Proposal for the configuration of multi-domain network monitoring architecture

Aymen Belghith, Bernard Cousin, Samer Lahoud, Siwar Ben Adj Said

Proposal for the Configuration of multi-domain Network Monitoring Architecture

Aymen Belghith, Bernard Cousin, Samer Lahoud, and Siwar Ben Hadj Said
Université de Rennes I - IRISA, Campus de Beaulieu,
35042 Rennes Cedex, France
Email: aymen.belghith@univ-rennes1.fr, bernard.cousin@irisa.fr, samer.lahoud@irisa.fr, siwar.ben_hadj_said@irisa.fr

***Abstract*—In Internet networks, monitoring is necessary to guarantee the performance of the services. In this paper, we review the state-of-the-art monitoring architectures proposed for multi-domain networks. We note that these architectures do not support measurement configuration that enables the providers to perform flexible multi-domain measurements. Therefore, we present our proposal for the configuration of the multi-domain network monitoring architecture in order to give more flexibility in network monitoring and solve the heterogeneity and interoperability problems. We also present our collaboration schemes that can be applied in our configurable monitoring architecture. These collaboration schemes, based on the proactive selection and reactive selection, are used to select the measurement points that participate in the multi-domain monitoring and configure the parameters of the measurement points selected. 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 network monitoring. Many monitoring architectures were proposed for intra-domain networks such as in [1] and [2] or proposed for multi-domain networks. A monitoring architecture can use standard protocols such as RTFM [3], IPFIX [4], and PSAMP [5]. In this paper, we interest in multi-domain monitoring.

Many projects proposed multi-domain network monitoring architectures. 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 objective of the monitoring system of the ENTHRONE project is to verify whether the QoS performance are respected using active and passive measurements [7]. The Monitoring and Measurement System (MMS) of the EuQoS project provides traffic measurements in real-time [8]. More details of these multi-domain monitoring architectures are presented in section II.

The heterogeneity aspect of the different domains makes the multi-domain network monitoring an important and challenging problem. However, we note that all the above monitoring 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. Moreover, each domain wants to keep some monitoring processes or measurement results private. This requirement is called the confidential domain requirement.

Network 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, the export parameters such as the export methods have to be configurable. This requirement is called the adaptive export process requirement.

Due to the heterogeneity of the measurement parameters which can be used by different domains, 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.

In this paper, we present our proposal for the configuration of multi-domain network monitoring architecture that resolves the heterogeneity problems by providing the adaptive measurement process and the adaptive export process requirements. So, both the measurement parameters and the export parameters can be configured. Our proposal also resolves the confidentiality problems by providing the confidential requirement. For instance, 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.

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

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.

A. INTERMON architecture

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 [6]. 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 network 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 measurement results request, the distant provider checks if the sender has the right to obtain such information, using the AAA server.

B. ENTHRONE architecture

The management monitoring architecture of ENTHRONE consists of three levels: Node level Monitoring (NodeMon), Network level Monitoring (NetMon), and Service level Monitor (ServMon) [7].

- 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 NetMon 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.

C. EuQoS architecture

The Monitoring and Measurement System (MMS) of the EuQoS project provides traffic measurements in real-time [8]. 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 [9] 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.

D. 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

TABLE I
MULTI-DOMAIN MONITORING ARCHITECTURES VS MONITORING REQUIREMENTS.

Architectures	Confidential domain	Adaptive measurement process	Adaptive export process
INTERMON	Yes	Partially	No
ENTHRONE	No	Partially	No
EuQoS	No	No	No
Our architecture	Yes	Yes	Yes

block of the INTERMON architecture uses a standardized export protocol (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. 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 parameters are not sufficient in a heterogeneous environment. Then, the adaptive measurement process requirement is not totally fulfilled while the adaptive export process requirement is not fulfilled.

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, there is no configuration functional block in the EuQoS architecture. Therefore, this monitoring architecture does not fulfill the adaptive measurement process and the adaptive export process requirements.

Therefore, we propose that the multi-domain network monitoring architecture has to be configurable in order to fulfill these requirements: the confidential domain, the adaptive measurement process, and the adaptive export process requirements. Table I presents whether these requirements are fulfilled by the different monitoring architectures.

