Network-Wide Initiatives to Control Measurement Mechanisms: A Survey

Jéferson Campos Nobre, Bruno Augusti Mozzaquatro, and Lisandro Zambenedetti Granville

***Abstract*—Measurement mechanisms have steadily evolved over the last years and are a key tool for network management. These mechanisms produce results for several network metrics and can be used in different contexts by network administrators. However, the deployment and operation of measurement mechanisms consumes valuable computational and human resources. In this context, approaches to help the administrators to control measurement mechanisms are of paramount importance. In this context, network-wide approaches for such control can provide a larger impact than single device ones. The purpose of this paper is to look at initiatives on the network-wide approaches to control measurement mechanisms in order to provide an integrated perspective. Moreover, we describe criteria that can be used to analyze and compare these initiatives. Furthermore, future trends are discussed in order to predict what the future holds for network-wide control of measurement mechanisms.**

***Index Terms*—Computer network management, measurement mechanisms, metwork-wide control, metrics.**

I. Introduction

MEASUREMENT mechanisms are one of the most important tools employed by network operators. Such mechanisms are used in different contexts, such as pre-deployment validation and in-band live network performance analysis, and in several applications, such as intrusion detection systems (IDS) and lawful interception. Results from measurement mechanisms produce metrics like delay (one-way or round-trip), jitter, throughput, packet loss, and protocol/application usage. Distinct mechanisms can be used to enable network measurements.

In general, network measurements are divided into three groups: active, passive, and hybrid measurement mechanisms. Active measurement is deployed through measurement probes that inject synthetic traffic and compute the current network performance. Passive measurement collects parameters inside network devices, for example, when they observe the passing traffic flows. Furthermore, hybrid measurements use a combination of methods from both active and passive measurements. Although these measurement mechanisms can be employed for the execution of network management tasks, they are also expensive in terms of the computing power required to deliver measurement results.

The deployment and/or use of measurement mechanisms consume what could be useful for primary network functions (*e.g.,* routing and switching). In addition, the operation of these mechanisms also requires valuable human resources, since such operation is usually a complex process based on the network operator's experience and knowledge of the monitored infrastructure. In this context, approaches to help the operators and to decrease resource consumption concerning measurement mechanisms are of vital importance and subject to ongoing research. Some current approaches aim at single devices, *e.g.,* sampling flow packets at a network device and setting thresholds to trigger the injection of a specific test traffic. However, network-wide approaches can provide a larger impact, *e.g.,* coordinating measurement probe activation to enable the optimal monitoring coverage for a network infrastructure. Nevertheless, to the best of our knowledge, a survey of network-wide approaches to control measurement mechanisms has not been provided so far.

In the present paper, we provide an integrated perspective of network-wide approaches to control measurement mechanisms and insights in the rationale for the deployment and applicability of such approaches. A systematic review of the current efforts produces this perspective on initiatives to control measurement mechanisms, restricted to network-wide ones. Moreover, we describe criteria that can be used to analyze and compare the reviewed efforts.

The remainder of this paper is organized as follows. In Section II, we present an overview of three network measurement mechanisms and their controls of measurement mechanisms. In Section III, the initiatives on the network-wide control of measurement mechanisms are presented. Next, the surveyed initiatives are highlighted and a comparison between such initiatives is described in Section IV. We present a discussion of current challenges and future research trends in Section V. Finally, Section VII offers concluding remarks.

II. 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

Manuscript received April 25, 2017; revised November 7, 2017; accepted January 1, 2018. Date of publication January 23, 2018; date of current version May 22, 2018. *(Corresponding author: Jéferson Campos Nobre.)*

J. C. Nobre is with the Polytechnic School, University of Vale do Rio dos Sinos, São Leopoldo 93022-000, Brazil (e-mail: jcnobre@unisinos.br).

B. A. Mozzaquatro is with the Polytechnic School, Federal University of Santa Maria, Santa Maria 97105-900, Brazil.

L. Z. Granville is with the Institute of Informatics, Federal University of Rio Grande do Sul, Porto Alegre 91501970, Brazil.

Digital Object Identifier 10.1109/COMST.2018.2797170

TABLE I
LIST OF ABBREVIATIONS USED IN THIS PAPER

Acronym	Definition
ACM	Association for Computing Machinery
AS	Autonomous System
cSamp	Coordinated Sampling
DNM	Distributed Network Management
FCAPS	Fault, Configuration, Accounting, Performance, Security
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ILP	Integer Linear Program
IP	Internet Protocol
IPFIX	Flow Information eXport
IPPM	Performance Metrics
IRTF	Internet Research Task Force
LEISURE	Load-EqualIzed meaSUREment
LMAP	Large-Scale Measurement of Broadband Performance
LP	Linear Programming
MILP	Mixed Integer Linear Programming
MINLP	Mixed-Integer Non-Linear Program
M-Lab	Measurement Lab
MMPR	Measurement-aware Monitor Placement and Routing
NMRG	Network Management Research Group
NSQM	Network and Service Quality Measurement
OWAMP	One-way Active Measurement Protocol
perfSONAR	PERFormance Service Oriented Network monitoring ARchitecture
RTFM	Realtime Traffic Flow Measurement
SCTP	Stream Control Transport Protocol
SPAND	Shared Passive Network Performance Discovery
SLA	Service Level Assurance
SLAm	Service Level Assurance Monitor
SLO	Service Level Objectives
SPoF	Single Point of Failure
TWAMP	Two-Way Active Measurement Protocol

several applications, such as intrusion detection [1] and lawful interception [2]. Measurements can be performed considering end-to-end paths, individual segments or even domains in a network infrastructure. Finally, different network layers collect information such as messages exchange due to specific protocols. The list of abbreviations used in this paper is presented on Table I.

Results from measurement mechanisms encompass different network metrics, which are a (mostly) quantitative way to verify particular network behavior. These mechanisms produce some of the most important metrics as a measure of time needed for the data to travel between two measurement points; one-way and 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 that are dropped is known as packet loss, and the number of packets that are duplicated is known as packet duplication. These basic metrics can also be 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, the classification of each one of these mechanisms considers the injection of measurement traffic. It leads initially to three kinds: passive, active, and hybrid measurement mechanisms. Passive measurements are conducted inside network devices to collect parameters through the use of packet sniffers. Active measurements are deployed through measurement probes hosted along the network, which inject synthetic traffic and compute the current network performance. Furthermore, hybrid measurements are composed from active measurement to generate the desired traffic, and passive measurement monitors the generated packets.

In this section, we first cover some passive measurement mechanisms and their main concepts. After that, we describe most prominent active and hybrid measurement mechanisms. 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 the background on the control of measurement mechanisms.

A. Passive Measurement Mechanisms

In a passive measurement, network conditions are said to be checked in a non-intrusive way because the measurement process itself creates no monitoring traffic. There are a variety of purposes for the passive measurement data. Considering the FCAPS (Fault Management, Configuration Management, Accounting Management, Performance Management, Security Management) model [3], there are applications on Fault Management (*e.g.,* abnormal traffic behavior), Configuration 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). For example, some network devices perform passive measurement when they observe passing traffic flows.

Flows can be defined as unidirectional sequences of packets that pass through a network device and that are grouped according to some common properties. These properties can consider several packet fields, such as source/destination IP address and port number, layer three protocol type, Type of Service (ToS), and size (aggregated number of bytes). In addition, other information, such as source/destination Autonomous System (AS), and input/output interfaces can also be used to define flows. Uniformity in the representation of flow data and the means of communicating such data from the network elements to corresponding collection points are necessary [4]. There are several protocols used to enable flow data producing and exchange.

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 [5]. This method contains, 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 the least, one-meter reader is needed to collect the measured data from the meters, and a single manager is required to control the meters and meter readers [6].

sFlow [7] 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 that it is monitoring. sFlow datagrams are used to immediately forward the sampled traffic statistics to an sFlow analyzer for processing.

Cisco NetFlow [8] is a widely deployed protocol used to provide 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 sends 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 the 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, NetFlow v9 defines a flexible record format through the use of record templates. Although the NetFlow protocol is a proprietary solution developed by Cisco, the RFC 3954 [8] describes the NetFlow v9.

The IETF IP Flow Information eXport (IPFIX) Working Group has released several documents describing a protocol based on version 9 of NetFlow [4]. The IPFIX protocol incorporates some enhancements in different domains (*e.g.,* congestion-aware transport protocol and built-in security). In addition, IPFIX adopts a better 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. IPFIX has a larger number of field types than NetFlow and also a "vendor ID", which allows one to assign a specific identifier along with different kinds of data. Fig. 1 shows the IPFIX/NetFlow logical model as an example of passive measurement models. In such models, metering exporters hosted in network elements (*e.g.,* routers and switches) gather flow data and export IPFIX/NetFlow records to configured receivers, *i.e.,* collectors (or collecting points).

