted model which discuses management functions was proposed by the International Organisation for Standardisation (ISO) on the the definition of a framework for network management, the Open System Interconnection (OSI) network management. Such framework is divided into specific management functional areas: Fault Management, Configuration Management, Accounting Management, Performance Management, and Security Management. These functional areas are commonly referred to as the FCAPS model (Joint Technical Committee ISO/IEC,

1994).

The initiatives on P2PBNM address different management tasks in the same way as traditional network management initiatives. Thus, the FCAPS model can be also employed to classify management tasks performed using P2P technology. The surveyed initiatives are presented with respect to their primary focus and the management functions they perform. It is important to mention that neither of these initiatives was classified within the Accounting Management functional area.

Fault Management. Fault management is one of the principal concerns of network administrators since it is related with the dependability of network infrastructures. Tran and Schönwälder (2007) proposed the use of P2P CBR for fault management using online knowledge sources and decentralized reasoning capabilities. S^3 aims at scalable fault detection for large systems (YALAGANDULA et al., 2006). Cartographer (KRUPCZAK, 2015) employs distributed root cause analysis and event correlation for fault detection. ManP2P (DUARTE et al., 2011) supports fault detection through the use of P2P management services. Santos et al. (2008) developed a notification service to carry the event notifications messages for the use in P2PBNM solutions. Nobre and Granville (2009) proposed the use of truth maintenance features for consistent detection of OAM Ethernet faults. Binzenhöfer et al. (2006) employed P2P overlays to providing the detection of connectivity faults.

Configuration Management. Configuration management is concerned with handling of configuration information in order to prepare, start, and enable the operation of networked services. Idhaw et al. (2006) proposed the use of a P2PBNM system to improve the distribution of network device configuration commands and policies for the an airborne network. SMC also employs policy-based techniques in the context of health monitoring applications (LUPU et al., 2008). Nobre and Granville (2010) proposed the use of truth maintenance features for the consistent configuration of distributed polices. Regarding Ambient Networks, Simon et al. (2005) detailed the employment of a P2P approach to enable the composition of Ambient Networks and Mathieu et al. (2007) proposed the use of P2P technology for pooling and sharing management information within and across heterogeneous composed networks. Madeira platform used P2P communication facilities to configure multiple customized network management topologies (FALLON et al., 2007). SMON proposed the use of P2P technology to support the deployment and maintenance of the distributed application management system as well as upgrade itself to new versions online (GAO et al., 2010). RELOAD is a P2P signaling protocol

to configure overlay network services and efficient message routing (JENNINGS et al., 2012).

Performance Management. Performance management is focused on ensuring effectiveness of networked services, which is usually done through collecting and analyzing data statistics. In the context of network traffic, DITA (MORARIU; STILLER, 2011) aims at combining resources of multiple peers to perform P2P metering and analysis and DECON (PIETRO et al., 2010) matches the monitoring probes and the set of flows which increase network coverage. Alternatively, S^3 (YALAGANDULA et al., 2006) and DNAs (BINZENHÖFER et al., 2006) are used for scalable SLA monitoring. Concerning large-scale monitoring, PRISm (JAIN et al., 2008), ManP2P (MELCHIORS et al., 2011), and AgS (FIORESE; SIMOES; BOAVIDA, 2011) use P2P overlays to enable performance tools. Regarding the use of gossip for monitoring, G-GAP (WUHIB et al., 2009) and Mobi-G (STINGL et al., 2014) are employed for performance estimation. Finally, Pattern-Based Management Programs were also proposed to estimate the performance of management operations (LIM; STADLE, 2001).

Security Management. Security management is related with the enforcement of security policies, which includes the control of security services and the distribution of security information. Badis, Doyen and Khatoun (2015) proposed an approach to enable a collaborative egress detection of DDoS attacks in a cloud environment through a DHT. Barshan, Fathy and Yousefi (2009) proposed a fault-tolerant hierarchical overlay, which uses redundancy to increase the availability and decrease failure sensitivity (*i.e.*, performability). ManP2P (DUARTE et al., 2011) supports fault-tolerant healing features through the use of peer groups.

3.5 The Employment of P2P Technology on Management Approaches

There is not an widely accepted taxonomy which defines and characterizes distribution aspects of network management approaches, but network management researchers usually consider distribution aspects which bring, at least, centralized and distributed approaches (*e.g.*, (PAVLOU, 2007) (SCHÖNWÄLDER; QUITTEK; KAPPLER, 2006) (MARTIN-FLATIN; ZNATY; HABAUX, 1999) (LEINWAND; CONDROY, 1996). Some authors believe Distributed Network Management (DNM) is essential to cope with current large-scale network infrastructures because DNM improves the execution of management tasks in respect to scalability and robustness (MARTIN-FLATIN; ZNATY; HABAUX,

Table 3.2: Initiatives on the Use of P2P Technology to Support Traditional Network Management Approaches

Initiative	DNM Model	Described Entities
Fiorese, Simões and Boavida (2009)	MbD	MLM, TLM
ManP2P	MbD	MLM, TLM
Barshan, Fathy and Yousefi (2009)	MbD	LLM, MLM, TLM
Kamienski et al. (2006)	PBNM	PDP
Idhaw et al. (2006)	PBNM	PDP
Fallon et al. (2007)	TMN	NE
Lim and Stadler	NMMA	MA

Source: by author (2015).

1999). P2PBNM is usually considered as one of the DNM "flavors". In this context, we classified all initiatives described in the present work as distributed management. Despite this, some P2PBNM initiatives employ some form of centralization. For example, Tran and Schönwälder (2007) outlined a P2P CBR in which super peers bear CBR engines due to bandwidth and power processing capabilities.

Traditional DNM approaches are challenged in some environmental settings (*e.g.*, cross-domain management tasks). The employment of P2P technology can be an interesting possibility to address these challenges. Management peers can play the role of the constitutive elements of traditional DNM models, executing their intrinsic management functions. The depicted initiatives are organized according to their support to the most common DNM models: Management by Delegation (MbD), Policy-based Network Management (PBNM), Telecommunications Management Network (TNM), and Network Management-based on Mobile Agents (NMMA). A summary of such initiatives regarding the use of P2P technology to support traditional DNM models is described in Table 3.2. In this table, we present the aforementioned initiatives along with the used DNM model and the described management entities.

In the quite recognized Management by Delegation (MbD) approach, Goldszmidt and Yemini (1995) proposed the introduction of Mid-Level Managers (MLMs) in order to enable more flexible and scalable network management. In MbD, managers delegate the execution of management tasks to MLMs closer to the managed devices, thus decentralizing the execution of management actions. Delegation is used to move management functions (*e.g.*, management scripts) towards the managed devices. However, even with MbD, network management systems may not provide important distributed features such as supporting the interaction among human operators located in multiple administrative domains.

P2P technologies can be employed to overcome some limitations of MbD model (*e.g.*, flexibility). This seems to be the most common integration between P2P technology and DNM models. For instance, P2P technology can improve the connectivity for message exchange among management entities of a MbD system (*e.g.*, MLMs) since P2P routing services are more flexible than those provided in IP networks. Some proposals focused on enhancing the connectivity among MLMs and introducing Top-Level Managers (TLMs), *i.e.*, peers that, reacting to human operator requests, communicate with other management entities to accomplish management tasks (FIORESE; SIMõES; BOAVIDA, 2009) (PANISSON et al., 2006) (MELCHIORS et al., 2011). Barshan, Fathy and Yousefi (2009) proposed a 3-tier hierarchical architecture using MLMs, TLMs, and introducing Low-Level Managers (LLMs).

Sloman (1994) proposed the use of policies to meet a set of pre-specified high-level business objectives and goals through the Policy-Based Network Management (PBNM) approach. Although the original conception of PBNM did not enforce any specific architecture, one of the often mentioned ones is the architecture defined by the Internet Engineering Task Force (IETF) (WESTERINEN et al., 2001), which is composed by four main components: Policy Management Tool (PMT), Policy Repository, Policy Decision Point (PDP), and Policy Enforcement Point (PEP). The definition and placement of PBNM entities within a managed network can create distributed management systems (VERMA, 2002).

P2P technology can be integrated with PBNM model in order to improve its scalability and robustness. The functions of these entities can be implemented through management peers. Besides that, the P2P management overlay can be used to support the distribution of updated policies. For example, different works proposed the distribution of PDP functions. This can be done keeping the same hierarchical concept behind the PBNM model, but instead of using a single PDP, replacing it using PDPs implemented as peers of a P2P management overlay (IDHAW et al., 2006) (KAMIENSKI et al., 2006). Besides that, Lupu et al. (2008) proposed policy-based techniques for driving P2P adaptation decisions without relying on the traditional PBNM architecture.

The Telecommunications Management Network (TNM) is an architecture proposed by the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) to manage telecommunication networks (UNION, 2000). TMN is defined in M series of ITU-T and uses Open System Interconnect (OSI) management specifications (ITU-T Recommendation series X.700). TMN introduces different levels

of abstraction: element management, network management, service management, and business management. Managers at one layer are only aware of their subordinate Network Element (NE) in the next layer, thus there is no communication between managers at the same level.

P2P technology can be integrated with TNM in order to improve its flexibility and robustness. Since TNM uses a highly coupled hierarchy model which allows only vertical interactions, P2P technology can be used to improve the interaction model to allows more complex management tasks (*e.g.*, service composition). Fallon et al. (2007) employed a P2P approach to autonomously form network management topologies in order to accomplish specific network management tasks. The NEs are grouped into clusters and these clusters form P2P overlays that can be arranged hierarchically according to the requirements of the management task to be executed.

Mobile Agents (MAs) were proposed regarding different application areas. One of such areas is network management. A MA is a software agent able to move between locations, according to a life-cycle model, a computational model, a security model, a communication model, and a navigation model. Mobile agents can be implemented using one of two fundamental technologies: mobile code (*e.g.*, AgentTCL and Telescript) or remote objects (*e.g.*, Aglets). Several MA mechanisms were adapted for DNM, also known as Network Management-based on Mobile Agents (NMMA), and a comprehensive review of them is available on network management literature (BIESZCZAD; PAGUREK; WHITE, 1998).

MAs approaches can be integrated with P2P technology in order to perform management tasks. A P2P management overlay can be used to ease the support of code mobility, *i.e.*, hosting MAs. Since P2P technology is known to better support code update, they offer the flexibility required to enable movement among different network locations. Besides that, since some mechanisms related to MAs were already adapted for DNM (*e.g.*, remote objects), such mechanisms can also be deployed on P2PBNM system. An example of a joint use of MAs and P2P technology is the Pattern-Based Management Programs (LIM; STADLE, 2001), which employ the distribution of mobile code considering a P2P management overlay.

The utilization of P2P technology can be a better alternative to traditional distributed technologies in autonomic and self-management. P2P systems have good performance to overcome challenges related with dynamic systems, specially in large-scale, ubiquitous, or mobile environments (KOUBARAKIS, 2003). Besides that, some ap-

proaches to autonomous features in network management seem to require that management data must be maintained in a distributed way. These features usually aim at to achieve lower management costs and reaction times (SAMAAN; KARMOUCH, 2009).

Some works explore P2P technology and self-management as a whole. On the one hand, this can be done considering a specific and well-defined environments which eases self-management features. For example, some authors proposed P2P technology in the self-management of contexts associated to overlays of Ambient Networks (BRUNNER et al., 2005) (MATHIEU et al., 2007). On the other hand, some works employ distributed autonomous entities and such entities present P2P interactions. In this context, Lupu et al. (2008) proposed Self-Managed Cells (SMC) as an architectural pattern for ubiquitous computing applications and Binzenhöfer et al. (2006) described an architecture aimed at providing generic connectivity tests and Quality of Service (QoS) monitoring.

P2P technology can be used to enable some autonomic properties on network management systems. Nobre and Granville (2010) proposed the use of Multi-Agent Truth Maintenance for the self-configuration of consistent management information. Self-healing features are described in ManP2P system through the use of peer groups which are composed by cooperative management peers (DUARTE et al., 2011). Self-optimization is also proposed in some initiatives. For example, Fallon et al. (2007) employed a P2P approach to self-optimize network management topologies in the presence of environment changes. In addition, Tran and Schönwälder (2007) outlined a distributed CBR which uses a self-optimized platform provided by a P2P management overlay.

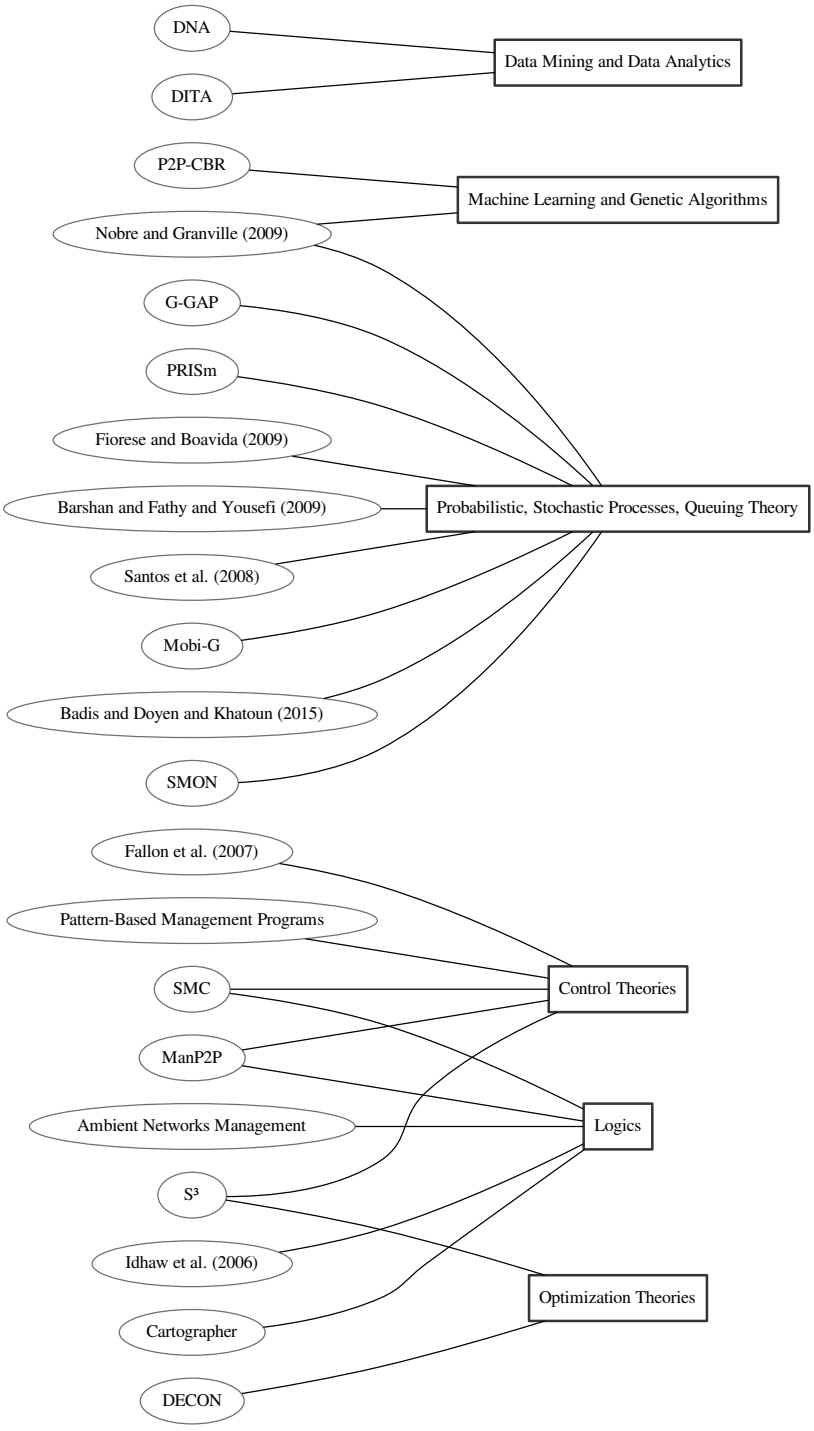
3.6 The Employment of P2P Technology with Management Methods

Network management tasks can be performed using several methods. Such methods are used to support features on management systems, such as task distribution, self-organization, and fault tolerance. In this context, the employment of P2P technology enhances the dynamic deployment of management methods. This deployment can use the flexibility of P2PBNM to distribute the computation due to management methods. For example, the P2P management could be used to update the software of management peers in order to adapt management methods for different network environments.

The composition of P2P technology and network management methods allows the introduction of different characteristics in P2PBNM. The methods used to classify the initiatives surveyed in the literature review are control theories; optimization theories; logics;

machine learning and genetic algorithms; probabilistic, stochastic processes, queuing theory; and data mining and data analytics. A summary of the classification described in the present section is described in Figure 3.2.

Figure 3.2: Classification of P2PBNM Initiatives in Respect to Management Methods.



Source: by author (2015).

Control theories. Distributed management services can address tasks using methods from control theories. Lim and Stadle (2001) proposed Pattern-Based Management Programs, which are P2P control schemes that determine the degree of parallelism and internal synchronization of a distributed management operation through mobile code. SMC employs a closed-loop system where changes of state in the resources trigger adaptation which in turn affects the state of the system (LUPU et al., 2008). S^3 uses an adaptive placement based on observed performance by the sensor pods for the inference and operation control services (YALAGANDULA et al., 2006). Fallon et al. (2007) proposed Adaptive Management Components (AMCs) which are containers on Network Elements (NEs) that run management software entities and communicate with entities running on other NEs. ManP2P employs autonomic control loops to support self-* properties, such as self-healing (DUARTE et al., 2011).

Machine learning and genetic algorithms. Some works proposed embedding methods related to machine learning and genetic algorithms features into P2PBNM solutions. Nobre and Granville (2009) introduced multi-agent truth maintenance features in the P2PBNM to improve the consistency of states of management data considering autonomic management environments. Such consistency is necessary since each management peer can be viewed as an intelligent agent in P2P-Based Autonomic Network Management (ANM). P2P-CBR employs CBR engines in a P2P management overlay, thus considering a distributed CBR solution (TRAN; SCHÖNWÄLDER, 2007). Such engines are deployed in super peers since these peers bear more computational resources than regular peers.

Optimization theories. Distributed management approaches, such as P2PBNM, can use optimize management tasks considering specific and dynamic characteristics of network environments. In this context, management peers can implement methods from optimization theories in order to improve such tasks. DECON uses batch optimization to reduce messaging overhead in monitoring reports and response messages directed to a monitoring probe (PIETRO et al., 2010). S^3 employs a near-optimal dynamic service placement for resource provisioning using information about different aspects of the environment (YALAGANDULA et al., 2006).

Data mining and data analytics. There are proposals concerning the employment of data mining and data analytics in P2PBNM. In this context, such proposals support the dissemination of management data in an overlay. DITA computes a routing hash value for each processed flow record using a routing function (MORARIU; STILLER, 2011). This

is done to determine the forwarding of such records to different nodes (*i.e.*, management peers). DNA uses hash value to provision the P2P management overlay, *i.e.*, to keep the DNAs connected in one logical network and to enable a single DNA to find another DNA in reasonable time (BINZENHÖFER et al., 2006).

Probabilistic, stochastic processes, queuing theory. P2PBNM system often use non-deterministic methods due to different aspects. For example, such methods can be known to be more efficient that deterministic ones for a given scenario (*e.g.*, large network infrastructures). Badis, Doyen and Khatoun (2015) employ a detection algorithm based on Principal Component Analysis (PCA) for data normalization. Barshan, Fathy and Yousefi (2009) employed redundancy in management roles to increase availability. PRISm uses the concept of conditioned consistency using network imprecision to address the distortion of monitoring results by network churn (JAIN et al., 2008). Santos et al. (2008) employed queue theory to support notification messages over a P2P management overlay. Epidemic protocols aim at robustness and resilience; Nobre and Granville (2009) proposed eventual consistency of states of management data using biology-inspired processes (*e.g.*, replication) as a P2P communication strategy; and SMON uses an epidemic algorithm to monitor and maintain the management peers themselves, *i.e.*, the P2P management overlay (GAO et al., 2010). Besides that, gossip protocols (a special case of epidemic protocols) were also used in P2PBNM to spread management information in G-GAP (WUHIB et al., 2009) and Mobi-G (STINGL et al., 2014). Finally, Fiorese, Simoes and Boavida (2011) employed aggregation for P2P service searching.

Logics. Different approaches can be used to integrate logics and the employment of P2P technology in network management. Cartographer enables distributed root cause analysis and event correlation (KRUPCZAK, 2015). Regarding the use of polices, Idhaw et al. (2006) applied PBNM for the management of airborne networks, Kamienski et al. (2006) distributed the functions of some PBNM entities for the management of ambient networks, Lupu et al. (2008) used policies in SMCs to specify which adaptation should occur in response to environmental changes, and ManP2P supports autonomic features using the concept of workplan (a form of policy).

3.7 Trends and Analysis of Future Research Directions

The network management area has evolved into an important scientific discipline due to the increasing complexity of computer networks. Some authors even claim that

the management of current and emerging network technologies is becoming the main bottleneck to any further advancements (SAMAAN; KARMOUCH, 2009). Thus, it is important to investigate approaches that improve the performance of network management systems concerning several challenges (*e.g.*, scalability, robustness, and broadness). In this context, the employment of P2P technology in the network management discipline presents itself as a strong alternative for enhancing the solutions on such discipline.

As the survey described in this chapter points out, the research relating P2P systems and network management tends to spread over several directions at the present moment. The benefits of enlarging the spectrum of P2P-Based Network Management (P2PBNM) research can increase the chances of finding revolutionary mechanisms and techniques for network management as a whole. However, this tendency also often leads to unclear definitions of terms and borders among different research initiatives. For example, some authors in the network management community do not explicitly use the term "P2P", despite the use of this type of interactions in their solutions, which makes more difficult to fully understand the employment of P2P technology across the network management research area.

Despite the adversities on delineating the employment of P2P technology into network management solutions, it is safe to state that more advances in the joint use of P2P and network management can further contribute for the design of distributed network management systems. In this context, it is also safe to say that, although DNM has been widely recognized as a necessity, there is no definitive solution for technology employed to develop DNM systems. Some examples of potential scenarios that could be explored under the P2PBNM approach are: networking devices with increasing processing capacity, P2P network management algorithms, and new network environments.

Current network equipment vendors provide an increasing level of processing power and programmability in their networking devices (*e.g.*, Cisco Embedded Event Manager and Juniper Script Automation) which differs significantly from the beginning of the development of network management discipline. This programmability capability is already used to enable rudimentary management functions. Thus, following the same path, it is possible to use such capability to embed management peers inside these network devices. This way, in-network P2P management overlays can be formed to offer management services and, thus, dispensing additional hardware to host the management peers.

Indeed, the literature shows that P2P infrastructures are being well explored to

build network management infrastructures. Nevertheless, management applications keep on being developed following traditional hierarchical network management approaches, and this scenario presents many opportunities for developing revolutionary management algorithms based on the distributed and cooperative capabilities of P2P technology. For instance, P2PBNM applications could be used to enable customer-based management, or even, to introduce domestic users in the management process. Users of P2P systems, usually, cooperate (consciously or not) to perform P2P distributed tasks. In most common settings, users install an application (*i.e.*, a peer) in their desktops in order to share and access other peers resources, possibly in different administrative domains. Thus, the participation in P2P systems is intuitively simplified and easily accessible. These characteristics of general P2P systems were not effectively introduced in P2PBNM.

New network environments, such as Delay-Tolerant Networks (DTNs), are interesting contexts where P2PBNM can show its strength. Some examples of these environments are unstructured personal communication systems (KANSAL; GORACZKO; ZHAO, 2007), vehicular networks (ZHAO; CAO, 2008), and interplanetary networks (BURLEIGH et al., 2003). Indeed, some authors propose the utilization of traditional DNM approaches in these environments (PEOPLES et al., 2010). However, these approaches operate using connectivity premises not found in such environments (*e.g.*, stable connectivity). On the other hand, general purpose P2P systems have already demonstrated that they cope graciously with new network environments (SCOTT et al., 2006). Therefore, the characteristics of P2PBNM solutions can be a natural alternative for managing these environments.

The employment of P2P technology in network management, however, despite its known advantages, has some important limitations. First, in the context of structural aspects, it can be discussed some critical issues inherited from general purpose P2P systems, such as the importance of routing protocols (specially in non-hierarchical overlays). Second, it is necessary to put more effort on the investigation of P2P management algorithms to improve the exploitation of P2P features on management tasks (*e.g.*, collaborative fault management (NOBRE; GRANVILLE, 2009)). Several proposals just transpose DNM infrastructures for P2P overlays without exploiting genuine P2P features. Lastly, some works state that there is a lack of implemented solutions for many functions required to perform management tasks, such as coordination services support (KONSTANTINOU; YEMINI, 2009) and consistency of states of management information (NOBRE; GRANVILLE, 2010).

3.8 Final Remarks

The support of new demands faced by traditional network management is a key research issue in the network management area. Distributed Network Management (DNM) has been proven to be a feasible approach for these demands. Indeed, the research community understands as a common sense that distributed solutions are more suitable to handle the current scenarios where network management is employed. Despite the existence of such sense, there is not a consolidated and wide accepted consensus on how to provide the proper infrastructure for DNM systems. One alternative that has gained attention in the past years is the employment of P2P technology for network management, also known as P2P-Based Network Management (P2PBNM).

In this chapter, we presented a comprehensive review of the state of art regarding the P2PBNM. First, it was presented a review of the definitions associated with P2P systems and P2PBNM approaches. Then, the method used in the literature review was introduced. In the sequence, the main initiatives for the employment of P2P technology in network management were presented. After that, a comparison of the initiatives considering the review question was described. This chapter is closed with the discussion about the future trends and analysis of future research directions for P2PBNM.

Based on our analysis, we could verify the remarkable diversity of contexts and areas where P2PBNM solutions are employed. The main conclusions of our analysis are twofold. First, we identified that regardless the context or area there is a predominant employment of P2P infrastructures to enhance the underlying conditions of DNM systems. In this context, very few initiatives use the concepts behind the P2P technology in order to enhance the execution of management tasks themselves. Second, the research on the employment of P2P technology in network management can contribute for the DNM area as a whole. Furthermore, the use of P2PBNM concepts can lead to the development of better DNM systems.

4 PRINCIPLES TO STEER AUTONOMICALLY THE ACTIVATION OF ACTIVE MEASUREMENT SESSIONS

Active measurement mechanisms are an effective technique for monitoring Service Level Objectives (SLOs). In this context, the detection of Service Level Agreements (SLAs) violations is based on the idea of identifying deviations from the contracted SLOs. In order to identify these deviations using active measurements, it is necessary to have measurement sessions activated on problematic end-to-end destinations. However, such activation is expensive in terms of the consumption of human and computational resources (both on network devices and bandwidth). Since a better monitoring coverage requires more activated sessions, it increases the amount of consumed resources. On the other hand, enabling the observation of just a small subset of all network flows decreases the resource consumption, but it can lead to insufficient coverage.

