Configurable Monitoring for Multi-domain Networks

Aymen Belghith, Bernard Cousin, Samer Lahoud

OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Configurable Monitoring for Multi-domain Networks

Aymen Belghith[1], Bernard Cousin[2], and Samer Lahoud[2]
*University of Sfax, Road of Aeroport Km 0.5, 3029 Sfax, Tunisia
Email: aymen.belghith@gmail.com
**University of Rennes 1- IRISA, Campus de Beaulieu, 35042 Rennes Cedex, France
Email: {bernard.cousin, samer.lahoud}@irisa.fr

ABSTRACT: *In this paper, we review the state-of-the-art monitoring architectures proposed for multi-domain networks. We establish the five requirements a multi-domain monitoring architecture must fulfilled. We note that these architectures do not support measurement configuration that enables the providers to perform flexible multi-domain measurements. Therefore, we propose a configurable multi-domain network monitoring architecture in order to give more flexibility in monitoring and solve the heterogeneity and interoperability problems. We also propose two collaboration schemes that can be applied in our configurable monitoring architecture. These collaboration schemes are based on the proactive selection and the reactive selection. We show through extensive simulations that the proactive collaboration scheme provides a more flexible multi-domain monitoring and reduces the delay and the overload of the monitoring establishment.*

I. INTRODUCTION

Network monitoring is necessary to guarantee precise and efficient management of a network communication system. It is required to control the Quality of Service (QoS) provided by the network. The performance requirements of the services are typically specified through a contract called Service Level Agreement (SLA). In order to guarantee the performance of the services, the network performance has to be verified by performing measurements on well chosen metrics. Once the metrics to be measured are determined, it is required to define the monitoring architecture to be used. A monitoring architecture can be based on standard protocols, proposed for intra-domain networks, or proposed for multi-domain networks.

Many monitoring architectures were standardized such as Real-time Traffic Flow Measurement (RTFM), IP Flow Information eXport (IPFIX), and Packet Sampling (PSAMP). The architecture of RTFM [1] contains four components: a manager that configures the measurement points (meters), a meter that performs the measurements, a meter reader that exports the results, and an analysis application that analyzes the results. The architectures of IPFIX [2] and PSAMP [3] contain three processes: a metering process which performs the measurements, an exporting process which exports the results, and a collecting process which analyzes the results. The major difference between these architectures is that PSAMP exports information about individual packets while IPFIX exports information about flows.

Some monitoring architectures were proposed for intra-domain networks. For example, the monitoring architecture of AQUILA [4] contains three tools: a tool that produces traffic that emulates the traffic generated by the Internet applications, a tool that injects probes into the network to evaluate the performance of a defined path, and a tool that monitors the QoS parameters. The intra-domain monitoring architecture proposed in [5] contains two services: a measurement service that measures a set of metrics and stores the results in a database and an evaluation and violation detection service that retrieves the results from the database, analyzes them, and sends notifications when detecting violations.

All the above architectures do not take into account the multi-domain heterogeneous structure of the network. They suppose that the same set of monitoring services can be provided by any equipment of the network homogeneously and independently of the domain owner of the equipment. This assumption is in general erroneous. Particularly, every domain wants to apply its own policy and its own monitoring process. This requirement is called the autonomously managed domain requirement. Moreover, each domain wants to keep some monitoring processes or measurement results private. This requirement is called the confidential domain requirement.

A domain can be either collaborative or non-collaborative. A domain is collaborative only and only if it is ready to share measurement results as well as information about its measurement points with distant domains. Obviously, when the domains do not collaborate, the networks monitoring becomes more complicated. However, it is very interesting to monitor the services even if the domains are non-collaborative because the assumption that all the domains are collaborative is in general erroneous. This requirement is called the non-collaborative monitoring requirement.

Monitoring is used to extract measurement results for performance analysis and, in multi-domain networks, these measurement results may have to be exchanged between different domains or sent to a third party for aggregation and multi-domain analysis. In order to have efficient and meaningful measurement results, we want to assess in this paper that the export parameters such as the export methods and the export protocols have to be configurable. This requirement is called the adaptive export process requirement. When the export parameters of the different domains are configurable, we can request a domain to modify, for example, its export method in order to have more frequent measurement results for better fault detection.

Due to the heterogeneity of the measurement parameters which can be used by different domains, we want to assess in this paper that the measurement parameters such as the metrics to be measured and the measurement protocols to be used have to be configurable. This requirement is called the adaptive measurement process requirement. This requirement is mandatory especially when active measurements are performed between two domains because these domains have to agree on the measurement process. Moreover, when the measurement parameters of the different domains are configurable, we can modify, for example, the measurement protocol used by two domains without applying any modification on other domains along the path of the monitored service. This modification allows the providers, for example, to use a more efficient measurement protocol without requiring implementing the same measurement protocol in all domains. This configuration capability also offers more flexibility since multi-domain measurements can be provided even if a non-collaborative domain exists in the path of the monitored service. Indeed, multi-domain measurements can be performed measurements between two adjacent domains and these multi-domain measurements require the configuration of these adjacent domains.

In this paper, we propose a configurable multi-domain network monitoring architecture that resolves the heterogeneity problems by providing the adaptive measurement process and the adaptive export process requirements. In this architecture, both the measurement parameters and the export parameters can be configured. For a more efficient monitoring adaptation, we propose that the analysis functional block reacts to anomaly detections and this also could require some adaptations of the monitoring process such as the reconfiguration of the monitoring. Therefore, the measurement parameters and the export parameters have to be reconfigured.

Our monitoring architecture also resolves the confidentiality problems and allows the different domains to use own monitoring processes by providing the confidential domain and the autonomously managed domain requirements, respectively. In order to provide the confidentiality of the domain topology, we propose to perform multi-domain monitoring only between measurement points located at the border of the domains. Furthermore, our monitoring architecture can perform measurements even if all domains are not collaborative by providing the non-collaborative monitoring requirement.

Our work studies functionalities required for multi-domain network monitoring, thus this paper will propose a functional architecture and the relevancy of a proposal has to be evaluated against the five requirements listed previously. Moreover, we propose, in this paper, two collaboration schemes. These collaboration schemes are used by our proposed configurable monitoring architecture in order to select the measurement points participating in the multi-domain monitoring and to configure the different parameters of the selected measurement points. These collaboration schemes are based on the proactive selection and the reactive selection, respectively.

This paper is organized as follows. In section II, we discuss the main architectures already proposed for multi-domain networks. We present our proposals for a configurable multi-domain network monitoring architecture in section III. In section IV, we perform a functional evaluation of our configurable multi-domain monitoring architecture. Section V presents the simulation model and performance evaluations and comparisons of our proposed collaboration schemes. Conclusions are provided in section VI.

II. STATE-OF-THE-ART MONITORING ARCHITECTURES FOR MULTI-DOMAIN NETWORKS

We identify four functional blocks that are used by the current monitoring architectures: a configuration block, a measurement block, an export block, and an analysis block. The configuration functional block configures the monitoring. The measurement functional block performs measurements. The export functional block exports measurement results for further analysis. The analysis functional block analyzes the measurement results. In this section, we discuss the main monitoring architectures proposed for multi-domain networks. We also verify whether these architectures allow the providers to perform multi-domain measurements and whether the monitoring is configurable.

II.1. INTERMON architecture

The objective of the INTERMON project is to improve the QoS in inter-domain networks and to analyze the traffic in large scale [6]. The INTERMON architecture consists of four layers: a tool layer, a tool adaptation layer, a central control and storage layer, and a user interface layer [7]. In each domain, a central server called Global Controller (GC) coordinates the interaction between the different components of the architecture. We can identify the following functional blocks:

- The measurement functional block, which is located in the tool layer, consists of active and passive measurement points.
- The configuration functional block, which is located in the tool adaptation layer, is responsible for configuration of the measurement points.
- The export functional block, which is located in the central control and storage layer, is responsible for the export of the results using IPFIX and the results are then stored in the global database.
- The analysis functional block that is located in the central control and storage layer is responsible for the data post processing.

