A Collaborative Solution for SNMP Traces Visualization

Vinícius Tavares Guimarães, Gléderson Lessa dos Santos, Guilherme da Cunha Rodrigues,
Lisandro Zambenedetti Granville, Liane Margarida Rockenbach Tarouco
Computer Networks Group
Institute of Informatics
Federal University of Rio Grande do Sul
Porto Alegre, Brazil
Email: {vtguimaraes,gcrodrigues,glsantos,granville,tarouco}@inf.ufrgs.br

***Abstract*— RFC 5345 proposed by NMRG of the IRTF, outlines a consistent methodology for SNMP traffic measurements and analysis. However, it does not address how to visualize the SNMP traffic being observed, *i.e.*, network operators are left with no proper resources to visually recognize behaviors and patterns on SNMP traffic traces. In this sense, Information Visualization concepts have been investigated, thus complementing RFC 5345. Although previous work showed the feasibility of Information Visualizations as an end-user tool on top of RFC 5345 methodology, an important aspect has not been exploited: collaboration among users (*e.g.*, network operators). In this paper we present the design, implementation, and a proof of concept of a solution to support SNMP analyses using a collaborative approach and visualization techniques.**

***Keywords*—SNMP Analyses, Collaboration, Visualization.**

I. Introduction

In 2008, the Network Management Research Group (NMRG) of the Internet Research Task Force (IRTF) proposed a Request for Comments (RFC) entitled "Simple Network Management Protocol (SNMP) Traffic Measurements and Trace Exchange Formats" [1]. While RFC 5345 outlines a consistent methodology for SNMP traffic measurements and analysis, it does not address how to visualize the SNMP traffic being observed. Network operators are then left with no proper resources to visually recognize behaviors and patterns on SNMP traffic traces.

Our previous [2][3][4] work exploited the use of Information Visualization concepts in SNMP traffic analysis, thus complementing RFC 5345 methodology. The main goal was to increase the potential insights operators could have by using a set of proposed visualization techniques. Although the previous work showed the feasibility of Information Visualizations as an end-user tool on top of RFC 5345 methodology, an important aspect has not been exploited: collaboration among network operators. As a consequence, insights experienced by an operator was restricted to him/her, once the proposed visualizations did not provide additional features, for example, to take notes about particular pattern, to share insights with other operators, and to search for similar use cases.

We argue that an approach to increase collaboration among network operators is important because: (*i*) network operators that manage different production environments can exchange experience in order to recognize management patterns; (*ii)* researchers can use the approach to better understand the actual employment of SNMP; and (*iii)* inexperienced operators have the opportunity to learn from more experienced ones.

In this paper we present the design, implementation, and a proof of concept of a solution, named *mtAnalyzerV2*, to support the analysis of SNMP traces in a collaborative way. As such, we take a step further than our previous efforts by providing visualization techniques and a set of user-friendly capabilities that enable the collaboration among network operators. To achieve that, we have used the background from our previous work to design our conceptual solution, and new Web technologies (*e.g.*, HTML5, CSS3, SVG, D^3 Data-Driven Documents [5]) to materialize our proposal. As a proof of concept, we have implemented a Web tool prototype that presents two visualizations with collaboration support.

The remainder of this paper is organized as follows. In section II, we present the background and related work. In Section III we introduce our proposed solution. In Section IV, we present a proof of concept to demonstrate the feasibility of our proposal. Finally, we close this paper in section V, where final remarks and directions for future work are discussed.

II. Related Work

Information Visualization techniques is the use of computer-supported, interactive, visual representations of abstract data to amplify cognition [6]. In this sense, Information Visualization techniques are able to provide a set of capabilities to assist network operators in their day-to-day tasks. Actually, visualizations as a tool to help human operators in management tasks is as an old topic and is highlighted as a research challenge in the area of network management [7].

In the literature, the first investigations in this field started in a half of the 80s [8][9]. In the 90s, Becker *et al.* [10] presented a relevant research (the most cited article, by Google Scholar) showing the deployment of in telecommunication network management. They used techniques such as spatial link-node representation, matrix layout, and glyphs representation. Other works were published by this research team in the 90s [11][12][13]. Still in the 90s, Rohrer and Swing [14] developed two Web-based information visualization prototypes to visualize computer network topologies and network traffic monitoring. Munzner *et al.* [15] presented a case study of visualizing the global topology of the Internet multicast backbone using interactive 3D maps through Web.

Over the last years, several works have been related to security discipline. Shivari *et al.* [16] presents a wide survey about visualization systems for network security, where the visualization systems are grouped by use-case class and classified by the employed visualization techniques. Additionally, this research outlines several specific aspects related to each analyzed visualization system and potential data source(s) for security visualizations.