The current best practice in activating measurement sessions along a provider's network consists in relying on the network administrator's expertise to infer which would be the best destinations to activate the sessions. As discussed in Chapter 2, this practice has major shortcomings. Network management researchers have investigated how to overcome analogous shortcomings considering different scenarios and management tasks (SAMAAN; KARMOUCH, 2009). This scenarios include, for example, high dynamics and complexity of network environments and delivered services. In order to provide solutions that better suit these scenarios, network-wide management solutions can be employed.

A network-wide control of network devices can improve their abilities to accomplish management tasks. For example, a distributed network management algorithm can be use to allow that some devices provide additional resources for the execution of management tasks by other devices. This can be useful when either the computational load is not equally distributed among the network devices or there is heterogeneity in the computational resources of network devices. In this context, the global capability of the devices in a network can be greater than the sum of the capability of each device. As described in Chapter 3, networking devices with increasing capabilities and distributed network management algorithms are examples of potential scenarios to be explored under P2P-Based Network Management (P2PBNM).

P2P technology can provide the foundations for increasing the intelligence applied in the control of active measurement mechanisms through sophisticated distributed net-

work management algorithms. Network devices could benefit from a network-wide and distributed control of such mechanisms since it is feasible that measurement decisions (*e.g.*, activation of active measurement sessions) are better taken considering the sharing of computational resources and management information. Thus, such decisions may take into account local and remote information as well as consider resources just from the device itself and from remote devices.

Network devices have increased substantially their level of programmability. Thus, it is feasible to embed management software to control the activation of active measurement mechanisms. Embedded management peers can have direct access to the internal API of active measurement mechanism which could speed the configuration of measurement sessions. Since activating measurement sessions should be a dynamic process in several modern network infrastructures, this speed can improve measurement efficiency (*e.g.*, in terms of monitoring coverage). Embedded P2PBNM systems also make the growth of management resources more "organic" since they can grow without requiring a fork-lift upgrade. In this context, these systems could grow as new devices are added, bundled with embedded management peers.

A pragmatical approach to employ P2P technology in the network-wide control of the activation of active measurement sessions is to define principles to guide this employment. We devise the following principles: $i)$ local information to prioritize destinations using past measurement results and resource constraints; $ii)$ correlated peers to provision the P2P measurement overlay; and $iii)$ virtual measurement sessions to optimize resource consumption. In simple terms, these principles are used to capture the common sense used by network administrators when using active measurement mechanisms to detect SLA violations. Thus, we aim at a solution which is adaptive to changes in network conditions, independent of the underlying active measurement technology and autonomic (in the sense that avoids human intervention). The remaining of the chapter describes these principles and their implicit concepts.

4.1 Local Information for The Destinations Prioritization Using Past Service Level Measurement Results and Resource Constraints

The detection of SLA violations using active measurement mechanisms needs measurement probes hosted both on the source and the destination. Such probes are software components which run on the network devices, usually in those specialized in

networking functions (*e.g.*, switches and routers). Besides probe hosting, it is necessary to activate measurement sessions in order to monitor destinations and, consequently, detect SLA violations. Since the destinations that will eventually violate SLA are not known *a priori* and it is usually too costly to measure all destinations in a network, an approach to define which destinations should be primarily measured is necessary. Such approach is the destinations prioritization as described in Definition 4.1.

Definition 4.1. *Destinations prioritization is the definition of the set of destinations which is believed that their monitoring will increase the probability of the detection of SLA violations.*

The main goal of destinations prioritization is to increase the number of detected SLA violations over the total number of such violations, *i.e.*the percentage of detected SLA violations. In addition, the prioritization is dependent of instant network conditions, thus, adaptivity is necessary for a successful detection of SLA violations. In this context, it is desirable that the network devices themselves can autonomously and dynamically select a set of destinations, consequently, activate measurement sessions on this set. The decentralization pushes the local autonomy of management entities, increasing the use of local logic to make management decisions.

P2P technology can be employed to use local logic for the control of active measurement mechanisms. This technology can be used to introduce a high degree of decentralization concerning the execution of management tasks (as shown in Chapter 3), such as the detection of SLA violations. Besides that, local data can be also employed to decide which measurement sessions should be activated and how to interpret the results regarding the SLA monitoring. Service level results from such sessions are an example of local data, which are already gathered and stored by network devices.

Local information, logic and data, can be used to prioritize destinations for the activation of measurement sessions regarding the detection of SLA violations. This is done using past service level measurement results and resource constraints to steer autonomically local management decisions. This is described in the next sections.

4.1.1 Past Service Level Measurement Results to Prioritize Destinations

Active measurement sessions can be used to monitor Service Level Objectives (SLOs) regarding a destination if such sessions are configured and activated for this des-

tination. In this context, SLA violations are detected when service level measurement results do not meet the contracted SLOs. Thus, probing technique for the SLA monitoring involves activation of measurement sessions which affects the diagnosis capability of the active measurement mechanisms. The utilization of past service level measurement results is our approach to establish if a destination is likely to disrespect SLOs (*i.e.*, violate the SLA).

Past service level measurement results provide metrics to infer the network conditions in a given time. Therefore, it must be avoided the utilization of out of date results since they can lead to erroneous inferences. One approach to assure the freshness of results is the is employment of a sliding window. Such window can consider either a number of results or a time span, both considering the last collected result from a given measurement session. Besides that, discounted contributions can be also employed in order to strength newer results over older ones. In any case, it is necessary to evaluate the closeness of past service level measurement results in respect to the SLO.

Descriptive statistics metrics are our choice to measure the closeness of past service level measurement results regarding the SLO for a given destination. For example, it is possible to use a composition of a measure of the central tendency (*e.g.*, mean) and a measure of spread (*e.g.*, standard deviation) as chosen metrics. If the past measurements results for a given destination are close to a SLO, then the probability of activating a measurement session in this destination should be increased. This is done by local logic, *i.e.*, an application that run locally on the network devices. However, in order to maintain an exploratory SLA monitoring, it is important to avoid that destinations keep without activated measurement sessions for a significant time.

It is important to assure that each destination is measured frequently, even if its measurement results are not close to the SLOs. In order to induce frequent probing on all destinations, we use the time elapsed from the last measurement session result for a given destination to increase the probability of this destination to be measured. Clearly, if a destination had not been measured recently, then it should be more likely to be selected in the next measurement decisions. The joint use of the past service level measurement results and the time elapsed from the last measurement for a given destination enables the network devices to determine how to activate sessions in an autonomic manner.

4.1.2 Resources Constraints

Active measurement mechanisms need to be carefully deployed in order to save computational resources of network devices. There is an inherent resources consumption related to the generation and forwarding of synthetic test packets and their analysis. This consumption comes primarily in terms of CPU cycles and memory footprint. It is widely known that even dedicated routers (as mentioned in Chapter 2) are deployed to handle active measurement mechanisms and save resources of main (core) routers. Thus, it is necessary to employ an approach to manage resource utilization.

The destinations prioritization affects the selection of the set of destinations considered for SLA monitoring. Since the number of detected SLA violations depends on the activated measurement sessions, the rationale for such monitoring is to activate sessions while there are available resources. In addition, the prioritization allow to rank destination that are more likely to disrespect SLOs. Therefore, the size of the set of destinations that should be probed is the key to manage consumed resources while providing an efficient SLA monitoring coverage. Constraints can be used to control such set and, consequently, the number of activated measurement sessions.

Resources utilization on the devices can be managed using constraints. These constraints are defined according to the maximum number of measurement sessions expected to be deployed in a given time. This number is used as an abstraction for the resources available for active measurement mechanisms. Thus, it abstracts the different kinds of resources used in the measurement sessions considering a single number. This simplifies the resource management from the device point of view. Since the available resource may vary over time, the constraints should also follow this variation.

The number of active measurement sessions can be enforced locally and globally. On the one hand, local enforcement (*i.e.*, in a specific device) considers only a local upper bound for active measurement sessions. Devices can easily ensure the local upper bound since this can be done just checking the local information. On the other hand, in order to control a global upper bound (*i.e.*, concerning devices that exchange management information) is harder since it is necessary to consider information from different devices and exchanged in the network infrastructure.

4.2 Correlated Peers for P2P Measurement Overlay Provisioning

Service level measurement results are produced by active measurement mechanisms around the network infrastructure. In this context, human administrators usually can predict if SLA violations are likely to happen in a part of the network infrastructure using information from measurements of other parts of the network. This is possible because human administrators can use their experience and knowledge to infer the relation among the links and services within the network infrastructure. After that, such administrators can change the configuration of active measurement sessions in order to undoubtedly detect inferred SLA violations. P2P technology can be used to help the control of measurement mechanisms in an analogous way.

Service level measurements produced by active measurement mechanisms around the network infrastructure could be also shared by the devices to help the local measurement session control. However, it is necessary to assure that results received from remote devices have local relevancy. For example, if the network paths used by two devices, device *a* and device *b*, to reach a third device, *c*, are completely disjoint, the contribution due to network transmission for measurement results would be probably different. In this context, the use of measurement results exchanged by the device *a* and device *b* concerning device *c* could lead to undesirable results (*i.e.*, decrease the number of detected SLA violations). In order to guarantee local relevance of remote measurement results, we use the concept of correlated peers (described in Definition 4.2.

Definition 4.2. *Two nodes are considered as correlated peers (correlation is symmetrical) if the results of their measurements for a given destination are correlated.*

Correlated peers can be used to enable the adaptation of active measurement mechanisms to changing conditions in networks based on the state monitored by different peers. Thus, the control of such mechanism can consider service level measurement results locally collected or received by other network devices (*i.e.*, correlated peers). The definition of correlated peers creates a P2P measurement overlay (described in Definition 4.3), which is a specific kind of P2P management overlay (depicted in P2PBNM literature).

Definition 4.3. *P2P measurement overlay is a P2P management overlay in which the relationship among the participating peers is defined through the use of measurements.*

Different models can be employed for a P2P overlay (as described in Chapter 3). We consider a flat overlay for correlated peers for different reasons. Considering a P2P

measurement overlay deployed for the detection of SLA violations, a direct access to the internal API of active measurement mechanism for P2P software is highly desirable. For example, such access can speed configuration tasks of measurement sessions like their activation. Besides that, a hierarchical structure can be impacted in some network settings, where the hierarchy might not be correctly established. In this context, additional information, such as the network topology and the hardware of network devices, would be necessary to build the hierarchical relationships.

We describe in the present section concepts and processes related to correlated peers and P2P measurement overlays. In order to establish whether different devices should be considered correlated peers, we propose the utilization of correlation scores. Since the use of correlated peers introduces a P2P measurement overlay to deal with, it is necessary to describe its operational procedures. Then, we present bootstrapping and peer advertisement procedures regarding the formation of a P2P measurement overlay.

4.2.1 Correlation Scores for The Definition of Correlated Peers

Correlated peers are defined considering whether their measurements for a given destination (or a set of destinations) are correlated. Therefore, it is necessary to determine an approach to verify measurement correlation, *i.e.*, whether the local and remote results are in the same vicinity (*e.g.*, low variance). Clearly, measurement correlation can varies numerically regarding the utilized measurement results. We propose correlation scores (described in Definition 5.3) as a measure of such correlation.

Definition 4.4. *Correlation score is a measure of the correlation between two sets of measurement results.*

Correlated scores can be produced through different correlation functions. In this context, there are different mathematical ways to compare the locally produced measurement results and those received by other devices in order to produce correlation scores. For example, correlation coefficients for both regular variables (*e.g.*, Pearson Product-Moment Correlation Coefficient) and ranked variables (*e.g.*, Spearman Rank Correlation Coefficient) are functions used to verify the relationship of variables. Besides these functions, it is also feasible to use tests which compare samples using summary information (*e.g.*, mean and variance), either considering parametric statistics (*e.g.*, One-Way Analysis of Variance) or non-parametric statistics (*e.g.*, Kruskal–Wallis One-way Analysis of

Variance). The Table 4.1 present a summary of some statistical functions that can be employed for measurement correlation along with properties of such functions.

Table 4.1: Summary of the Statistical Functions for Measurement Correlation.

Function	Data	Parameter Inference	Range
Pearson Product-Moment Correlation Coefficient	Individual Points	Parametric	[-1,+1]
Spearman Rank Correlation Coefficient	Individual Points	Non-Parametric	[-1,+1]
One-Way Analysis of Variance	Sample	Parametric	Unbounded
Kruskal–Wallis One-Way Analysis of Variance	Sample	Non-Parametric	Unbounded

Source: by author (2015).

Each device uses correlation scores in order to rank other devices in terms of measurement correlation. In order to increase confidence on such scores, it is necessary a substantial amount of past measurements results related to the same destination. The magnitude of correlation scores is used twofold. On the one hand, the remote devices which have higher scores are chosen as correlated peers. On the other hand, the minimum correlation score required for a correlated peer sets a lower bound constraint. This is necessary to assure local relevance of remote results.

4.2.2 Bootstrapping and Peer Advertisement on The Formation of a P2P measurement overlay

P2P technology has several distinctive characteristics that make it interesting for network management (as described in Chapter 3). Besides easing the access on local resources, an embedded P2PBNM system makes the growth of the management system more “organic”. This is because the addition of new devices can be followed by the introduction of new management peers, just adding P2P software on such devices. However, the overlay provisioning must be transparent as possible in order to enable such growth. This overlay should support the message forwarding for correlated peers as well as the maintenance of the peer list.

In order to bootstrap overlay formation, each device uses their known endpoints neighbors (*e.g.*, manually provided, from routing/forwarding information bases, or inferred using traffic records) as the initial seed to identify candidates for correlated peers, *i.e.*, remote devices that may be evaluated for correlation purposes. Then, devices send information about their measurements for such candidates. Each device compares this received information with their own measurements, then remote devices are ranked by

their correlation scores. Devices which have higher scores are chosen as correlated peers.

The utilization of correlation scores enables a P2P measurement overlay with peers that share some characteristics regarding the measurement sessions. Peers eventually advertise their correlated peers in order to permit evaluation of "peers of peers". Thus, a subset of received "peers of peers" can be also evaluated using the measurement results correlation. Measurement information is sent to this subset in order to allow the verification of correlation scores. Furthermore, it is also possible to pick, as candidate peers, other known devices to allow for a degree of randomness and avoid over clustering.

The P2P measurement overlay maintenance needs to control the resources consumed by the overlay itself. Such consumption is due to the exchanged messages and the processing and storage of the peers list in each device. In this context, an upper bound constraint on the number of correlated peers can restrict resource consumption. Such constraint is the maximum number of correlated peers that a device can have in a given time. In addition, the schedule to reevaluate the peer list can be also modified in order to allow more time between iterations and, consequently, decrease overlay maintenance consumption.

4.3 Virtual Measurement Sessions for Resource Consumption Optimization

Network administrators try to maximize the monitoring coverage of a network infrastructure regarding the number of detected SLA violations. However, even considering a naïve attempt of maximum coverage, the number of measurements that a device can perform is still bounded by the available resources (*i.e.*, the number of measurement sessions which a device can actually activate considering their resource consumption). Our proposed principle to increase such number, in respect to the number of local available active measurement sessions, tries to capture one of the behaviors commonly employed by network administrators, the sharing of measurement results.

Sharing active measurement results among devices can improve SLA violation detection regarding the resource consumption and monitoring coverage. Sometimes a single device cannot achieve the desired measurement coverage in isolation due to its own capabilities. Besides that, the administrator can choose not to achieve a defined coverage considering the device in isolation, usually to save resources for main network functions. Furthermore, it is useful to reduce redundant active measurement sessions. This is because such sessions can interfere with each other since the measurement traffic

of one device is viewed as network traffic by others. In this context, P2P technology can be used to enable resources sharing and information exchanging among a P2P measurement overlay.

The sharing of active measurement results through a P2P measurement overlay should consider which network devices are prone to share measurement results, considering their own capabilities, the quality constraints, and the available resources. Besides that, it is necessary to assure a high local relevance of specific remote measurement results. We devise two concepts to enable an efficient sharing of results from active measurement mechanisms: virtual measurement sessions (as described in Definition 4.5) and measurement contracts (as described in Definition 4.6).

Definition 4.5. *Virtual measurement session is the local use of results from remote measurement sessions by a device as such results were locally produced.*

Definition 4.6. *Measurement contract is the process in which two devices agree on exchanging results from a measurement session.*

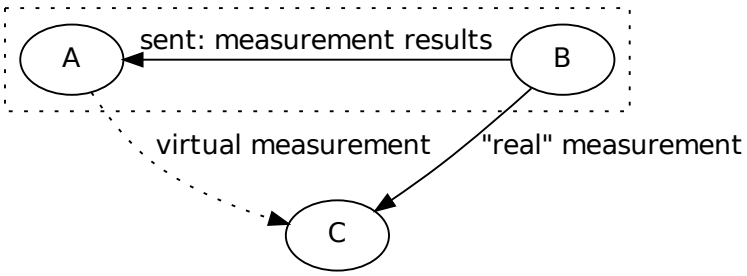
We describe in the present section concepts and processes related to virtual measurement sessions and measurement contracts which are based on P2P technology and are characterized by a high degree of distributed decision making across network devices. In the next sections these concepts and process are explained in more detail.

4.3.1 Virtual Measurement Sessions

Devices perform virtual measurement session when they use of results from remote measurement sessions as their own. On the one hand, the bulk of the computation and bandwidth, and storage needed to operate the measurement session is contributed by the remote device (*i.e.*, a correlated peer). This decreases the local resources necessary to monitor destinations and, consequently, to detected SLA violations. On the other hand, these results probably are not as accurate as if they had been produced locally. Thus, virtual measurement sessions could result in false positives and negatives regarding the detection of SLA violations. Therefore, virtual measurement sessions should be usually employed for SLA monitoring screening.

The Figure 4.1 represents a virtual measurement session. In this figure, device *b* is performing an active measurement session using device *c* as destination. Then, device *b* sends measurement results produce in this measurement session to device *a* which, in

Figure 4.1: Virtual Measurement Session.



Source: by author (2015).

its turn, uses these results as its own results, *i.e.*, as a virtual measurement session. The resource consumption due to the traffic injection and packet handling concerning this example is carried by device *b* since it is the one actually performing the measurement session. Device *a* has the benefit of using the (virtual) measurement session results to device *c*, avoiding the measurement session overhead.

The concept of correlated peers can be used to assist the definition of virtual measurement sessions. Devices can use their own list of correlated peers to decide which peers are the best choices for the sharing of measurement sessions. Since the definition of correlated peers is performed using information from past service level measurement results (described in Section 4.2), the choice of virtual measurement sessions is already initially related with the same results. Clearly, top correlated peers, *i.e.*, peers which have the higher correlation scores, may be considered as candidates for virtual measurement sessions in order to assure the confidence on the shared results. Furthermore, the P2P measurement overlay is responsible to forward remote results. In any case, virtual measurement seasons can be improved by performing some measurements exclusively to validate the correlation among nodes, which we define as validation sessions (as described in Definition 4.7).

Definition 4.7. *Validation session is the local activation of a measurement session only to validate the correlation among network devices.*

Validation sessions are composed of measurements to destinations selected by a device to ensure that there is a common set of results to determine correlation from. Such sessions may incur less overhead than regular measurement session, as the measurement does not necessarily have to be as precise, but represents a kind of sanity check to see

if the observed service levels are still in the same ballpark. Therefore, the result of a validation session can make a peer to finish the virtual measurement session for a given destination and, possibly, start a local regular measurement session.

4.3.2 Measurement Contracts for Virtual Measurement Sessions

Measurement contracts can be viewed as a kind of negotiation between two devices to exchange results from a measurement session. In P2PBNM, as an instantiation of Distributed Network Management (DNM), the execution of management tasks can be distributed among the management entities (*i.e.*, peers). In this context, the execution of measurement tasks by remote devices considering a P2P management overlay is a fairly typical example of the use of P2P technology in network management, and by consequence, of DNM. In order to accomplish the contract of virtual measurement sessions between peers, we developed a simple protocol.

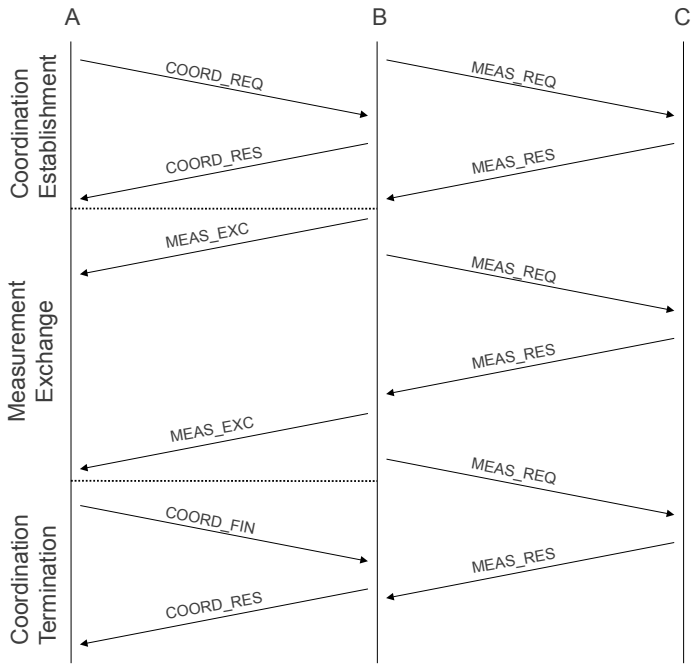
The protocol to contract virtual measurement sessions is inspired in the same kind of mechanism found in coordinated decision making protocols from multi-agent research area. For example, the *Contract Net Protocol* (CNP) (SMITH, 1980) is a multi-agent task-sharing protocol, consisting of a collection of agents, which can act like a manager or a contractor (*e.g.*, for different tasks). Unlike CNP, the proposed protocol is aimed at soft coordination, *i.e.*, a loosely coupled coordination. Besides that, the protocol focuses only in the contract of virtual measurement sessions.

Measurement contracts take place in different stages. First, in order to start the virtual measurement session, a device (*i.e.*, initiator device) needs to request such session to a (chosen) correlated peer (*i.e.*, contributing device). Then, this peer, which receives the request, can either accept or deny the execution of the virtual measurement session. After that, the peer starts to send results from the requested measurement session for the initiator. Both devices can asynchronously terminate the virtual measurement session for different reasons, which must be informed by the terminating party to the other device. The protocol to contract measurement sessions employs some messages exchanged in the P2P measurement overlay.

In Figure 4.2, we describe the messages exchanged due to the contract of virtual measurement session using the same example from the Figure 4.1. Coordination request (COORD_REQ) is sent by the local device to the chosen correlated peer. Correlated peer return the request with either a positive or a negative coordination response (CO-

ORD_RES) (Coordination Establishment phase in Figure 4.2). Peers exchange measurement results (MEAS_EXC) (Measurement Exchange phase in Figure 4.2). Both peers can finish the virtual measurement session anytime (COORD_FIN). Correlated peer returns the finish request with coordination response (COORD_RES) (Coordination Termination phase in Figure 4.2).

Figure 4.2: Message Exchange for Virtual Measurement Sessions.



Source: by author (2015).

Devices send messages regarding measurement contracts asynchronously in a network. This is because each device perform its measurement activation decisions in its own schedule. Thus, the requests and the results of such contracts are also communicated respecting the local schedules. In addition, the time needed for the messages to travel in the network varies too. By avoiding the synchronization in the control of measurement mechanisms, we achieve flexibility. However, it is necessary to use timeouts in order to avoid long waiting times which can impair measurement activation decisions.

4.4 Final Remarks

The activation of active measurement sessions is of interest to human administrators to uncover SLA violations. The use of an integrated approach to control such activation (as described in Chapter 2) can improve the detection of SLA violations. In this context, P2P technology can be used to enable a network-wide control of measurement mechanisms. The employment of such technology has several desirable benefits in the execution of network management tasks (described in Chapter 3). In the present chapter, we described principles to steer autonomically the activation of active measurement sessions using P2P technology. These principles try to capture some behaviors commonly employed by human administrators on such activation.

The definition of principles to steer autonomically measurement session activation decisions aims at increasing the number of SLA violations that can be detected in network. These principles enable a self-organizing, embedded P2P measurement overlay that uses the capabilities of the network devices to control session activation for SLA monitoring. First, we propose the use of local logic for the destinations prioritization using past service level measurement results and resource constraints. Second, we describe the concept of correlated peers for P2P measurement overlay provisioning. Finally, we depict the concept of virtual measurement sessions for the optimization of resource consumption.

The detection of SLA violations using active measurement mechanisms usually requires manual activation from human administrator. The decision on the set of destinations that should be probed is based on the administrators' experience and information provided by measurements themselves. The goal of the principles proposed in this chapter is to decrease the need for human and computational resources, while increasing the SLA monitoring coverage. However, these principles must be materialized to enable their effective deployment. In the following chapter, we describe strategies to activate active measurement sessions which embrace the presented principles. Such strategies are composed of algorithms which use P2P technology embedded in network devices.

5 STRATEGIES TO ACTIVATE ACTIVE MEASUREMENT SESSIONS USING P2P TECHNOLOGY

The goal of network devices in the solution proposed in the present thesis is to increase autonomously and dynamically the number of detected SLA violations using active measurement mechanisms. P2P technology can be embedded in network devices in order to meet this goal. In Chapter 4, we describe some principles to use P2P technology to control the activation of active measurement sessions. This technology increases the use of local information to make management decisions which avoids the contact to centralized management parties. However, it is necessary to materialize the principles regarding active measurement mechanisms.

Each device can consider a list of destinations which can be probed, *i.e.*, destinations that can have active measurements sessions configured and activated. Past service level measurement results and resource constraints can be used to rank such destinations through destination scores. Destinations ranks (described in Definition 5.1) can be built locally by network devices themselves using embedded P2P management software. In addition, such ranks must be performed iteratively in order to aim at accuracy and adaptivity to changes in network traffic conditions. The rationale and the algorithms that are employed by the destination ranks to perform the activation of measurement sessions in a cost effective way are called strategies.

Definition 5.1. *Destination rank is the list of destinations which can have activated measurement sessions along with information about each destination and sorted in a particular way.*

Strategies to activate measurement session (as described in Definition 5.2) are used to deploy a P2P control on the decisions about measurement sessions. In this context, the use of such strategies is twofold: they are used to define the information sources for the destination ranks and to establish resource sharing among network devices. In principle, as more information is used, the measurement session activation should capture better the service level violations. Furthermore, the choice of the strategy also influences on the resource consumption of measurement sessions regarding the devices.