III. PROPOSALS FOR THE CONFIGURATION OF THE MULTI-DOMAIN MONITORING

Our proposal for the configuration of the network monitoring should adapt to any compatible multi-domain network architecture like the architecture model defined by the IPSphere forum [10]. 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.

A. Configuration functionality localization

We propose to locate the multi-domain configuration functionality at the AO since the global network resources are managed by this entity. Likewise, we propose that the intra-domain configuration functionality is coupled with the EO as this entity manages the resources of its network domain. Therefore, the AO is responsible for the configuration of all the domains that participate in the multi-domain monitoring through their EOs.

B. Measurement points selection

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 measurement points that participate in this monitoring are selected by the AO. The selection of the measurement points can be done during or after the service establishment. An EO can participate in the selection by preselecting a list of useful measurement points in its domain. The selection can be proactive or reactive. For both selection methods, the configuration entities 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, and its monitoring capacity (that represents the maximum number of services that can be monitored simultaneously).

1) Proactive selection: In the 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 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 that the path routing can take into account the characteristics of the measurement points. For example, the routing algorithm selects compatible measurement points which can still monitor other services, i.e. having a monitoring capacity greater than zero.

2) Reactive selection: In the reactive selection, on the AO request, each concerned domain transmits the information about the useful measurement points for a specific monitored service. Each EO preselects the measurement points and answers the request. The reactive selection allows the EOs to avoid measurement points update procedure and decreases, for a given service, the amount of exchanged data for the publication (only preselected measurement points are sent). However, the selection has to be performed with each new incoming multi-domain monitoring request. Furthermore, the

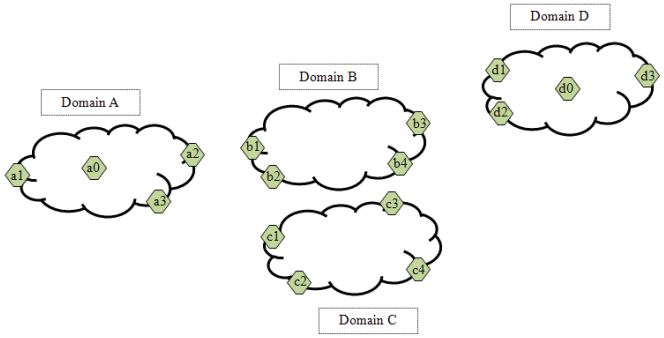

Fig. 1. Multi-domain network monitoring scenario.

AO can select the measurement points only when it receives all the responses from all the domains concerned by the multi-domain monitoring request. Therefore, the measurement points selection can produce extra delay.

In practice, when the monitoring is established after the service path establishment, the reactive selection mode becomes more interesting while the proactive selection mode becomes useless. Indeed, there is no need to send all the measurement points characteristics to the AO when the path of the monitored service is already established.

C. Measurement points configuration

After selecting the measurement points that will participate in the multi-domain monitoring of a given service, the AO configures the domains that belong to the path of this monitored service. In both above selection methods, we propose that the AO requests the configuration entities of the domains on the monitored path to activate the selected measurement points. Furthermore, we propose that each intra-domain configuration entity configures its measurement and export parameters. 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 $a0$ belonging to domain A and measurement point $d2$ belonging to domain D (see Fig. 1), 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 One-Way Delay [11]), the same measurement protocol (for example One Way Active Measurement Protocol [12]), and the same export method (for example periodic, each 5 s). These monitoring parameters are selected among the set of the metrics, 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 as the values of these parameters have to be chosen properly. Moreover, even if the values of the different parameters are chosen in a coordinated and suitable manner, the configuration is still necessary. Indeed, when the active monitoring is used, the localization of the measurement points have to be configured. For example, for confidentiality reasons, when we need to perform active measurements between measurement point $a0$ and measurement point $d2$ (see Fig. 1) 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 $a0$ and $a2$ and between measurement point $a2$ and $d2$. Therefore, the localization of measurement point $a0$ 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. Performance evaluation of the proposed collaboration schemes

A. Simulation model

In this section, we consider a multi-domain network topology formed by four domains and fourteen measurement points (see Fig. 1). 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 simulation time is equal to 1500 s. The monitoring requests arrival is chosen according exponential distribution on $[1, 200]$. The measurement point capacity is chosen according uniform distribution on $[100, 120]$. The measurement point capacity represents the maximum number of services that a measurement point can monitor simultaneously. The different values of the incompatibility ratio are 0 (all the MPs are compatibles), 0.1, 0.3, and 0.5. 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 we take ten measurement points, then there is, in average, one measurement point that is not compatible with all the other ones.