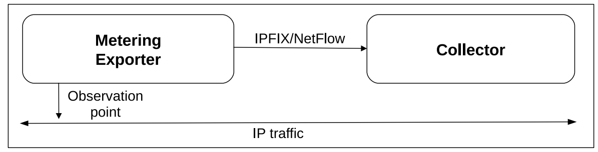


Fig. 1. IPFIX Logical Model.

B. Active Measurement Mechanisms

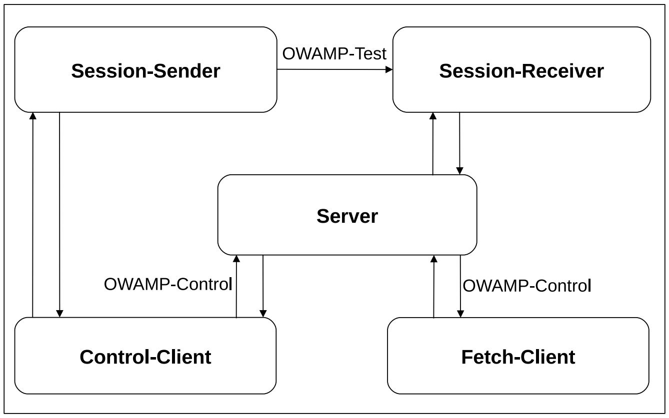
Active measurement mechanisms are an important tool to monitor Service Level Objectives (SLO) and the health of a network as a whole. Such mechanisms inject synthetic traffic into specific network paths to measure the network performance in terms of, for example, delay, loss, jitter, and packet/frame 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 (Internet Protocol) 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.

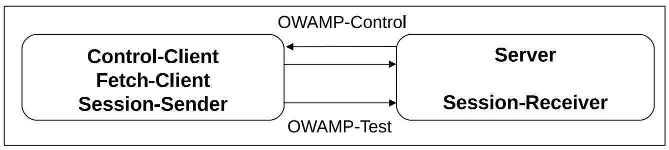
The generation of synthetic traffic and its computation to provide measurement results is usually performed by an architecture comprised of two hosts with specific roles, a sender and a responder, also collectively known as (active) measurement probes. Two inter-related protocols usually define the exchange of packets between probes: 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 offers Real-time Performance Monitoring (RPM) 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; it 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. During the measurement session, the client device sends a packet to a remote server, which in turn returns the packet with an acknowledgment to the sender. The main use for RPM is performance monitoring on layers three and four, 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 [9]. This widely deployed protocol measures service levels related to data link and network layers, and 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.



(a) Roles Distributed on Different Hosts



(b) Roles Integrated on Two Hosts

Fig. 2. O/TWAMP Logical Model.

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) [10] and Two-Way Active Measurement Protocol (TWAMP) [11]. 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. The control protocol is performed by the control-client (requests, starts, and ends test sessions) and server (manages test sessions); and the test control is executed by the sender (sending endpoint) and session-receiver/reflector (receiving endpoint). In addition, 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 Fig. 2 (*a*) shows the logical model used on O/TWAMP. Different hosts play distinct logical roles, but some of these roles can also be played by the same host as shown in the second part of the Fig. 2 (*b*).

C. Hybrid Measurement Mechanisms

The notions of active and passive measurement mechanisms are well-established. Instead, hybrid measurement mechanisms, which combine active and passive ones, are fuzzier, and their definition vary in terms of the standardization bodies. In this context, existing standards, such as the ITU-T Recommendation Y.1540 [12], have already considered metrics that apply to the hybrid measurement [13]; such metrics can be derived from fields or field values, which are dedicated to measurement in a stream of interest [14].

The hybrid measurement mechanisms aim at providing some of the benefits of both active and passive mechanisms, without incurring in their disadvantages. In this context, the metrics produced by hybrid measurement usually have distinct properties, and they consume different amounts of resources for delivering the results. For example, in terms of delay, hybrid methods could provide results with better accuracy than passive methods, but without the network cost of active methods. On the other hand, active mechanisms deliver the most accurate delay measurements, and passive mechanisms do not need to interfere with the (passing)network flows.

The IETF IPPM proposed a categorization for hybrid measurement mechanisms [14]. The first type, Hybrid Type I, is based either on the augmentation or modification of the stream of interest or employment of methods that modify the treatment of such stream. The second type, Hybrid Type II, defines the use of mechanisms that use two or more different streams of interest with some degree of mutual coordination to collect both active and passive metrics and enable additional joint analysis. Some use of hybrid measurement mechanisms is also defined as spatial metrics and methods [15].

The IPv6 Option Header for Performance and Diagnostic Measurements (PDM) Internet-draft [16] proposes the addition of "fields which are dedicated to measurement" on user traffic streams. The measured stream has unknown characteristics until it is processed to add the PDM Option header. The use of PDM intends to have a minor effect on the measured stream and other streams in the network when it is added to strategic interfaces. Considering the IPPM classification, this is a Hybrid Type I method, having at least one characteristic of both active and passive mechanisms for a single stream of interest.

Capello *et al.* [17] proposed coloring packets by rewriting a field of the stream at strategic interfaces to support performance measurements. In fact, the term "coloring" is commonly used to describe the Hybrid Type I method. The measured stream has unknown characteristics until it is processed to add the coloring in the header. Ideally, the coloring would not have effects on the measured stream, but there are conditions where this intent may not be realized.

The IP Flow Performance Measurement (IPFPM) Internet-draft [18] is a method similar to those from Capello *et al.* [17]. Thus, this is a Hybrid Type I method as well. In the method, the stream is measured and time-stamped during that process to deliver network metrics. Thus, data packets are marked into different blocks of markers by changing one or more bits of packets without altering normal processing in the network. No additional delimiting packets are needed, and the measurement can be performed in-service without the insertion of additional (*i.e.,* synthetic) traffic.

D. Control of Measurement Mechanisms

Measurement mechanisms enable performance monitoring features in order to assess and analyze network efficiency. However, there is an inherently human and computational cost related to the deployment of measurement probes and their continuous 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. In addition, it is necessary to save network equipment resources, which are required for routing and switching. Thus, it is crucial to find the sweet spot considering each network infrastructure. 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 the 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 [19]. In active mechanisms, resource consumption also has an impact on the hosting devices. In this context, even active measurement protocol descriptions usually include advice on configuration parameters to limit the use of computational resources [10]. The cost of measurement mechanisms is strongly related to the size and complexity of network infrastructures. However, such cost also limits the monitoring target to being 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 is under such control but that an integrated approach can control several devices.

Network-wide control of measurement mechanisms can help network operators to better understand 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, network-wide control of measurements among multiple distributed probes can further improve measurement tasks.

III. Surveyed Initiatives of Network-Wide Approaches to Control Measurement Mechanisms

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. 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 [20]) 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). Thus, the complete list of relevant initiatives considering the selected keywords and inclusion and exclusion criteria are classified using the method present in Section III-A.

A. Method for the Literature Review

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.

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 management methods employed in 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 V). In the following, we briefly describe the features that we focus on this literature review.

Network measurements can be classified concerning 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 also be 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 make 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.

Initiatives on network-wide control of measurement mechanisms use different management methods to perform their tasks. We use of an existing and acknowledged network management taxonomy [21], considering 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.

The network-wide control of measurement mechanisms can aim at different application areas. In the literature review, we find five 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 separate some application areas effectively. In this context, we focus on the features explicitly stated as the main ones by the authors.

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 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*, *traffic observation points*, *flow monitoring*, *probe activation*, and *probe placement*. Alternative spellings and synonyms for these keywords are also considered, *e.g., active measurement* and *active monitoring*.

Inclusion and exclusion criteria were defined to adjust and calibrate the survey focus. We aim at network-wide approaches to control measurement mechanisms as our review topic. These criteria are used to delineate the final set of papers regarding this topic. The inclusion criteria are 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 in 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 approaches to evaluate their own proposals (experiments, case studies, etc).

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.

B. Papers Classification and Analysis

In this section, we adopt a classification proposed by dos Santos *et al.* [21] to categorize the selected papers in this survey. In Table II, 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 based on a template with information well defined to each proposal such as authors, proposal, addressed problem, advantages, and disadvantages.