The INTERMON architecture is applied in each domain and the communication between the different domains is performed using Authorization, Authentication, and Accounting (AAA) local servers. Each provider can request a distant provider to get intra-domain measurement results on one or some metrics. When receiving this request, the distant provider checks if the sender has the right to obtain such information, using the AAA server, and answers the request.

II.2. ENTHRONE architecture

The objective of the monitoring system of the ENTHRONE project is to verify whether the QoS performance are respected using active and passive measurements. The management monitoring architecture of ENTHRONE consists of three levels: Node level Monitoring (NodeMon), Network level Monitoring (NetMon), and Service level Monitor (ServMon) [8].

- The NodeMon performs intra-domain active and passive application-level measurements at the edge nodes. These per-flow measurements are used to detect SLA violations such as QoS degradations, and then launch failure localization procedures.
- The NetMon processes and aggregates the measurements collected by the different NodeMons belonging to its domain. Then, it exports only the relevant measurement results to the ServMon. Therefore, the ServMon minimizes the quantity of the exported information since it exports only the relevant measurement results. The exported measurement results depend on the analysis process.
- The ServMon is responsible for reporting the QoS measurements between the different domains using XML-based measurement statistic.

Two monitoring signaling protocols are added to the monitoring architecture: an inter-domain monitoring signaling protocol (EQoS-RM) and an intra-domain active measurement signaling protocol (EMon). A disadvantage of the ENTHRONE architecture is that the measurements are mostly done at an application-level. The EQoS-RM and the EMON are used for monitoring exchanges between the ServMons of the different domains and between the NodeMons of the same domain, respectively. The EMon also configures the characteristics of the active measurements sessions (such as the one-way delay and the flow identification) between the effective NodeMons.

II.3. EuQoS architecture

The Monitoring and Measurement System (MMS) of the EuQoS project provides traffic measurements in real-time [9]. The EuQoS architecture consists of:

- Measurement Points (MP) that perform QoS measurements.
- Measurement Controller (MC) that launches and terminates the intra-domain measurements and collects the results from the different MPs.
- Monitoring, Measurement and Fault Management (MMFM) module that stores the measurement results obtained from the MC in the Resource Management Database (RM DB). Each domain contains a single RM DB and this database is accessible for the MMFM modules of all the domains.

For QoS performance evaluation, Net Meter [10] is selected as the intra-domain measurement tool. This active tool provides measurements on QoS metrics such as the delay, the delay variation, and the packet loss ratio. Moreover, the Monitoring and Measurement System (MMS) of EuQoS provides real-time measurements using an on-line monitoring passive tool called Oreneta. The MMS is limited to monitor a single class of service in a single domain. An active measurement tool, called Link Load Measurement Tool (LLMT), was developed by EuQoS to perform inter-domain measurements (on inter-domain links). The measurement results obtained by LLMT are then stored in the RM DB.

II.3. Synthesis of the state-of-the-art monitoring architectures for multi-domain networks

We note that the measurement, export, analysis and configuration functional blocks exist in the INTERMON and ENTHRONE monitoring architectures. Besides, the export block of the INTERMON architecture uses a standardized export process (IPFIX). Moreover, the INTERMON architecture provides the confidential domain requirement using the AAA servers. However, the INTERMON and ENTHRONE architectures do not allow the providers to perform full multi-domain measurements and they are limited to the exchange of the intra-domain measurement results between the providers. These architectures provide partial multi-domain measurements because inter-domain measurements are not performed. Moreover, these architectures require that all the domains are collaborative and each of them performs intra-domain measurements and exchanges its measurement results with other domains. Therefore, the non-collaborative monitoring requirement is not provided. Furthermore, the configuration block of the INTERMON and ENTHRONE architectures are limited to the configuration of the measurement points and the configuration of the active measurement sessions, respectively. However, these configurable parameters are not sufficient in a heterogeneous environment (see subsection III.1). Then, the adaptive measurement process requirement is not totally provided while the adaptive export process requirement is not provided.

The main advantage of the EuQoS monitoring architecture is that it performs full multi-domain measurements by providing intra-domain and inter-domain measurements. However, this architecture uses its own inter-domain measurement tool. Therefore, all the domains must use the same measurement tool and this does not respect the autonomously managed domain requirement. Moreover, there is no configuration functional block in the EuQoS architecture. Therefore, this monitoring architecture does not provide the adaptive measurement process and the adaptive export process requirements.

Therefore, we propose in the following a configurable multi-domain networks monitoring architecture that provides these five requirements: the autonomously managed domain, the confidential domain, the non-collaborative monitoring, the adaptive measurement process, and the adaptive export process requirements. Table I presents whether these five requirements are provided by the different monitoring architectures. In the following section, we present our proposals for a configurable multi-domain monitoring in section III.

III. PROPOSALS FOR A CONFIGURABLE MULTI-DOMAIN MONITORING

Our monitoring proposals should adapt to any compatible multi-domain network architecture like the architecture model defined by the IPSphere forum [11]. This model allows providers to overcome scalability and interoperability issues. The IPSphere forum has defined the role of each system entity: Administrative Owner (AO), Element Owner (EO), and customer. AO is the entity that is responsible for providing and guaranteeing end-to-end services over a multi-domain network. These services are requested by customers. EO is the entity that manages the resources of a network domain. Each service provided by the AO uses the resources of one or several EOs.

Table I. Multi-domain monitoring architectures vs monitoring requirements

Architectures	Autonomously managed domain	Confidential domain	Non-collaborative monitoring	Adaptive measurement process	Adaptive export process
INTERMON	Yes	Yes	No	Partially	No
ENTHRONE	Yes	No	No	Partially	No
EuQoS	No	No	No	No	No
Our configurable monitoring	Yes	Yes	Yes	Yes	Yes

The principal elements of our monitoring architecture are represented in Fig. I. Each domain contains measurement, export, analysis, and configuration blocks. We propose that the configuration block has the capacity to configure the measurement and the export blocks to overcome the heterogeneity issues. The configuration block can be initialized using a configuration file. To have more flexibility in monitoring, it is required to have a dynamic configuration. For example, when the analysis block detects a network failure, it can modify the measurement and/or the export parameters through the configuration block in order for instance to locate the source of the failure. The details of our monitoring architecture and our proposals for a configurable multi-domain network monitoring are giving in the following.