B. Simulation results for compatible measurement points

First, we consider the case where all the measurement points are compatible (incompatibility ratio is equal to zero). We evaluate the following performance criteria:

- The blocking percentage due to the measurement points surcharge: represents the percentage of the monitoring requests that are blocked because there is at least one measurement point on the path that reaches its maximum monitoring capacity. We note that the blocking percentage due to the measurement points incompatibility is equal to zero since all the measurement points are compatible.
- The monitoring throughput: represents the throughput of messages used to publish the measurement points

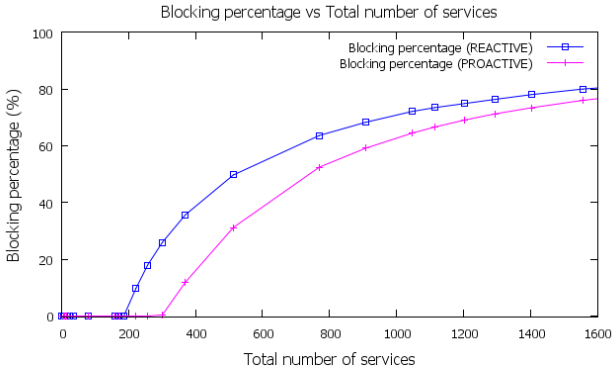

Fig. 2. Blocking percentage vs total number of the generated services during simulation.

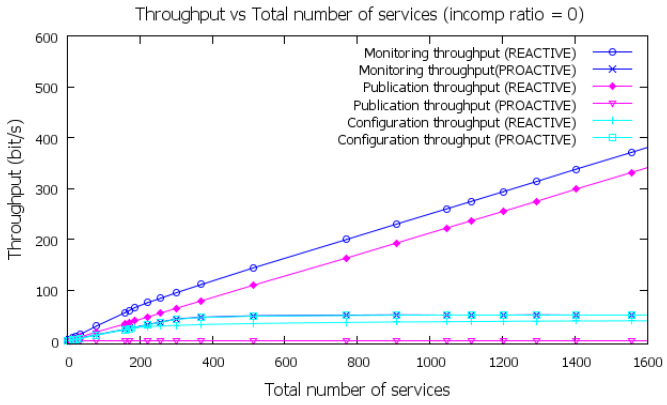

Fig. 3. Throughput vs total number of services.

characteristics (called publication throughput) added to the throughput of messages used to configure the measurement points (called configuration throughput).

- The delay of the monitoring establishment: represents the difference between the time of configuration of all the measurement points that participating in the monitoring of a given service and the time of the reception of the monitoring request by the AO. We consider only the accepted monitoring requests (the blocked monitoring requests are not considered in the delay computations).

1) Blocking percentage evaluation: Fig. 2 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 subsection IV-A, 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 not reach their maximum monitoring capacity yet. From a total number of services approximatively equal to 200, the blocking percentage of the reactive mode starts increasing while the blocking percentage of the proactive mode remains null for a total number of services equal to 300.

We notice that the proactive mode outperforms the reactive mode because when the proactive 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 still have the capacity to monitor further services. However, when the reactive mode is applied, the path for a given service is already established and thus sometimes it must use a measurement point that has already reached its maximum monitoring capacity.

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

2) Throughput evaluation: Fig. 3 represents the monitoring throughput, the publication throughput, and the configuration 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 configurable monitoring architecture to monitor more services than the reactive mode (the proactive mode is flexible and thus it generates lower monitoring requests blocking percentage, see Fig. 2). Indeed, more monitoring requests are blocked, less throughput is generated.

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 (i.e., the measurement points characteristics remains the same during 1500 s). 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. This is because the AO does not know the measurement points that are on the service path. The AO knows only the source node, the destination node, and the domains on the path.

Recall that the monitoring throughput is equal to the configuration throughput added to the publication throughput. The publication throughput is more important than the configuration throughput and so it has more effect on the monitoring throughput. Consequently, 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. Moreover, the number of accepted monitoring requests depends on the monitoring capacity of the different measurement points as well as on the total number of the generated monitoring requests.