Cantieni *et al.* [22] proposed an optimal algorithm to solve such problem given a network to monitor all links. Also, a formulation of the probe placement problem was performed. It is described a performance study considering measurement session activation and sampling rate for specific measurement task regarding accuracy and resource consumption. Finally, the authors discuss methods to deploy the proposed solution in real backbone networks. The applicability of this proposal is generic, also considering new NetFlow versions without modifications. Even though, the newer versions are increasing the amount of information exported in each record. One relevant negative aspect is about the optimization method is not specific regarding estimation origin-destination pair sizes.

Chaudet *et al.* [23] presented a combinatorial view of such problem from which it is derived complexity and approximability results. The study of 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. Besides that, the minimization of the number of measurement probes and the definition of optimal locations were performed regarding monitoring coverage goals. The authors proposes a very simple approach based on Mixed Integer Programming formulation to achieve the best way to position for a limited number of devices. In another side, the proposed solution offer good performance with POP limited between 15 and 29 routers.

CMON: Zang and Nucci [24] proposed a methodology to provide optimized coverage and lowest cost to the problem of deploying measurement probes in a real world network based either on NetFlow or CMON [41] solutions. The authors proposed solutions to enable a significant monitoring coverage using a significant portion of traffic instead of the entire traffic. It is done to save resources while at the same time giving administrators enough insight to their network. However, to reduce the operating costs, CMON uses a centralized management approach that has several limitations on current network scenarios such as scalability. It causes a proportional growth to in the computational load and network traffic to the management station according to increasing the number of managed

TABLE II
SUMMARY OF THE NETWORK-WIDE APPROACHES TO CONTROL MEASUREMENT MECHANISMS

Proposal	References	Intrusiveness	Distribution	Method Classification	Application
Cantieni et al.	[22]	Passive	Centralized	Optimization theories	Resource Consumption, Monitoring Accuracy
Chaudet et al.	[23]	Hybrid	Centralized	Optimization theories	Resource Consumption, Monitoring Coverage
CMON	[24]	Passive	Centralized	Optimization theories	Resource Consumption, Monitoring Coverage
cSamp	[25]	Passive	Centralized	Optimization theories	Resource Consumption, Monitoring Coverage
DECON	[26]	Passive	Distributed	Optimization theories	Resource Consumption, Monitoring Coverage
Eriksson et al.	[27]	Hybrid	Centralized	Machine learning and Genetic algorithms	Topology Discovery
Gangam and Fahmy	[28]	Active	Centralized	Experimental approach	Monitoring Accuracy
Kamiyama et al.	[19]	Passive	Distributed	Control theories	Resource Consumption, Monitoring Coverage
Lassoued et al.	[29]	Passive	Centralized	Control theories	Resource Consumption, Monitoring Accuracy
LEISURE	[30]	Passive	Centralized	Optimization theories	Resource Consumption
MMPR	[31]	Passive	Centralized	Optimization theories	Resource Consumption
NetQuest	[32]	Active	Centralized	Probabilistic, Stochastic processes, Queuing theory	Monitoring Accuracy
Nobre et al.	[33]	Active	Distributed	Probabilistic, Stochastic processes, Queuing theory	Resource Consumption, Monitoring Coverage
NSQM	[34]	Hybrid	Distributed	Experimental approach	Resource Consumption
Patil et al.	[35]	Active	Centralized	Control theories	Fault Localization
SLAm	[36]	Active	Centralized	Probabilistic, Stochastic processes, Queuing theory	Fault Localization
SPAND	[37]	Passive	Distributed	Experimental approach	Monitoring Accuracy
Suh et al.	[38]	Passive	Centralized	Optimization theories	Resource Consumption, Monitoring Coverage
Wren	[39]	Hybrid	Distributed	Experimental approach	Resource Consumption
MOZART	[40]	Passive	Centralized	Experimental approach	Resource Consumption

network devices. Also, when compared with NetFlow, CMON demonstrated costs about 4% more to deploy than NetFlow.

cSamp: Sekar *et al.* [25] 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. The engine performs such distribution 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. However, cSamp does not deal load-balancing of workloads for multiple measurement monitors. It could lead to high workloads for some monitors than others. Also, due to practical networks, this approach has limitations to identify origin-destination pairs from all packets. So, the authors proposed another solution, called cSamp-T [42], to use local information instead of the origin-destination pairs.

DECON: Di Pietro *et al.* [26] proposed DECON, a decentralized coordination system aimed at assigning monitoring probes. This proposal tries to maximize the number of flows monitored and removing redundancies. 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. However, this solution requires the consideration of the ownership cost of additional hardware due to the detached P2P overlay. Also, the authors did not discuss the handling of multipath flows in his paper.

Eriksson *et al.* [27] proposed a new methodology for inferring network structures from measurement data. The authors described 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. The authors extended his work [43], to resolve the distance in router hops between each pair of end hosts. They proposed a new method for accurately estimating the hop distances between arbitrary pairs of hosts in a network. The idea is the identification of the shortest paths between nodes in the failures case, making more robust overlay network design. In the end, the authors focused on a novel data analysis methodology to estimating pairwise hops using only massively incomplete pairwise measurements between the routers [44]. This proposal used a modified matrix completion technique that exploits network structure.

Gangam and Fahmy [28] modeled the measurement interference problem and showed the scheduling of measurement tasks to reduce interference and, then, increase measurement accuracy. The authors defined such problem considering that two active measurements are said to interfere when the injected packets of one measurement sessions 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. This proposal does not work with Atlas probes[1] as destinations for external measurements [45].

Kamiyama *et al.* [19] 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 the load balancing autonomously, probes exchange their load information with adjacent probes. Despite the presented autonomous features, the authors described that widely load oscillations and a large number of repetitions of the load-balancing procedure could occur in some settings.

Lassoued *et al.* [29] proposed a network-wide cognitive monitoring system. 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. However, this proposal does not explore to the real time adaptation of monitoring time T that is the focus on flow data analysis.

LEISURE: Chang *et al.* [30] 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 complete view of network behavior. Besides that, the authors consider different load-balancing objectives. However, the authors did not consider solutions to deal with LEISURE scalability issues regarding the employed centralized approach.

MMPR: Huang *et al.* [31] proposed MMPR (Measurement-aware Monitor Placement and Routing), a framework that jointly optimizes probe placement and dynamic routing strategy to achieve maximum measurement utility. Several heuristic algorithms are responsible for performing these functions. The authors claimed that their heuristic solutions could achieve measurement gains that are quite close to the optimal solutions while reducing the computation time. However, MMPR requires the prior knowledge of traffic importance in order to route flow sets differently and does not let monitors dynamically adjust their monitoring capability using sample rate.

NetQuest: Song *et al.* [32] propose NetQuest, a flexible framework for a 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 establishing a support of multiple users in several parts of the network. NetQuest is not concerned with achievement of the best performance from the measurement of the available bandwidth since it is more oriented to a wider knowledge of the general network status. However, the accuracy of this proposal depends on the amount of data collected.

Nobre *et al.* [46] studied the problem of prioritizing autonomically destinations for active measurement sessions regarding an SLA. The authors claimed that using a P2P measurement overlay is possible to decrease the use of human and computational resources regarding such sessions as well as to increase the monitoring coverage regarding a given time. The authors described the concept of correlated peers to enable P2P overlay provisioning [33] and the concept of virtual measurement sessions to enable the sharing of measurement results [47]. However, the authors did not enhance the individual measurement tasks that can be made by each measurement peer.

NSQM: Racz *et al.* [34] proposed the Network and Service Quality Measurement (NSQM) architecture, which integrates network- and service-specific measurements and can configure measurement probes dynamically to setup network-wide measurements in an automated manner. NSQM integrates both active and passive measurements and supports a measurement of a fine-grained selection of traffic to reduce the amount of collected and processed measurement data. Besides that, NSQM supports the correlation of measurement data from multiple locations. On the other hand, the authors do not describe how these values are linked and how could deduce service parameters on the network measurements.

Patil *et al.* [35] presented an approach for minimal measurement probe selection for fault localization purposes. Probe set for fault localization requires the minimal amount of time, and at the same time, the network in the identified problem areas should not be overwhelmed with the management traffic. The authors claim that the utilization of smaller probe sets reduces computational resources required to localize faults within a network infrastructure. Besides that, proposed algorithms also decrease the deployment cost of measurement probes on nodes and the activation of measurement sessions. However, the authors described that the employed approach lacks probe station selection based on nodes and links covered in order to detect node and link failures.

SLAm: Barford *et al.* [36] proposed a framework for detecting and localizing performance anomalies through of an active probe-enabled measurement infrastructure localized on the network periphery. This proposal considers the possibility of comparison between probe-based measures of performance characteristics with performance guarantees for the network. The authors aim at full coverage through decomposing end-to-end paths. After this decomposition, there is a selection of paths in which probes will be configured. This framework assumes a centralized controller for path selection. However,

[1]RIPE Atlas probes. Available: https://atlas.ripe.net.

the work did not address more complex anomaly scenarios (*e.g.,* multiple and non-persistent anomalies). Moreover, this proposal considers that routes have not changed.