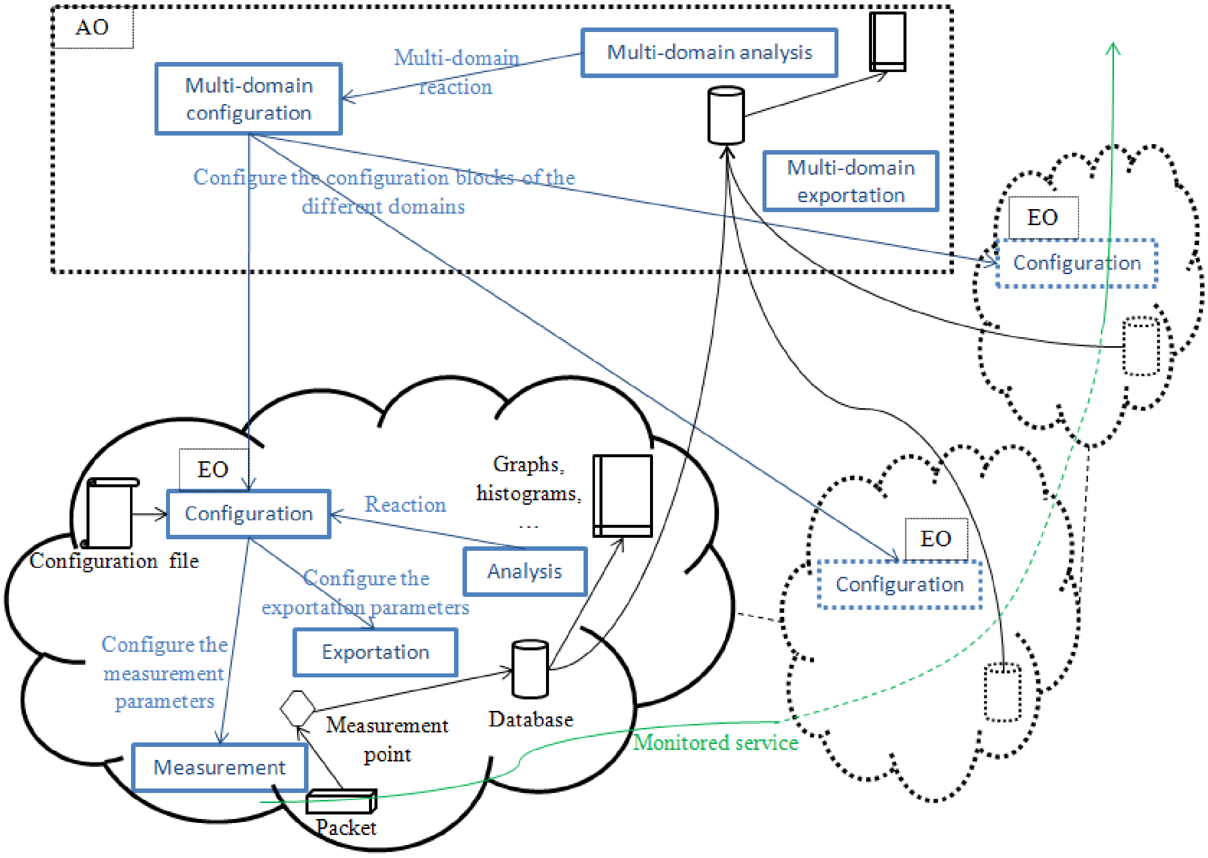

Figure I. Principal elements of a configurable multi-domain monitoring

III.1. Configurable parameters of network monitoring

In this section, we present the main parameters of the measurement and the export functional blocks that have to be configured. The parameters of the measurement functional block that should be adequately chosen in order to have an effective network monitoring in a heterogeneous environment are the following:

- Metrics: depend on the constraints defined in the contract that is already established between the user and the provider and recursively between providers on the service path. In this paper, we consider the metrics that have been standardized by the Internet Engineering Task Force (IETF) such as the network capacity [12], One Way Delay (OWD) [13], IP Packet Delay Variation (IPDV) [14], One Way Packet Loss (OWPL) [15], and connectivity [16]. We note that the International

Telecommunication Union (ITU) defines additional metrics in [17] such as IP Packet Transfer Delay (IPTD), and IP Packet Loss Ratio (IPLR). However, these metrics can be easily mapped with the metrics defined by the IETF. For example, IPLR can be mapped with OWPL.

- Monitoring type: depends on the metrics to be measured as well as the capabilities of the measurement point. The monitoring can be passive or active. A measurement point can support passive monitoring and/or active monitoring. A well chosen monitoring type can ease the measurement process of the metrics. For example, the number of transmitted packets is adequately computed using passive monitoring, while delay is easily measured using active monitoring. Nevertheless, the same metric can be measured by both monitoring types.
- Measurement protocols: define the procedures used to perform the measurements of metrics into a network. A measurement protocol can be passive and/or active. For example, Bidirectional Forwarding Detection (BFD) [18], which is an active protocol, is used to determine the connectivity. In [19], it is recommended to use standardized measurement protocols in order to ensure the interoperability between heterogeneous measurement points. For example, it is recommended to use One Way Active Measurement Protocol (OWAMP) [20] to provide one-way measurements such as OWD. Two-way measurements can be provided using Two-Way Active Measurement Protocol (TWAMP) [21]. Once the measurement protocol is selected, its parameters have to be chosen. For example, when the measurement protocol is active, the characteristics of the additional traffic such as the packet size, the probe rate and the probe duration have to be chosen. The choice of the additional traffic characteristics depends on the model used to infer the network traffic.
- Sampling methods: determine when the packets are captured. These methods can reduce the network resource utilization of the path between the physical channel and the measurement point. This path is called the supervision path (see Fig. II). The sampling methods depend on the metrics to be measured. For example, the periodic and the random sampling can provide acceptable performance when measuring the delay and the packet loss [22]. When measuring the delay variation, the batch sampling provides the best performance. In practice, the periodic sampling is almost always used because this sampling method is easier to implement [23].
- Packet filtering methods: determine the packets that will not be taken into account in the measurements. These methods can reduce the network resource utilization (computations at the measurement point level). For example, a packet filtering method can specify to do not measure packets having a source IP address equal to 205.10.0.0/24. A packet filtering method can be applied on packet field(s), flow field(s), and/or service class field(s).

The parameters of the export functional block that should be configured are:

- Statistic computation methods: determine how the measurement results are computed. For example, when the OWD is measured, the export functional block can export the minimum OWD or the average OWD. Generally, the statistic computation method depends on the analysis process.
- item Export methods: determine when are the results exported. The export method has a direct influence on the reaction time of the analysis process and the utilization of the path between the measurement point and the database (where the measurement results are stored). We note that the results can be immediately exported when they are obtained using the real-time method. This export method has the advantage of speeding up the results analysis time and then reduce the violation detection delay. However, the quantity of exchanged data can be quite large. To reduce the network resource utilization, the results can be exported periodically. This method can also provide acceptable results analysis time when the export period is finely tuned. The results can also be exported in a random method. This export method has the advantage of following the random aspect of the failure generation instants. Another solution to reduce the network resource utilization while rapidly reacting against failures is to export results using a trigger mechanism. For example, the results are compared against thresholds. However, this method has the disadvantage that it requires additional processing in the measurement functional block. The results can also be exported when they are requested by the analysis block (on-demand, e.g. Simple Network Management Protocol (SNMP) [24] request) or once at the end of the measurement campaign. In both methods, long delays can affect the results analysis time.
- Export protocols: define the procedures used to send the measurement results from the measurement point to the analysis point. These measurement points can be stored in a database. For interoperability issues, standardized export protocols are more interesting. For example, export protocol IPFIX is used by two standardized monitoring architectures: IPFIX and PSAMP. The IPFIX protocol is described in [25].

- Collecting methods: gather several measurement results in the same packet. The collecting method (applied on the same metric, for example, the minimum delay) can be temporary or spatial. The temporary collecting method consists of gathering several measurement results obtained in different sampling periods. The spatial collecting method consists of gathering several measurement results obtained from different measurement points. The collecting methods can reduce the network resource utilization of the path between the measurement point and the database (export path, see Fig. II), and then minimize the amount of data stored in the database.
- Result filtering methods can minimize the amount of the measurement results to be exported while getting enough measurement results for efficient analysis. For example, a result filtering method can specify to do not export measurement results that have already been provided from packets having an source IP address equal to 205.10.0.0/24. A result filtering method can be applied on packet field(s), flow field(s), and/or service class field(s). The result filtering methods (like the collecting methods) can reduce the network resource utilization of export path, and then minimize the amount of data stored in the database.

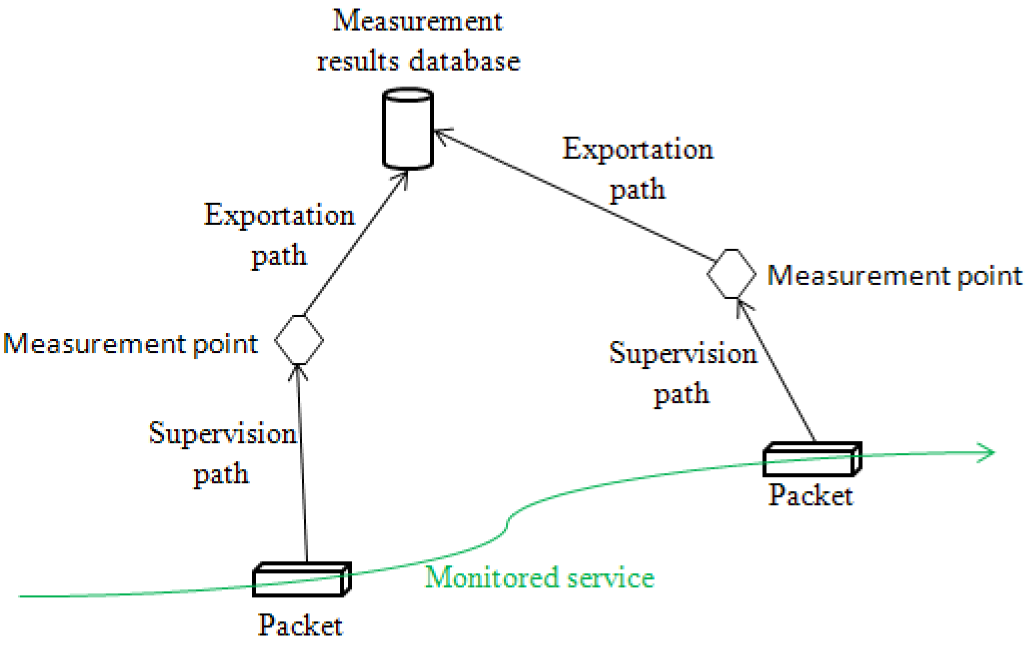

Figure II. Example of supervision paths and export paths

The main configurable parameters of the measurement and export functional blocks are presented in Table II.