The efforts in other management disciplines are more spread. Oberheide *et al.* [17] presented a software tool called Flamingo that can be used to explore Internet traffic flow data, offering a set of interactive visualizations and associated manipulation tools that can help users in network data analysis. Hofstede and Fioreze [18] introduced a network monitoring tool (SURFmap) that provides network traffic information at a geographical dimension by using the Google Maps API, and allows different levels of abstraction in the network data visualization. In the SNMP analysis context, Schoenwaelder *et al.* [19] introduced an approach to capture and analyze SNMP traffic traces, as well as showing preliminary static visualizations. Although the main goal of this work was not on visualizations, the flow topologies created from analyzed traces highlights the facilities provided by visualizations.

In our previous works [2][3][4], we introduced the employment of Information Visualization techniques to assist SNMP analysis based on the methodology described in RFC 5345. This document presents a systematic methodology for measurements and statistics generation of SNMP traces in order to identify usage patterns of the protocol, and can be depicted in a bottom-up approach composed by five steps. However, it does not address how to visualize the SNMP traffic being observed. In this sense, our previous works proposed a vertical extension [2][3][4], wherein a new step is accomplished on the top of RFC 5345 as shown in Figure 1.

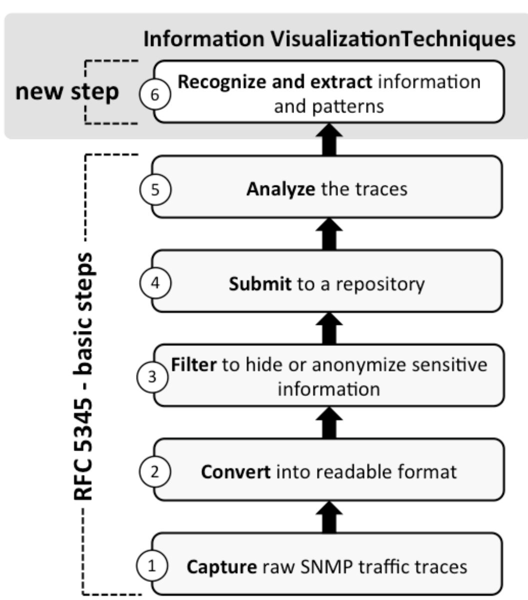

Figure 1. Bottom-up approach for RFC 5345 with a new step

From that perspective, Salvador and Granville [2][3] presented three visualization techniques (*i.e.*, nodes and links, MIB-tree, and histogram) for visualizing information related to SNMP traffic measurements. Barbosa and Granville [4] proposed a set of interactive visualization techniques (*e.g.*, management topology, scatterplot, bar histogram, and force-directed layout) adapted for the study of SNMP and an insight-oriented approach to evaluate the employed visualization techniques.

Although these investigations showed the feasibility of Information Visualizations as an end-user tool on top of RFC 5345 methodology, an important aspect has not been exploited: collaboration among network operators. We argue that an approach to increase collaboration among network operators is important because: (*i*) network operators that manage different production environments can exchange experience in order to recognize management patterns; (*ii*) researchers can use the approach to better understand the actual employment of SNMP; and (*iii*) inexperienced operators have the opportunity to learn from more experienced ones. Additionally, we believe that this approach is according to ease of use requirement from the operators' point of view [20].

III. Proposal

In our first investigations about SNMP traffic analysis, we built a prototype tool named *mtAnalyzer* (acronym for Management Traffic Analyzer) [2][3][4]. The solution proposed in this work is based on the acquired knowledge from the development of previous release of *mtAnalyzer*. Hereinafter, we name the current proposal as *mtAnalyzerV2*. In this section we first present a description of the conceptual building blocks of our proposed solution. Afterwards, we present the end-users perspective. Next we present the collaborative model. Finally, we discuss about the solution functionalities to achieve collaboration among network operators.

A. Conceptual Solution

Figure 2 presents the conceptual building blocks of the proposed solution. In order to include collaboration in SNMP traffic observations, we have designed the proposed solution based on traditional client-server model for Web applications. Thus, it encompasses three main layers: (*i*) **Front-end Layer (L1):** provides a user-friendly interface for the end-users of solution, by allowing these users to interact with the system features in a collaborative fashion. Based on Figure 1, this layer encompasses the fifth and sixth step; (*ii*) **Back-end Layer (L2):** it is responsible for the control engine that orchestrates the low-level tasks and the business logic. Based on Figure 1, this layer encompasses the second, third, fourth and fifth step; and (*iii*) **Storage Layer (L3):** it is responsible for store system information (*i.e.*, system database) and system files (*i.e.*, SNMP traces repository and analysis scripts repository).

We highlight that our proposal does not consider the first step shown in Figure 1, since the SNMP traffic traces are submitted by end-users. The functionalities offered by our solution can be understood under the end-user perspective. For instance, the end-users can be network operators that intend perform SNMP observations from their traffic traces, researchers, or simply a beginner that wants to learn about SNMP analysis.