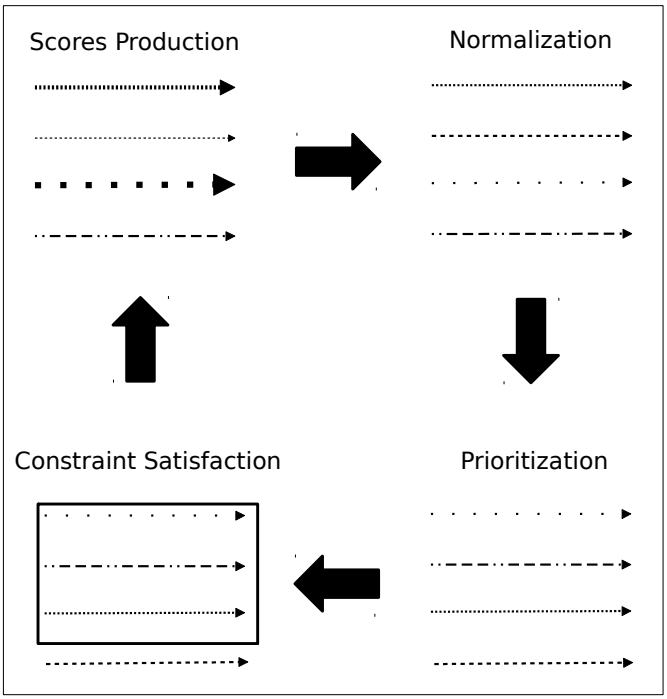
Definition 5.2. *Measurement session activation strategies define the expected behavior from the network devices concerning the activation of measurement sessions, thus, the approach employed for the operation of the destination ranks.*

This chapter is organized as follows. First, we depict how the destination ranks are composed. Then, measurement session activation strategies and their algorithms are described. Finally, concluding remarks are presented.

5.1 Destination Rank

Destination ranks are composed in order to determine which destinations should be probed considering the different measurement session activation strategies. The destination rank process is presented in Figure 5.1. The different possible end-to-end destinations for sessions of a specific network device are represented in this figure using arrows. Since network conditions may change over time, measurement session activation decisions must cope with these changes. Hence some mechanism is needed to dynamically adapt the decisions to network conditions. Each device has its own destination rank which leads to a distributed destination rank among the network infrastructure. Besides that, such distribution also promotes the local autonomy of the devices, incrementing the production of local management decisions.

Figure 5.1: Phases for the Destination Rank Process.



Source: by author (2015).

Destination ranks try to capture the common sense used by network administrators. This common sense is abstracted through destination scores (as described in Definition 5.3). Destination scores are composed by several management data (*e.g.*, past service level measurement results) and from different sources (*e.g.*, the device itself or other device in the network infrastructure). Different kinds of scores can be used, *e.g.*, based on service level measurement results, time, or even manually set.

Definition 5.3. *Destination scores are numbers assigned to destinations which are used to prioritize such destinations regarding measurement session activation decisions.*

P2P software can be embedded on network devices to compute the destination ranks. Such software is responsible for several tasks related to the execution of these ranks. Initially, local information enables the local computation of the destination scores. These scores are produced taking into account a variety of information from the network itself. In this context, P2P software also supports a P2P measurement overlay, which enables the communication among the devices themselves. Despite some limitations inherent to being hosted by dedicated network devices, embedded software can have direct access to the features exposed by active measurement mechanisms.

The destination rank is composed by the destinations list and their respective scores. We employ a computationally simple mechanism for prioritization which is opposite to heavyweight optimization. This mechanism is divided in four phases. First, in the Scores Production phase, destination scores are calculated for the available destinations. Then, these scores are normalized in the Normalization phase. After that, the destinations are prioritized (according to their score) in the Prioritization phase. Finally, constraints are applied to define the final destination set in Constraints Satisfaction phase. In Figure 5.1, we represent these phases which are described in the following sections.

5.1.1 Scores Production

Destination scores are produced for each destination in the Score Production phase. Score components can be of different kinds. Initially, we use two kinds of components: distance from Service Level Objective (SLO) and elapsed time from the last measurement session. These components are related to the principle of using past service level measurement results (as described in Chapter 4). The distance from SLO is aimed at measuring destinations that are likely to violate the SLA. Besides that, the elapsed time from the last

measurement session avoids that a destination keep without sessions for a long time.

Different score components can be composed to form a destination score. Regarding past service level measurement results, they may be either locally-collected or received data from correlated peers (which are depicted in Chapter 4. In addition, it is also possible to manually tune the destination rank. This can be done defining constant scores for specific destinations and specific weights to different score components. In this context, the sum of the score components for a destination is equal to the destination score.

There is considerably diversity on score components that can be used for the measurement decisions regarding the destination of measurement sessions. In Figure 5.1, we represent such diversity using arrows of different thickness. Thus, it is necessary to normalize such components in order to make them comparable. Since the destination scores are locally updated by network devices in each iteration of the destination rank, the normalization should also follow the same schedule.

5.1.2 Normalization

Normalization of score components allows the comparison of corresponding normalized values for different kinds of components. In this context, the contributions for such components must be comparable in terms of magnitude and granularity. For example, regarding the proposed use of historical measurement data, the score components show different features: distance from Service Level Objective (SLO) and elapsed time from the last measurement session. Thus, some form of normalization is necessary.

Normalization means adjusting values produced on different scales to a common scale. Thus, normalized values are usually produced through some rescaling in respect to a function. In this context, normalization on the score components can be performed using different kinds of normalization approaches. Initially, two kinds of normalizations are defined in the present thesis: piecewise-defined functions and standard scores. These approaches are chosen because they are widely used for normalization and consider functions which are readily available from the numeric packages of programming languages.

Piecewise-defined functions, *i.e.*, functions that can be defined in pieces, can be used for normalization in the destination rank. For example, step functions (*e.g.*, *Heaviside* step function) and ramp functions (*e.g.*, *Heaviside* step function times the input) are piecewise-defined functions since they behave differently based on the input value. The

advantages of using these functions for normalization is that they are computational cheap and it is easier to predict their behavior. The disadvantages are that they are probably less adaptively and it is possible to occur oscillations around switching points

Standard Scores can be used for normalization (*i.e.*, standardization). They are the number of standard deviations an observation or datum is above the mean, either positive (value above the mean), or negative (value is below the mean). The advantages of using standard scores for normalization is that they can be used in different settings and there is no switching points. As disadvantages, it can be cited that these scores have positive and negative values and they are computationally more expensive (comparing to piecewise-defined functions). Besides that, the behavior of standard scores is dependent of the distribution of values in the sample.

5.1.3 Prioritization

The goal of the destination rank is to increase the number of detected SLA violations through better measurement decisions. These decisions are related to the activation of measurement sessions. Thus, ultimately, the destination rank should define locally the subset of destinations that are more likely to violate the SLA. This subset is built in this work as the destinations which present the higher total scores, therefore the ones that should have activated measurement sessions. In this context, it is necessary some form of prioritization of the destination rank using these scores. Prioritization phase is presented in Figure 5.1.

The prioritized list of destinations represents the top destinations for probing in a given iteration. The prioritization is usually performed at each time interval necessary for measurement decisions, *i.e.*, destination rank iterations. In addition, prioritizations made in previous iterations can be taken in order to decrease resource consumption. Thus, it is possible to avoid unnecessary computations, specially when considering the repetitive activation of measurement sessions in troubled destinations.

The prioritization can be performed using different approaches. One of the possible approaches is the utilization of sorting algorithms using the destination scores. Despite the existence of several algorithms, sorting can be computationally expensive. Besides that, usually only the top destinations will be used for measurement purposes. Thus, it is also possible to use selection algorithms which includes either the cases of finding the minimum and maximum items in a list or k^{th} smallest item (*i.e.*, k^{th} order statistics). In

spite of being shown a sorted list of destinations in Figure 5.1, it is possible that just top destinations are selected.

5.1.4 Constraint Satisfaction

The number of activated measurement sessions has an important impact on the performance of the device. Intuitively, a larger number can lead to better coverage but also to significant resource consumption. Thus, it is usually necessary to restrict such number. Since the destination rank is prioritized before the constraint satisfaction, the definition of a subset of measurement sessions respecting constraints supposedly increase the number of detected SLA violations over other subsets of the same measurement sessions.

Resources constraints are used in our solution to select a subset of the destinations (constraint satisfaction in Figure 5.1). Once this subset has been selected, measurement sessions are activated on these destinations over a given time interval (usually the next iteration of the destination rank). Thus, resources constraints define the size of the final subset of destinations. Besides that, these constraints may vary over time. For example, this can happen due to changes in the available resources for measurement mechanisms in the network device.

Destination rank and the resource constraints are used to select the destinations that should be measured. However, considering the principles to control the activation of measurement sessions (as explained in Chapter 4), it is possible to consider both local and remote information to perform this control. In this context, devices can easily ensure that local resource constraints are respected because this can be done just checking the local number of activated sessions. Instead, global constraints depend on information exchanged by remote devices. When local and global constraints are considered, the final local subset is produced using the minimum between these constraints.

The network devices can use virtual measurement sessions (as explained in Chapter 4) in order to increase the possible number of detected SLA violations without consuming significant local resources. In this context, additional constrains may be applied since this use still causes resource consumption. Thus, besides a subset of destinations that should be locally probed, the destination rank can define another subset for virtual measurement sessions.

The definition of the behavior of the destination rank is depicted in the strategies for the

activation of measurement session. Such strategies configure specific characteristics of this behavior, which will be described in the next section.

5.2 Strategies to Activate Measurement Sessions

The principles presented in Chapter 4 are defined to steer autonomically measurement session activation decisions. In order to accomplish basic functionality regarding these principles, destination ranks are used (as shown in Section 5.1). These ranks can be computed using either only information available locally or information exchange by correlated peers. *A priori*, as more information from the network is used in destination ranks, measurement session activation decisions capture better the service level violations. Besides that, virtual measurement session can be deployed to increase SLA monitoring coverage. The approach employed to take these decision is controlled by strategies to activate measurement sessions.

The utilization of measurement session activation strategies assumes that the active measurement mechanisms can be controlled without internal modification (as described in Chapter 1). In other words, the strategies should be able to handle current versions of active measurement mechanisms (*e.g.*, O/TWAMP and IPSLA). Thus, the strategies aim at increasing the efficiency of the detection of SLA violations solely through efficient sessions activation decisions. The assumption of "agnostic" strategies increases the applicability of the present work considering academic and commercial implementations of active measurement mechanisms.

Initially, we define three strategies to choose which destinations will be probed: measurement session activation based solely on local information, measurement session activation based on both local and remote information, and measurement session activation considering the use of virtual measurement sessions. Each strategy builds up on the previous one, increasing the used information for measurement session activation decisions. We also define a random measurement session activation in order to demonstrate basic features of the destination rank. Now we describe the different measurement session activation strategies and their respective algorithms.

5.2.1 Random Strategy

The random strategy is the simplest measurement session activation strategy defined in the present work. The rationale behind this strategy is to randomly activate sessions over the possible end-to-end destinations. These destinations are manually provided by human administrators which in turn compose destination ranks in a per node basis. The random strategy is described in more detail on Algorithm 5.1.

Algorithm 5.1 Random Strategy

```
{Function parameters: α, β, dest[]}
shuffle(dest[])
k ← min((β, α/sizeOf(dest[]), sizeOf(dest[]))
for i = 1 → k do
   activateSession(dest[i])
   i ← i + 1
end for
```

In each iteration of the destination rank, first the algorithm shuffles the list of possible destinations ($dest[]$). After that, the number of measurement session that will be activated (k) is defined. In this context, k is the minimum between β (local upper bound for activated measurement sessions), local inferred α (global upper bound for activated measurement sessions), and the number of available destinations ($sizeOf(dest[])$). Then, k destinations from the the list of possible destination are chosen to have activated measurement sessions ($activateSession(dest[i])$.

Despite the use of local logic and data, the random strategy does not introduce a measurement policy in the sense of an approach to improve the detection of SLA violations. Thus, considering that there are k possible destinations to choose from, they will be chosen approximately with the same probability ($1/k$). However, even in the simplest proposed algorithm, the use of the destination rank expose interesting features. For example, this use avoids multiple local measurement session towards the same destination (due to a configuration error). Furthermore, nodes can control their own resource consumption using the α and β constraints.

5.2.2 Local Strategy

The local strategy builds up on the random strategy and it is the simplest one that aims at improving the detection of SLA violations through measurement activation

decisions. Such decisions take into account the probability of occurring a SLA violation in a given destination and the available resources for activated sessions. In this context, the local strategy is performed using only information (data and logic) locally available on a node to compute scores for each destination. This information comes from past service level measurement results. The local strategy is described in more detail on the Algorithm 5.2.

Algorithm 5.2 Local Strategy

{Function parameters: $\alpha, \beta, A, B, windowSize, dest[]$}
shuffle($dest[]$)
$k \leftarrow min((\beta, \alpha/sizeOf(dest[]), sizeOf(dest[]))$
for $t = 1 \rightarrow sizeOf(dest[]$ **do**
  $rankLast[t] \leftarrow getLastLocal(dest[t])$
  $rankPast[t] \leftarrow getPastLocal(dest[t], windowSize)$
  $t \leftarrow t + 1$
end for
prioritize($dest[], key \leftarrow A*$ normalize($rankLast[]) + B*$ normalize($rankPast[])$)
for $i = 1 \rightarrow k$ **do**
  activateSession($dest[i]$)
  $i \leftarrow i + 1$
end for

The differences between the random and the local strategy start in the definition of destination scores. Now the probability of a destination to be chosen is related with two score components: the average distance of past measurement results to SLOs ($rankPast[]$) in a sliding window ($windowSize$) and the time elapsed from the last measurement ($rankLast[]$) for a given destination (t). The first score tries to capture the destinations which are closer to violate the SLA, which should have a higher probability of being probed in the following iterations of the destination rank. The second score aims at maintaining frequent measurements on destinations. Even if a destination is not close to violate specific SLOs, it is important that it be measured frequently. Thus, if a destination had not been measured recently, then it should be more likely to be selected in the next iterations.

The normalization phase is necessary in order to make the different score components comparable. Thus, a specific (normalized) score components of a destination must vary between a minimum and a maximum. In addition, and it is also possible to "tune" the contribution of $rankPast[]$ and $rankLast[]$ using the constants A and B, respectively. After that, destinations are prioritized according to their total score. Finally, the algorithm greedily chooses the k highest scored destinations for activating measurement

sessions. Since the measurement results are updated dynamically, the strategy could adapt to changes in network conditions. Auxiliary functions ($getLastLocal$ and $getPastLocal$) are described in the Appendix B.

Despite the use of local logic and data, the local strategy uses only a few desirable features of P2P technology. In principle, as more information from the network is used, measurement activation decisions can capture better SLA violations. However, local strategy uses only information locally available, thus it lacks is the ability of using remote information what is a key feature in P2P systems. In any case, there is a locally-restricted prioritization of destinations considering one of the principles described in Chapter 4, local information for the destinations prioritization using past service level measurement results and resource constraints.

5.2.3 Local and Remote Strategy

The local and remote strategy is performed using information available from the local network device and received from other devices. The rationale behind this strategy is to increase the use of information from the network to improve measurement session activation decisions. In this context, these decisions may take into account local and remote information to better adapt to network environment conditions. Therefore, the main difference between this strategy and the local one is the source of measurement results. The local and remote strategy is described in more detail on Algorithm 5.3.

The local and remote strategy is composed by two distinguished phases: peer topology phase and measurement session activation phase. In the first phase, we use the concept of correlated peers (as described in Chapter 4). After that, the measurement session activation decision are performed using the locally collected information and also measurement results received from correlated peers. As a note, peer topology updates and the activation of measurement sessions may run on separate schedules; they do not have to adhere to the same time intervals.

The peer topology phase of the local and remote strategy uses a P2P measurement overlay built using correlated peers. Network devices peers are considered as correlated peers if their measurements for a given destination (or a set of destinations) are correlated. Each device compares measurements from remote devices with its own measurements in order to rank the remote devices that have more correlated measurements ($getCorrelatedPeers$). Therefore, the use of correlated peers enables the grouping of

Algorithm 5.3 Local and Remote Strategy

{parameters: $\alpha, \beta, A, B, C, windowSize, dest[], correlationMin, peersMax$}
shuffle($dest[]$)
$k \leftarrow min((\beta, \alpha/sizeOf(dest[]), sizeOf(dest[]))$
if $correlatedPeers[] == null$ **then**
  $correlatedPeers[] \leftarrow getEndpoints(dest[])$
else
  $correlatedPeers[]$
  $\leftarrow getCorrelatedPeers(dest[], correlationMin, peersMax)$
end if
for $t = 1 \rightarrow sizeOf(dest[])$ **do**
  $rankLast[t] \leftarrow getLastLocal(dest[t])$
  $rankPast[t] \leftarrow getPastLocal(dest[t], windowSize)$
  $rankRemote[t] \leftarrow getPastRemote(dest[t])$
  $t \leftarrow t + 1$
end for
prioritize($dest[], key \leftarrow A*$ normalize($rankLast[]$)$+B*$ normalize($rankPast[]$)$+C*$ normalize($rankPastRemote[]$)
for $i = 1 \rightarrow k$ **do**
  activateSession($dest[i]$)
  $i \leftarrow i + 1$
end for
$sendMeasurementResults(correlatedPeers[])$
$sendCorrelatedPeers(correlatedPeers[])$

devices which share similar properties regarding measurements. Such comparison is performed through different statistical functions (as explained in Section 4.2).

Some constraints are necessary to enable an efficient operation of the P2P measurement overlay. The assurance of remote information relevancy uses the concept of correlated peers. Thus, a minimum correlation score is defined to set the required correlation between such peers ($correlationMin$). In addition, remote devices which have higher correlation scores are chosen as correlated peers respecting the maximum number of such peers ($peersMax$) that a device can have in a given time (size of local view of the P2P measurement overlay). Since resources are needed for peer maintenance, the upper bound restricts the resource consumption.

In order to define its correlated peers, a device needs past measurement results from other devices. Thus, each iteration is preceded by peer selection, which determine the set of candidate peers, *i.e.*, remote devices that may be evaluated for correlation purposes, to share measurement results. In order to bootstrap peer selection, these candidates can be seeded randomly or determined via topology relationship ($getEndpoints(dest[])$). Devices send information about their measurements for their candidate peers. After the first interaction, current peers can be used for re-evaluation. Eventually, peers also spread their correlated peers in order to permit evaluation of "peers of peers" ($sendCorrelatedPeers(correlatedP$ After determine actual correlated peers from candidate peers, the device starts to send its past measurement results for the correlated peers ($sendMeasurementResults(correlatedPeers[])$).

The measurement session activation phase takes place in a similar fashion that in local strategy. However, the destination score also takes into account past measurement results from correlated peers. Thus, this score is composed of one more component, the summary of received remote measurement results ($rankRemote[]$) for a given destination (t). It is also possible to "tune" the contribution of $rankRemote[]$ using the constant C. The resource consumption from activated measurement sessions is controlled in a similar fashion using the α and β constraints. However, as α considers information from different nodes, now the amount of remote information that is exchanged by nodes influences how α is computed. Auxiliary functions regarding the local and remote strategy ($getEndpoints$, $getCorrelatedPeers$, $getPastRemote$, $sendCorrelatedPeers$, and $sendMeasurement$ are described in the Appendix B.

The local and remote strategy employs local and remote information to make measurement session activation decisions. The use of remote information is performed considering one of the principles described in Chapter 4, correlated peers for P2P measure-

ment overlay provisioning. Such overlay can improve the adaptivity of measurement session activation decisions, since SLA violations detected in different parts of the network can steer the activation of local measurement sessions. However, the detection of such violation is still bounded by the maximum number of measurement sessions that can be locally activated.

5.2.4 Virtual Strategy

The virtual strategy enhances the the concept of correlated peers in order to choose which peers are interesting to share measurement sessions with, *i.e.*, to have virtual measurements with (described in Chapter 4). The use of virtual measurement sessions permits that the number of detected SLA violations be higher than the number of locally available measurement sessions. This strategy builds up on the local and remote strategy, thus the measurement session activation and peer topology phase are also performed. We consider a scenario of multiple devices which observe multiple events (end-to-end measurements) and those devices need to perform measurement session decisions in a dynamic network. Hence some mechanism is needed to dynamically adapt the contract of virtual measurement sessions to network conditions. The virtual strategy is described in more detail on Algorithm 5.4.

The virtual strategy assumes a common objective among the peers that form the P2P measurement overlay which is to improve the detection of SLA violations. The policy employed by this strategy is to reserve local measurement sessions for top priority destinations and then use virtual measurement session to increase SLA monitoring coverage. In addition, devices control the resource consumption due to virtual measurements using the γ, besides α and β (described in the previous strategies). In this context, the Algorithm 5.4 divides the SLA monitoring task (*i.e.*, available destinations for measurement sessions) in different parts.

Network devices partition the SLA monitoring task in three kinds of destinations considering the prioritization of the destination rank ($dest[]$) and the resource constraints. In this context, the resulting parts can be presented considering such prioritization in a descending order. The first part is the set of destinations which will be measured locally ($i = 1 \rightarrow k$) through activated measurement sessions. The second part is the set of destinations which cannot be measured locally, but they can be monitored through virtual measurement sessions ($z = k \rightarrow k + \gamma$). The third part is the set of destinations that will

Algorithm 5.4 Virtual Strategy

{parameters: $\alpha, \beta, \gamma, A, B, C, windowSize, dest[]), correlationMin, peersMax,$}
{$virtualMin, virtualMax$}
shuffle($dest[]$)
$k \leftarrow min((\beta, \alpha/sizeOf(dest[]), sizeOf(dest[]))$
if $correlatedPeers[] == null$ **then**
  $correlatedPeers[] \leftarrow getEndpoints(dest[])$
else
  $correlatedPeers[]$
  $\leftarrow getCorrelatedPeers(dest[], correlationMin, peersMax)$
end if
for $t = 1 \rightarrow sizeOf(dest[])$ **do**
  $rankLast[t] \leftarrow getLastLocal(dest[t])$
  $rankPast[t] \leftarrow getPastLocal(dest[t], windowSize)$
  $rankRemote[t] \leftarrow getPastRemote(dest[t])$
  $t \leftarrow t + 1$
end for
prioritize($dest[], key \leftarrow A*$ normalize($rankLast[]$)$+B*$ normalize($rankPast[]$)$+C*$
normalize($rankPastRemote[]$)
for $i = 1 \rightarrow k$ **do**
  activateSession($dest[i]$)
  remove($dest[i]$)
  $i \leftarrow i + 1$
end for
if $k + \gamma <= sizeOf(dest[])$ **then**
  for $z = k \rightarrow k + \gamma$ **do**
    $candidateVirtualMeasurementPeer \leftarrow$
      $getCorrelatedPeer(dest[z], virtualMin, 1)$
    $sendVirtualCommand(candidateVirtualMeasurementPeer, request)$
    $z \leftarrow z + 1$
  end for
end if
$sendMeasurementResults(correlatedPeers[])$
$sendCorrelatedPeers(correlatedPeers[])$
$sendVirtualMeasurement(virtualPeers[])$

not be measured ($k + \gamma \rightarrow sizeOf(destinations[])$).

Each device may choose which peer is the best candidate to share specific measurements. The choice is made considering the top correlated peer ($candidateVirtualMeasurementPeer$) *i.e.*, peer with the highest correlation score ($getCorrelatedPeer(destinations[z], virtualMin)$). We assume that higher correlation scores between peers are an indicative of trustiness in the virtual measurement sessions. Since correlated peers are defined using information from past service level measurement results, therefore, indirectly, the probability of a peer to be chosen as a source for virtual measurement sessions is also related with the same results.

Peers employ a simple algorithm that contracts virtual measurements sessions from other devices through message exchange in a P2P measurement overlay. In order to accomplish this, we developed a simple protocol (described in Chapter 4). In Algorithm 5.4, we just present the procedure to start a virtual measurement session($sendVirtualRequest$). The chosen correlated peer ($candidateVirtualMeasurementPeer$) is the destination of the virtual session request.

The virtual strategy increases the maximum number of detected SLA violations that can be detected in a network infrastructure. This number can be higher than the number of local activated measurement sessions considering the use of virtual measurement sessions. However, results from virtual sessions are not as accurate as if they had been produced locally. Thus, virtual measurement sessions can result in false positives and negatives regarding the detection of SLA violations. In order to improve virtual session accuracy, it is possible to restrict the use of virtual measurement session only from top correlated peers.

5.3 Final Remarks

The use of P2P technology in network management (also known as P2P-based Network Management - P2PBNM) can control the operation of SLA monitoring performed by measurement probes. This technology may be employed in network devices themselves. Embedded management peers can be used to deploy the principles to steer the activation of active measurement sessions (presented in Chapter 4). In this chapter, we describe the deployment of such principles through destination ranks and strategies to activate measurement sessions.

The destination rank is composed by the ranked list of destinations considered by

a network device for probing purposes. Top ranked destinations represent the ones which should be prioritized in the activation of active measurement sessions. In order to perform the ranking, it is assigned a score to each destination in this list. Different properties and sources of past active measurement results are used to compose destination scores. In this context, the behavior of the destination rank is controlled by the chosen strategy to activate measurement sessions.

The measurement session activation strategies are depicted in this chapter. These strategies determine how the subset of destinations to be probed are defined. In this context, the principles presented in Chapter 4 are incrementally materialized in definition of such subset, which should improve measurement decisions. In Table 5.1, we provide a summary of measurement session activation strategies according to their adherence to such principles.

Table 5.1: Summary of the Proposed Measurement Session Activation Strategies.

Strategy	Principles		
	Local Logic	Correlated Peers	Virtual Measurements
Local	Yes	No	No
Local and remote	Yes	Yes	No
Virtual	Yes	Yes	Yes

Source: by author (2015).

P2P management software inside network devices can be used to enable a network-wide control of the activation of active measurement sessions in a decentralized fashion. We hypothesize that as more information from the network is used, the measurement session activation decisions detect better the SLA violations. Thus, the proposed measurement session activation strategies should present different performance on such detection. Besides that, while detecting such violations, it is also necessary to control the resource consumption on the network devices. Therefore, it is necessary to evaluate such strategies as well as the the use of the destination rank *per se*.

6 EVALUATION

Actively monitoring SLA performance is an important step in the early identification of SLA violations. This identification can be done using active measurement mechanisms. In this context, the control of such mechanisms affects probing efficiency, monitoring coverage, and consumed resources. In order to accomplish this control, it is possible to steer the expected behavior from the network devices concerning the activation of active measurement sessions. We propose the use of P2P technology to improve the detection of SLA violations by the network devices themselves.

We studied the performance of our proposed solution by defining and implementing simulation experiments. The focus of such experiments is to evaluate the features of the solution proposed in this thesis regarding the decentralized detection of SLA violations. The principles to steer autonomically measurement session activation decisions (explained in Chapter 4) as well as the properties of the destination rank and the measurement session activation strategies (described in Chapter 5) are considered for the definition of the experiments and the discussion of the results.

The remaining of the chapter is organized as follows. First, we present the implementation produced regarding the proposed solution. After that, we describe the experimental setup used to evaluate the present work. Then, results produced on the execution of the simulation experiments are depicted. Finally, some concluding remarks are presented.