SPAND: Seshan *et al.* [37] proposed Shared Passive Network Performance Discovery (SPAND), a system that determines network characteristics by making shared passive measurements from a collection of hosts. Sharing network states maintained by different flows can lead to significant improvement. The authors employed such measurement in order to replace the use of individual active ones while maintaining the accuracy, especially to avoid the injection of synthetic traffic. Besides that, SPAND can be used to address the use of redundant network probes by nearby hosts. However, SPAND does provide an achievable bandwidth metric, which is similar to the bulk transfer capacity metric [48].

Suh *et al.* [38] 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 the network. However, the proposed approach to solve the problem of the measurement probes and create a traffic load on the generated topologies need to perform traffic matrix estimation.

Wren: Zangrilli and Lowekamp [39] developed a bandwidth monitoring tool as part of the Wren network measurement system to decrease the measurement traffic on the network. The authors combine active and passive monitoring techniques to reduce the need for intrusive measurements. This measurement is made by passively obtaining measurements from existing application traffic whenever possible, instead of actively probing the network. When there is less traffic on the network, they use active measurements since the intrusiveness of active measurement sessions is bearable. Moreover, the authors demonstrate the principles supporting active bandwidth tools can be applied to passive traces of the LAN and WAN traffic generated by high-performance grid applications [49]. Nevertheless, the authors have previously analyzed the efficiency of the Wren, and it adds little overhead to the kernel.

MOZART: Liu *et al.* [40] proposed MOZART (MOnitor flowZ At the Right Time), which offers coordinated monitoring, efficient communications, and joint placement at selectors and monitors. The authors claim that the temporal coordination of network devices may be more efficient when the monitoring is to the right flows at the right time instead of monitoring all the flows all the time. MOZART achieves selective of flows of interest and improves on overall monitoring resource utilization with network operators. However, this proposal requires careful coordination in time and location of the monitoring.

In the following sections, we classify the presented initiatives to produce an integrated perspective of such initiatives. The formulation of this classification considers the review questions. After that, opportunities and challenges in network-wide approaches to control measurement mechanisms are described.

TABLE III
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.	NetFlow
CMON	NetFlow
Kamiyama et al. (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 et al. (2013)	Simulated Passive Mechanism
Gangam and Fahmy (2011)	Simulated Active Mechanism
Wren	Implemented Hybrid Mechanism

IV. Comparison of the Surveyed Initiatives of Network-Wide Approaches to Control Measurement Mechanisms

Whereas Section III surveys prominent research initiatives and their salient features, the present section compares these initiatives using a set of qualitative metrics. In particular, we evaluate each proposal using the following three criteria: intrusiveness of the measurement mechanism, distribution features, management methods, and application areas. In the following subsections, we will provide a more detailed discussion of each metric and the evaluation of the surveyed initiatives.

A. 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 II, such mechanisms can be classified as active, passive or hybrid 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. In addition, 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. Next, the steering of active measurements mechanisms is illustrated. Finally, control approaches that mix active and passive measurement mechanisms are presented. In Table III, we provide the specific measurement mechanisms controlled by such initiatives.

1) Control of Passive Measurement Mechanisms: Passive measurement mechanisms do not inject synthetic traffic that can influence actual network traffic. This non-intrusive nature is one of the most appealing features of such mechanisms. Therefore, it is expected that the control of passive measurement mechanisms will not be intrusive along with other characteristics. Several different mechanisms are used to passively collect data from network infrastructures, as shown in Section II-A.

As one of the most common passive measurement mechanisms, Cisco NetFlow is the most common in terms of initiatives to investigate network-wide control. Cantieni *et al.* [22] formulated the placement problem (also known as the 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.*[29] tackled a similar problem but with an emphasis on the maximum possible accuracy and adaptivity to changes in network traffic conditions. Also, di Pietro *et al.* [26] 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 also [24].

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) [50] as the measurement probe. cSamp (Coordinated Sampling) [25] provides flow sampling steering, hash-based packet selection, and the distribution of responsibilities across routers with the dissemination of the routing manifests for IPFIX-enabled Autonomous Systems (AS). Sekar *et al.* [42] proposed a variation of cSamp to use local information instead of the origin-destination pairs. Kamiyama *et al.* [19] 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 also be investigated using implementations developed for research reasons alone or simulated mechanisms. MMPR (Measurement-aware Monitor Placement and Routing) [31] and LEISURE (Load-EqualIzed meaSUREment) [30] used simulation experiments for evaluating solutions for probe placement and load balancing across distributed probes, respectively. Suh *et al.* [38] 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 accurately determine network characteristics [37].

The network-wide control of passive measurement mechanisms can use the advantages of collecting flows from different measurement probes. One of these advantages is to present a similar level of accuracy found in active measurements, but without the intrusiveness. In addition, 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) 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 II-B.

Some study initiatives developed an active measurement mechanisms to evaluate network-wide control characteristics. Barford *et al.* [36] 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 [51]. NetQuest is a framework to select active measurements that maximize the amount of information gained about the network path properties from active measurement sessions [32]. 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 *et al.* [35] presented an approach for fault localization that aims at minimal probe selection. The authors used simulation to evaluate such an approach. Gangam and Fahmy [28] 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 that use Cisco IPSLA and IETF TWAMP. One reason that could explain this is the shortage of readily available implementations. There are only partial TWAMP implementations publicly available. In the case of IPSLA, only the Cisco proprietary implementation is obtainable. In any case, this situation can change with the IPSLA protocol disclosure through an IETF RFC [9]. Furthermore, active measurement datasets are not readily available. Thus, it is difficult to perform evaluations considering real network infrastructures.

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 [39].

Hybrid network-wide control can be deployed to decrease resource consumption. Zangrilli and Lowekamp [39] proposed the Wren bandwidth monitoring tool, which aims at 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 [34]. Chaudet *et al.* [23] 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 *et al.* [27] described a methodology for inferring network structure from passive and active

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

measurements, which can recover from missing information on the measurements.

Passive and active measurement mechanisms have different characteristics and produce network performance data with particular properties. For example, an 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 is possible to say that hybrid network-wide control is less investigated than the control of each kind of mechanism separately. One possible reason for this is the difficulty in integrating different data and configuration models from passive and active measurement mechanisms.

B. Distribution Aspects of the Control of Measurement Mechanisms

The control of measurement mechanisms does not follow the distribution features of the mechanisms themselves. Despite the fact that there is not a widely accepted taxonomy that defines and characterizes the distribution aspects of network management models, network management studies usually consider distribution aspects that bring, at least, centralized and distributed (or decentralized) models (*e.g.,* [52]–[55]). In addition to being effectively accepted in the 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 system scalability is a common classification approach [53]. In the present work, we do not employ a specific taxonomy, nor do we propose a new one; however, we use a simplified taxonomy considering only centralized and distributed control. The main aspect used for our classification is the local to perform the majority of the control logic.

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

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 Fig. 3, we present a model of a centralized control. This model seems to be the most common distribution model. In such control, the management station connects passive or active measurement probes which perform the control logic. The management station configures such probes, in addition to running management applications (*e.g.,* traffic engineering). Typically hosted on network devices, measurement probes are limited to collecting data and sending, either synchronously or asynchronously, measurement results.

The central station can integrate the measurement data to provide a potential view of a larger network. In this context, centralized approaches ease the enforcement of more general measurement policies, *e.g.,* handling specific flows in different portions of the network. However, it is necessary to enable measurement probes to inform the central station about their results (and state) and support configuration and deployment from a centralized point of view. For example, the distribution of responsibilities across management elements can be done through the dissemination of “manifests” [25].