III.2. Proposals for the measurement functional block

In intra-domain, each provider configures its domain with its own method without taking into account the monitoring characteristics of the other domains. However, in multi-domain, the providers have to share and exchange configuration information to perform multi-domain measurements. For example, the operators have to select the measurement protocol to be used. Indeed, each provider can have one or many measurement protocols. We note that it is possible to perform the monitoring between two points (without performing intermediate measurement, for example between measurement point *a2* and measurement point *b3* without performing measurements between measurement point *a2* and measurement point *b1*, see Fig. III) only if these measurement points support the same measurement protocol to be used.

Table III. Configurable parameters of the measurement and export functional blocks

Configurable parameters	Mandatory conditions	Examples of possible values
Metrics	Always mandatory	Delay, packet loss, etc.
Monitoring types	Always mandatory	Active, passive
Measurement protocols	Mandatory if the monitoring type is active (in this case, the additional traffic characteristics such as the probe size, and the probe rate have to be defined)	BFD, OWAMP, TWAMP, etc.

Sampling methods	Mandatory if the sampling is used (in this case, the sampling duration and the sampling frequency have to be defined)	Periodic, random, batch, etc.
Packet filtering methods	Mandatory if the filtering is used (in this case, the filtering rules have to be defined)	Filtering according to packet or flow field(s), etc.
Statistic computation methods	Always mandatory (this parameter depends on the metric measured)	Minimum delay, average delay, etc.
Export protocols	Always mandatory	IPFIX, etc.
Export methods	Always mandatory	Periodic, random, triggered, etc.
Collecting methods	Mandatory if the measurement results collecting is used	Temporary, spatial, etc.
Result filtering methods	Mandatory if the filtering of the measurement results is used (in this case, the filtering rules have to be defined)	Filtering according to packet or flow field(s), etc.

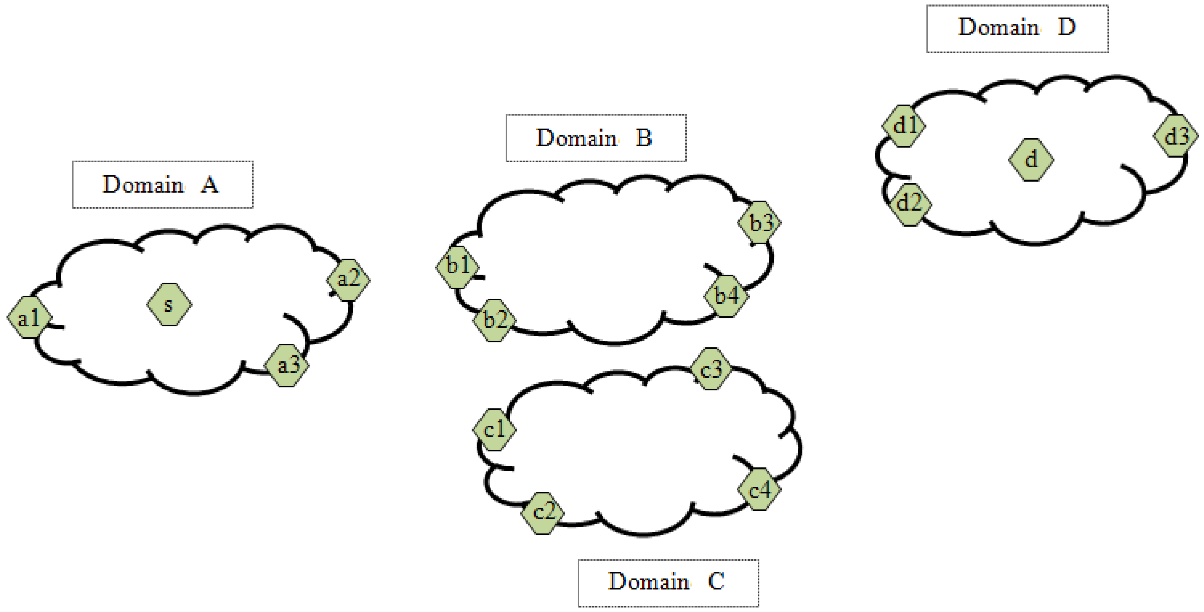

Fig. III. Multi-domain network monitoring scenario

In a close monitoring of a multi-domain flow or path, the providers have to perform multiple measurements (segment by segment) and the measurement results have to be correlated. The multiple domain measurements can be performed in two ways:

- All the providers use the same measurement protocol and measurement parameters and this makes easier the correlation of the measurement results. However, this assumption of homogeneity cannot always fulfill. For instance, let suppose a set of domains which share the same measurement protocol and have preselected a fixed measurement parameter set. Let suppose now that a new type of service requires a new monitoring method. When the homogeneity is a requirement, to monitor a new service, either all domains supported the new monitoring method or none. In the latter case, the new service cannot be properly monitored. In the first case, the new service will be monitored when and only when all domains support the new monitoring method. This could be unnecessary because the path to be monitored could use only a subset of the domains.
- The providers use different measurement protocols but two contiguous providers should mandatory run the same measurement protocol. Therefore, there is more flexibility in the choice of the measurement protocol to be used. However, the result correlation can become complex and each pair of providers have to select the measurement protocol to be used. This requires an additional negotiation phase for each choice of measurement protocol pair.

In both above ways, we make the assumption that the providers collaborate in the use of the measurement protocols. However, a provider may be non-collaborative; for instance, he does not want to publish measurement results on its traffic. A provider may do not support monitoring or the chosen measurement parameters are not available or its measurement capacity is already allocated to other services. In these cases, we can perform active measurements between his adjacent domains in order to monitor the traffic that traverses this domain. However, it can be difficult to perform a passive monitoring between the adjacent domains because it could be difficult to identify the traffic to be measured. Indeed, the outgoing border router of the non-collaborative domain (and thus the incoming border router of the following domain) cannot be assessed with sufficient precision. When monitoring a Label Switched Path (LSP) in Multi Protocol Label Switching (MPLS) networks, it is possible to perform active and passive monitoring on the adjacent domains as the path of an LSP is well-known.

In addition to the measurement protocol that is used in the remote measurement point, the local provider has to know at least the localization of the remote measurement point. However, confidentiality problems can take place since the router localization and then the network topology can be unveiled. One usual policy is to propose that only the localization of the border measurement points is unveiled to distant domains.

III.3. Proposals for the export functional block

For scalability and interoperability purposes, we recommend that the intra-domain export block exports the results to the AO for multi-domain analysis. The multi-domain analysis functional block verifies whether the measured network performance complies with the performance specified in the contract. When this functional block detects anomalies, some interventions of the multi-domain monitoring configuration are required (see Fig. I).

For correlation purposes, it is required that statistic computation methods, the result filtering methods, and the collecting methods used are the same for all the measurement points located on the monitored path.

Finally, we propose that the export and the collecting methods are compatible in order to have meaningful results. For example, when the AO receives results from a domain that uses the periodic export method and from another domain that exports results using a trigger mechanism, the AO can analyze the measurement results if it can identify the trigger generation instants.