6.1 Implementation

The software needed to perform the simulation experiments was implemented in Java using PeerSim[1] (MONTRESOR; JELASITY,), which is an open source event-based simulator of P2P systems. The simulator provides the basic node communication infrastructure as well as transport layer models, which can emulate some characteristics of IP networks (*e.g.*, packet loss and delay). Furthermore, we introduced some changes in the transport layer models of PeerSim in order to allow explicitly dynamic modifications in network conditions in a per link basis. Thus, it is possible to have an almost complete control of the simulation environment.

We implemented software components for the active measurement mechanism, the destination rank, and the measurement session activation decision algorithms. Be-

[1] PeerSim: A Peer-to-Peer Simulator - http://peersim.sourceforge.net

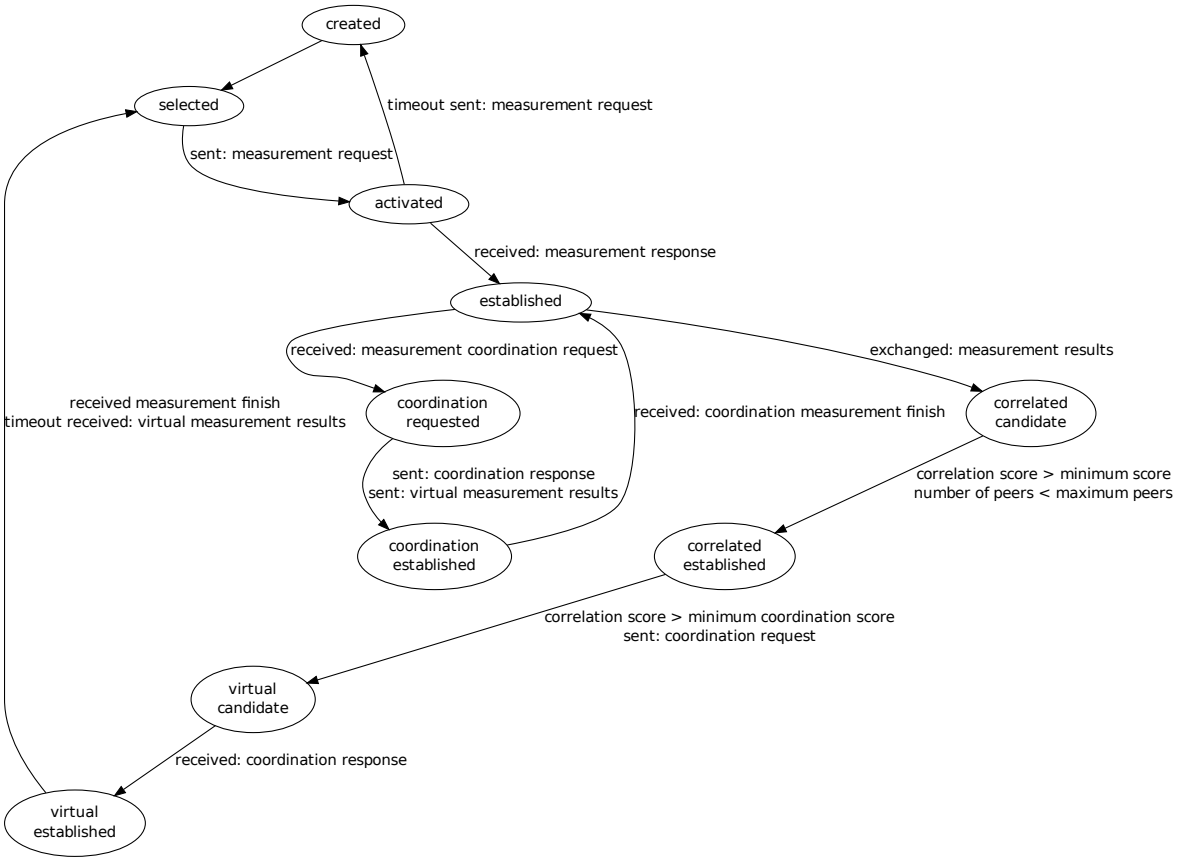
cause our proposed principles consider embedding peers in network devices (as described in Chapter 4), the implementation is contained in the node class of PeerSim. Thus, in order to simulate the use of devices programmability, each instance of such class (*i.e.*, an individual node) performs all these software components in the simulation experiments.

A simple active measurement mechanism was implemented in the simulation environment. Since we believe our proposed solution can be used with different active measurement mechanisms, it is necessary just to support basic features of such mechanisms which are common in respect to academic implementations, *e.g.*, TWAMP (HEDAYAT et al., 2008), and commercial implementations, *e.g.*, IPSLA (CHIBA et al., 2013). More specifically, the implemented mechanism is heavily based on TWAMP-light, therefore there is no control protocol and it is assumed that measurement probes are configured and reflect the incoming measurement request in a appropriate fashion. The implemented mechanism enables the measurement of network metrics such as one-way/round-trip delays, jitter, and packet loss in real time.

Monitoring resolution and polling frequency regarding the active measurement sessions is restricted to simulation cycles. Despite the measurement computation being performed within one cycle by the nodes, the collection of measurement session results depends on the return of measurement response (analogous to the operation of commercial active measurement mechanisms). This is true for both one-way and two-way measurements. The interval of the send of measurement requests in a session is configurable.

The implementation of the destination rank follows the division in four phases (as described in Section 5.1): the Scores Production phase, the Normalization phase, the Prioritization phase, and Constraints Satisfaction phase. Destination scores are produced for the available destinations considering the employed measurement session activation strategy (and, consequently, the decision algorithm). Besides that, we implemented two normalization approaches: piecewise function (multiple sub functions applying to a certain interval of the function domain) and standards scores (subtracting the mean of destinations from an individual raw score and dividing by the standard deviation). After that, the destinations are prioritized using either quicksort (a sorting algorithm) or quickselect (a selection algorithm). Finally, constraints are applied to define the destination to be probed. We implemented the control of the maximum number of locally activated measurement sessions (β) as well as the maximum number of virtual measurement sessions (γ). We did not implemented the maximum number of globally activated measurement sessions (α) since its definition can be reduced to β regarding the proposed algorithms.

Figure 6.1: State Diagram for Measurement Sessions



Source: by author (2015).

We implemented the measurement session activation decision algorithms (which are described in Chapter 5) in PeerSim. Regarding the local and remote strategy and the virtual strategy, the correlation of measurement sessions results is performed using historical measurement data. This is done in addition to the execution of the destination rank. Such correlation is implemented through two approaches: we implemented a Student's t-test for the comparison of summary characteristics from samples and the Pearson Product-Moment Correlation Coefficient for statistical dependence. Finally, virtual measurement sessions are activated using the protocol proposed in Section 4.3.

The measurement decisions taken considering the destination ranks change the state of the active measurement sessions hosted by a device. In Figure 6.1, we represent the states considered by the described implementation. Initially, every destination in the list considered by the destination rank is a measurement session in created state. This means that the measurement probe is configured for these destination, but there is not a significant resource consumption. The destinations selected by the destination rank to be

probed have their state changed to selected. Then, when the measurement probe initiates a measurement session towards a destination, what is done through a measurement request message, the state of this measurement session changes to activated. The acknowledgement of the measurement request message by a measurement response message changes the state of the measurement session to established. On the other hand, if this response is not received in a defined time frame, the state returns to created.

The local and remote strategy uses P2P technology to perform decisions about measurement sessions using results shared among network devices. Regarding measurement sessions states, this is represented in Figure 6.1 by the states correlated candidate and correlated established. After an exchange of measurement results, the measurement session has its state changed from established to correlated candidate. If the correlation score is greater than minimum correlation score and number of peers is smaller than maximum number of correlated peers, the remote device can be selected as a correlated peer. In this case, the measurement session state is changed to correlated established.

The virtual strategy enables the execution of virtual measurement sessions besides the ones locally performed by the network devices. In order to become virtual, the measurement session must be first in the correlated established state. Besides that, the correlation score must be greater than minimum coordination score. The activation of a virtual measurement session between peers is performed by a simple contract protocol. From the view point of the device which request the virtual measurement session (represented in Figure 6.1 by the states virtual candidate and virtual established), the initiation is performed by a coordination request message. This changes the state to virtual candidate. A received coordination response, which means that the peer agreed to exchange measurement results, changes the measurement session state to virtual established. If the device either receives a coordination measurement finish or results are not received for a defined time frame, the measurement session state returns to selected.

The states of a virtual measurement session can be represented by the point of view of the device which performs the measurement session and provides the results for the remote device. This is represented in Figure 6.1 by the states coordination requested and coordination established. After a reception of a measurement coordination request message, the measurement session has its state changed from established to coordination requested. After the coordination response response is sent, the measurement results start to be forwarded to the remote device and the state of the measurement session is changed to coordination established.

Configuration parameters should be provided to the implemented code in order to perform the measurement session activation. This parameters are passed through a configuration file. Some parameters are required for any strategy (and, consequently, for all algorithms). For example, the chosen strategy, measurement session destinations, the metric that represents the measurement type, value used to define the SLO threshold, and the maximum number of local sessions (β). Besides that, some parameters are used in some strategies, such as the minimum correlation score (when using either local and remote or virtual strategy), the maximum number of correlated peers (when using either local and remote or virtual strategy), and the maximum number of virtual measurement sessions (only when using the virtual strategy).

An event parser was implemented to ease the results processing in PeerSim. This parser is responsible to handle measurement sessions events in the form of measurement reports. Such events are measurement sessions results locally collected and messages received from other nodes, such as overlay messages from correlated peers. The reports are composed of the summary of the detected SLA violations per time as well as additional information about the operation of the measurement session activation decisions. Some examples of this information are the list of activated sessions along with their configuration (*e.g.*, destination and metric) per time and the list of destination scores per time. Furthermore, information pertaining to some strategies is also provided, such as the local vision of the peer topology per time.

6.2 Experimental Setup

The approach employed for the evaluation of the solution proposed in the present thesis was performed using simulation experiments. The choice of using such experiments to analyze the use of P2P technology on the decentralized of detection of SLA violations is due to the simulation environment control. Anyway, it is important to produce network properties in the simulation close to those found on production network in order to increase the confidence in the experimental results. In this section, we describe the experimental setup employed in the simulation experiments.

The simulation experiments are performed in topologies which present different properties. These topologies can be classified in synthetic ones, inferred from real network environments, and Point of Presence (PoP) level aggregation of National Research and Education Networks (NRENs). The synthetic HOT-link topologies were created us-

Table 6.1: Summary of the Topologies Selected for the Experiments

Topology	Interior nodes	Leaf nodes	Total nodes	Interior/Leaf nodes ratio
Hot-like A	8	19	27	0.42
Hot-like B	17	34	51	0.5
Rocketfuel-derived A	21	19	40	1.11
"4-post" DC	20	64	84	0.31
Internet2 PoP level	11	11	22	0.5
Rede Ipê PoP level	28	28	56	0.5

Source: by author (2015).

ing the Orbis topology generator (MAHADEVAN et al., 2007) and the inferred topology is obtained using available data from the Rocketfuel project (SPRING; MAHAJAN; WETHERALL, 2002). Besides that, we deployed our implementation on "4-post", a Data Center (DC) topology used and advertised by Facebook (FARRINGTON; ANDREYEV, 2013). Finally, the Internet2[2] and RedeIpê[3] NRENs are also used for the experiments, considering a PoP level aggregation. The selected topologies are illustrated through graphs in Figure 6.2 and some properties of these topologies are presented in Table 6.1.

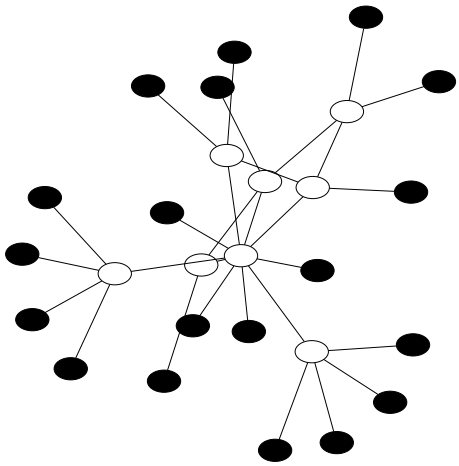
Routing on the network topologies used in the evaluation is performed through static routing. Thus, there is no routing protocols and the configuration is defined manually. In addition, traffic between twoendpoints are carried always by same service path in a defined routing state, *i.e.*, there is no multipath traffic. The end-to-end paths were calculated using shortest paths, considering only the number of hops. In this context, knowledge about the Routing Information Bases (RIBs) as well as about the network topology is not required by the measurement session activation strategies.

We consider that all leaf nodes (depicted as black circles on Figure 6.2) in these topologies deploy active measurement probes. The assumption of measurement probes being located on leaf nodes is related to the investigation focus: detection of end-to-end SLA violations. These assumptions also holds considering the common practices on field deployments. Leaf nodes are instrumented to initiate and respond measurement sessions, thus they can act as both senders and responders. In this context, the chosen topologies vary significantly regarding the number of interior and leaf nodes (as can be noticed in Table 6.1).

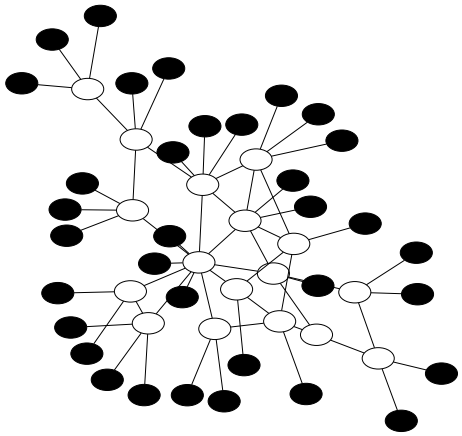
[2]Internet2: American Advanced Computer Networking Community - http://www.internet2.edu

[3]RedeIpê: Brazilian Academic Computer Networking Infrastrucure - http://www.rnp.br/servicos/conectividade/rede-ipe

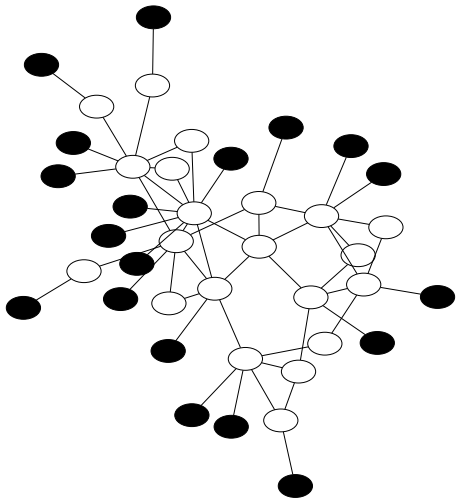
Figure 6.2: Selected Topologies Used for Simulation Experiments.



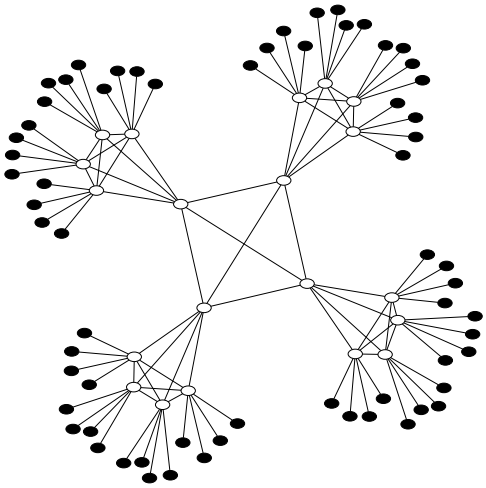
(a) Hot-like A Topology



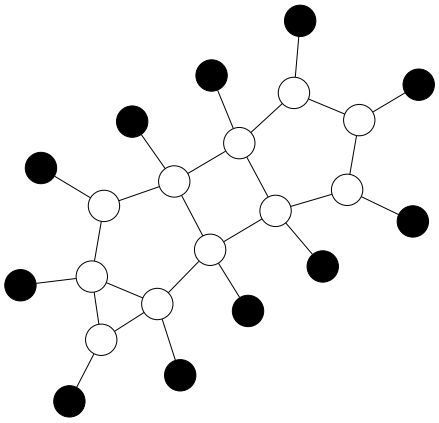
(b) Hot-like B Topology.



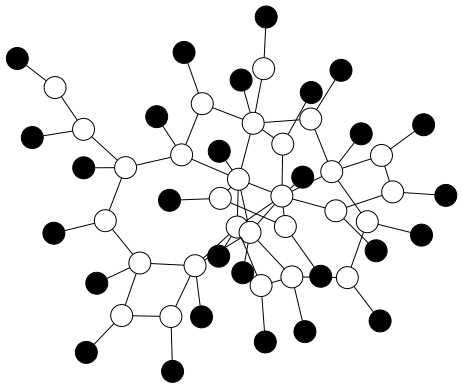
(c) Rocket-derived A Topology.



(d) “4-post” Data Center Topology.



(e) Internet2 PoP Level Topology.



(f) RedeIpê PoP Level Topology.

Source: by author (2015).

Leaf nodes run exactly the same measurement session activation strategy in a given experiment. Besides that, all these nodes are considered as candidate destinations to be probed in each simulation cycle. Measurement probes, which run on leaf nodes, always reply positively to measurement requests (to complete the activation of measurement sessions). In addition, nodes also reply positively to coordination messages (to start virtual measurement sessions). Finally, the implemented measurement mechanism is controlled as a local interface by the measurement session activation strategies. This is done to simulate the behavior of a P2P code embedded in a regular network device.

The simulation experiments consider a network-wide SLO for detecting SLA violations (for simplicity reasons). However, it is possible to operate with multiple SLAs as well as considering SLOs in a per node basis. In the experiments, deviations from SLOs (*i.e.*, detection of SLA violations) can be identified by single network devices considering single measurement sessions. Defining metrics that matter to a network infrastructure depends on the networked services. However, typically, network performance is assessed based on the latency metrics, such as delay and jitter. Thus, we introduce modifications in the delay of links to simulate latency-related service level problems. All network modifications are injected in one direction for a given link and are defined in terms of simulation cycles.

The simulation experiments consider the minimum granularity of the implemented active measurement mechanism. Thus, when activated, a measurement session has a measurement request message sent by the probe at every cycle. Since SLOs are defined in simulation cycles and the destination rank is computed at every cycle, the measurement resolution is adequate for SLA detection. Regarding the experiments, we included results from the random strategy to present basic features of the destination rank. Besides that, local strategy can be viewed as a baseline for measurement session activation strategies which enable more P2P features, the local and remote strategy and the virtual strategy.

6.3 Experiments

The focus of the simulation experiments is to evaluate the detection rate of SLA violations as well as the properties of the measurement session activation strategies and the destination rank. The use of P2P technology enable the use of local information, logic and data, to steer active measurement mechanisms. Such use is defined regarding the measurement session activation strategies, which vary in terms of the employed informa-

tion and P2P features. Thus, the common objective of the performed experiments is to compare such strategies in a controlled environment.

The measurement session activation strategies aim at increasing the efficiency of the detection of SLA violations solely through a network-wide control of the activation of active measurement sessions. In this context, we believe such strategies can be used with different active measurement mechanisms, thus, we explicitly do not focus on the accuracy characteristics of the implemented mechanism itself. For this reason, we did not experiment with a variety of network metrics either.

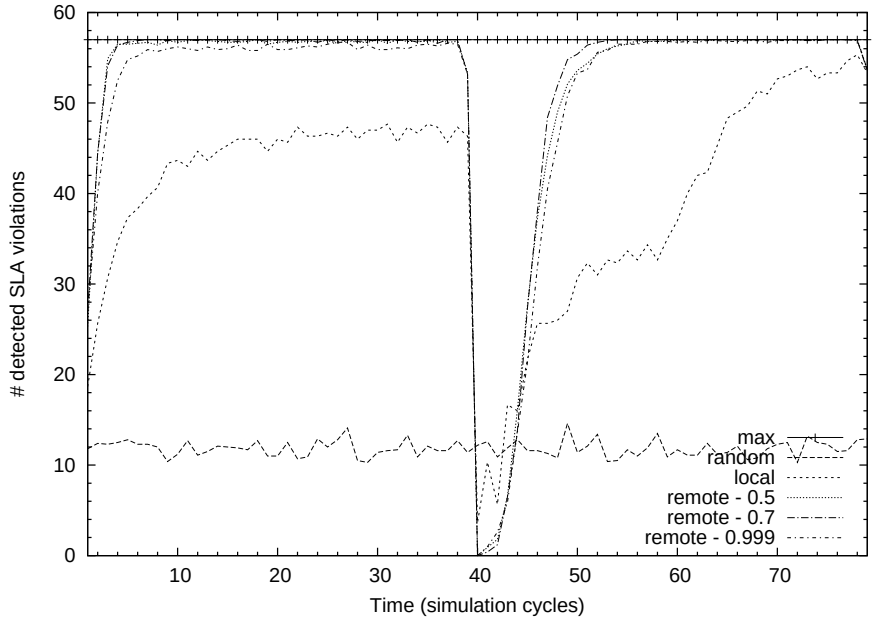
The experiments were performed in a way to decrease the effects of certain influences (anomaly results). We used series of 10 simulation experiments and the graphics present the mean values, unless stated otherwise. Such experiments were started using different random seeds. It is important to mention that the observed variance in the experiments was low.

6.3.1 The Influence of Measurement Session Activation Strategies on the Detection of SLA Violations

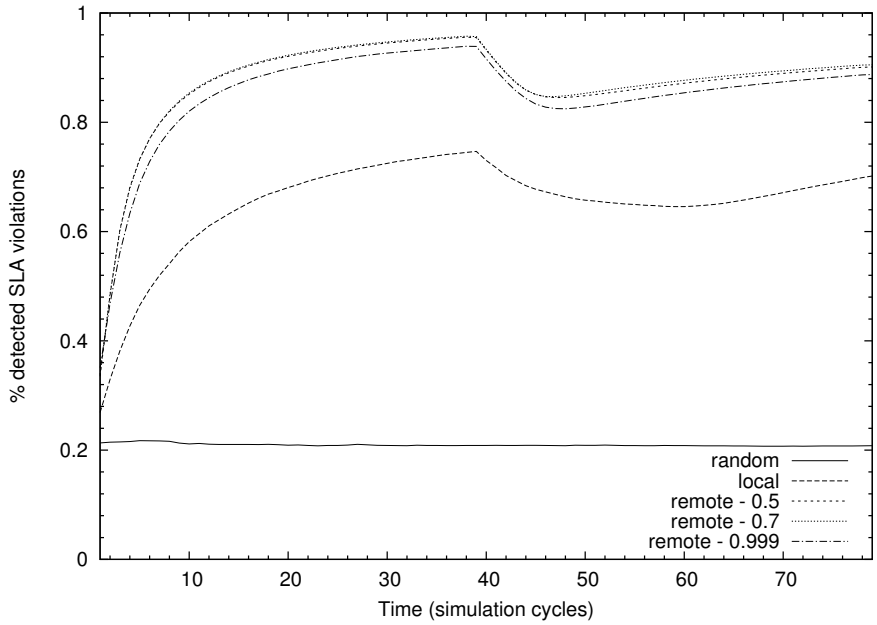
We performed some experiments in order to assess the influence of measurement session activation strategies on the detection of SLA violations. Obviously, a static activation of measurement sessions cannot follow short-term and longterm variations in network dynamics. Thus, the strategies should adapt to such variations in order to increase and maintain the efficiency of the SLA monitoring. In this section, we were just considering the control of the activation of local deployed sessions, thus the virtual strategy is excluded, *i.e.*there is not any virtual measurement sessions.

In the first experiment, we aim at determining the adaptation features of measurement session activation strategies. In order to accomplish that, we collected the number of SLA violations detected by nodes regarding a specific network environment scenario. In this scenario, initially there is not any SLA violation. Then, we increased the one-way delay on 4 access links for 40 cycles, which makes the end-to-end destinations that traverse these links to appear as SLA violators for the simulated active measurement mechanism. Then, we decreased the delay for these links and increased the delay for other 4 links for the same amount of cycles. This is done to simulate an almost instantly change in the placement of violations in the topologies, which is worst case situation for an adaptive approach. We chose the number of cycles in which the experimental scenario is changed

Figure 6.3: Number of Detected SLA Violations for Hot-like A Topology.



(a) Raw Number of Detections



(b) Cumulative Percentage of Detections

Source: by author (2015).

in order to permit that the proposed strategies go through steady state. We chose $\beta = 3$ in order to have a slightly lower potential number of detection than the injected violations.

The results for the first experiment are shown on Figures 6.3, 6.4, and 6.5, considering the Hot-like A, Hot-like B, and Rocket-derived A topologies (respectively). In

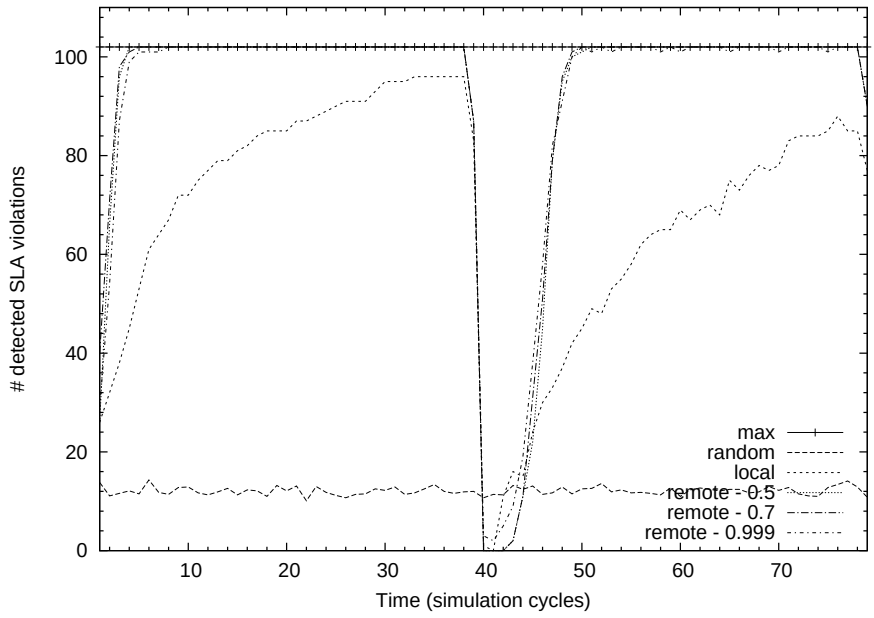
these figures, we present the mean raw number and cumulative percentage of detected SLA violations as a function of simulation cycles. The performance of measurement session activation strategies is depicted in the following curves: random strategy ("random"), local strategy ("local"), and local and remote strategy using the Student's t-test and the following values of confidence as minimum correlation score: 0.5, 0.7, and 0.999 ("remote - 0.5", "remote - 0.7", and "remote - 0.999"). Results for the random strategy and the local strategy are depicted as baselines. Besides the curves for the proposed strategies, we also present the maximum number of SLA violations that can be detected ("max") considering the number of sessions that can be activated by each node and the total number of nodes that can deploy sessions (leaf nodes). As we primarily focus upon the local resource constraint (β = 3), we do not consider α for this experiment.