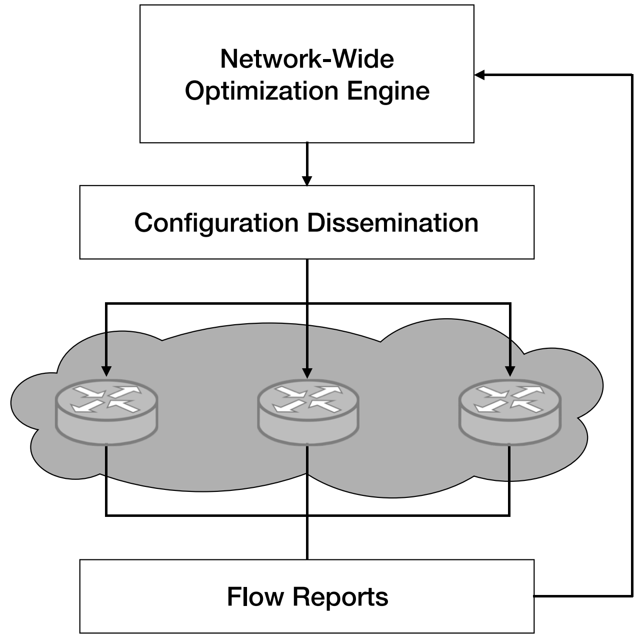


Fig. 3. Centralized Control of Measurement Mechanisms Model. Adapted from Sekar *et al.* [25]

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 common approach considering [23]–[25], [30], [31], and [38]. Some solutions employed in centralized controllers of measurement mechanisms are outside the spectrum of linear and integer programming ([22], [27]–[29], [32], [35], [36]).

The use of a centralized control could reduce management complexity and operating costs. However, centralized management approaches, despite being widespread, have several limitations in current network environments [56]. One of these limitations is related to scalability since an increase in the number of managed network devices turns out to proportionally increase 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) Distributed Control of Measurement Mechanisms: The control of measurement mechanisms can be performed in a distributed fashion. In Fig. 4, we present a model of a distributed control. Distribution features can be employed to improve the control task with respect to scalability, flexibility, and robustness [54]. In any case, there is a close relationship between the network infrastructure and the way that 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

TABLE IV
SUMMARY OF THE MANAGEMENT METHODS EMPLOYED BY NETWORK-WIDE APPROACHES

Proposal	Method Classification	Management Method
Cantieni et al.	Optimization theories	Lagrange multipliers
Chaudet et al.	Optimization theories	Mixed integer linear programming
CMON	Optimization theories	Integer linear programming
cSamp	Optimization theories	Linear programming
DECON	Optimization theories	Batch optimization
Eriksson et al.	Machine learning and genetic algorithms	Clustering
Gangam and Fahmy	Experimental approach	Measurement scheduling
Kamiyama et al.	Control theories	Autonomic computing
Lassoued et al.	Control theories	Autonomic computing
LEISURE	Optimization theories	Mixed integer linear programming
MMPR	Optimization theories	Mixed integer linear programming
NetQuest	Probabilistic, stochastic processes, queuing theory	Bayesian experimental design
Nobre et al.	Probabilistic, stochastic processes, queuing theory	Path weighting
NSQM	Experimental approach	Measurement task classification
Patil et al.	Control theories	Adaptive probing
SLAm	Probabilistic, stochastic processes, queuing theory	Path weighting
SPAND	Experimental approach	Measurement results sharing
Suh et al.	Optimization theories	Mixed Integer non-linear program
Wren	Experimental approach	Application monitoring
MOZART	Experimental approach	Temporal coordination

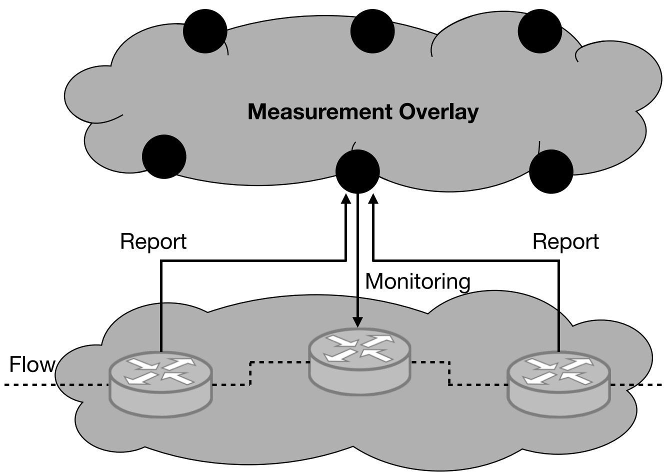


Fig. 4. Distributed Control of Measurement Mechanisms Model. Adapted from di Pietro *et al.* [26]

the network-wide distributed control. In addition, different ways accept the measurement data distribution.

P2P technology can be employed to control measurement mechanisms. This technology is known to be successful regarding the support of different types of applications. For example, DECON [26] employs a detached P2P coordination system 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 or packet marking. Considering grid environments, Zangrilli and Lowekamp [39] proposed a bandwidth monitoring tool to adapt measurement mechanisms for changing network conditions and to make efficient use of grid resources.

Measurement sharing can be employed to organize the control system and to feed the control process itself. For example, SPAND [37] 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 [34] supports the correlation of measurement data from multiple locations, enabling the localization of faulty links. In addition, NSQM can use measurement data correlation to control the aggregation level used by the measurement probes. Finally, Kamiyama *et al.* [19] 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). In addition, 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 the 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).

C. Management Methods Employed on the Network-Wide Control of Measurement Mechanisms

Network-Wide Control of Measurement Mechanisms can be performed using several management methods. Such methods are used to support different features in measurement systems, such as the ability to process large amounts of measurement results. In this context, a network-wide control can enhance an integrated deployment of management methods for measurement mechanisms. For example, management methods could be used to steer such control in order to adjust distinct network environments.

The management methods used to classify the initiatives surveyed in the present literature review were proposed by dos Santos *et al.* [21]. Such methods are control theories; optimization theories; machine learning and genetic algorithms; logics; probabilistic, stochastic processes, queuing theory; simulation; experimental approach; design; monitoring & measurements; economic theories; and data mining and (big) data analytics. A summary of the classification described in the present section is described in Table IV. Next, we depict the methods found in our survey.

Control theories: Some research initiatives used control theories to control measurement mechanisms considering dynamic and localized characteristics of network environments and the measurement results. Kamiyama *et al.* [19] proposed an autonomic load balancing method to maximize the number of monitored IPFIX flows in the entire network. The authors employed information exchange about load within adjacent probes to assure such balancing. Lassoued *et al.* [29] employed a self-configuring adaptive system to achieve maximum accuracy and adaptivity to changes in network traffic conditions. The authors were inspired by the adaptation process used by TCP for the adjustment of its congestion window and use the gradient Projection Method to identify the monitors that should be reconfigured. Patil *et al.* [35] proposed an approach to defining a minimal probe selection for fault localization. The authors developed an adaptive probing strategy based on the iterative use of additional measurement sessions to obtain further information about network faults.

Optimization theories: A common approach for the network-wide control of measurement mechanisms is to employ optimization frameworks. In fact, it is possible to argue that this is the most used approach considering the literature. For example, several linear and integer programming formulations are used: MILP (Mixed Integer Linear Programming) to optimize the probe placement [31], the load balance of network measurement workloads [30], and the number of required probes [23]; Integer Linear Program (ILP) to optimize the number of probes required to cover a major portion of network traffic [24]; Mixed Integer Non-Linear program (MINLP) to optimize probe placement and packet sampling [38]; and Linear Programming (LP) to perform probe placement, flow sampling and hash-based packet selection [25]. DECON uses batch optimization to reduce messaging overhead in monitoring reports and response messages directed to a monitoring probe [26]. Finally, Cantieni *et al.* applied Lagrange multipliers to formulate which probes should be activated and which sampling rate should be set on such probes in order to achieve a given measurement task.

Machine learning and genetic algorithms: Management methods related to machine learning and genetic algorithms features can be embedded into the network-wide control of measurement mechanisms. In this context, Eriksson *et al.* [27] described a methodology for inferring network structure that can recover from missing information on the measurements. This methodology defines the use of clustering techniques considering traffic sources to infer network infrastructure from passive and active measurement results [27].

Probabilistic, stochastic processes, queuing theory: Methods from probabilistic, stochastic processes and queuing theory can address the network-wide control measurement mechanisms. Non-deterministic methods can be more efficient than deterministic ones for specific scenarios. NetQuest proposed the use of Bayesian experimental design to select active measurement sessions that maximize the amount of information gained about the network path properties [32]. Barford *et al.* [36] proposed a framework network-wide SLA probing using local path weights. Such weights enable a probabilistic monitoring coverage. Nobre *et al.* [46] also proposed the use of path weights but considering local and remote measurements regarding a node. Correlation functions assure the relevance of remote measurement.