III.4. Proposals for the configuration functional block

We propose to locate the multi-domain configuration block at the AO since the global network resources are managed by this entity. Likewise, we propose that the intra-domain configuration block is coupled with the EO as this entity manages the resources of its network domain (see Fig. 1). The multi-domain configuration block is responsible for the configuration of all the domains that participate in the multi-domain monitoring by acting on their intra-domain configuration blocks.

We suppose that the client launches a multi-domain monitoring of a service by sending a multi-domain network monitoring request. When receiving this request, the AO configures the domains concerned by the multi-domain network monitoring of the service. These domains belong to the path of the monitored service. The measurement points that participate in this monitoring are selected by the AO. However, an EO can participate in the selection by preselecting a list of useful measurement points. The selection of the measurement points can be with or after the service establishment. The selection can be proactive or reactive. For both selection methods, the configuration blocks of the concerned domains have to transmit the information about the useful measurement points (or the information about all the available measurement points in its domain). The information about a measurement point consists in its localization (e.g. the Internet Protocol address of the measurement point), its configurable parameters (see subsection III.1), and its monitoring capacity (that represents the maximum number of services that can be monitored simultaneously).

In proactive selection, each domain publishes the information about all its measurement points. When all the information is available, the AO can efficiently select the measurement points to be used. However, the transmitted information can be quite large. The proactive selection has two major drawbacks. First, the providers cannot preselect the measurement points to be used. Second, the providers have to transmit update messages when they need to update the list of the measurement points as well as their parameters or their monitoring capacities.

In reactive selection, the AO requests each concerned domain to transmit the information about the useful measurement points. Each provider preselects the measurement points and answers the request. The reactive selection allows the providers to avoid measurement points update procedure and decreases the amount of exchanged data for the publication (only preselected measurement points are sent). However, the selection has to be performed with each incoming multi-domain monitoring request. Furthermore, the AO can select the measurement points only when it receives all the responses from the domains concerned by the multi-domain monitoring. Therefore, the measurement points selection can receive extra delay.

In both above selection methods, we propose that the AO requests the configuration blocks of the domain on the monitored path to activate the selected measurement points.

In practice, the proactive selection mode is required when the monitoring establishment is performed simultaneously with the service establishment. The major advantage of this selection mode is that the LSP routing can take into account the characteristics of the measurement points. For example, the routing algorithm selects compatible measurement points which can still monitor further services, i.e. having monitoring capacity greater than zero. When the monitoring is established after the service establishment, the proactive selection mode becomes useless as there is no need to send all the measurement points characteristics to the AO. In this case, the reactive selection mode becomes more interesting

Finally, we propose that each intra-domain configuration block configures its measurement and export parameters (see Table II). This configuration can be determined locally when performing intra-domain network monitoring. However, this configuration has to be determined by the AO when performing multi-domain network monitoring for two reasons: the heterogeneity and the confidentiality. For example, when we perform active measurements between measurement point *a1* belonging to domain *A* and measurement point *d2* belonging to domain *D* (see Fig. 3), we have to configure these two measurement points in a coordinated way. For example, in a heterogeneous environment, in order to measure the delay, we have to select the same metric (for example OWD), the same statistic computation method (average OWD), the same measurement protocol (for example OWAMP), and the same export method (periodic, each 5 s). These monitoring parameters are selected among the set of the metrics, the statistic computation methods, the measurement protocols, and the export methods available at these two measurement points.

Even in a homogeneous environment (all the measurement points use the same parameters), the multi-domain monitoring configuration is still necessary for confidentiality reasons. Indeed, when we need, for example, to perform active measurements between measurement point *s* and measurement point *d2* (see Fig. 3) without unveiling the localization of the measurement points located inside a local domain to any distant domain, we can perform multiple segmented measurements. For example, we can perform active measurements between measurement point *s* and *a1* and between measurement point *a1* and *d2*. Therefore, the localization of measurement point *s* is known by measurement point *a2* that belongs to the same domain. Moreover, measurement point *d2* uses only the localization of measurement point *a2* that is located at the border of the distant domain.

IV. FUNCTIONAL EVALUATION OF OUR PROPOSED MONITORING ARCHITECTURE

Now, we evaluate our configurable multi-domain monitoring architecture functionally. Recall that we do not evaluate our propositions through prototype measurements or performance modeling since we study a functional architecture. We consider the scenario presented in Fig. III. It is required to perform measurements between measurement point *s* and measurement point *d3* and these measurements are used to verify whether the delay constraint is respected (the end-to-end delay of the service has to be lower than 150 ms). The domains concerned by the monitoring are *A*, *B*, and *D*. The supported measurement protocols by the different measurement points that can participate in these measurements are presented in Table III. We assume that the service has been already established. The measurement protocols that can be used are *p1*, *p2*, and *p3* and all these protocols can provide measurements on OWD using active monitoring. The statistic computation method of all the measurement points provides average delay. All the measurement points can export the measurement results periodically or using a trigger mechanism. From the list of the configurable parameters (see Table II), we consider only the metric, the monitoring type, the measurement protocol, the statistic computation method, and the export method but we do not loss any generality if any additional configurable parameter is selected.

Table III. Supported measurement protocols by measurement points

Measurement points	Supported measurement protocols
s	p1
a2	p1 and p2
b1	p1 and p3
b3	p3
d2	p2 and p3
d3	p2

IV.1. Autonomously managed domain requirement

We note that we cannot perform measurements directly between measurement point *s* and measurement point *d3* because they do not support the same measurement protocol (these measurement points support *p1* and *p2*, respectively). Moreover, we also note that the inter-domain measurements are performed using two different measurement protocols: *p1* (performed between domain *A* and domain *B*, in particular between measurement point *a2* and measurement point *b1*) and *p3* (performed between domain *B* and domain *D*, in particular between measurement point *b3* and measurement point *d2*). So, even advanced inter-domain monitoring architecture (like the EuQoS architecture) cannot provide inter-domain measurement results in our scenario since the same measurement protocol has to be used in all multi-domain measurements.

Our proposed architecture allows the AO to configure and perform multi-domain monitoring between measurement point *s* and measurement point *d3* in spite of the heterogeneity of the measurement protocols of these measurement points. In fact, the AO can select measurement protocol *p1* between *s* and *a2* and between *a2* and *b1*, measurement protocol *p3* between *b1* and b3 and between *b3* and *d2*, and measurement protocol *p2* between *d2* and *d3*. We note that the autonomously managed domain requirement is provided since the domains do not have to use the same monitoring process (in our scenario they can use different measurement protocols).

IV.2. Confidential domain requirement

Using our monitoring architecture, the characteristics of the measurement points located inside the domains and especially their localizations are not unveiled to the distant domains. For example, the measurement point *s* characteristics are known only by domain *A*. Only the characteristics of the border measurement points are unveiled to the distant domains (for example the characteristics of measurement point *a2* are unveiled to domain *B*). Therefore, the topology confidentiality of the different domains is assured using our configurable monitoring architecture. We also notice that the border measurement points do not have a global view of the possible values of the configuration parameters. For example, domain *A* does not know that measurement point *b1* supports measurement protocol *p3* and this specificity can be useful for confidentiality purposes. We note that the confidential domain requirement is provided.

IV.3. Non-collaborative monitoring requirement

Now, we assume that the AO thinks that domain *B* exports spurious measurement results. As consequence, the AO can decide to perform measurements between the adjacent domains of domain *B* along the path of the monitored service. Measurements can be performed between *a2* and *d2* and then these measurement points have to be reconfigured. For example, the AO specifies to domain *A* that measurement point *a2* will communicate with measurement point *d2* (instead of measurement point *b1*) using measurement protocol *p2* (instead of measurement protocol *p1*). This reaction can also be performed when domain *B* is or becomes non-collaborative. We note that the non-collaborative monitoring requirement is provided. We also note that the existing monitoring architectures cannot react in this situation. Indeed, the INTERMON and ENTHRONE architectures require that all domains used by the monitored service exchange their measurement results. The EuQoS architecture has no configuration block and therefore the measurement protocol used by measurement point *a1*, for example, cannot be replaced. In our case, measurement protocol *p1* is replaced by measurement protocol *p2* that represents the only common measurement protocol with the distant measurement point (*d2*).