The experiment shows that the proposed strategies behave as expected, without stability and convergence problems. As can be seen in Figure 6.4(a), 6.5(a), and 6.6(a), the utilization of both local and remote information on measurement session activation decisions increases significantly the raw number of detected SLA violations in the experimental scenario. Clearly, even the unique utilization of local information (which can be view also as a baseline for the P2P strategies) has a better performance than the random placement. It can be also noted the fluctuation after achieving the steady state area. This fluctuation is due to the effect of the utilization of the time of the last measurement for a given destination as an input for destination rank. Despite the fact that this utilization slightly decreases the number of the SLA violations for this scenario, it ensures that no destination remains without measurement sessions for a long time.

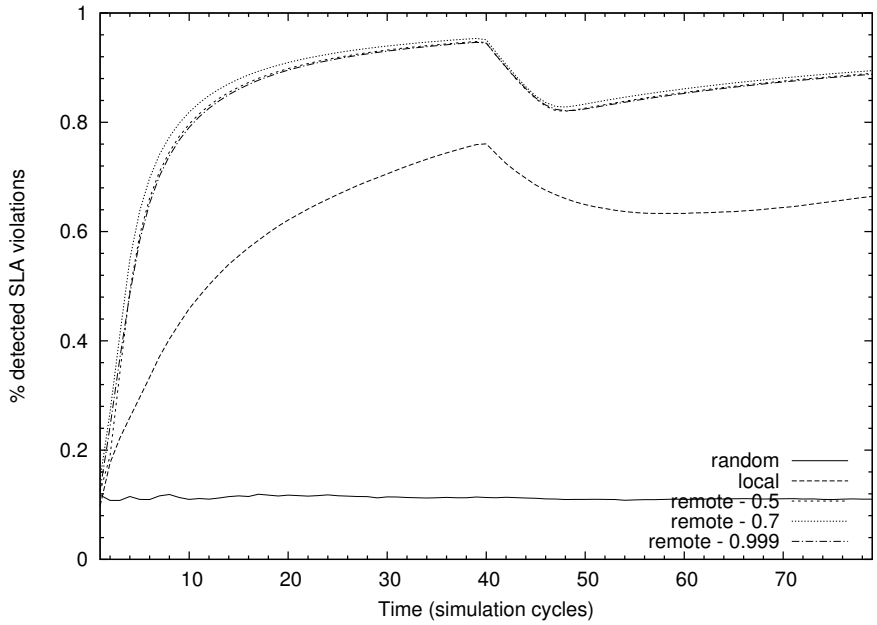
The measurement session activation strategies almost approach the maximum number of detected SLA violation for the resource constraints when using local and remote strategy. The cumulative results show that this strategy can accurately match up to 95% SLA violations to the available measurement sessions considering the described scenario. The depression seen around 40 cycles is expected, since there is no immediate feedback for the destination rank and it represents the cycles needed for adaptation. Besides that, an additional feature of the use of the destination rank (even for the random strategy) is that it is avoided the activation of multiple sessions for the same destination by individual devices.

The adaptation features of measurement session activation strategies can be impacted by the hysteresis related by the use of historical measurement data. Therefore, we perform a longer run of the scenario employed in the first experiment (one-way delay in-

Figure 6.4: Number of Detected SLA Violations for Hot-like B Topology.



(a) Raw Number of Detections



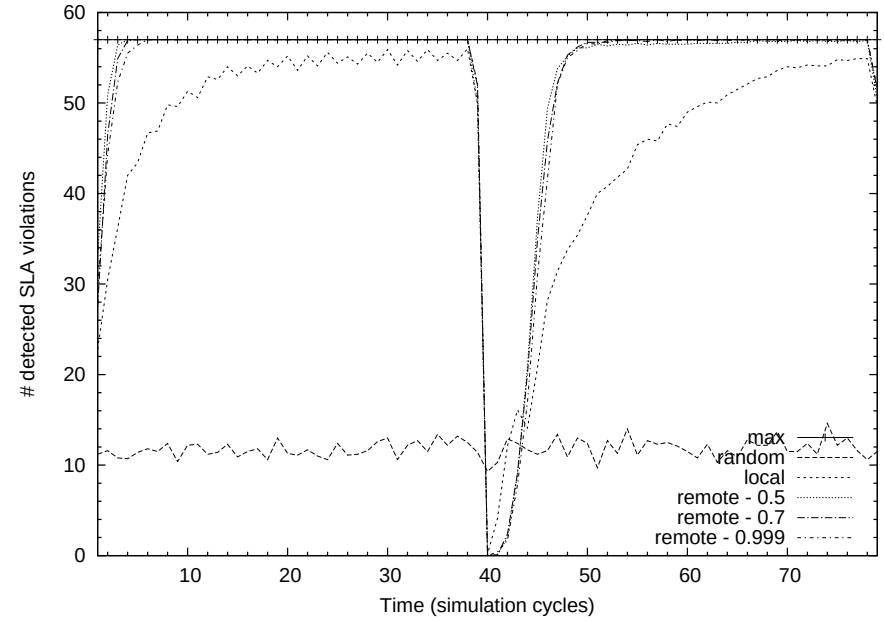
(b) Cumulative Percentage of Detections

Source: by author (2015).

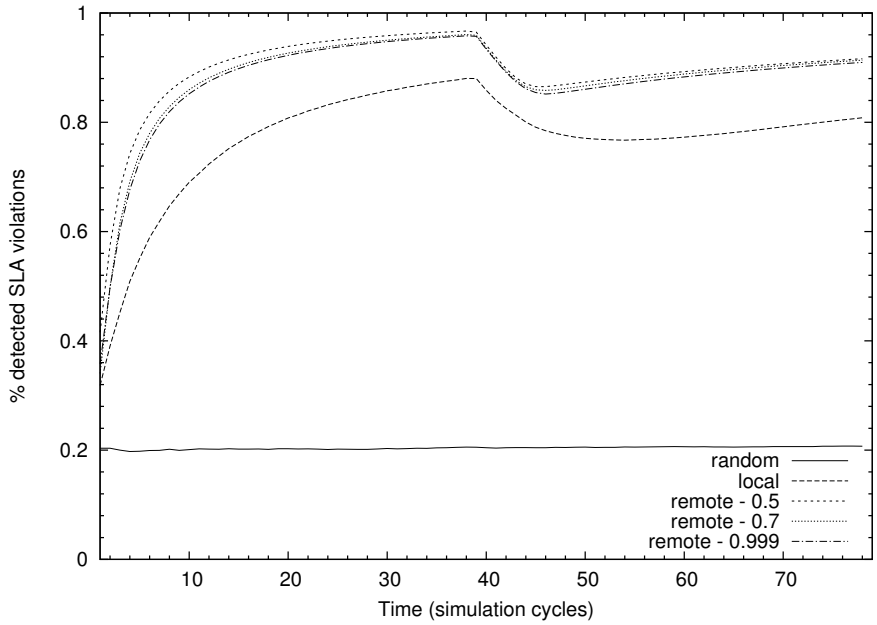
creased on 4 access links for 40 cycles, then change for other 4 access links for 40 cycles), but repeat the change for another 2 times. Besides that, the violating links were chosen randomly. We show on Figure 6.6 mean results, considering the Hot-like A topology.

The execution of multiple changes highlight hysteresis effects on the execution of

Figure 6.5: Number of Detected SLA Violations for Rocket-derived A Topology.



(a) Raw Number of Detections

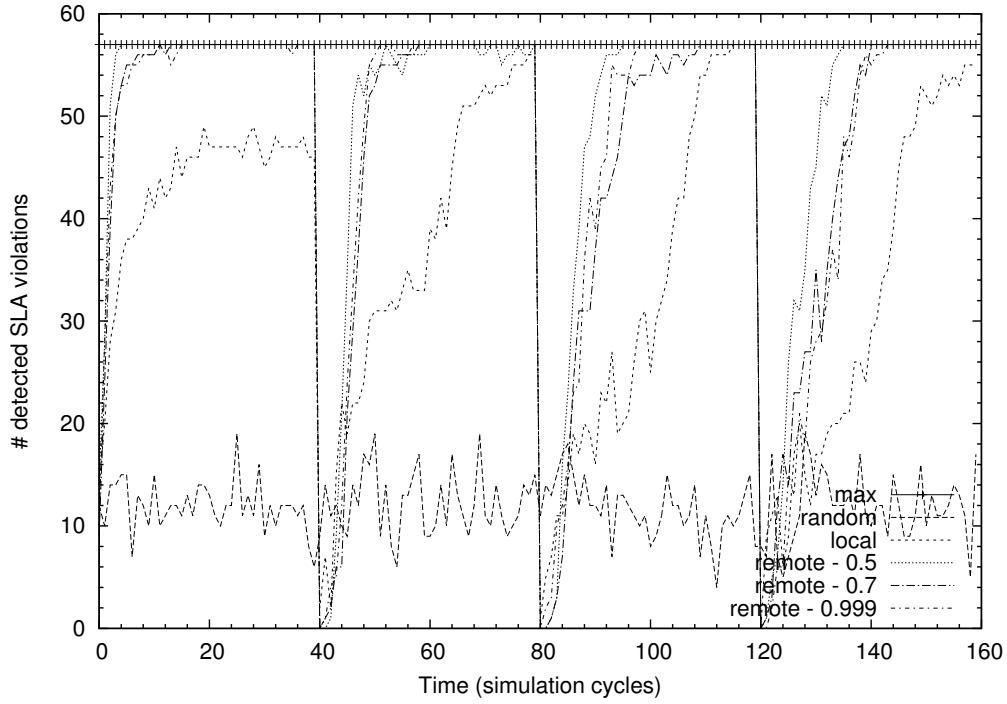


(b) Cumulative Percentage of Detections

Source: by author (2015).

the measurement session activation strategies. However, the adaptation features remain in place as well as the advantage of local and remote strategy over the local strategy. In this context, the local and remote strategy approaches the maximum number of SLA violations that can be detected without using virtual measurement sessions (*i.e.*, every

Figure 6.6: Number of Detected SLA Violations for Hot-like A Topology.



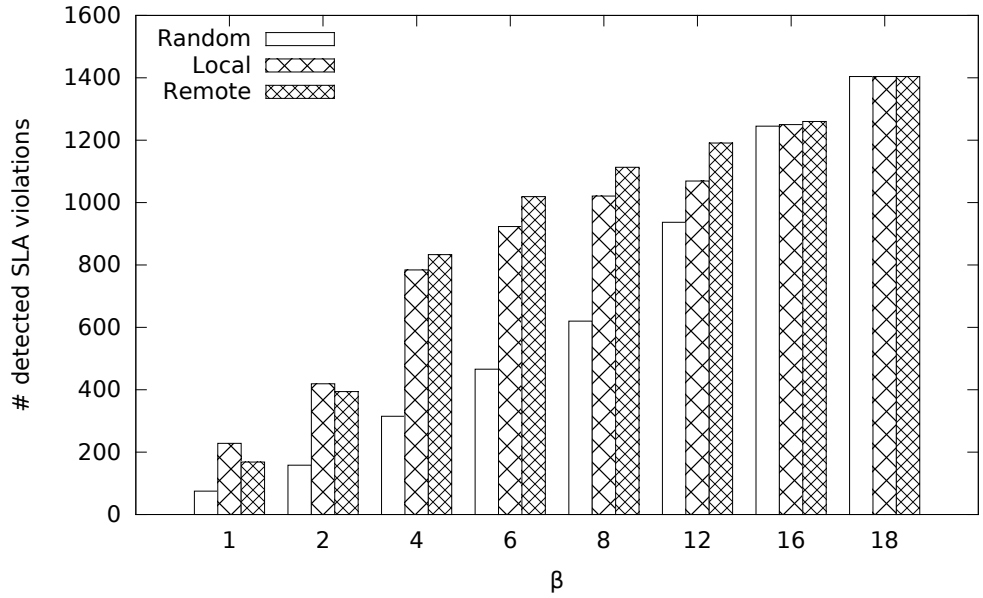
Source: by author (2015).

activated session detects a SLA violation per cycle). As a side note, the random strategy maintains the same performance, as expected. It is important to state that the hysteresis effects are impacted by the sliding window size employed to collect past service level measurement results.

In the second experiment, we aim at evaluating the number of detected SLA violation as a function of the number of activated measurement sessions (β), considering the proposed measurement session activation strategies. In this experiment, we use the same delay function from the previous experiments (one-way delay increased on 4 access links for 40 cycles, then change for other 4 access links for 40 cycles), however the number of detected SLA violation is now consolidated for each experiment. We show on Figures 6.7 and 6.8 mean results, considering the Rocket-derived A and Internet2 PoP level topologies (respectively). The β values were chosen to permit that the proposed approaches be evaluated according to different available resources, from 1 to the number of possible end-to-end destinations in the selected topologies.

The experiment shows how efficiently the proposed measurement session activation strategies use the available resources. As can be seen from the results in Figure 6.7 and 6.8, more available resource (higher β values) evidently lead to a higher number of detected SLA violations for all approaches. However, the proposed measurement session activation decisions strategies perform significantly better than the random strategy for

Figure 6.7: Consolidated Number of Detected SLA Violations for Rocket-derived A Topology.

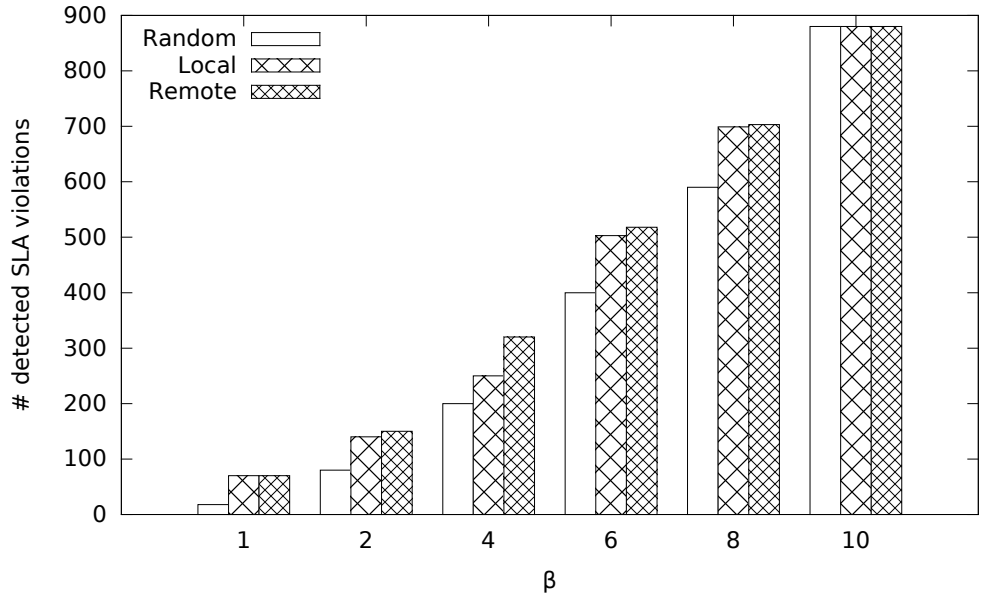


Source: by author (2015).

most values of the β range. In fact, excluding the situation where the available resource are sufficient to probe all possible destinations (β = 18) and obviously all approaches have the same performance, the use of past measurement results leads to a smarter employment of resources and, consequently, a higher number of detected SLA violations. Besides that, it is possible to note that the use of both local node and remote information even improves the detection of SLA violations. Finally, in terms of a comparison of both figures, the SLA monitoring space is smaller in Internet2 PoP level, thus, the gain from better measurement activation decision is decreased.

In the third experiment, we aim at evaluating time elapsed from the last performed measurement for the different destinations in the network. In this experiment, we use the same delay function from the previous experiments (one-way delay increased on 4 access links for 40 cycles, then change for other 4 access links for 40 cycles). We chose β = 3 in order to have a slightly lower potential number of detection than the injected violations. Considering the proposed measurement session activation strategies, the local and remote strategy is the worst case for the evaluation of time elapsed from the last measurement. This is because the destination rank in such strategy considers 3 score components for the destination score: local measurement results, remote measurement results, and the time elapsed from the last measurement. Thus, each component responds to a third of the total score (without using different weights). In Figures 6.9 and 6.10, we present the frequencies of normalized score component for time elapsed from the last measurement

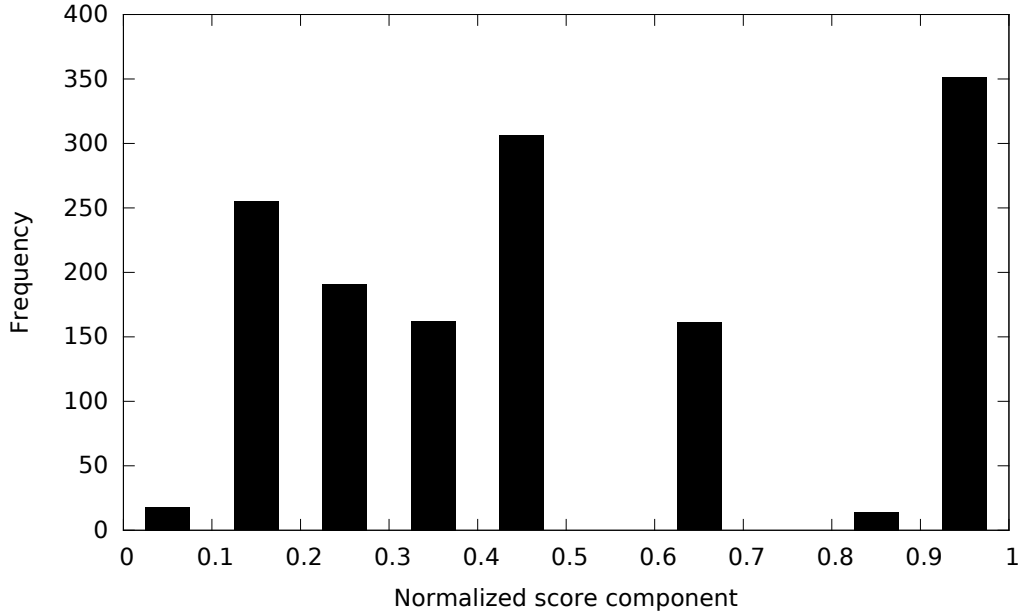
Figure 6.8: Consolidated Number of Detected SLA Violations for Internet2 PoP level Topology.



Source: by author (2015).

considering Hot-A and Hot-B topologies.

Figure 6.9: Normalized Score Component of the Time Elapsed from the Last Measurement for Local and Remote Session Activation Strategy on Hot-A Topology.

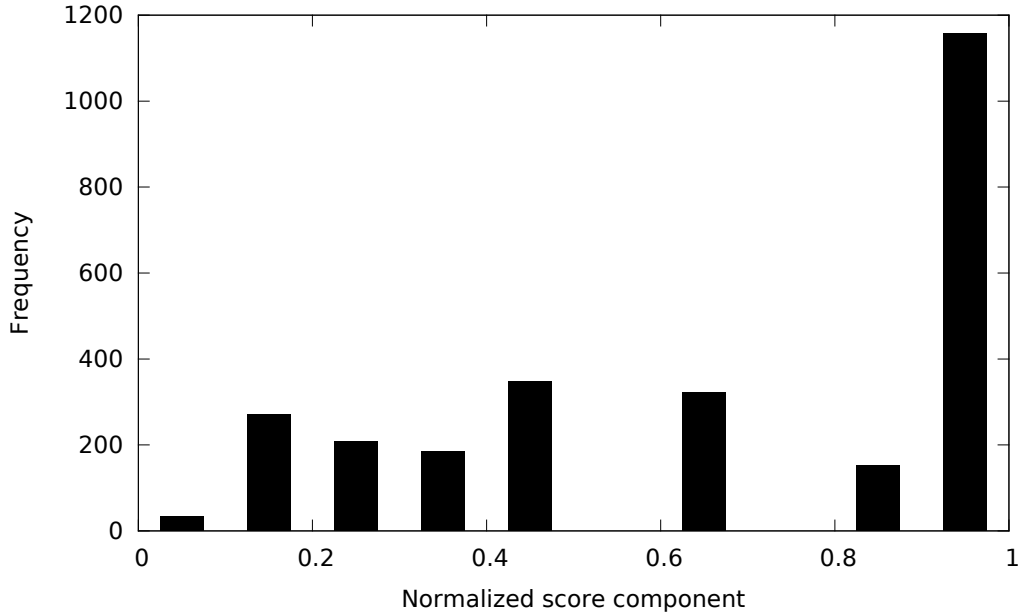


Source: by author (2015).

The experiment shows that there are significant differences between the results for topologies Hot-A and Hot-B. Since the results are normalized values, ranging from 0 to 1, the maximum value presented is 1. Besides that, lower values represent less time elapsed from the last measurement, *i.e.*, the activation of measurement sessions is more frequent.

As can be seen from the results in Figure 6.9 and 6.10, the frequency of lower values is higher on the Hot-A topology. This is due the difference between the number of leaf nodes of the selected topologies. Such difference impacts on the monitoring space which has to be explored by the measurement sessions.

Figure 6.10: Normalized Score Component of the Time Elapsed from the Last Measurement for Local and Remote Session Activation Strategy on Hot-B Topology.



Source: by author (2015).

It is important to note that the weight of the score component related to the time elapsed from the last measurement could be manually tunned by a network administrator. This can be done to prioritize frequent probing on each individual destination instead of the detection of SLA violations. However, since we aim at the number of detected SLA violations and adaptivity in this research, we did not performed experiments specially designed to investigate the frequency of destination probing.

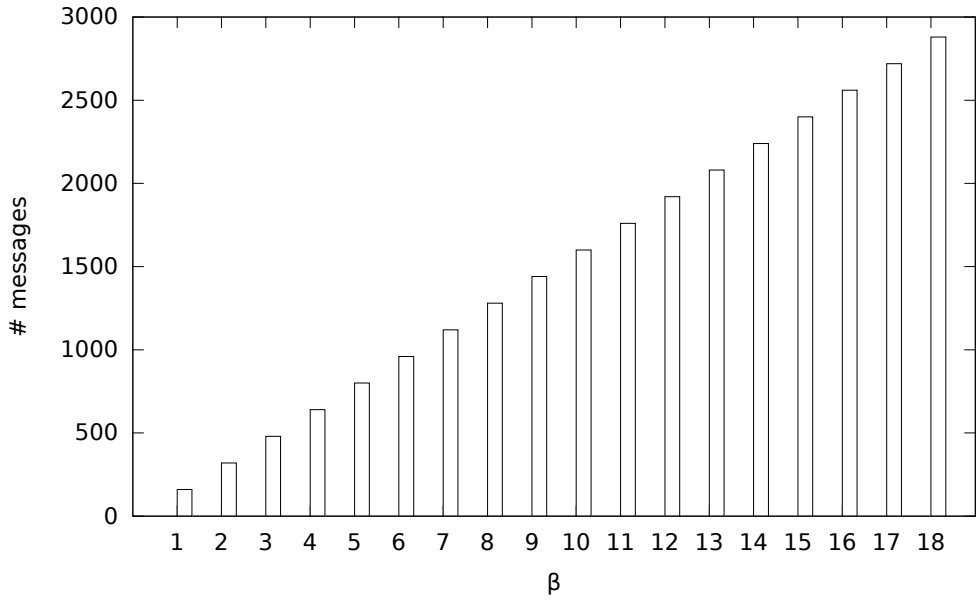
6.3.2 Analysis of the Number of Exchanged Messages for the Detection of SLA Violations and the Operation of the P2P Measurement Overlay

We performed some experiments in order to analyze the number of exchanged messages for the detection of SLA violations and the operation of the P2P measurement overlay. This number is an indicative of the consumed network resources and, therefore, the efficiency of the SLA monitoring. In this section, we were just considering the active

measurement sessions *per se* and the control of their activation by the P2P measurement overlay. Thus, the virtual strategy is excluded.

The first experiment shows the number of messages exchanged by the implemented active measurement mechanism. These messages are used to derive the end-to-end service level metrics and, consequently, the SLA monitoring. In Figure 6.11, we present the number of exchanged messages as a function of the number of activated measurement sessions (β). We consolidate the messages considering a period of 80 cycles.

Figure 6.11: Consolidated Number of Messages Exchanged for the Execution of Measurement Sessions.



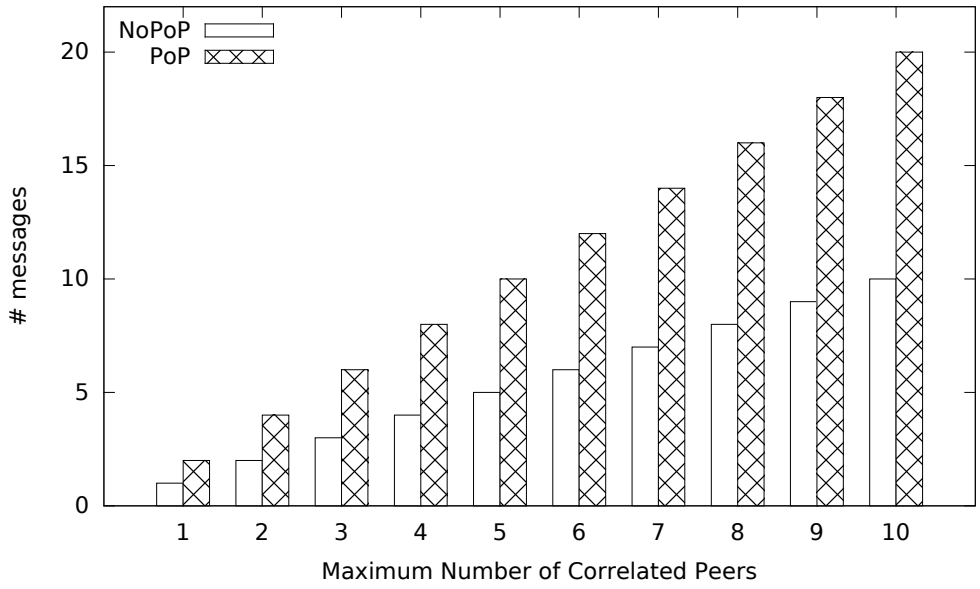
Source: by author (2015).

As can be seen from the results in Figure 6.11, the analysis of number of the exchanged messages for the execution of measurement sessions is trivial. These are the expected results excluding the situations that lead to packet loss, such as re-routing events and link failures. However, the activation of measurement sessions does not always lead to the detection of SLA violations, *i.e.*, measurement sessions towards non-problematic destinations. In addition, a static activation of measurement sessions cannot follow variations in network dynamics, which can also lead to an inefficient probing. In fact, these results strengthens the need for a network-wide control of the activation of measurement sessions.

The second experiment is an analysis focused on the maximum number of messages to enable the P2P measurement overlay. These messages carry measurement results which are used to define such overlay as well as to ensure that remote results have local significance (regarding the concept of correlated peers). In Figure 6.12, we present the

number of the exchanged messages as a function of the maximum number of correlated peers considered per iteration of the peer topology phase. Such phase is found on the local and remote strategy and the virtual strategy. The results are depicted in the following curves: without the use of “peers of peers” (“NoPoP”) and with the use of “peers of peers” (“PoP”).