Experimental approach: Since most of the surveyed initiatives stated that the problem formulations are NP-hard, several heuristic algorithms are proposed and evaluated. These heuristics are the materialization of experimental approaches to control measurement mechanisms and consider different aspects of such mechanisms. Gangam and Fahmy [28] proposed algorithms for measurement scheduling to reduce interference through the decrease of the total completion time of measurement tasks. MOZART proposed temporal coordination to maximize the monitoring accuracy while staying within memory constraints [40]. NSQM integrates active and passive measurement mechanisms in order to reduce the amount of measurement data to be collected and processed [34]. NSQM employed the classification of measurement tasks in types and modes to deliver QoS metrics. Zangrilli and Lowekamp [39] also integrated different kinds of measurement mechanisms to reduce the mean measurement burden on the network. This is done monitoring the running state of a target application to decide the use of more intrusive measurements. SPAND employed the sharing of passive measurement results to determine network characteristics accurately [37].

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

Several different application areas can employ network-wide control of measurement mechanisms. Such areas can be used to group applications that aim to achieve similar goals. As mentioned in Section II, 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 with respect to their main features.

In this section, we describe initiatives on the network-wide control of measurement mechanisms with respect to the application area. In Fig. 5, we present the classification of such initiatives. It is important to emphasize that an initiative may address more than one application area. Then, we describe in more detail each of them. Initially, the applications that have the resource consumption as the main area are presented. After that, the steering of measurement mechanisms for monitoring accuracy purposes is represented. Then, applications that perform fault localization are illustrated. Subsequently, applications that focus on monitoring coverage area presented. Finally, we describe the utilization of network-wide control of measurement mechanisms for topology discovery.

1) Resource Consumption: One of the most common application areas 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

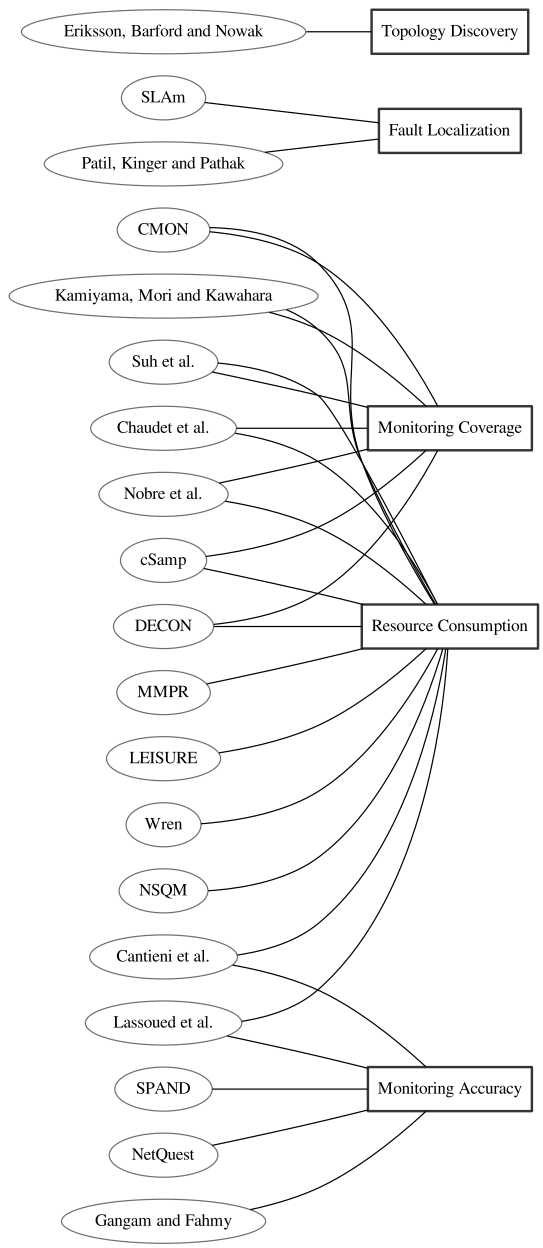


Fig. 5. Classification of Network-Wide Control of Measurement Mechanisms in Respect to Application Area.

mechanism control can reduce the number of 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 [25], DECON [26], LEISURE [30], Chaudet *et al.* [23], and Patil *et al.* [35] use such frameworks. The employment of heuristic algorithms is present in some initiatives, such as Suh *et al.* [38] and MMPR [31]. Finally, the correlation of different measurements is specially employed in hybrid (active and passive) approaches, *e.g.,* NSQM [34] and Zangrilli and Lowekamp [39] in order to choose a less intrusive mechanism when it is feasible.

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 mechanisms to concurrently perform several sessions (possibly from different network administrators), which can interfere with each other.

The location of measurement probes affects monitoring accuracy. Thus, some initiatives try to address the issue through the formulation of the placement problem (also known as location problem), such as Cantieni *et al.* [22] and Lassoued *et al.* [29]. SPAND employs information sharing between probes to increase measurement accuracy [37]. NetQuest selects active measurement sessions that maximize the amount of information gained about the network path properties [32]. Finally, Gangam and Fahmy [28] proposed a solution to schedule measurement tasks to avoid measurement interference.

3) Fault Localization: Network measurements are essential for identifying and locating network problems. In this context, fault diagnosis is usually the first step in 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. In addition, 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 is carried out to perform diagnostics. In this context, active measurement mechanisms are the prime choice for fault localization. Patil *et al.* [35] presented an approach for fault localization that aims at the minimal multi-path selection. Barford *et al.* [36] proposed a framework for identifying and localizing network-wide service level performance anomalies through the unification of the results from different measurement sessions.

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 better monitoring coverage.

Several initiatives presented in the present literature review emphasize network-wide monitoring coverage goals while respecting (and possibly decreasing) resource consumption. This is usually done to address the placement problem and packet sampling. cSamp [25], DECON [26], Suh *et al.* [38], Chaudet *et al.* [23], CMON [24], and Kamiyama *et al.* [19] are examples of such initiatives.

5) Topology Discovery: The network-wide control of measurement mechanisms can be used to perform topology discovery. Understanding network infrastructure through empirical measurements is essential for different network management tasks, such as traffic engineering and troubleshooting [27]. However, there is an inherent trade-off between the number and 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 an *ad hoc* manner. Eriksson *et al.* [27] described a methodology for inferring network structure from passive and active measurements, which can recover from missing information on such measurements.

V. 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 in several contexts and for different ends. However, there are limitations on such use, especially 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 of network infrastructures.

As the survey described in this paper 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 [10]). In addition, some control approaches aim at single devices, *e.g.,* setting the default configuration on the resource that uses limits for low values. We chose to focus only on network-wide approaches since they can provide a larger impact on the network infrastructure as a 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 that could potentially attract more attention. Examples of these areas are the architecture and relationship of test and control protocols as well as measurement federations and approaches to deploying large-scale measurements.

Some measurement mechanisms 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 [11]). In addition, 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 the case of IPFIX [4]). The control of measurement mechanisms of a network-wide could exploit the relationship of these protocols and localization of roles. 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 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 [10].

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 ensure 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 many 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. In addition, there are some standardization efforts to make large-scale performance measurement platforms interoperable. An example of such efforts is the IETF-chartered Large-Scale Measurement of Broadband Performance (LMAP) Working Group (WG).[7] Bajpai and Schönwälder [57] provided a survey describing measurement federations as well as large-scale measurement standardization efforts. In any case, in the context of a network-wide control, the LMAP WG currently considers out of scope several important features such as discovering and provisioning the MAs, a management protocol for MA bootstrapping, and MA coordination and information sharing.

VI. Related Work

Network-wide control of measurement mechanisms can play an important role in the current practice of Internet measurement. However, to the best of our knowledge, there is no specific survey or tutorial on such control. In this context, a few related reviews discuss similar aspects to the survey described in the present article. In this section, we present 3 survey articles that we consider work related to the present investigation.

Li *et al.* [58] presented a survey on network flow applications with emphasis on NetFlow. The authors also provided a brief introduction to other standards, such as sFlow, and on network traffic analysis. The authors pointed out the rise of machine learning and network security as emerging research topics. Finally, they present challenges, future directions, and ideas for potential integration regarding such applications. However, this survey only focuses on passive measurement mechanisms, especially Cisco-based. In addition, there is no specific analysis of network-wide control despite the fact that some applications require this kind of control.

Duffield [20] presented a survey on packet sampling regarding passive measurements. The authors described the classical sampling methodology in the context of Internet measurements

[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/.
[7]Large-Scale Measurement of Broadband Performance (LMAP) Working Group (WG) - http://datatracker.ietf.org/wg/lmap/.

and newer applications and sampling methods. In addition, the authors identified emerging areas in packet sampling, with the special focus on the application of statistical expertise to improve such sampling. However, this survey only focuses on packet sampling of passive measurement mechanisms. Despite the fact that there are network-wide mechanisms focused on the control of packet sampling in passive measurement, there is no specific analysis of these mechanisms.