IV.4. Adaptive export process requirement

We suppose that the AO selects the measurement result export method using a trigger mechanism in order to minimize the volume of data exported to the database. We assume that the measurement results are exported only if the delay exceeds 55 ms for measurements performed between measurements points belonging to the same domain (for example between measurement point *s* and measurement point *a2*) or if the delay exceeds 5 ms for measurements performed between measurements points belonging to two different domains (for example between measurement point *a2* and measurement point *b1*). These thresholds are determined by the AO.

Now, we assume that the mean delay between measurement point *b1* and measurement point *b3* is equal to 60 ms. Then, since this intra-domain measurement value exceeds the corresponding threshold (55 ms), domain *B* exports measurement results to the AO. We propose that domain *B*, in a first stage, locally reacts to minimize the delay before the client detects service degradation. In order to verify whether the multi-domain delay constraint is respected (whether the end-to-end delay is lower than 150 ms), the AO can reconfigure the different domains by requesting them to replace their current export methods by the periodic export method. We note that the adaptive export process requirement is provided. After reconfiguring the export methods, the different domains periodically export their measurement results. We assume that the total average delay is equal to 130 ms. As the multi-domain constraint is respected, it is no necessary to perform further reactions. However, if the end-to-end delay exceeds 150 ms and domain *B* is the domain which does not respect its delay constraint, the AO may, for example, give penalty to the faulty domain, renegotiate the contracts between the different domains, and eliminate the faulty domain from the negotiation. The impact of configuration on monitoring reactions will be studied in future work. Anyhow, we think that it will introduce a great enhancement.

In general, the monitoring reactions are performed once the multi-domain analysis functional block detects anomalies, it has to react. We indicate that we do not consider anomaly diagnosis and fault detection. Many works have already been done on these important fields such as [26], [27], and [28], and our solutions should be compatible with any of them. The anomalies can be detected, for example, when the client announces service degradation or using the measurement results exported by the different domains. Detection fault mechanisms will be proposed and evaluated in future work.

IV.5. Adaptive measurement process requirement

We suppose that measurement protocol *p3* is the least efficient. Now, we assume that measurement point *b3* supports measurement protocol *p1* (in addition of measurement protocol *p3*). As measurement point *b1* also supports measurement protocol *p1*, we can reconfigure measurement point *b3* and measurement point *b1* without reconfiguring the other measurement points. This reconfiguration allows domain *B* to use a more efficient measurement protocol without disturbing domain *A* and domain *D*. This reconfiguration can also ease the measurement results collecting in the AO because measurement points *s*, *a2*, *b1*, and *b3* use the same measurement protocol. We note that the adaptive measurement process requirement is provided.

V. PERFORMANCE EVALUATION OF THE PROPOSED COLLABORATION SCHEMES

V.1. Simulation model

In this section, we consider a topology formed by four domains and fourteen measurement points (see Fig. III). We consider only measurement points that are located at the border of the domains for confidentiality reasons. Domain A, Domain B, domain C, and domain D contains three measurement points (a1, a2, and a3), four measurement points (b1, b2, b3, and b4), four measurement points (c1, c2, c3, and c4), and three measurement points (d1, d2, and d3), respectively. The main simulation parameters are presented in Table IV}. The measurement point capacity represents the maximum number of services that this measurement point can monitor simultaneously. The incompatibility ratio represents the ratio of the measurement points that are not compatible with any other one. Two measurement points are compatible if and only if they can perform active measurement between them. For example, if the incompatibility ratio is equal to 0.1 and if there are 10 measurement points, then we have, in average, one measurement point that is not compatible with all the other ones.

Table IV. Simulation parameters

Simulation parameters	Values
Number of domains	4
Number of measurement points	14
Simulation time	1500 s
Monitoring requests arrival	is chosen according exponential distribution on the interval [1, 200]
Measurement point capacity	is chosen according uniform distribution on the interval [100, 120]
Incompatibility ratio	0 (all the MPS are compatibles), 0.1, 0.3, and 0.5 (the half of the

	measurement points are incompatible)

V.2. Simulation results for compatible measurement points

First, we interest in the case when all the measurement points are compatible (incompatibility ratio is equal to zero). We evaluate the blocking percentage due to the measurement points surcharge (the blocking percentage due to the measurement points incompatibility is equal to zero), the monitoring throughput (that represents the throughput of messages used to publish the measurement points characteristics and to configure the measurement points), and finally the delay of the monitoring establishment.

V.2.1. Blocking percentage evaluation

Fig. IV represents the blocking percentage as a function of the total number of the generated services during simulation. We note that, using the simulations parameters listed in Table IV, the blocking percentage is equal to zero for both collaboration schemes when the total number of services is lower than 200. Indeed, the measurement points do no reach their maximum monitoring capacity yet. From a total number of services approximately equal to 200, the blocking percentage of the reactive mode starts increasing while the blocking percentage of the proactive mode remains equal to zero until a total number of services equals to 300.

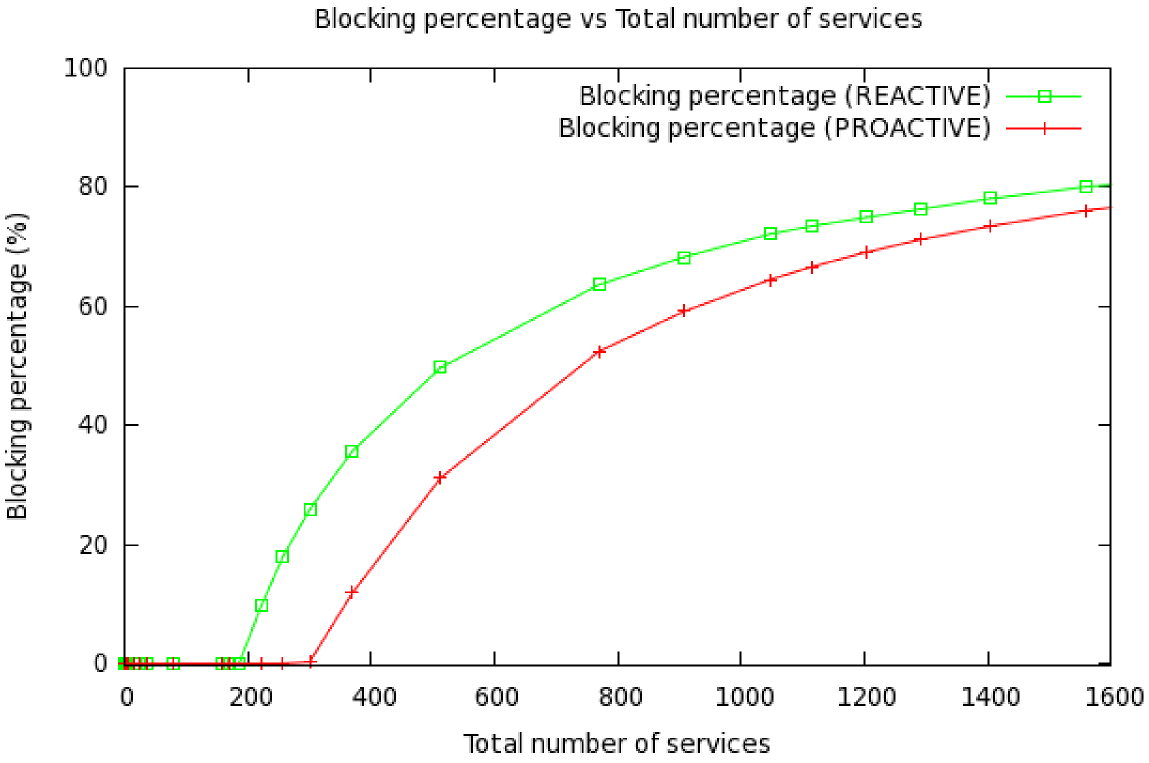

Fig. IV. Blocking percentage vs total number of the generated services during simulation

We notice that the proactive mode outperforms the reactive mode because when the first mode is applied, the AO has a global view on the capacity of all the measurement points. Therefore, the AO can select the measurement points that have the capacity to monitor further services. However, when the reactive mode is applied, the LSP for a given service is already established and so it can cross a measurement point that has already reached its maximum monitoring capacity.