Figure 6.12: Maximum Number of Messages to Enable the P2P Measurement Overlay.



Source: by author (2015).

The results depicted in Figure 6.12 represent the worst case situation in terms of messages required to enable the P2P measurement overlay. As can be seen from the results, the number of messages is directly related to the maximum number of correlated peers. Besides that, the number of messages doubles when “peers of peers” are being advertised. Thus, the overlay-related traffic must be considered in order to maintain the P2P measurement overlay. In this context, the local vision of the P2P measurement overlay is represented by the number of correlated peers a device has in a given time.

Some measures can be taken in order to avoid scalability issues regarding the maintenance of the P2P measurement overlay. First, the maximum number of peers in a given moment is controlled by a constraint. Besides that, it is also possible to control the candidates for each iteration, which can also decrease the number of transmitted messages. In addition, the peer topology phase does not to be executed in the same scheduled as the activation of measurement sessions. In this context, less frequent scheduling reduces the number of transmitted messages. Finally, the “peers of peers” information can be included in the measurement results messages, which would decrease the number of messages in spite of an increase in the individual message size.

6.3.3 The Influence of Virtual Measurement Sessions on the Detection of SLA Violations

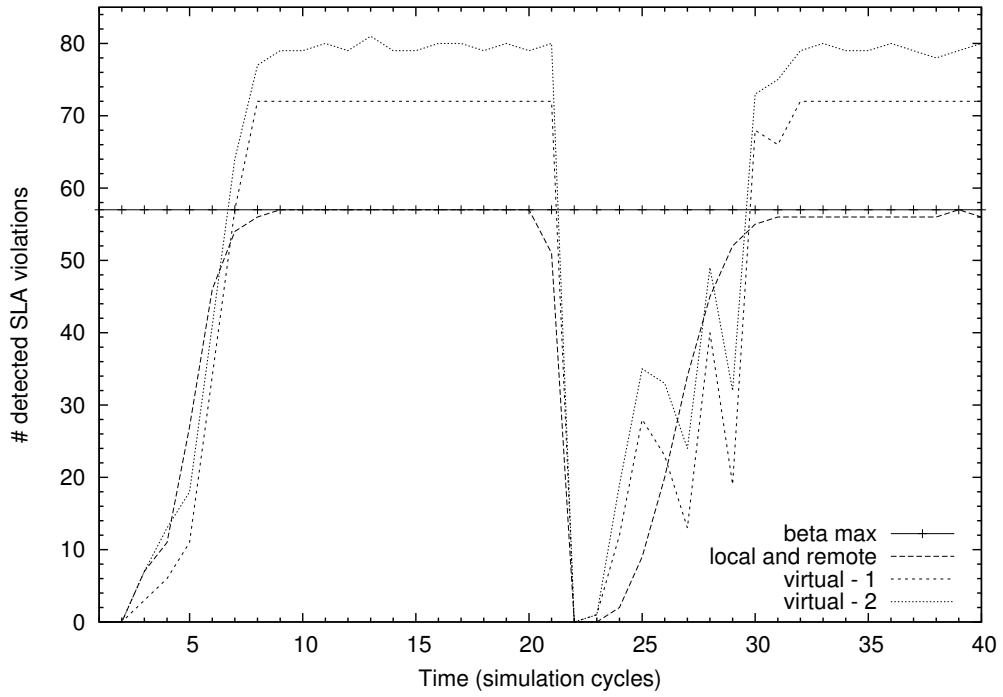
We performed some experiments in order to assess the influence of virtual measurement sessions on the detection of SLA violations. In theory, virtual measurement sessions allow the number of detected SLA violations to be higher than the number of locally available measurement sessions. Thus, the virtual strategy could decrease the local resources necessary to monitor destinations, thus improving the scalability of the SLA monitoring process. Besides that, the use of virtual measurement sessions could be also used to increase SLA monitoring coverage.

In the first experiment, we aim at determining whether such measurements can increase the number of detected SLA violations over the maximum detections made by local measurements. In order to accomplish that, we collected the total number of SLA violations detected by nodes regarding a specific network environment scenario. In this scenario, we increased the one-way delay on 4 access links for 20 cycles, then we changed for other 4 links for the same amount of cycles. This increase makes the end-to-end destinations that traverse the changed links to appear as SLA violators for the simulated active measurement mechanism. We chose the number of cycles in which the experimental scenario is changed in order to permit that the proposed approaches go through their steady state.

The results for the first experiment are shown on Figures 6.13 and 6.14, considering the Rocket-derived A and "4-post" DC topologies (respectively). The performance of virtual strategy is depicted in respect to the maximum number of virtual measurement sessions (γ) with the following values: 1 ("virtual - 1") and 2 ("virtual - 2"), as a function of simulation cycles. Results for the local and remote strategy ("local and remote") are depicted as baselines and the number of locally activated measurement sessions (β) is equal to 3. Besides that, we also present the maximum number of SLA violations that can be detected by local measurement sessions ("beta max"), *i.e.*, every activated session detects a SLA violation per cycle.

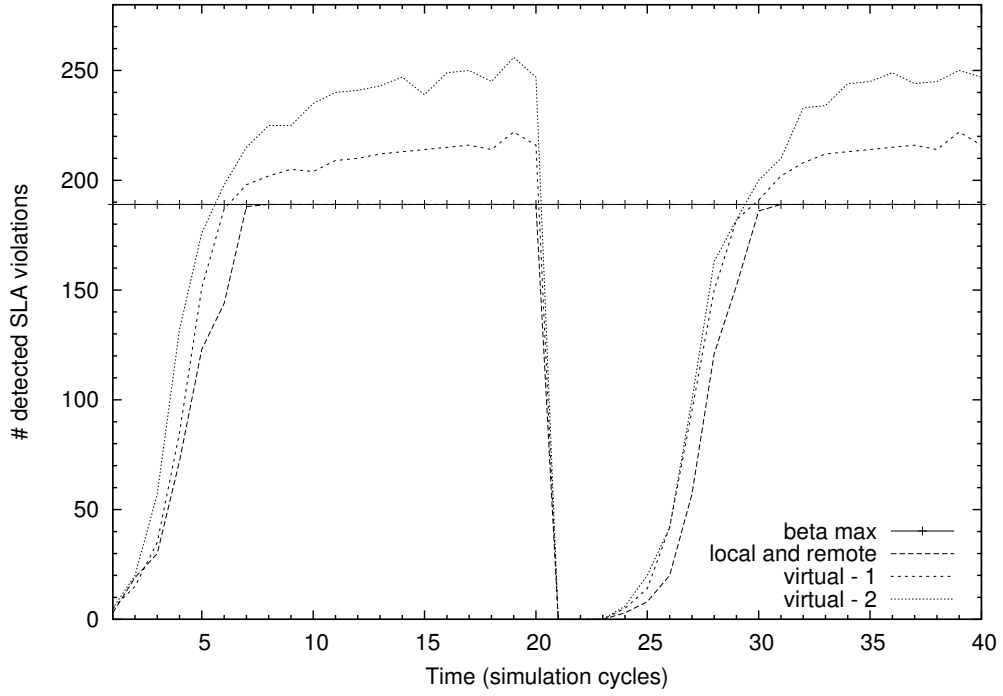
The experiment shows that the virtual strategy behaves as expected, without stability and convergence problems. As can be seen in Figures 6.13 and 6.14, the utilization of virtual measurement sessions can increase significantly the number of detected SLA violations in the experimental scenario. Clearly, even the employment of just 1 virtual measurement is positive since it enables overcoming the constraint on the use of local

Figure 6.13: Number of Detected SLA Violations Considering Virtual Measurement Sessions for Rocket-derived A Topology.



Source: by author (2015).

Figure 6.14: Number of Detected SLA Violations Considering Virtual Measurement Sessions for “4-post” Data Center Topology.



Source: by author (2015).

resources (β). It can be also noted the fluctuation after achieving the steady state area on both figures. This fluctuation is due to the effect of the utilization of the time of the last measurement for a given destination as an input for destination rank. Regarding the "4-post" DC topology (Figure 6.14), it is also possible to note the slower adaptivity, comparing to the Rocket-derived topology. On the other hand, the "4-post" DC topology shows smoother adaptivity features than the Rocket-derived A topology, which can be noticed in the transient state of the figures.

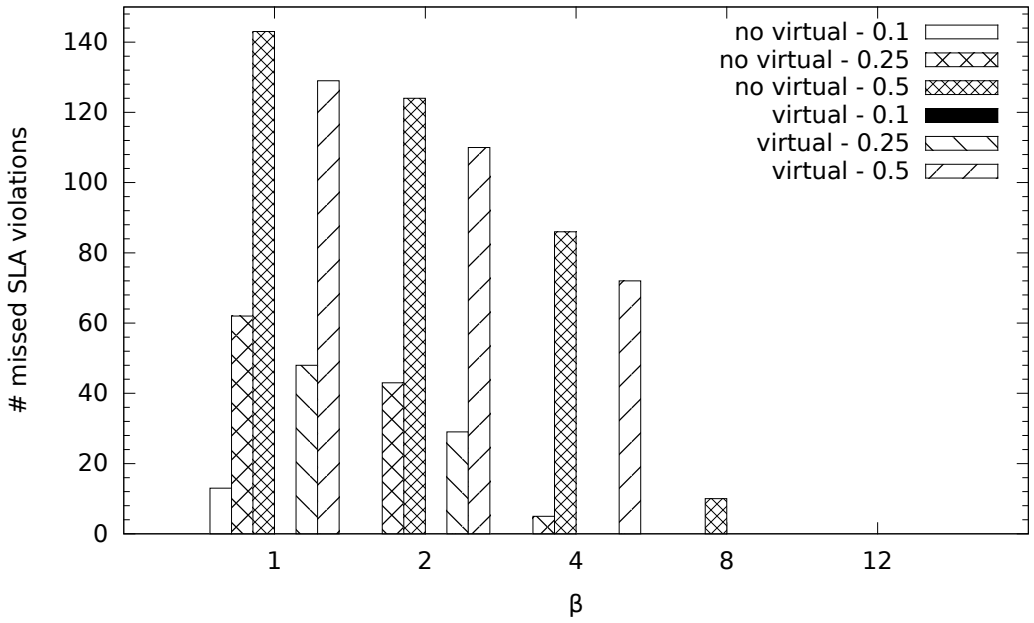
In the second experiment, we aim at analyzing the potential number of missed SLA violations as a function of the number of locally activated measurement sessions (β) and the number of virtual measurement sessions (γ). This analysis dose not take int account the partition of the detection of SLA violations in those performed by virtual and non-virtual sessions. Instead, the focus is at the SLA monitoring coverage per iteration, specially regarding the monitoring space which is not covered (*i.e.*, probed). This space is important because it can lead to undetected violations.

In order to accomplish the evaluation of the potential number of missed SLA violations, we compared the number of locally detected SLA violation by nodes regarding a specific network environment scenario. In this scenario, we increased the one-way delay in such scenario using 3 different percentages on access links: 10%, 25%, and 50% (considering the local device view). This increase makes the end-to-end destinations that traverse the changed links to appear as SLA violators for the simulated active measurement mechanism. We chose these percentages in order to simulate distinct network conditions.

The results for the second experiment are shown on Figures 6.15 and 6.16, considering the Rocket-derived A and Rede Ipê PoP level topologies. The curves depicted on these figures represent the potentially missed SLA violations as a function of the number of activated measurement sessions (β), considering either the use of virtual (γ = 1) and local measurements sessions ("virtual - 0.1" for 10%, "virtual - 0.25" for 25%, "virtual - 0.5" for 50%) or only the use of local measurement sessions ("no virtual - 0.1" for 10%, "no virtual - 0.25" for 25%, "no virtual - 0.5" for 50%). These curves present the consolidated performance on steady state. The β values were chosen to permit that the proposed approaches be evaluated according to different available resources, from 1 to 12. After that, the results remain the same, *i.e.*, there are not missed SLA violations.

As can be seen in Figures 6.15 and 6.16, the utilization of the virtual strategy decreases the number of missed SLA violations in the experimental setup (less is better on these figures). It is possible to realize that the utilization of solely 1 virtual measurement improves the SLA detection performance. Since the protocol to contract virtual mea-

Figure 6.15: Number of Potentially Missed SLA Violations for Rocket-derived A Topology.



Source: by author (2015).

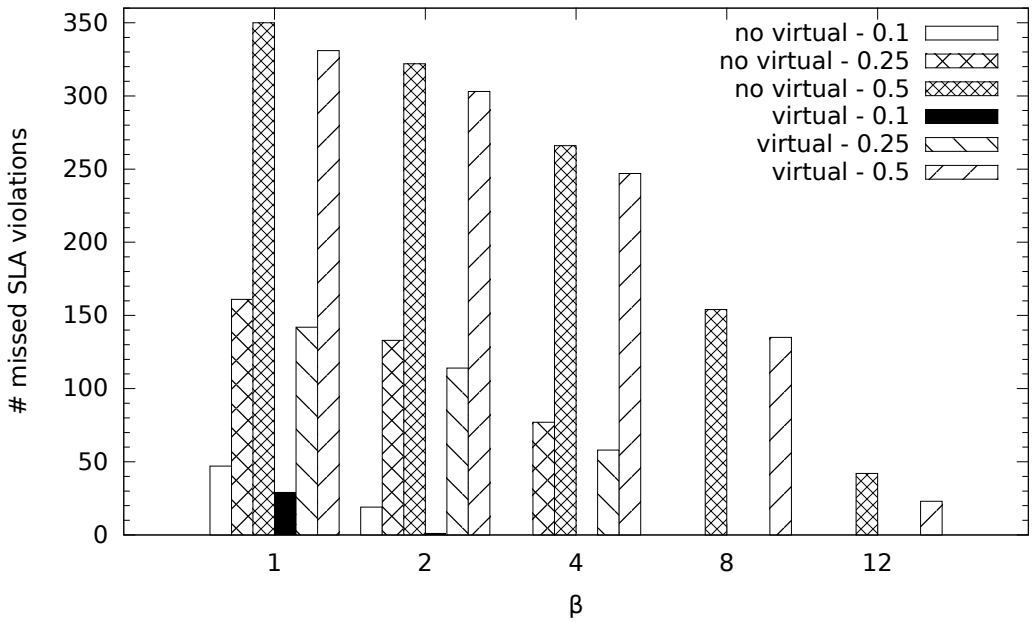
surement (as described in Section 4.3) is simple, it is safe to consider that the trade-off between the contract overhead (*i.e.*, messages exchanged between correlated peers) and the performance improvement is positive.

6.3.4 Analysis of the Number of Exchanged Messages for the Virtual Measurement Sessions

We performed some experiments in order to analyze the number of exchanged messages for the execution of virtual measurement sessions. This number is an indicative of the consumed network resources in such sessions and, therefore, the efficiency of the virtual strategy. In this section, the emphasis in on the comparison of the number of messages due to activated measurement sessions, the P2P measurement overlay, and the virtual measurement sessions.

The first experiment is a comparative analysis of the number of messages exchanged in the virtual strategy. These messages are used to derive (active sessions) and infer (virtual sessions) the end-to-end service level metrics. Thus, there is an increase in the SLA monitoring coverage in respect to local and remote strategy. Thus, the number

Figure 6.16: Number of Potentially Missed SLA Violations for Rede Ipê PoP level Topology.



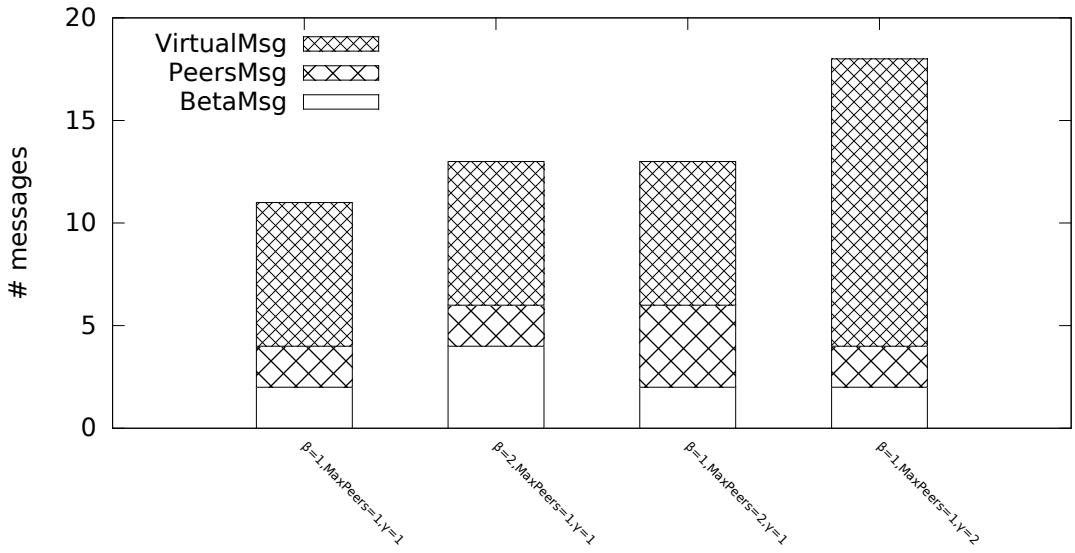
Source: by author (2015).

of messages considered are the ones exchanged by the implemented active measurement mechanism, to enable the P2P measurement overlay, and for virtual measurement sessions. In Figure 6.17, we present the number of exchanged messages regarding 4 defined scenarios.

The results in Figure 6.17 employed scenarios defined which distinguish the number of activated measurement sessions (β), the number of correlated peers ($MaxPeers$), and the number of virtual measurement sessions (γ). The bars $BetaMsg$, $PeersMsg$, and $VirtualMesg$ represent the resulting exchanged messages, respectively. First, all these numbers are set to 1, then each number is increased to 2 in order to produce scenarios that distinctly describe impacts on the number of exchanged messages. The scenarios depict the start-up state of the sessions and the P2P measurement overlay.

As can be seen from such results in 6.17, the analysis of the exchanged messages shows that the impact of virtual measurement sessions is important considering the employed scenarios. These are the expected results for the start-up state of such sessions since there is an inherent overhead to contract and finish the sessions (coordination establishment and termination), both considered in the results. In this context, this overhead is also what enables the decentralized fashion of the proposed virtual measurement sessions. In fact, these results strengthens the need for high minimum correlation scores for virtual measurement sessions to assure the relevancy of such sessions. Besides that, the

Figure 6.17: Number of Exchanged Messages Considering Virtual Measurement Sessions.



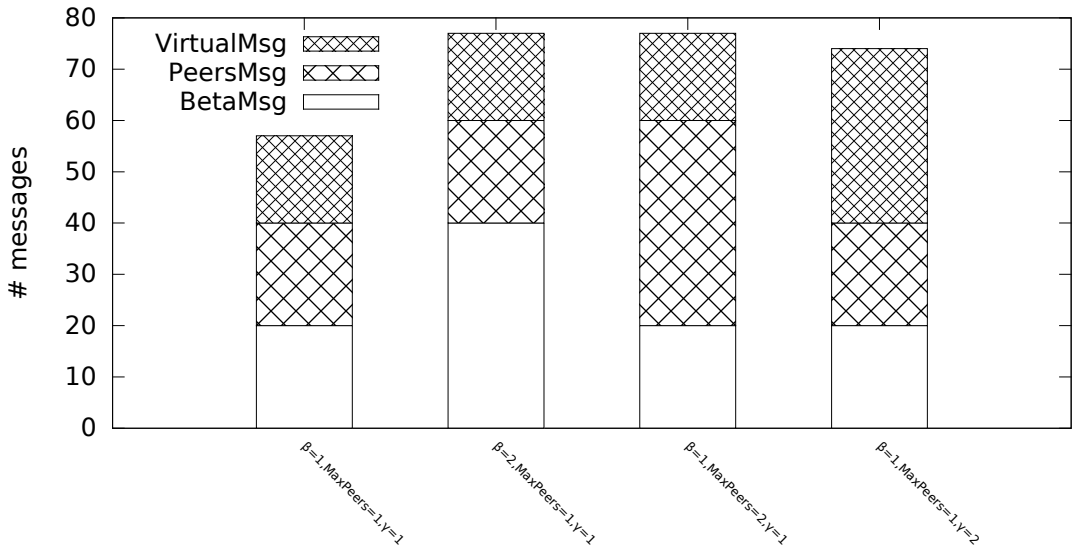
Source: by author (2015).

maximum number of virtual measurement sessions in a given moment is controlled by a constraint (γ). Finally, the results do not picture the steady sate which is achieved after the start-up and dilutes the impact of coordination establishment and termination.

The second experiment is an analysis focused on the consolidated number of exchanged messages in virtual strategy. This consolidation considered messages in a period of 10 cycles. This is done in order to depict the steady state of virtual measurement sessions and also to highlight the attenuation of the impact of the start-up of such sessions. We employed the same 4 scenarios from the first experiment. The results in terms of the transmitted messages are presented in Figure 6.18.

The results of Figure 6.18 presented a more balanced contribution of the causes for the exchanged messages in comparison to those depicted in Figure 6.17. As can be seen from these results, the number of messages due to virtual measurement sessions has a diminished impact when considering 10 cycles. This is because, while activated measurement sessions and overlay-related message traffic is constant, the only messages of virtual measurement sessions that remain being transmitted are those related to measurement exchange. In this context, less frequent start-ups reduce the number of overhead messages and we can expect a further attenuation for longer periods of observation.

Figure 6.18: Consolidated Number of Messages Considering Virtual Measurement Sessions.



Source: by author (2015).

6.4 Final Remarks

The goal of the evaluation described in the present chapter is to investigate the properties exposed by the proposed use of P2P technology to enable a network-wide control of the activation of active measurement sessions. In this context, the principles described to guide such use (described in Chapter 4) as well as the measurement session activation strategies (described in Chapter 5) must be evaluated. Simulation experiments were employed to perform the evaluation in the present thesis.

The destination rank and the measurement session decision strategies were implemented in an event-driven P2P simulator in order to perform simulation experiments. In addition, modifications were implemented in this simulator to support the establishment of a P2P measurement overlay using correlated peers. Besides that, an active measurement mechanism which can monitor Service Level Objectives (SLOs) was implemented. Finally, an event parser was implemented to ease the results processing of simulation experiments.

Several topologies were used to perform the evaluation using the implementation. Since static scenarios are easier to adapt, changes in network dynamics were instrumented in these topologies. Such changes simulate network conditions found on real network environments. The deployment of an infrastructure of active measurement probes in the

selected topologies was depicted. The characteristics found in this infrastructure enable the execution of simulation experiments tailored for the evaluation of the use of P2P technology for the network-wide control of the activation of active measurement sessions.

The goal of network devices in our proposed solution is to improve the network-wide detection of SLA violations in terms of the number of detected violations and the adaptivity to changes in network conditions. The simulation experiments performed in the present chapter show positive results considering these terms. Despite that, it is necessary to confront the results collected in the experiments with the research questions (as described in Chapter 1) proposed in this thesis. This can highlight some properties of the experimental results.

7 FINAL REMARKS

Critical networked services established between service provider and customer are expected to operate respecting Service Level Agreements (SLAs). Likewise, the communication requirements of such services have become increasingly accurate. In this context, active measurement mechanisms are the prime choice for SLA monitoring. However, these mechanisms are expensive in terms of resource consumption and also increase the network load because of the injected traffic. Thus, monitoring all destinations in a large and complex network infrastructure is usually too costly. Furthermore, if the number of SLA violation in a given time is higher than the number of available measurement sessions, certainly some SLA violations will be missed.

Human administrators employ different strategies to improve the SLA coverage of a network infrastructure. As described in Chapter 1, there is an inherent trade-off between attempting to maximize SLA coverage over destinations and minimizing the resource consumption due to the deployment of active measurement sessions. The current best practice, the observation of just a subset of destinations driven by human administrators' expertise, is error prone, does not scale well, and is ineffective on dynamic network conditions. This can lead to SLA violations being missed, which invariably affects the performance of critical networked services and usually incurs in costly penalties. In this context, solutions to help network human administrators in SLA monitoring are a must have.

In this concluding chapter, we summarize in Section 7.1 the main findings provided in this thesis along with a discussion of their implications. Next, in Section 7.2 we present some possible future work based on these findings and the provided contributions.

7.1 Summary of Contributions

The goal of the present thesis (as described in Chapter 1) is to investigate the decentralized detection of SLA violations using active measurement mechanisms to propose an approach to improve such detection. To accomplish this, we defined a Fundamental Research Question (and a Research Hypothesis) as well as additional Research Questions. In this section, we employ these questions to highlight properties of the experimental results.

The Fundamental Research Question focuses on how to improve the network-

wide detection of SLA violations in terms of the number of detected violations and the adaptivity to changes in network conditions. The relevance of the Fundamental Research Question is related to the effect of undetected SLA violations and the computational cost of active measurement mechanisms on network devices. We hypothesized that employing P2P technology it is possible to improve the network-wide detection of SLA violations (considering such terms) through an autonomically steering of active measurement mechanisms. The hypothesis was defined considering the investigation of several initiatives regarding P2P-Based Network Management (P2PBNM) and network-wide control for active measurement mechanisms.

The main focus of the simulation experiments is to evaluate the Fundamental Research Question and the Fundamental Hypothesis. Considering the employed experimental setup and the performed simulation experiments, the Fundamental Hypothesis is confirmed. Thus, the detection of SLA violations can be improved through the use of Peer-to-Peer (P2P) technology to steer autonomically the activation of active measurement mechanisms. According to the proposed solution (described in Chapter 5), the concept of destination score as a label for the prioritization of destinations and the concept of destination rank as an approach to autonomically prioritize destinations can improve the number of detected violations and the adaptivity to changes in network conditions.

The results obtained from the performed experiments in Section 6.3 can be seen as an holistic evaluation of the proposed P2P concepts and algorithms. Since our Fundamental Hypothesis highlights an autonomic steering of the activation of active measurement sessions, an increase in the adaptability of session activation is expected. This adaptability can be seen in the experiments as faster reactions to changes in management scenarios. Obviously, static scenarios are easier to adapt, thus, a major concern was how would be the system response to highly dynamic changes. The experiments showed that detection rate of SLA violations quickly converges considering the employed scenario. In the "wild", it is usually infeasible to know how many SLA violations are missed (*i.e.*, not detected) in a given situation, but our experiments allowed to infer that the proposed strategies work better than a non-adaptive approaches (represented by the random strategy on the experiments).

In Research Question 1, we focused in aspects of the employment of P2P technology on the network-wide detection of SLA violations. Since the number of detected violations and adaptivity are already emphasized in the Fundamental Question, other aspects can be highlighted. The distributed approach for the activation decision of measure-

ment sessions, enabled by P2P technology, has several advantages over a centralized one. For example, the load of activation decision functions is shared through P2P execution through the use of local logic and data by the network devices themselves. Besides that, there are not critical nodes to the system operation. Finally, in the context of the control of measurement mechanisms, it is usually necessary a local access to the API of such mechanisms. This also impairs the adoption of other approaches, such as hierarchical ones.