Bajpai and Schönwälder [57] presented a survey on the Internet measurement platforms. The authors provided a taxonomy of these measurement platforms on the basis of their deployment use-case. In addition, the authors described standardization efforts to make large-scale performance measurement platforms interoperable. However, this survey is only focused on measurement platforms, especially those who promote toolkits for measurement federations. Despite the related work being closer to the survey described in the present article, there are significant differences that should be mentioned. First, the survey is restricted to only measurement platforms, but there are several network-wide mechanisms to control measurement mechanisms that do not consider such platforms. Finally, the authors did not employ a published (and peer-reviewed) taxonomy. The taxonomy used in the present article [21] reflects the experience produced in the network management literature, which can strengthen the classification.

VII. Final Remarks

Network monitoring is becoming more important because of the number of critical services that network infrastructures support as well. In order to uncover network behavior, it is necessary to employ both active, passive, and hybrid measurement mechanisms. However, there are several challenges concerning such mechanisms, such as those related to 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 single devices. In the present literature review, we focus on the network-wide since in order to reveal global network behavior, it is usually necessary to go beyond single measurement sessions. The network-wide control of measurement mechanisms can be deployed at 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 research initiatives is usually NP-hard, and the parameters are dynamic.

In summary, an efficient network-wide control of measurement mechanisms is still difficult task in spite of the new research advances. Members of the Network Management Research Group (NMRG) of the Internet Research Task Force (IRTF) highlighted some of the research challenges to be investigated on future network and services management [59]. Among these challenges, large-scale network-wide measurements, network-wide configuration, and autonomic management were reported. 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.

References

[1] V. Sekar, R. Krishnaswamy, A. Gupta, and M. K. Reiter, "Network-wide deployment of intrusion detection and prevention systems," in *Proc. 6th Int. Conf. Co NEXT*, Philadelphia, PA, USA, 2010, pp. 1–12. [Online]. Available: http://doi.acm.org/10.1145/1921168.1921192

[2] F. Baker, B. Foster, and C. Sharp, "Cisco architecture for lawful intercept in IP networks," Internet Eng. Task Force, Marina del Rey, CA, USA, RFC 3924 (Informational), Oct. 2004.

[3] "ISO/IEC 7498-4, information technology, open systems interconnection, basic reference model: Management framework," Joint Tech. Committee ISO/IEC, Geneva, Switzerland, Rep. 7498-1:1994, 1994.

[4] B. Claise, "Specification of the IP flow information export (IPFIX) protocol for the exchange of IP traffic flow information," Internet Eng. Task Force, Marina del Rey, CA, USA, RFC 5101 (Standard), Jan. 2008.

[5] N. Brownlee, C. Mills, and G. Ruth, "Traffic flow measurement: Architecture," Internet Eng. Task Force, Marina del Rey, CA, USA, RFC 2722 (Informational), Oct. 1999.

[6] N. Brownlee, "RTFM: Applicability statement," Internet Eng. Task Force, Marina del Rey, CA, USA, RFC 2721 (Informational), Oct. 1999.

[7] P. Phaal, S. Panchen, and N. McKee, "InMon corporation's sFlow: A method for monitoring traffic in switched and routed networks," Internet Eng. Task Force, Marina del Rey, CA, USA, RFC 3176 (Informational), Sep. 2001.

[8] B. Claise, "Cisco systems netflow services export version 9," Internet Eng. Task Force, Marina del Rey, CA, USA, RFC 3954 (Informational), Oct. 2004.

[9] M. S. Chiba *et al.*, "Cisco service-level assurance protocol," Internet Eng. Task Force, Marina del Rey, CA, USA, RFC 6812 (Informational), Jan. 2013.

[10] S. Shalunov, B. Teitelbaum, A. Karp, J. Boote, and M. Zekauskas, "A one-way active measurement protocol (OWAMP)," Internet Eng. Task Force, Marina del Rey, CA, USA, RFC 4656 (Proposed Standard), Sep. 2006.

[11] K. Hedayat, R. Krzanowski, A. Morton, K. Yum, and J. Babiarz, "A two-way active measurement protocol (TWAMP)," Internet Eng. Task Force, Marina del Rey, CA, USA, RFC 5357 (Proposed Standard), Oct. 2008.

[12] "ITU-T recommendation Y.1540—Internet protocol data communication service—IP packet transfer and availability performance parameters," Int. Telecommun. Union, Geneva, Switzerland, Rep. 1540, 1999.

[13] N. Seitz, "ITU-T QoS standards for IP-based networks," *IEEE Commun. Mag.*, vol. 41, no. 6, pp. 82–89, Jun. 2003, doi: 10.1109/MCOM.2003.1204752.

[14] A. Morton, "Active and passive metrics and methods (with hybrid types in-between)," Internet Eng. Task Force, Marina del Rey, CA, USA, RFC 7799 (Informational), May 2016.

[15] E. Stephan, L. Liang, and A. Morton, "IP performance metrics (IPPM): Spatial and multicast," Internet Eng. Task Force, Marina del Rey, CA, USA, RFC 5644 (Informational), Oct. 2009.

[16] N. Elkins, R. Hamilton, and M. Ackermann, "IPv6 option header for performance and diagnostic measurements (PDM)," Work in progress as an Internet-Draft, Internet Eng. Task Force, Marina del Rey, CA, USA, Sep. 2016.

[17] A. Capello, M. Cociglio, L. Castaldelli, and A. T. Bonda, "A packet based method for passive performance monitoring," Internet-Draft, Internet Eng. Task Force, Marina del Rey, CA, USA, Feb. 2014.

[18] M. Chen, L. Zheng, G. Mirsky, G. Fioccola, and T. Mizrahi, "IP flow performance measurement framework," Internet-Draft, Internet Eng. Task Force, Marina del Rey, CA, USA, Sep. 2016.

[19] N. Kamiyama, T. Mori, and R. Kawahara, "Autonomic load balancing of flow monitors," *Comput. Netw.*, vol. 57, no. 3, pp. 741–761, Feb. 2013, doi: 10.1016/j.comnet.2012.10.018.

[20] N. Duffield, "Sampling for passive Internet measurement: A review," *Stat. Sci.*, vol. 19, no. 3, pp. 472–498, Aug. 2004. [Online]. Available: http://www.jstor.org/stable/4144398

[21] C. R. P. dos Santos *et al.*, "Taxonomy for the network and service management research field," *J. Netw. Syst. Manag.*, vol. 24, no. 3, pp. 764–787, Jul. 2016, doi: 10.1007/s10922-015-9363-7.

[22] G. R. Cantieni, G. Iannaccone, C. Barakat, C. Diot, and P. Thiran, "Reformulating the monitor placement problem: Optimal network-wide sampling," in *Proc. ACM Conf. Emerg. Netw. Exp. Technol. (CoNEXT)*, Lisbon, Portugal, Dec. 2006, pp. 1–12.

[23] C. Chaudet, E. Fleury, I. G. Lassous, H. Rivano, and M.-E. Voge, "Optimal positioning of active and passive monitoring devices," in *Proc. ACM Conf. Emerg. Netw. Exp. Technol. (CoNEXT)*, Toulouse, France, 2005, pp. 71–82.

[24] H. Zang and A. Nucci, "Traffic monitor deployment in IP networks," *Comput. Netw.*, vol. 53, no. 14, pp. 2491–2501, Sep. 2009, doi: 10.1016/j.comnet.2009.05.004.

[25] V. Sekar *et al.*, "CSAMP: A system for network-wide flow monitoring," in *Proc. USENIX Symp. Netw. Syst. Design Implement. (NSDI)*, San Francisco, CA, USA, Apr. 2008, pp. 233–246.

[26] A. di Pietro, F. Huici, D. Costantini, and S. Niccolini, "DECON: Decentralized coordination for large-scale flow monitoring," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, San Diego, CA, USA, Mar. 2010, pp. 1–5.

[27] B. Eriksson, P. Barford, and R. Nowak, "Network discovery from passive measurements," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 4, pp. 291–302, Oct. 2008. [Online]. Available: http://doi.acm.org/10.1145/1402946.1402992

[28] S. Gangam and S. Fahmy, "Mitigating interference in a network measurement service," in *Proc. IEEE Int. Workshop Qual. Service (IWQoS)*, San Jose, CA, USA, Jun. 2011, pp. 1–9.

[29] I. Lassoued, A. Krifa, C. Barakat, and K. Avrachenkov, "Network-wide monitoring through self-configuring adaptive system," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Shanghai, China, Apr. 2011, pp. 1826–1834.

[30] C.-W. Chang, G. Huang, B. Lin, and C.-N. Chuah, "LEISURE: Load-balanced network-wide traffic measurement and monitor placement," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 1059–1070, Apr. 2015, doi: 10.1109/TPDS.2013.188.