When the number of services becomes very important, the curves of the proactive mode and of the reactive mode become close as most of the measurement points cannot monitor further services.

V.2.2. Throughput evaluation

Fig. V represents the monitoring throughput, the publication throughput, and the publication throughput as a function of the total number of services. The configuration throughput presented by the proactive mode is more important than that presented by the reactive mode. This is explained by the fact that the proactive mode allows our monitoring architecture to monitor more services than the reactive mode (the proactive more is flexible and thus it generates lower monitoring requests blockage, see Fig. IV).

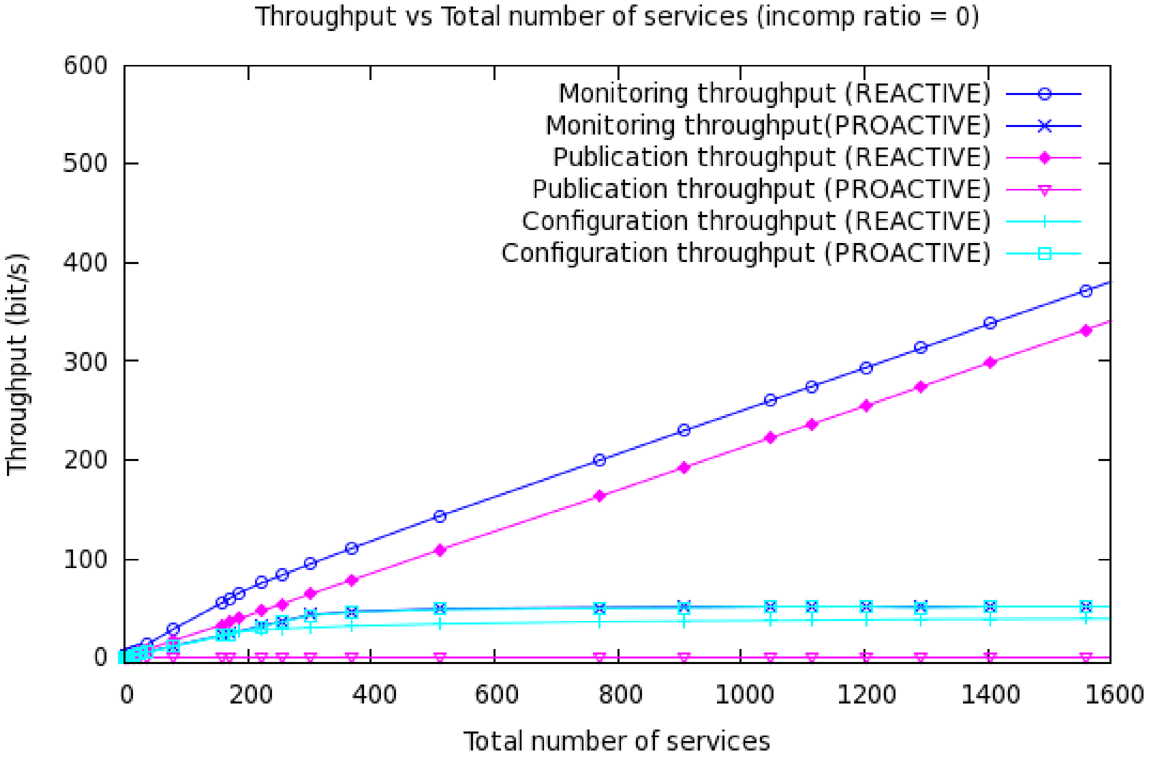

Fig. V. Throughput vs total number of services

Now, we consider the publication throughput. We note that the reactive mode generates higher publication throughput than the proactive mode. Indeed, we assumed that the refreshment period of the measurement points characteristics update is longer than the simulation time and therefore, when the proactive mode is used, each EO publishes the characteristics of its measurement points once during the simulation. However, when the reactive mode is used, the EO sends the list of the preselected measurement points at each monitoring request.

Recall that the monitoring throughput is equal to the configuration throughput added with the publication throughput. As the publication throughput is more important than the configuration throughput and therefore it has more effect on the monitoring throughput, we observe that the monitoring throughput of the reactive mode is higher than that of the proactive mode. Evidently, the monitoring throughput depends on the configuration and publication messages length as well as the number of accepted (non blocked) monitoring requests. The number of accepted monitoring requests depends on the monitoring capacity of the different measurement points as well as on the total number monitoring requests.

V.2.3. Delay evaluation

The mean delay of the monitoring establishment is presented in Table V. We note that the mean delay of the monitoring establishment when the reactive mode is used is greater than that when the proactive mode is used. This is because that, when the proactive mode is used, the AO has the characteristics of all the measurement points. Therefore, in opposition to the reactive mode, the AO can locally select the useful measurement points without needing to send messages (for requesting the list of the preselected measurement points) to the EOs concerned by the multi-domain monitoring and so waiting their responses.

Table V. Mean delay of the monitoring establishment

Collaboration mode	Proactive	Reactive
Mean delay	0.1 s	0.18 s

V.3. Simulation results for measurement points having different incompatibility ratios

Now, we study the blocking percentage for measurement points having incompatibility ratio equal to 0, 0.1, 0.3, and 0.5. Fig. VI represents the blocking percentage due to the MPs incompatibility as a function of the total number of services. Evidently, when all the MPS are compatible (incompatibility ratio is equal to zero), the blocking percentage due to the MPS incompatibility is equal to zero for the proactive and reactive modes (the curves of this incompatibility ratio are not presented is Fig. VI).

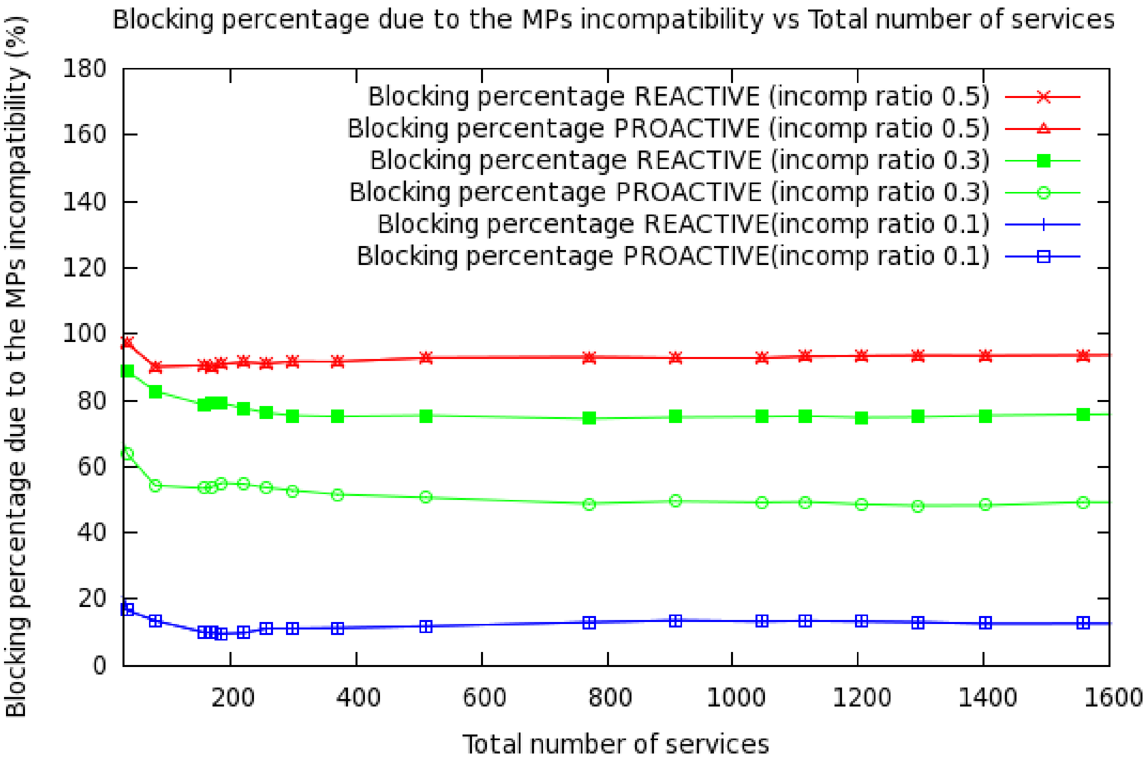

Fig. VI. Blocking percentage due to the MPs incompatibility vs total number of services (for different incompatibility ratios)

When the incompatibility ratio is equal to 0.1, the blocking percentage due to the MPs incompatibility is the same independently of the collaboration mode. This is due to the small solicitation of the incompatible measurement points for the multi-domain monitoring when the incompatibility ratio is too lower.