3) Delay evaluation: The mean delay of the monitoring establishment is presented in Table II. 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 and

TABLE II
MEAN DELAY OF THE MONITORING ESTABLISHMENT.

Collaboration mode	Proactive	Reactive
Mean delay (s)	0.1	0.18

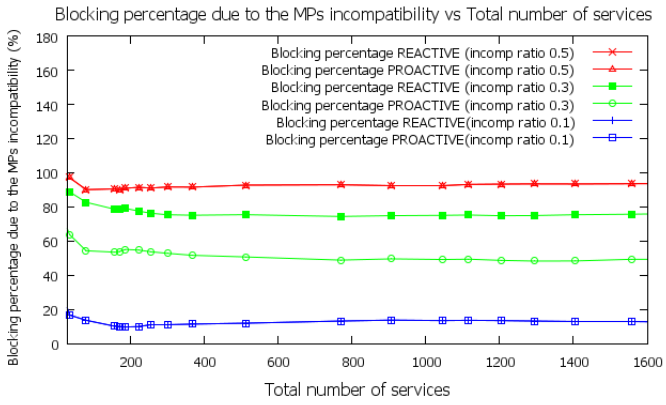

Fig. 4. Blocking percentage due to the MPs incompatibility vs total number of services (for different incompatibility ratios).

does not need further information from the EOs to select the useful measurement points. However, when the reactive mode is used, the AO cannot locally select the useful measurement points. It has to send messages to the EOs concerned by the multi-domain monitoring in order to request the list of the preselected measurement points and then has to wait their responses before making decision.

C. Simulation results for measurement points having different incompatibility ratios

Now, we study the blocking percentage due to the MPs incompatibility for measurement points having incompatibility ratio equal to 0.1, 0.3, and 0.5. Fig. 4 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.

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

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. However, when the reactive mode is used, the services paths are already established and then the measurement points that can participate in the multi-domain monitoring are limited.

For an incompatibility ratio equal to 0.5, both collaboration modes present the same blocking percentage due to the MPs incompatibility. Indeed, when the incompatibility ratio is important, even the proactive mode cannot find a path (specially if the path has to cross many domains and then many measurement points) that contains only compatible measurement points.

V. CONCLUSION

In this paper, we have presented 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 configuration of the monitoring parameters to achieve an efficient monitoring of the multi-domain networks.

Our proposal for the configuration of the multi-domain network monitoring consists in the localization of the configuration entities, the selection of the measurement points, and the configuration of the selected measurement points. Two collaboration modes are proposed for the selection and the configuration of the measurement points: the proactive and the reactive modes. We have showed, through extensive simulations, that the proactive mode outperforms the reactive mode in terms of blocking percentage, monitoring throughput, and delay of monitoring establishment.

ACKNOWLEDGMENT

This work has been performed within a collaboration with Alcatel-Lucent Bell Labs France, under the grant n. 09CT310-01.

REFERENCES

[1] Strohmeier, F., Dörken, H., Hechenleitner, B.: AQUILA distributed QoS measurement. In: International Conference on Advances in Communications and Control, Crete, Greece, 2001.
[2] 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.
[3] Brownlee, N., Mills, C., Ruth, G.: Traffic Flow Measurement: Architecture. RFC 2722, October 1999.
[4] Sadasivan, G., Brownlee, N., Claise, B., Quittek, J.: Architecture for IP Flow Information Export. RFC 5470, May 2009.
[5] Claise, B., Johnson, Ed. A., Quittek, J.: Packet Sampling (PSAMP) Protocol Specifications. RFC 5476, March 2009.
[6] 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.
[7] A. Mehaoua et al.: Service-driven inter-domain QoS monitoring system for large-scale IP and DVB networks. In: Computer Communications, Volume 29, 2006.
[8] 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.
[9] Net Meter. http://www.hootech.com/NetMeter/ [6 October 2008].
[10] Uzé, J.-M.: IPSphere Forum: status on technical specifications. In: TERENA Networking Conference 2007, Copenhagen, Denmark, 2007.
[11] Almes, G., Kalidindi, S., Zekauskas M.: A One-way Delay Metric for IPPM. RFC 2679, September 1999.
[12] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., Zekauskas, M.: A One Way Active Measurement Protocol (OWAMP). RFC 4656, September 2006.