The results obtained from the performed experiments illustrated some properties of the proposed measurement session activation strategies. Even the solely use of past measurement results and the observation of resources constraints (*i.e.*, local strategy) lead to better results than the random activation. As more information from the network is used, the measurement session activation decisions capture better the network dynamics. Besides that, it is also possible to say that the available resources are used more efficiently since the deployed measurement sessions have a better chance to detect existing SLA violations.

The Research Question 2 explored the characteristics of the use of P2P technology in network management that could be successfully deployed on the steering of active measurement mechanisms. P2PBNM inherits properties from general use of P2P technology and combine them with Distributed Network Management (DNM). Peers in the proposed strategies implement both client and server functionality and do not require additional configuration to maintain the system after peers introduction. Besides that, the P2P measurement overlay can be used to exchange management information among network devices.

The experiments performed in Section 6.3 showed that proposed measurement session activation strategies (depicted in Chapter 5) are resilient to changes in network conditions, at least considering the experimental scenario. Specially considering the local and remote strategy and the virtual strategy, it is possible to save devices resources through an efficient activation of measurement sessions. In these strategies, there is a dynamic federation of network devices to steer the activation of active measurement probes using P2P principles. This federation can improve the detection of SLA violations.

In Research Question 3, the impacts on using P2P technology to control active measurement mechanisms are discussed. For example, a P2P approach for such a control must also take into considerations the resources necessary to implement itself. P2PBNM has its additional usually associated with, such the minimal traffic generated to maintain

the P2P measurement overlay. Since this computational resources can be used for primary network functions (*e.g.*, routing and switching), it is important to assure that they support an efficient activation of active measurement sessions. This leads to an increase of the benefits of the SLA monitoring infrastructure.

The performed experiments (described in Section 6.3) showed positive results considering the adaptivity of the proposed measurement session activation strategies. Anyway, there were fluctuations in some setups after changes in network conditions. This happened because the algorithms aim at frequent measurements in each destination, even if its measurement results are not close to violate SLAs. Even so, such algorithms do not by themselves guarantee that, during a given probing interval, destinations are covered at most once. Finally, the number of exchanged messages for the bootstrapping and maintenance of the P2P measurement overlay is not negligible. Thus, measures should be taken by human administrators to keep a reasonable number of such messages.

The Research Question 4 was proposed to investigate how to decide whether different nodes are management peers. Some characteristics of network devices can be used to identify which devices have similar features, such as service level performance given a specific destination. Results produced by active measurement mechanisms are an indicator of this performance, thus each device can compare its own results with remote ones in order to look for similarities. We introduced the concept of correlation peers as the binding of two network devices which have similar (*i.e.*, correlated) active measurement results. Correlation peers enable an autonomic and "organic" provisioning of a P2P measurement overlay for the exchange of relevant active measurement results and present better scalability features in terms of configuration needs.

The experiments performed in Section 6.3 show that the use of correlated peers assures that the received remote information is locally applicable. Besides that, the correlation scores can be used to rank the more relevant remote information. This can be seen in the difference between the adaptivity of the local strategy and the local and remote strategy. In this context, it is interesting that P2P technology can be used to include heuristics employed by human administrators, the grouping of similar devices. Correlation peers also decrease the amount of management traffic and resource consumption regarding the P2P measurement overlay.

The Research Question 5 aimed at the necessary conditions to enable the sharing of active measurement results among network devices. The concept of virtual measurement sessions was inspired by one of the behaviors commonly employed by network

administrators, the sharing of active measurement results considering their own expertise. Since the devices which share results should be similar (in terms of SLA performance), the concept of correlated peers is used to enable such sharing. Besides that, we also proposed an algorithm to contract the results exchange and a measurement session activation strategy which considers the virtual measurement sessions, the virtual strategy (as described in Chapter 5).

The experiments performed in Section 6.3 show that it is possible to overcome the number of detected network SLA violations over the available measurement sessions using the virtual strategy. From the initial state, devices were able to find other devices to share results in a static network condition. In this context, this strategy must to respond to unanticipated situations or changes in the network environment. This can be seen in the experiment results as the total number of detected SLA violations continue to surpass the maximum number of locally detected ones after changes in the network conditions. Finally, since the contract of virtual measurement sessions does not use hard coordination, there is no strong coupling among devices. Thus, a network device peer does not need to access information from other peers to take measurement activation decisions even when using the virtual strategy.

7.2 Future Work

The present thesis is intended to be an initial step towards the decentralized detection of violation of SLAs using P2P technology. Thus, there will likely be other interesting topics that can be investigated in the context of present work, *i.e.*, concerning the utilization of active measurement mechanisms to detect SLA violations. Thus, we present some future research opportunities and directions in the closing section.

Refinements in peering could be investigated in order to turn the strategies more selective about the construction of the P2P measurement overlay. One of the possibilities to enhance this selection is to employ a prospective phase for the measurement session activation strategies. Simpler measurement sessions could be activated just to enable agreements among network devices about activation decisions, *i.e.*, validating the peering. Finally, throttling overlay traffic could be used in order to protect "popular" peers.

The formation of the P2P measurement overlay could use additional information besides the results of service level measurement. In this context, network devices could be grouped in an infrastructure according either to their "behavior" or other properties of

the devices themselves. Some examples of these properties are the role of the device in the network infrastructure (*e.g.*, core and access routers) and hardware model/operating system version. The use of additional information could help the execution of more customized network measurement tasks.

We made the assumption that the detection of each SLA violation is completely performed by individual network devices. However, it would be possible to break down some measurements into sub-tasks which leads to composite measurement tasks. For example, this could be done to enable the monitoring of more complex SLAs. Multiple peers among the P2P measurement overlay could cooperate to present composed results. In order to enable the cooperation, it would be necessary to employ a full coordination protocol. We suppose that this protocol should allow explicit agreements on what destinations to monitor and how to compose measurement results.

The increasing needs of management metrics and the co-existence of several monitoring solutions can interfere in the execution of measurement sessions by different network devices. In order to solve this problem as future work, the P2P measurement overlay could be used to enable some form of "active measurement session marketplace". In this context, network devices with activated measurement session send out an advertisements of such sessions which includes a specification of the sessions themselves (metadata). This specification could include a description of the sessions and the constraints. Besides that, devices could also advertise their desired measurement session, for which they do not have local available resources. Peers, then, make contracts to exchange measurement sessions, which would be virtual measurement sessions (using the terminology of the present thesis).

Network-wide control of active measurement sessions is important for various network management tasks besides the detection of SLA violations. In this context, the management information produced in the P2P measurement overlay could have other uses regarding such tasks. For example, information about correlated peers could be used to allow inferences about the underlying (physical) topology. This is because variations in service level performance due to network reasons could lead to measurement sessions which have correlated results. Thus, this correlation could be analyzed in order to discover path intersections.

REFERENCES

AGHAMAHMOODI, S.; RANKOOHI, S. M. T. R.; AGHAMAHMOODI, F. A new ant colony optimization-based algorithm for range query answering problem in relational schema-based p2p database systems. **Knowledge and Information Systems**, Springer, New York, NY, USA, vol. 43, no. 3, p. 719–749, 2014. Available from Internet: <http://dx.doi.org/10.1007/s10115-014-0739-x>.

AGUIRRE, J.-V.; ALVAREZ, R.; ZAMORA, A. Darkcube: A k-hypercube based p2p voip protocol. **Peer-to-Peer Networking and Applications**, Springer, New York, NY, USA, p. 1–14, 2015. Available from Internet: <http://dx.doi.org/10.1007/s12083-015-0415-2>.

ANDROUTSELLIS-THEOTOKIS, S.; SPINELLIS, D. A survey of peer-to-peer content distribution technologies. **ACM Computing Surveys**, ACM Press, New York, NY, USA, vol. 36, no. 4, p. 335–371, 2004. Available from Internet: <http://doi.acm.org/10.1145/1041680.1041681>.

BADIS, H.; DOYEN, G.; KHATOUN, R. A collaborative approach for a source based detection of botclouds. In IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK AND SERVICE MANAGEMENT (IM), 14., 2015, Ottawa, Canada. **Proceedings...** New York, NY, USA: IEEE, 2015. p. 906–909.

BAJPAI, V.; SCHÖNWÄLDER, J. A report on the 1st nmrg workshop on large scale network measurements. **Journal of Network and Systems Management**, Springer, New York, NY, USA, vol. 23, no. 1, p. 238–245, 2014. Available from Internet: <http://dx.doi.org/10.1007/s10922-014-9328-2>.

BARFORD, P. et al. Network performance anomaly detection and localization. In IEEE INTERNATIONAL CONFERENCE ON COMPUTER COMMUNICATIONS (INFOCOM), 28., 2009, Rio de Janeiro, Brazil. **Proceedings...** New York, NY, USA: IEEE, 2009. p. 1377–1385.

BARSHAN, M.; FATHY, M.; YOUSEFI, S. Fault-tolerant architecture for peer to peer network management systems. In BALANDIN, S.; MOLTCHANOV, D.; KOUCHERYAVY, Y. (Ed.). **Smart Spaces and Next Generation Wired/Wireless Networking**. Springer Berlin Heidelberg, 2009, (Lecture Notes in Computer Science, vol. 5764). p. 241–252. ISBN 978-3-642-04188-4. Available from Internet: <http://dx.doi.org/10.1007/978-3-642-04190-7_22>.

BIESZCZAD, A.; PAGUREK, B.; WHITE, T. Mobile agents for network management. **IEEE Communications Surveys**, vol. 1, no. 1, p. 2–9, 1998.

BINZENHÖFER, A. et al. A p2p-based framework for distributed network management. In CESANA, M.; FRATTA, L. (Ed.). **Wireless Systems and Network Architectures in Next Generation Internet**. Springer Berlin Heidelberg, 2006, (Lecture Notes in Computer Science, vol. 3883). p. 198–210. ISBN 978-3-540-34025-6. Available from Internet: <http://dx.doi.org/10.1007/11750673_16>.

BJUREFORS, F.; LARZON, L.-A.; GOLD, R. Performance of pastry in a heterogeneous system. In IEEE INTERNATIONAL CONFERENCE ON PEER-TO-PEER

COMPUTING (P2P), 4., 2004, Zurich, Switzerland. **Proceedings...** Washington, DC, USA: IEEE, 2004. p. 278–279. ISBN 0-7695-2156-8. Available from Internet: <http://dx.doi.org/10.1109/P2P.2004.40>.

BLANTON, E. et al. Design and evaluation of the s 3 monitor network measurement service on geni. In IEEE INTERNATIONAL CONFERENCE ON COMMUNICATION SYSTEMS AND NETWORKS (COMSNETS), 4., 2012, Bangalore, India. **Proceedings...** New York, NY, USA: IEEE, 2012. p. 1–10.

BONFIGLIO, D. et al. Revealing skype traffic: When randomness plays with you. **ACM SIGCOMM Computer Communication Review**, ACM, New York, NY, USA, vol. 37, no. 4, p. 37–48, August 2007. Available from Internet: <http://doi.acm.org/10.1145/1282427.1282386>.

BROWNLEE, N. **RTFM: Applicability Statement**. Marina del Rey, CA, USA: IETF Trust, 1999. RFC 2721 (Informational). (Request for Comments, 2721).

BROWNLEE, N.; MILLS, C.; RUTH, G. **Traffic Flow Measurement: Architecture**. Marina del Rey, CA, USA: IETF Trust, 1999. RFC 2722 (Informational). (Request for Comments, 2722).

BRUNNER, M. et al. Towards ambient networks management. In MAGEDANZ, T. et al. (Ed.). **Mobility Aware Technologies and Applications**. Springer Berlin Heidelberg, 2005, (Lecture Notes in Computer Science, vol. 3744). p. 215–229. ISBN 978-3-540-29410-8. Available from Internet: <http://dx.doi.org/10.1007/11569510_21>.

BURLEIGH, S. et al. Delay-tolerant networking: an approach to interplanetary internet. **IEEE Communications Magazine**, vol. 41, no. 6, p. 128–136, June 2003.

CANTIENI, G. R. et al. Reformulating the monitor placement problem: Optimal network-wide sampling. In ACM CONFERENCE ON EMERGING NETWORK EXPERIMENT AND TECHNOLOGY (CONEXT), 2., 2006, Lisboa, Portugal. **Proceedings...** New York, NY, USA: ACM, 2006. p. 5:1–5:12. ISBN 1-59593-456-1. Available from Internet: <http://doi.acm.org/10.1145/1368436.1368444>.

CHANG, C.-W. et al. Leisure: Load-balanced network-wide traffic measurement and monitor placement. **IEEE Transactions on Parallel and Distributed Systems**, vol. 26, no. 4, p. 1059–1070, April 2015.

CHAUDET, C. et al. Optimal positioning of active and passive monitoring devices. In ACM CONFERENCE ON EMERGING NETWORK EXPERIMENT AND TECHNOLOGY (CONEXT), 1., 2005, Toulouse, France. **Proceedings...** New York, NY, USA: ACM, 2005. p. 71–82. ISBN 1-59593-197-X. Available from Internet: <http://doi.acm.org/10.1145/1095921.1095932>.

CHIBA, M. S. et al. **Cisco Service-Level Assurance Protocol**. Marina del Rey, CA, USA: IETF Trust, 2013. RFC 6812 (Informational). (Request for Comments, 6812).

CLAISE, B. **Cisco Systems NetFlow Services Export Version 9**. Marina del Rey, CA, USA: IETF Trust, 2004. RFC 3954 (Informational). (Request for Comments, 3954).

CLAISE, B. **Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information**. Marina del Rey, CA, USA: IETF Trust, 2008. RFC 5101 (Standard). (Request for Comments, 5101).

COHEN, B. **The BitTorrent protocol specification**. 2015. Available at <http://www.bittorrent.com/>. Accessed in October 2015.

DUARTE, P. A. P. R. et al. A p2p-based self-healing service for network maintenance. In IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK MANAGEMENT (IM), 12., 2011, Dublin, Ireland. **Proceedings...** New York, NY, USA: IEEE, 2011. p. 313–320. ISBN 978-1-4244-9219-0. Available from Internet: <http://dx.doi.org/10.1109/INM.2011.5990706>.

DUFFIELD, N. Sampling for passive internet measurement: A review. **Statistical Science**, Institute of Mathematical Statistics, Beachwood, OH, USA, vol. 19, no. 3, p. 472–498, August 2004. Available from Internet: <http://www.jstor.org/stable/4144398>.

EBRAHIMI, M.; RANKOOHI, S. M. T. R. An ant-based approach to cluster peers in p2p database systems. **Knowledge and Information Systems**, Springer, New York, NY, USA, vol. 43, no. 1, p. 219–247, 2014. Available from Internet: <http://dx.doi.org/10.1007/s10115-014-0743-1>.

ENNS M. BJORKLUND, J. S. A. B. R. **Network Configuration Protocol (NETCONF)**. Marina del Rey, CA, USA: IETF Trust, 2011. RFC 6241 (Proposed Standard). (Request for Comments, 6241).

ERIKSSON, B.; BARFORD, P.; NOWAK, R. Network discovery from passive measurements. **SIGCOMM Comput. Commun. Rev.**, ACM, New York, NY, USA, vol. 38, no. 4, p. 291–302, August 2008. Available from Internet: <http://doi.acm.org/10.1145/1402946.1402992>.

FALLON, L. et al. Self-forming network management topologies in the madeira management system. In BANDARA, A.; BURGESS, M. (Ed.). **Inter-Domain Management**. Springer Berlin Heidelberg, 2007, (Lecture Notes in Computer Science, vol. 4543). p. 61–72. ISBN 978-3-540-72985-3. Available from Internet: <http://dx.doi.org/10.1007/978-3-540-72986-0_6>.

FARRINGTON, N.; ANDREYEV, A. Facebook's data center network architecture. In IEEE OPTICAL INTERCONNECTS (OI) CONFERENCE, 2., 2013, Santa Fe, NM, USA. **Proceedings...** New York, NY, USA: IEEE, 2013. p. 49–50. ISBN 978-1-4673-5061-7. Available from Internet: <http://dx.doi.org/10.1109/OIC.2013.6552917>.

FIORESE, A.; SIMOES, P.; BOAVIDA, F. Performance evaluation of service searching using aggregation in peer-to-peer service overlay networks. In IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK MANAGEMENT (IM), 12., 2011, Dublin, Ireland. **Proceedings...** New York, NY, USA: IEEE, 2011. p. 642–645. ISBN 978-1-4244-9219-0.

FIORESE, A.; SIMõES, P.; BOAVIDA, F. A p2p-based approach to cross-domain network and service management. In SADRE, R.; PRAS, A. (Ed.). **Scalability of Networks and Services**. Springer Berlin Heidelberg, 2009, (Lecture Notes in Computer

Science, vol. 5637). p. 179–182. ISBN 978-3-642-02626-3. Available from Internet: <http://dx.doi.org/10.1007/978-3-642-02627-0_16>.

GANGAM, S.; FAHMY, S. Mitigating interference in a network measurement service. In IEEE INTERNATIONAL WORKSHOP ON QUALITY OF SERVICE (IWQOS), 9., 2011, San Jose, California. **Proceedings...** Piscataway, NJ, USA: IEEE Press, 2011. p. 37:1–37:9. ISBN 978-1-4577-0104-7. ISSN 1548-615X. Available from Internet: <http://dl.acm.org/citation.cfm?id=1996039.1996082>.

GAO, C. et al. Smon: Self-managed overlay networks for managing distributed applications. In IEEE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM (NOMS), 12., 2010, Osaka, Japan. **Proceedings...** New York, NY, USA: IEEE, 2010. p. 80–87. ISBN 978-1-4244-5366-5. ISSN 1542-1201. Available from Internet: <http://dx.doi.org/10.1109/NOMS.2010.5488440>.

GAUTHIERDICKEY, C.; RITZDORF, C. Secure peer-to-peer trading in small-and large-scale multiplayer games. **Multimedia Systems**, Springer, New York, NY, USA, vol. 20, no. 5, p. 595–607, 2014.

GOLDSZMIDT, G.; YEMINI, Y. Distributed management by delegation. In IEEE INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS, 15., 1995, Vancouver, BC, Canada. **Proceedings...** Washington, DC, USA: IEEE Computer Society, 1995. p. 333–340. ISSN 1063-6927.

GONG, L. Jxta: a network programming environment. **IEEE Internet Computing**, IEEE Computer Society, Washington, DC, USA, vol. 5, no. 3, p. 88–95, May 2001. Available from Internet: <http://dx.doi.org/10.1109/4236.935182>.

GOOGLE. **Hangouts**. 2015. Available at <https://hangouts.google.com/>. Accessed in October 2015.

GRANVILLE, L. et al. Managing computer networks using peer-to-peer technologies. **IEEE Communications Magazine**, IEEE, New York, NY, USA, vol. 43, no. 10, p. 62–68, October 2005.

GRANVILLE, L. Z.; FESTOR, O. **Network Management Research Group Status Report 2012**. Marina del Rey, CA, USA: IETF Trust, 2012.

HEDAYAT, K. et al. **A Two-Way Active Measurement Protocol (TWAMP)**. Marina del Rey, CA, USA: IETF Trust, 2008. RFC 5357 (Proposed Standard). (Request for Comments, 5357).

HUANG, G. et al. Measurement-aware monitor placement and routing: A joint optimization approach for network-wide measurements. **IEEE Transactions on Network and Service Management**, IEEE, New York, NY, USA, vol. 9, no. 1, p. 48–59, March 2012.

IDHAW, E. et al. Policy-based management of the future airborne network via peer-to-peer networking. In IEEE MILITARY COMMUNICATIONS CONFERENCE (MILCOM). **Proceedings...** Washington, DC, USA: IEEE Computer Society, 2006. p. 1–10.

INACIO, C. M.; TRAMMELL, B. Yaf: Yet another flowmeter. In **Proceedings...** Berkeley, CA, USA: USENIX Association, 2010. p. 1–16.

JAIN, N. et al. Network imprecision: A new consistency metric for scalable monitoring. In PROCEEDINGS OF THE 8TH USENIX CONFERENCE ON OPERATING SYSTEMS DESIGN AND IMPLEMENTATION (OSDI), 8., 2008, San Diego, California. **Proceedings...** Berkeley, CA, USA: USENIX Association, 2008. p. 87–102.

JAVANMARDI, S. et al. Fr trust: a fuzzy reputation–based model for trust management in semantic p2p grids. **International Journal of Grid and Utility Computing**, Inderscience Publishers, vol. 6, no. 1, p. 57–66, 2014. Available from Internet: <http://dx.doi.org/10.1504/IJGUC.2015.066397>.

JENNINGS, C. et al. **REsource LOcation And Discovery (RELOAD) Base Protocol**. Marina del Rey, CA, USA: IETF Trust, 2012. Work in progress as an Internet-Draft. (Internet-Draft, draft-ietf-p2psip-base-21).

JIMENEZ, R.; OSMANI, F.; KNUTSSON, B. Connectivity properties of mainline bittorrent dht nodes. In IEEE INTERNATIONAL CONFERENCE ON PEER-TO-PEER COMPUTING (P2P), 9., 2009, Washington, WA, USA. **Proceedings...** New York, NY, USA: IEEE, 2009. p. 262–270. ISBN 978-1-4244-5066-4.

Joint Technical Committee ISO/IEC. **ISO/IEC 7498-4, Information Technology, Open Systems Interconnection, Basic Reference Model: Management Framework** . Geneva, Switzerland, 1994.

JONES, S. Toward an acceptable definition of service [service-oriented architecture]. **IEEE Software**, IEEE, New York, NY, USA, vol. 22, no. 3, p. 87–93, May 2005.

JUN, L. et al. A novel network management architecture for self-organizing network. In INTERNATIONAL CONFERENCE ON NETWORKING, ARCHITECTURE, AND STORAGE (NAS), 2., 2007, Guilin, China. **Proceedings...** Los Alamitos, CA, USA: IEEE Computer Society, 2007. p. 146–154. ISBN 0-7695-2927-5. Available from Internet: <http://dx.doi.org/10.1109/NAS.2007.5>.

KAMIENSKI, C. et al. On the use of peer-to-peer architectures for the management of highly dynamic environments. In IEEE INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING AND COMMUNICATIONS WORKSHOPS (PERCOM), 4., 2006, Pisa, Italy. **Proceedings...** Los Alamitos, CA, USA: IEEE Computer Society, 2006. p. 135–140. ISSN 0-7695-2520-2. Available from Internet: <http://dx.doi.org/10.1109/PERCOMW.2006.106>.

KAMIYAMA, N.; MORI, T.; KAWAHARA, R. Autonomic load balancing of flow monitors. **Computer Networks**, Elsevier, vol. 57, no. 3, p. 741–761, 2013. Available from Internet: <http://www.sciencedirect.com/science/article/pii/S1389128612003726>.

KANSAL, A.; GORACZKO, M.; ZHAO, F. Building a sensor network of mobile phones. In ACM INTERNATIONAL CONFERENCE ON INFORMATION PROCESSING IN SENSOR NETWORKS, 6., 2007, Cambridge, MA, USA. **Proceedings...** New York, NY, USA: ACM, 2007. p. 547–548. ISBN 978-1-59593-638-7. Available from Internet: <http://doi.acm.org/10.1145/1236360.1236433>.

KONSTANTINOU, A.; YEMINI, Y. A2a: An architecture for autonomic management coordination. In BARTOLINI, C.; GASPARY, L. (Ed.). **Integrated Management of Systems, Services, Processes and People in IT**. Springer Berlin Heidelberg, 2009, (Lecture Notes in Computer Science, vol. 5841). p. 85–98. ISBN 978-3-642-04988-0. Available from Internet: <http://dx.doi.org/10.1007/978-3-642-04989-7_7>.

KORPELA, E. et al. Setihome-massively distributed computing for seti. **Computing in Science & Engineering**, AIP Publishing, College Park, MD, USA, vol. 3, no. 1, p. 78 – 83, January-February 2001. Available from Internet: <http://dx.doi.org/10.1109/5992.895191>.

KOUBARAKIS, M. Multi-agent systems and peer-to-peer computing: Methods, systems, and challenges. In KLUSCH, M. et al. (Ed.). **Cooperative Information Agents VII**. Springer Berlin Heidelberg, 2003, (Lecture Notes in Computer Science, vol. 2782). p. 46–61. ISBN 978-3-540-40798-0. Available from Internet: <http://dx.doi.org/10.1007/978-3-540-45217-1_4>.

KRUPCZAK, B. **Cartographer**. 2015. Available at <http://www.krupczak.org/index.php/Cartographer/>. Accessed in October 2015.

LASSOUED, I. et al. Network-wide monitoring through self-configuring adaptive system. In IEEE INTERNATIONAL CONFERENCE ON COMPUTER COMMUNICATIONS (INFOCOM), 30., 2011, Shanghai, China. **Proceedings...** Washington, DC, USA: IEEE Computer Society, 2011. p. 1826–1834. ISBN 978-1-4244-9919-9. ISSN 0743-166X.

LEINWAND, A.; CONDROY, K. F. **Network Management: A Practical Perspective**. 2. ed. Menlo Park, CA, USA: Addison-Wesley Professional, 1996.

LI, J.; JIN, W. Routing mechanism in active peer-to-peer network. In IEEE INTERNATIONAL CONFERENCE ON COMPUTING, COMMUNICATION AND NETWORKING TECHNOLOGIES (ICCCNT), 5., 2014, Hefei, China. **Proceedings...** New York, NY, USA: IEEE, 2014. p. 1–3. ISBN 978-1-4799-2695-4.

LIM, K.-S.; STADLE, R. Developing pattern-based management programs. In AL-SHAER, E.; PACIFICI, G. (Ed.). **Management of Multimedia on the Internet**. Springer Berlin Heidelberg, 2001, (Lecture Notes in Computer Science, vol. 2216). p. 345–358. ISBN 978-3-540-42786-5. Available from Internet: <http://dx.doi.org/10.1007/3-540-45508-6_28>.

LINSNER, M. et al. **Large-Scale Broadband Measurement Use Cases**. Marina del Rey, CA, USA: IETF Trust, 2015. RFC 7536 (Informational). (Request for Comments, 7536).

LU, K.; WANG, J.; LI, M. An eigentrust dynamic evolutionary model in p2p file-sharing systems. **Peer-to-Peer Networking and Applications**, Springer, New York, NY, USA, p. 1–14, 2015. Available from Internet: <http://dx.doi.org/10.1007/s12083-015-0416-1>.

LUPU, E. et al. Amuse: autonomic management of ubiquitous e-health systems. **Concurrency and Computation: Practice and Experience**, John Wiley & Sons, Ltd., vol. 20, no. 3, p. 277–295, 2008. Available from Internet: <http://dx.doi.org/10.1002/cpe.1194>.

MAGDALENO, A. M.; WERNER, C. M. L.; ARAUJO, R. M. de. Reconciling software development models: A quasi-systematic review. **Journal of Systems and Software**, vol. 85, no. 2, p. 351–369, 2012. Available from Internet: <http://dx.doi.org/10.1016/j.jss.2011.08.028>.