When the incompatibility ratio is equal to 0.3, the proactive mode outperforms the reactive mode. In fact, when the proactive mode is used, the AO endeavors to select compatible measurement points while the LSP paths are already established and then the measurement points that can participate in the multi-domain monitoring are limited when the reactive mode is used.

For an incompatibility ratio equal to 0.5, both collaboration mode presents the same blocking percentage due to the MPs incompatibility. Indeed, when the incompatibility ratio is important, even the proactive mode cannot find a path (especially if the path has to cross many domains and then many measurement points) that contains only compatible measurement points. However, we predict that the proactive mode becomes more and more efficient than the reactive mode, even if the incompatibility ratio is important, when the number of measurement points per domain increases (in our scenario, we have at most two measurement points that can link two domains). We will study the influence of the increasing of the number of measurement points as well as the increasing of the number of the domains in future work.

VI. CONCLUSION

In this paper, we have studied the state-of-the-art monitoring architectures proposed for multi-domain networks.

We have concluded that these architectures assume that the set of monitoring methods is identical over all the domains. This assumption achieves the potential interoperability of the methods. However, in the case of autonomous domains (which is very common in practice), even with this homogeneous assumption, one important point is missed: the need of a coordinated and wise selection of the monitoring parameters to achieve an efficient monitoring of the multi-domain networks. Let us suppose that, for instance, one domain manages the sampling method (which is a configurable parameter of the measurement functional block) of a certain flow on a periodic basis which can be chosen between 100 ms and 200 ms, whereas another domain uses a period sampling between 100 ms and 500 ms. It could be wise to offer the capability to select, on a flow basis, either the lower period to have a precise monitoring or the larger period to have a lighter resource consumption. So, the adaptive measurement process requirement (as well as the adaptive export process requirement) must be provided.

We have supposed that in a multi-domain network, some domains can collaborate to monitor some segments of the monitored services whereas some domains do not want or cannot collaborate. In this context, it is required that the collaborative domains adjacent to the non-collaborative domains monitor a longer segment which spans the non-collaborative domain. Thus even non-adjacent domains (for instance the above domains which are adjacent to the non-collaborative domains) should have the mean to determine the most appropriated monitoring methods and parameters to use. We have shown that the non-collaborative monitoring requirement has to be provided.

Furthermore, we have shown that the autonomously managed-domain and the confidential domain requirements have an impact on every monitoring process: the measurement process, the export process, and the reaction process. This requires and induces a flexible configuration of all (monitoring) processes, thus we have made proposals for these monitoring processes.

In conclusion, configurable monitoring is required by in any current architecture (for instance IPSphere) which manages multi-domain services. Our proposals fit with them and complement them with a flexible monitoring function.

Acknowledgements

This work has been performed within collaboration with Alcatel-Lucent Bell Labs France.

REFERENCES

[1] Brownlee, N., Mills, C., Ruth, G.: Traffic Flow Measurement: Architecture. RFC 2722, October 1999.

[2] Sadasivan, G., Brownlee, N., Claise, B., Quittek, J.: Architecture for IP Flow Information Export. RFC 5470, May 2009.

[3] Claise, B., Johnson, Ed. A., Quittek, J.: Packet Sampling (PSAMP) Protocol Specifications. RFC 5476, March 2009.

[4] Strohmeier, F., Dörken, H., Hechenleitner, B.: AQUILA distributed QoS measurement. In: International Conference on Advances in Communications and Control, Crete, Greece, 2001.

[5] Molina-Jimenez, C., Shrivastava, S., Crowcroft, J., Gevros, P.: On the monitoring of Contractual Service Level Agreements. In: the first IEEE International Workshop on Electronic Contracting, WEC, San Diego , CA, USA, 2004.

[6] Schmoll, C, Boschi, E.: Final Architecture Specification. Delivrable 15, INTERMON, 2004.

[7] Boschi, E., D'Antonio, S., Malone, P., Schmoll, C.: INTERMON: An architecture for inter-domain monitoring, modelling and simulation. In: NETWORKING 2005, Pages 1397 - 1400, Springer Berlin / Heidelberg, 2005.

[8] A. Mehaoua et al.: Service-driven inter-domain QoS monitoring system for large-scale IP and DVB networks. In: Computer Communications, Volume 29, 2006.

[9] Dabrowski, M., Owezarski, P., Burakowski, W., Beben, A.: Overview of monitoring and measurement system in EuQoS multi-domain network. In: International Conference on Telecommunications and Multimedia (TEMU'06), Greece, 2006.

[10] Net Meter. http://www.hootech.com/NetMeter/ [6 October 2008].

[11] Uzé, J.-M.: IPSphere Forum: status on technical specifications. In: TERENA Networking Conference 2007, Copenhagen, Denmark, 2007.

[12] Chimento, P., Ishac, J.: Defining Network Capacity. RFC 5136, February 2008.

[13] Almes, G., Kalidindi, S., Zekauskas M.: A One-way Delay Metric for IPPM. RFC 2679, September 1999.

[14] Demichelis, C., Chimento, P.: IP Packet Delay Variation Metric for IP Performance Metrics (IPPM). RFC 3393, November 2002.
[15] Almes, G., Kalidindi, S., Zekauskas, M.: A One-way Packet Loss Metric for IPPM. RFC 2680, September 1999.
[16] Mahdavi, J., Paxson, V.: IPPM Metrics for Measuring Connectivity. RFC 2678, September 1999.
[17] Telecommunication Standardization Sector of ITU: Internet protocol data communication service - IP packet transfer and availability performance parameters. Y.1540, March 2000.
[18] Katz, D., Ward, D.: Bidirectional Forwarding Detection. draft-ietf-bfd-base-11.txt, January 2010.
[19] Amante, S. et al.: Inter-provider Quality of Service. White paper draft 1.1, 2006.
[20] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., Zekauskas, M.: A One Way Active Measurement Protocol (OWAMP). RFC 4656, September 2006.
[21] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., Babiarz, J.: A Two-Way Active Measurement Protocol (TWAMP). RFC 5357, October 2008.
[22] Hill, J.: Assessing the accuracy of active probes for determining network delay, jitter and loss". MSc Thesis in High Performance Computing, 2002.
[23] Evans, J. W., Filsfils, C.: Deploying IP and MPLS QoS for Multiservice Networks: Theory & Practice. Morgan Kaufmann, 2007.
[24] Case, J., Fedor, M., Schoffstall, M., Davin, J.: A Simple Network Management Protocol (SNMP). RFC 1157, May 1990.
[25] Claise, B.: Specification of the IP Flow Information Export (IPFIX) protocol for the exchange of IP traffic flow information. RFC 5101, January 2008.
[26] Naidu, K.V.M., Panigrahi, D., Rastogi, R.: Detecting anomalies using end-to-end path measurements. In: the 27th Conference on Computer Communications, INFOCOM 2008, Phoenix, AZ, USA, 2008.
[27] Barford, P., Duffield, N., Ron, A., Sommers, J.: Network performance anomaly detection and localization. In: the 28th Conference on Computer Communications, INFOCOM 2009, Rio de Janeiro, Brazil, 2009.
[28] Chu, L.W., Zou, S.H., Cheng, S.D., Wang, W.D., Tian, C.Q.: A distributed multi-domain oriented fault diagnosis algorithm. In: the 2nd IEEE International Conference on Computer Science and Information Technology, Beijing, China, 2009.