[31] G. Huang, C.-W. Chang, C.-N. Chuah, and B. Lin, "Measurement-aware monitor placement and routing: A joint optimization approach for network-wide measurements," *IEEE Trans. Netw. Service Manag.*, vol. 9, no. 1, pp. 48–59, Mar. 2012, doi: 10.1109/TNSM.2012.010912.110128.

[32] H. H. Song, L. Qiu, and Y. Zhang, "NetQuest: A flexible framework for large-scale network measurement," *SIGMETRICS Perform. Eval. Rev.*, vol. 34, no. 1, pp. 121–132, Jun. 2006. [Online]. Available: http://doi.acm.org/10.1145/1140103.1140293

[33] J. C. Nobre, L. Z. Granville, A. Clemm, and A. G. Prieto, "Decentralized detection of SLA violations using P2P technology," in *Proc. 8th Int. Conf. Netw. Service Manag. (CNSM)*, Las Vegas, NV, USA, Oct. 2012, pp. 100–107.

[34] P. Racz, D. Donni, and B. Stiller, "An architecture and implementation for IP network and service quality measurements," in *Proc. IEEE Netw. Oper. Manag. Symp. (NOMS)*, Osaka, Japan, Apr. 2010, pp. 24–31.

[35] B. Patil, S. Kinger, and V. K. Pathak, "Probe station placement algorithm for probe set reduction in network fault localization," in *Proc. Int. Conf. Inf. Syst. Comput. Netw. (ISCON)*, Mar. 2013, pp. 164–169, doi: 10.1109/ICISCON.2013.6524195.

[36] P. Barford, N. Duffield, A. Ron, and J. Sommers, "Network performance anomaly detection and localization," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Rio de Janeiro, Brazil, Apr. 2009, pp. 1377–1385.

[37] S. Seshan, M. Stemm, and R. H. Katz, "SPAND: Shared passive network performance discovery," in *Proc. USENIX Symp. Internet Technol. Syst. (USITS)*, Monterey, CA, USA, 1997, pp. 1–13.

[38] K. Suh, Y. Guo, J. Kurose, and D. Towsley, "Locating network monitors: Complexity, heuristics, and coverage," *Comput. Commun.*, vol. 29, no. 10, pp. 1564–1577, Jun. 2006, doi: 10.1016/j.comcom.2005.07.009.

[39] M. Zangrilli and B. B. Lowekamp, "Comparing passive network monitoring of grid application traffic with active probes," in *Proc. 4th Int. Workshop Grid Comput.*, Phoenix, AZ, USA, Nov. 2003, pp. 84–91.

[40] X. Liu, M. Shirazipour, M. Yu, and Y. Zhang, "MOZART: Temporal coordination of measurement," in *Proc. Symp. SDN Res.*, Santa Clara, CA, USA, 2016, pp. 1–12. [Online]. Available: http://doi.acm.org/10.1145/2890955.2890964

[41] G. Iannaccone, S. Bhattacharyya, N. Taft, and C. Diot, "Always-on monitoring of IP backbones: Requirements and design challenges," Sprint ATL, Burlingame, CA, USA, Sprint ATL Res. Rep. RR03-ATL-071821, 2003.

[42] V. Sekar, A. Gupta, M. K. Reiter, and H. Zhang, "Coordinated sampling sans origin-destination identifiers: Algorithms and analysis," in *Proc. 2nd Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bengaluru, India, 2010, pp. 1–10.

[43] B. Eriksson, P. Barford, and R. Nowak, "Estimating hop distance between arbitrary host pairs," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Rio de Janeiro, Brazil, 2009, pp. 801–809.

[44] B. Eriksson, P. Barford, J. Sommers, and R. Nowak, "DomainImpute: Inferring unseen components in the Internet," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Shanghai, China, 2011, pp. 171–175.

[45] T. Holterbach, C. Pelsser, R. Bush, and L. Vanbever, "Quantifying interference between measurements on the RIPE atlas platform," in *Proc. ACM Conf. Internet Meas. Conf.*, Tokyo, Japan, 2015, pp. 437–443.

[46] J. C. Nobre, L. Z. Granville, A. Clemm, and A. G. Prieto, "Coordination in P2P management overlays to improve decentralized detection of SLA violations," in *Proc. 28th IEEE Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Budapest, Hungary, May 2014, pp. 3456–3460.

[47] J. C. Nobre, L. Z. Granville, A. Clemm, and A. G. Prieto, "On the use of traffic information to improve the coordinated P2P detection of SLA violations," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Victoria, BC, Canada, Jun. 2013, pp. 613–620.

[48] M. Mathis and M. Allman, "A framework for defining empirical bulk transfer capacity metrics," Internet Eng. Task Force, Fremont, CA, USA, Rep. RFC 3148, 2001.

[49] M. Zangrilli and B. B. Lowekamp, "Using passive traces of application traffic in a network monitoring system," in *Proc. 13th IEEE Int. Symp. High Perform. Distrib. Comput.*, Honolulu, HI, USA, Jun. 2004, pp. 77–86.

[50] C. M. Inacio and B. Trammell, "YAF: Yet another flowmeter," in *Proc. USENIX Int. Conf. Large Installation Syst. Admin. (LISA)*, 2010, pp. 1–16.

[51] J. Sommers, P. Barford, N. Duffield, and A. Ron, "Accurate and efficient SLA compliance monitoring," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 4, pp. 109–120, Oct. 2007. [Online]. Available: http://doi.acm.org/10.1145/1282427.1282394

[52] G. Pavlou, "On the evolution of management approaches, frameworks and protocols: A historical perspective," *J. Netw. Syst. Manag.*, vol. 15, no. 4, pp. 425–445, Nov. 2007, doi: 10.1007/s10922-007-9082-9.

[53] J. Schonwalder, J. Quittek, and C. Kappler, "Building distributed management applications with the IETF script MIB," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 5, pp. 702–714, May 2000, doi: 10.1109/49.842986.

[54] J.-P. Martin-Flatin, S. Znaty, and J.-P. Habaux, "A survey of distributed enterprise network and systems management paradigms," *J. Netw. Syst. Manag.*, vol. 7, no. 1, pp. 9–26, 1999, doi: 10.1023/A:1018761615354.

[55] A. Leinwand and K. F. Condroy, *Network Management: A Practical Perspective*, 2nd ed. Boston, MA, USA: Addison-Wesley, 1996.

[56] A. Pras *et al.*, "Key research challenges in network management," *IEEE Commun. Mag.*, vol. 45, no. 10, pp. 104–110, Oct. 2007, doi: 10.1109/MCOM.2007.4342832.

[57] V. Bajpai and J. Schönwälder, "A survey on Internet performance measurement platforms and related standardization efforts," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1313–1341, 3rd Quart., 2015, doi: 10.1109/COMST.2015.2418435.

[58] B. Li, J. Springer, G. Bebis, and M. H. Gunes, "A survey of network flow applications," *J. Netw. Comput. Appl.*, vol. 36, no. 2, pp. 567–581, Mar. 2013, doi: 10.1016/j.jnca.2012.12.020.

[59] L. Z. Granville and O. Festor, *Network Management Research Group Status Report 2012*, Internet Res. Task Force, Marina del Rey, CA, USA, Aug. 2012.

Jéferson Campos Nobre received the B.Sc. degree in electrical engineering and the M.Sc. and Ph.D. degrees in computer science from the Federal University of Rio Grande do Sul, Brazil. He is an Associate Professor with the University of Vale do Rio dos Sinos, Brazil. His main topics of interest include distributed network management, delay/disruption-tolerant networking management, autonomic network management, and network measurements.

Bruno Augusti Mozzaquatro received the master's degree from the Federal University of Santa Maria (UFSM), Brazil. He is currently pursuing the Ph.D. degree with the New University of Lisbon, Portugal. He worked with anomaly-based intrusion detection and signal processing techniques with UFSM, where he is a Professor with Polytechnic School. His research interests include network management, security of the computer networks, and ontologies specification.

Lisandro Zambenedetti Granville is an Associate Professor with the Federal University of Rio Grande do Sul. He served as the TPC Co-Chair of IFIP/IEEE DSOM 2007 and IFIP/IEEE NOMS 2010, the General Co-Chair of IFIP/IEEE CNSM 2014, the TPC Co-Chair of IEEE NetSoft 2018, and the TPC Vice-Chair do IEEE ICC 2018. He is the Co-Chair of the IRTFs Network Management Research Group and the President of the Brazilian Computer Society. His interests include network management, software-defined networking, and network functions virtualization.