MAHADEVAN, P. et al. Orbis: Rescaling degree correlations to generate annotated internet topologies. **ACM SIGCOMM Computer Communication Review**, ACM, New York, NY, USA, vol. 37, no. 4, p. 325–336, ago. 2007. Available from Internet: <http://doi.acm.org/10.1145/1282427.1282417>.

MARQUEZAN, C. C. et al. Maintenance of monitoring systems throughout self-healing mechanisms. In TURCK, F. D.; KELLERER, W.; KORMENTZAS, G. (Ed.). **Managing Large-Scale Service Deployment**. Springer Berlin Heidelberg, 2008, (Lecture Notes in Computer Science, vol. 5273). p. 176–188. ISBN 978-3-540-85999-4. Available from Internet: <http://dx.doi.org/10.1007/978-3-540-87353-2_14>.

MARTIN-FLATIN, J.-P.; ZNATY, S.; HABAUX, J.-P. A survey of distributed entreprise network and systems management paradigms. **Journal of Network and Systems Management**, vol. 7, no. 1, 1999. Available from Internet: <http://dx.doi.org/10.1023/A:1018761615354>.

MATHIEU, B. et al. Self-management of context-aware overlay ambient networks. In IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK MANAGEMENT (IM), 10., 2007, Munich, Germany. **Proceedings...** Los Alamitos, CA, USA: IEEE Computer Society Press, 2007. p. 749–752. ISBN 1-4244-0798-2. Available from Internet: <http://dx.doi.org/10.1109/INM.2007.374704>.

MEGIAS, D. Improved privacy-preserving p2p multimedia distribution based on recombined fingerprints. **Transactions on Dependable and Secure Computing**, IEEE, New York, NY, USA, vol. 12, no. 2, p. 179–189, March 2015. Available from Internet: <http://dx.doi.org/10.1109/TDSC.2014.2320712>.

MELCHIORS, C. et al. **Advancements in Distributed Computing and Internet Technologies: Trends and Issues**. Hershey, PA, USA: IGI Global, 2011.

MONTRESOR, A.; JELASITY, M. Peersim: A scalable p2p simulator. In IEEE INTERNATIONAL CONFERENCE ON PEER-TO-PEER COMPUTING (P2P). **Proceedings...** Washington, DC, USA: IEEE Computer Society.

MORARIU, C.; RACZ, P.; STILLER, B. Script: A framework for scalable real-time ip flow record analysis. In IEEE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM (NOMS), 12., 2010, Osaka, Japan. **Proceedings...** New York, NY, USA: IEEE, 2010. p. 278–285. ISBN 978-1-4244-5366-5. ISSN 1542-1201. Available from Internet: <http://dx.doi.org/10.1109/NOMS.2010.5488476>.

MORARIU, C.; STILLER, B. Dicap: Distributed packet capturing architecture for high-speed network links. In IEEE CONFERENCE ON LOCAL COMPUTER NETWORKS (LCN), 33., 2008, Montreal, Canada. **Proceedings...** 2008. p. 168–175. ISBN 978-1-4244-2412-2. Available from Internet: <http://dx.doi.org/10.1109/LCN.2008.4664166>.

MORARIU, C.; STILLER, B. An open architecture for distributed ip traffic analysis (dita). In IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK MANAGEMENT (IM), 12., 2011, Dublin, Ireland. **Proceedings...** Washington, DC, USA: IEEE Computer Society, 2011. p. 952–957. ISBN 978-1-4244-9219-0. Available from Internet: <http://dx.doi.org/10.1109/INM.2011.5990528>.

NOBRE, J. C.; GRANVILLE, L. Z. Consistency of states of management data in p2p-based autonomic network management. In BARTOLINI, C.; GASPARY, L. P. (Ed.). **Integrated Management of Systems, Services, Processes and People in IT**. Springer Berlin Heidelberg, 2009, (Lecture Notes in Computer Science, vol. 5841). p. 99–110. ISBN 978-3-642-04988-0. Available from Internet: <http://dx.doi.org/10.1007/978-3-642-04989-7_8>.

NOBRE, J. C.; GRANVILLE, L. Z. Consistency of policy states in decentralized autonomic network management. In IEEE/IFIP NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM (NOMS), 12., 2010, Osaka, Japan. **Proceedings...** Washington, DC, USA: IEEE Computer Society, 2010. p. 519–526. ISBN 978-1-4244-5366-5. ISSN 1542-1201. Available from Internet: <http://dx.doi.org/10.1109/NOMS.2010.5488469>.

OSIRIS. **Osiris Serverless Portal System**. 2015. Available at <http://www.osiris-sps.org/>. Accessed in October 2015.

PANISSON, A. et al. Designing the Architecture of P2P-Based Network Management Systems. In IEEE SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS (ISCC). **Proceedings...** New York, NY, USA: IEEE Computer Society, 2006. p. 69–75. Available from Internet: <http://dx.doi.org/10.1109/ISCC.2006.60>.

PAPADAKIS, H. et al. Imbuing unstructured p2p systems with non-intrusive topology awareness. In IEEE INTERNATIONAL CONFERENCE ON PEER-TO-PEER COMPUTING (P2P), 9., 2009, Seattle, WA, USA. **Proceedings...** New York, NY, USA: IEEE, 2009. p. 51–60. ISBN 978-1-4244-5066-4. Available from Internet: <http://dx.doi.org/10.1109/P2P.2009.5284549>.

PATIL, B.; KINGER, S.; PATHAK, V. K. Probe station placement algorithm for probe set reduction in network fault localization. In INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS AND COMPUTER NETWORKS (ISCON). **Proceedings...** Washington, DC, USA: IEEE Computer Society, 2013. p. 164–169.

PAVLOU, G. On the evolution of management approaches, frameworks and protocols: A historical perspective. **Journal of Network and Systems Management**, vol. 15, no. 4, p. 425–445, 2007. Available from Internet: <http://dx.doi.org/10.1007/s10922-007-9082-9>.

PEOPLES, C. et al. Context-aware policy-based framework for self-management in delay-tolerant networks: a case study for deep space exploration. **IEEE Communications Magagazine**, IEEE Press, Piscataway, NJ, USA, vol. 48, no. 7, p. 102–109, July 2010. Available from Internet: <http://dx.doi.org/10.1109/MCOM.2010.5496885>.

PHAAL, P.; PANCHEN, S.; MCKEE, N. **InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks**. Marina del Rey, CA, USA: IETF Trust, 2001. RFC 3176 (Informational). (Request for Comments, 3176).

PIETRO, A. di et al. Decon: Decentralized coordination for large-scale flow monitoring. In PROCEEDINGS OF THE IEEE CONFERENCE ON COMPUTER COMMUNICATIONS (INFOCOM). **Proceedings...** Washington, DC, USA: IEEE Computer Society, 2010. p. 1–5. ISBN 978-1-4244-6739-6. Available from Internet: <http://dx.doi.org/10.1109/INFCOMW.2010.5466642>.

PRAS, A. et al. Key research challenges in network management. **IEEE communications magazine**, IEEE Communication Society, New York, vol. 45, no. 10, p. 104–110, October 2007.

RACZ, P.; DONNI, D.; STILLER, B. An architecture and implementation for ip network and service quality measurements. In IEEE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM (NOMS). **Proceedings...** Washington, DC, USA: IEEE Computer Society, 2010. p. 24–31. ISBN 978-1-4244-5366-5. ISSN 1542-1201. Available from Internet: <http://dx.doi.org/10.1109/NOMS.2010.5488429>.

RIMAC, I. et al. **A Survey on Research on the Application-Layer Traffic Optimization (ALTO) Problem**. Marina del Rey, CA, USA: IETF Trust, 2010. RFC 6029 (Informational). (Request for Comments, 6029).

RODRIGUES, R.; DRUSCHEL, P. Peer-to-peer systems. **Communincation of the ACM**, ACM, New York, NY, USA, vol. 53, no. 10, p. 72–82, October 2010. Available from Internet: <http://doi.acm.org/10.1145/1831407.1831427>.

SAINI, N. K.; CHATURVEDI, A.; YADAV, R. C. Identifying. collusion attacks in p2p trust and reputation systems. **International Journal of Computer Applications (IJCA)**, Foundation of Computer Science (FCS, New York, NY, USA, vol. 2, no. 2, p. 36–41, April 2014.

SAMAAN, N.; KARMOUCH, A. Towards autonomic network management: An analysis of current and future research directions. **IEEE Communications Surveys and Tutorials**, vol. 11, no. 3, p. 22–36, 2009.

SANTOS, C. R. P. d. et al. On the impact of using presence services in p2p-based network management systems. In IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE (GLOBECOM), 34., 2010, Miami, FL, USA. **Proceedings...** New York, NY, USA: IEEE, 2010. p. 1–6. ISBN 978-1-4244-5636-9. ISSN 1930-529X.

SANTOS, C. R. P. dos et al. On the design and performance evaluation of notification support for p2p-based network management. In ACM SYMPOSIUM ON APPLIED COMPUTING, 23., 2008, Fortaleza, Brazil. **Proceedings...** New York, NY, USA: ACM, 2008. p. 2057–2062. ISBN 978-1-59593-753-7. Available from Internet: <http://doi.acm.org/10.1145/1363686.1364184>.

SCHAEFFER-FILHO, A.; LUPU, E.; SLOMAN, M. Federating policy-driven autonomous systems: Interaction specification and management patterns. **Journal of Network and Systems Management**, vol. 23, no. 3, p. 753–793, 2014. Available from Internet: <http://dx.doi.org/10.1007/s10922-014-9317-5>.

SCHÖNWÄLDER, J.; QUITTEK, J.; KAPPLER, C. Building distributed management applications with the ietf script mib. **IEEE Journal on Selected Areas in**

Communications, IEEE Press, Piscataway, NJ, USA, vol. 18, no. 5, p. 702–714, September 2006. Available from Internet: <http://dx.doi.org/10.1109/49.842986>.

SCOTT, J. et al. Haggle: a Networking Architecture Designed Around Mobile Users. In IFIP ANNUAL CONFERENCE ON WIRELESS ON DEMAND NETWORK SYSTEMS AND SERVICES (WONS), 3., 2006, Les Menuires, France. **Proceedings...** New York, NY, USA: IEEE, 2006. p. 78–86. ISBN 1-4244-0860-1.

SEKAR, V. et al. Csamp: A system for network-wide flow monitoring. In USENIX SYMPOSIUM ON NETWORKED SYSTEMS DESIGN AND IMPLEMENTATION (NSDI), 5., 2008, San Francisco, CA, USA. **Proceedings...** Berkeley, CA, USA: USENIX Association, 2008. p. 233–246. ISBN 111-999-5555-22-1.

SESHAN, S.; STEMM, M.; KATZ, R. H. Spand: Shared passive network performance discovery. In USENIX SYMPOSIUM ON INTERNET TECHNOLOGIES AND SYSTEMS (USITS), 1., 1997, Monterey, CA, USA. **Proceedings...** Berkeley, CA, USA: USENIX Association, 1997. p. 1–13.

SHALUNOV, S. et al. **A One-way Active Measurement Protocol (OWAMP)**. Marina del Rey, CA, USA: IETF Trust, 2006. RFC 4656 (Proposed Standard). (Request for Comments, 4656).

SIMON, C. et al. Peer-to-peer management in Ambient Networks. In IST MOBILE & WIRELESS COMMUNICATIONS SUMMIT, 14., 2005, Dresden, Germany. **Proceedings...** New York, NY, USA: IEEE, 2005.

SLOMAN, M. Policy driven management for distributed systems. **Journal of Network and Systems Management**, vol. 2, no. 4, p. 333–360, 1994. Available from Internet: <http://dx.doi.org/10.1007/BF02283186>.

SMITH, R. The contract net protocol: High-level communication and control in a distributed problem solver. **IEEE Transactions on Computers**, IEEE Computer Society, Los Alamitos, CA, USA, vol. 29, no. 12, p. 1104–1113, 1980.

SOMMERS, J. et al. Accurate and efficient sla compliance monitoring. **ACM SIGCOMM Computer Communication Review**, ACM, New York, NY, USA, vol. 37, no. 4, p. 109–120, August 2007. Available from Internet: <http://doi.acm.org/10.1145/1282427.1282394>.

SONG, H. H.; QIU, L.; ZHANG, Y. Netquest: A flexible framework for large-scale network measurement. **SIGMETRICS Performance Evaluation Review**, ACM, New York, NY, USA, vol. 34, no. 1, p. 121–132, jun. 2006. Available from Internet: <http://doi.acm.org/10.1145/1140103.1140293>.

SPRING, N.; MAHAJAN, R.; WETHERALL, D. Measuring isp topologies with rocketfuel. **ACM SIGCOMM Computer Communication Review**, ACM, New York, NY, USA, vol. 32, no. 4, p. 133–145, ago. 2002. Available from Internet: <http://doi.acm.org/10.1145/964725.633039>.

STINGL, D. et al. Mobi-g: Gossip-based monitoring in manets. In IEEE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM (NOMS), 14., 2014, Krakow, Poland. **Proceedings...** New York, NY, USA: IEEE, 2014. p. 1–9. Available from Internet: <http://dx.doi.org/10.1109/NOMS.2014.6838313>.

STOICA, I. et al. Chord: a scalable peer-to-peer lookup protocol for internet applications. **IEEE/ACM Transactions on Networking**, IEEE Computer Society, New York, NY, USA, vol. 11, no. 1, p. 17 – 32, February 2003.

SUH, K. et al. Locating network monitors: complexity, heuristics, and coverage. **Computer Communications**, Elsevier, Philadelphia, PA, USA, vol. 29, no. 10, p. 1564–1577, 2006. Available from Internet: <http://dx.doi.org/10.1016/j.comcom.2005.07.009>.

SUN, J. et al. A low-latency peer-to-peer live and vod streaming system based on scalable video coding. In IEEE VISUAL COMMUNICATIONS AND IMAGE PROCESSING CONFERENCE, 4., 2014, Valleta, Malta. **Proceedings...** New York, NY, USA: IEEE, 2014. p. 319–319. Available from Internet: <http://dx.doi.org/10.1109/VCIP.2014.7051568>.

TRAN, H. M.; SCHÖNWÄLDER, J. **Inter-Domain Management: First International Conference on Autonomous Infrastructure, Management and Security (AIMS)**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007. vol. 4543. 200–203 p. Available from Internet: <http://dx.doi.org/10.1007/978-3-540-72986-0_25>.

TRAVERSO, S. et al. A performance comparison of hose rate controller approaches for p2p-tv applications. **Computer Networks**, Elsevier, Philadelphia, PA, USA, vol. 69, p. 101–120, 2014. Available from Internet: <http://dx.doi.org/10.1016/j.comnet.2014.04.010>.

UNION, I. T. **ITU-T Recommendation M.3000 - Overview of TMN Recommendation**. Geneva, Switzerland, 2000.

VERMA, D. Simplifying network administration using policy-based management. **Network, IEEE**, IEEE Computer Society, New York, NY, USA, vol. 16, no. 2, p. 20–26, March 2002.

VOULGARIS, S.; GAVIDIA, D.; STEEN, M. van. Cyclon: Inexpensive membership management for unstructured p2p overlays. **Journal of Network and Systems Management**, Springer New York, vol. 13, no. 2, p. 197–217, 2005. Available from Internet: <http://dx.doi.org/10.1007/s10922-005-4441-x>.

WESTERINEN, A. et al. **Terminology for Policy-Based Management**. Marina del Rey, CA, USA: IETF Trust, 2001. RFC 3198 (Standard). (Request for Comments, 3198).

WUHIB, F. et al. Robust monitoring of network-wide aggregates through gossiping. **Network and Service Management, IEEE Transactions on**, IEEE Computer Society, New York, NY, USA, vol. 6, no. 2, p. 95–109, jun. 2009.

WUHIB, F.; STADLER, R. Distributed monitoring and resource management for large cloud environments. In IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK MANAGEMENT (IM), 12., 2011, Dublin, Ireland. **Proceedings...** Washington, DC, USA: IEEE Computer Society, 2011. p. 970–975. ISBN 978-1-4244-9219-0. Available from Internet: <http://dx.doi.org/10.1109/INM.2011.5990531>.

XIE, H.; MIN, B.; DAI, Y. Soda: Towards a framework for self optimization via demand adaptation in peer-to-peer networks. In IEEE INTERNATIONAL CONFERENCE ON PEER-TO-PEER COMPUTING (P2P), 9., 2009, Seattle, Washington, USA. **Proceedings...** New York, NY, USA: IEEE, 2009. p. 163–170. ISBN 978-1-4244-5066-4. Available from Internet: <http://dx.doi.org/10.1109/P2P.2009.5284510>.

YALAGANDULA, P.; DAHLIN, M. A scalable distributed information management system. **ACM SIGCOMM Computer Communication Review**, ACM, New York, NY, USA, vol. 34, no. 4, p. 379–390, August 2004. Available from Internet: <http://doi.acm.org/10.1145/1030194.1015509>.

YALAGANDULA, P. et al. S3: a scalable sensing service for monitoring large networked systems. In ACM SIGCOMM WORKSHOP ON INTERNET NETWORK MANAGEMENT (INM), 1., 2006, Pisa, Italy. **Proceedings...** New York, NY, USA: ACM, 2006. p. 71–76. ISBN 1-59593-570-3. Available from Internet: <http://doi.acm.org/10.1145/1162638.1162650>.

ZANG, H.; NUCCI, A. Traffic monitor deployment in ip networks. **Computer Networks**, Elsevier, Philadelphia, PA, USA, vol. 53, no. 14, p. 2491–2501, 2009. Available from Internet: <http://dx.doi.org/10.1016/j.comnet.2009.05.004>.

ZANGRILLI, M.; LOWEKAMP, B. B. Comparing passive network monitoring of grid application traffic with active probes. In **Grid Computing, 2003. Proceedings. Fourth International Workshop on**. Washington, DC, USA: IEEE Computer Society, 2003. p. 84–91. ISBN 0-7695-2026-X.

ZHANG, X. et al. P2pcloud-w: A novel p2pcloud workflow management architecture based on petri net. **International Journal of Grid & Distributed Computing**, SERSC, Sandy Bay, Australia, vol. 8, no. 2, p. 191–200, 2015. Available from Internet: <http://dx.doi.org/10.14257/ijgdc.2015.8.2.18>.

ZHAO, J.; CAO, G. VADD: Vehicle-assisted data delivery in vehicular ad hoc networks. **IEEE Transactions on Vehicular Technology**, vol. 57, no. 3, p. 1910–1922, May 2008.

APPENDIX A RESUMO: DETECÇÃO DESCENTRALIZADA DE VIOLAÇÕES DE ACORDOS DE NÍVEL DE SERVIÇO USANDO TECNOLOGIA PAR-A-PAR

Serviços de rede críticos estabelecidos entre provedores de serviço e clientes devem operar respeitando Acordos de Nível de Serviço (*Service Level Agreements* - SLAs). Uma possibilidade interessante para monitorar tais SLAs é utilizar mecanismos de medição ativa. No entanto, esses mecanismos são custosos em termos do consumo de recursos nos dispositivos de rede e também aumentam a carga da rede por causa do tráfego injetado. Além disso, se o número de violações de SLA em um determinado momento é maior do que o número de sessões de medição disponíveis (lugar-comum em infraestruturas de rede grandes e complexas), seguramente algumas violações serão perdidas. A melhor prática corrente, a monitoração de apenas um subconjunto de destinos de rede baseada na experiência dos administradores, é propensa a erros, não possui boa escalabilidade e é ineficaz em condições da rede dinâmicas. Isto pode levar a perda de violações de SLA, as quais invariavelmente afetam o desempenho de diversas aplicações. Na presente tese, é defendido o uso da tecnologia Par-a-Par (*Peer-to-Peer* - P2P) para melhorar a detecção de violações de SLA. Tal uso é descrito através de princípios para controlar mecanismos de medição ativa. Esses princípios são materializados por meio de estratégias para ativar sessões de medição. Neste contexto, as principais contribuições desta tese são: i) Uma abordagem para aprimorar a detecção de violações de SLA através da orientação da ativação de sessões de medição ativa utilizando resultados anteriores de medições locais e remotas de nível de serviço considerando restrições para utilização de recursos; ii) O conceito de fila de destinos como uma abordagem para priorizar autonomicamente destinos para a ativação de sessões de medição ativa usando escores de destinos; iii) O conceito de pares correlacionados para permitir o provisionamento autonômico de uma rede de sobreposição P2P para troca de resultados de medição ativa relevantes; iv) O conceito de sessões virtuais de medição ativa para permitir o compartilhamento de resultados de medição entre pares correlatos a fim de economizar recursos de dispositivos de rede e aprimorar a cobertura de monitoração de SLA; v) A definição de estratégias descentralizadas para orientar a ativação de sessões de medições ativas utilizando-se princípios P2P. O método utilizado na investigação começou com a realização de revisões de literatura sobre o controle por toda a rede de mecanismos de medição e o emprego de tecnologia P2P no gerenciamento de rede. Após isso, os princípios para o controle de mecanismos de medição ativa e estratégias para ativar sessões de medição propostos

foram descritos. Finalmente, experimentos foram realizados para avaliar o desempenho assim como para ressaltar propriedades de tais princípios e estratégias. Os resultados mostraram propriedades as quais aprimoram a detecção de violações de SLA em termos do número das violações detectadas e da adaptividade a dinâmicas de rede. É esperado que tais resultados possam levar a melhores ferramentas e métodos de monitoração de SLAs.

Palavras-chave: Gerenciamento de redes. P2P. SLA. Medição ativa. Gerenciamento autonômico

APPENDIX B AUXILIARY ALGORITHMS

The P2P principles and strategies enable a decentralized decision making about the activation of active measurement sessions to improve the detection of SLA violations. In this appendix, the auxiliary algorithms employed for the decentralized detection of SLA violations using P2P technology are presented. These algorithms are called during the execution of the measurement sessions activation strategies. In this context, the implementation used for the simulation experiments (used as the evaluation approach) includes these algorithms.

The first presented algorithms are used to gather management data from active measurement results. Algorithm B.1 retrieves the timestamp of the last measurement performed for a given destination. On other hand, Algorithm B.2 retrieves the mean of past service level measurement results within a sliding window for a given destination. In local strategy, only algorithms B.1 and B.2 are employed. Besides that, the local and remote strategy as well as the virtual strategy also used data from remote devices. Algorithm B.3 also collects results, but measurement received from correlated peers. Random strategy does not use historical data, thus, it does not use these algorithms.

Algorithm B.1 getLastLocal(dest)

$lastMeasTimestamp \leftarrow max$ (search $timestamp$ in $measurements[dest]$)
return $lastMeasTimestamp$

Algorithm B.2 getPastLocal(dest, windowSize)

$pastMeasurements \leftarrow \lambda$ ($measurements[dest]$ within $windowSize$)
return $pastMeasurements$

Algorithm B.3 getPastRemote(dest)

$pastMeasurementsRemote \leftarrow \lambda$ (received $measurements[dest]$ within $windowSize$ from each correlated peer))
return $pastMeasurementsRemote$

The definition of the correlated peers (and, consequently the P2P measurement overlay) uses known endpoints as a initial seed. These endpoints can be collected from Routing Information Bases (RIBs) and Forwarding Information Bases (FIBs). Such bases are usually available for local access in network devices employed in operational networks. Algorithm B.4 retrieves endpoints from RIBs and FIBs and returns a merged list.

This algorithm is used on the local and remote strategy and the virtual strategy, which are the ones that employ a P2P measurement overlay.

Algorithm B.4 getEndpoints(dest[])

$endpoints[] \leftarrow$ (get endpoints from Routing Information Bases) + (get endpoints from Forwarding Information Bases)
return $endpoints[]$

The concept of correlated peers assures that the received remote information is locally applicable. Besides that, such peers enable the use of a self-organizing P2P overlay. Algorithm B.4 illustrates the definition of correlated peers. This algorithm uses the existing set of correlated peers and advertised peers from this set as candidates for comparison of local and remote service level measurement results using a correlation function. This comparison also produces a correlation score. After that, the candidates are descending sorted using such score as key. The top candidates, considering the maximum number of correlated peers, which have correlation scores above a lower bound are then returned as the new correlated peers. This algorithm is used on the local and remote strategy and the virtual strategy, which are the ones that employ a P2P measurement overlay.

Algorithm B.5 getCorrelatedtPeers(dest[], correlationMin, peersMax)

$candidateCorrelatedPeers[] \leftarrow correlatedPeers[] + peersOfPeers[]$
$SortDesc(candidateCorrelatedPeers, key \leftarrow$ (get correlation score between local and $candidateCorrelatedPeers[]$ measurement results)
return $newCorrelatedPeers \leftarrow$ (top $peerMax$ in $candidateCorrelatedPeers[]$ which have correlation score above $correlationMin$)

We introduced the concept of correlation peers in order to define a P2P measurement overlay and, consequently, bind network devices as correlated peers using active measurement results. The process to define such peers uses correlation functions applied on past service level measurement results, both locally collected and received from remote devices. Therefore, it is necessary to exchange message to transmit these results. Besides that, devices also inform their set of correlated peers for each one of their own peers. Algorithm B.6 and B.7 describes message exchanges for the definition of P2P measurement overlay. This algorithm is used on the local and remote strategy and the virtual strategy, which are the ones that employ a P2P measurement overlay.

Algorithm B.6 sendMeasurementsResults(correlatedPeers[]

$messageMeasurementsResults \leftarrow$ measurements[dest] within $windowSize$
send $messageMeasurementsResults \rightarrow correlatedPeers$

Algorithm B.7 sendCorrelatedPeers(correlatedPeers[])

$messageCorrelatedPeers \leftarrow correlatedPeers[]$
send $messageCorrelatedPeers \rightarrow correlatedPeers[]$

The virtual strategy overcome the maximum number of active measurements that a device can perform in a given time in respect to the available resources. This is done in order to improve the detection of SLA violations in terms of the SLA monitoring and the employed resources. The use of virtual measurement sessions needs the contract of such sessions between correlated peers. Algorithm B.8 describes a message exchanges for the transmission of commands required for such contract. These commands consider the messages presented in the contract protocol depicted in Section 4.3. After the contract is established, measurement results should be sent from the device which is performing the regular (*i.e.*, non-virtual) measurement session. Algorithm B.9 depicts how these results are sent for the operation of each virtual measurement session. These algorithms are used only on the virtual strategy, which is the one that employ virtual measurements.

Algorithm B.8 sendVirtualCommand(virtualMeasurementPeer, command)

$messageVirtualCommand \leftarrow$ coordination command and parameters
send $messageVirtualCommand \rightarrow virtualMeasurementPeer$

Algorithm B.9 sendVirtualMeasurements(virtualPeers[])

for $virtualPeerin(virtualPeers[])$ **do**
  $messageVirtualSession \leftarrow$ send measurement results related to the virtual peer
  send $messageVirtualSession \rightarrow virtualPeer$
end for