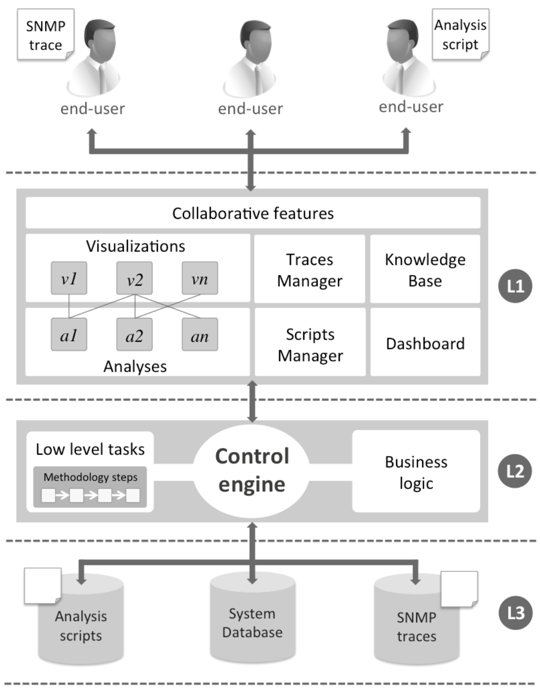

Figure 2. Proposed Solution

B. End-user perspective

Although the solution does not intend to control users by their skills or professional activities, we introduce some related aspects that underlie our approach. Network operators are the main target users of the solution. In practice, network operators are spread in many types of institutions, *i.e.*, they are owners of the most important information for any SNMP analysis, since they have access to SNMP traces from production network environments. Moreover, each network operator needs to deal with the peculiarities of the managed environment, *i.e.*, he/she has expertise obtained from different use cases that can be very important to reasoning over some SNMP usage pattern, for example.

On the other hand, the proposed solution is designed to support a range of users that are interested in SNMP observations and not necessarily are network operators. For instance, a developer who uses the Net-SNMP package to build SNNP managers, could offer relevant contributions from his/her experience about the implementation of SNMP operations (*e.g.*, Get, Get-Next). He/She can be regarded as a SNMP expert, although does not perform the same tasks of a traditional network operator. Another example refers to a researcher who studies the SNMP protocol. He/She can use the proposed solution to find novel research challenges, or contributing with his/her knowledge to develop further analysis scripts.

C. Collaborative model

Our proposal wishes to encourage the involvement of all people that are interested in SNMP measurements and analyses. In this sense, we believe that the collaborative features could not increase the end-user overhead, *i.e.*, they need to be designed using well-known concepts and with no hard operation rules. Based on this assumption, we adapted the 3C (*Communication*, *Cooperation*, and *Coordination*) collaboration model introduced by Fuks *et al.* [21] as shown in Figure 3. This model is flexible and widely employed to define the collaboration process in groupware solutions. For the proposed solution, the interaction between each *C* box is enforced by optional actions. For instance, *Cooperation* does not necessarily need to define *Coordination*, *i.e.*, it is an optional rule for users who cooperate.

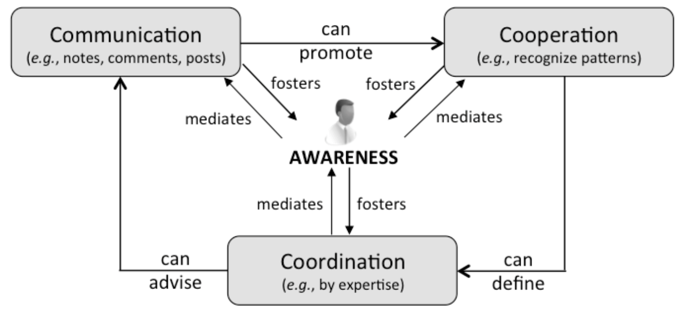

Figure 3. The 3Cs mapped onto our solution

The collaboration process is divided in three main dimensions: *Communication*; *Cooperation*; and *Coordenation*. *Communication* corresponds to the functionalities in which end-users can share or exchange information. By *Communication* process, end-users can promote *Cooperation*. For instance, a group of end-users who cooperate to understand or recognize a certain pattern arising from an analysis script. *Cooperation* can define *Coordination*, *i.e.*, depending upon the goal of analysis, end-users who cooperate, can choose for a coordinator to advise the *Communication*.

The collaborative rules were modeled to be represented in the *System database*. For instance, when an end-user shares a traffic trace with other users, this procedure is received by *Control engine* that sends to *Business logic* module. In the *Business logic* module this request is processed and stored in the *System database*. Another case refers to control the end-user groups in a cooperation process. For example, a group of users (*i.e.*, who cooperate) decide appoint a coordinator to mediate observations about certain SNMP traffic trace.

D. Functionalities

Under the end-user perspective, all functionalities are available in the layer L1. The block on the top provides the *Collaborative features*. This module encompasses the control of shared information, end-user groups, and communication tools. These control information are requested to the *Control engine* that retrieves the information from the system database (L2), processes this information in the *Business logic* component, and returns the processed information to the *Collaborative features* module. On the client-side of layer L1, we have used a set of technologies related to the ”Open Web Platform” [22]. In this sense, we have selected technologies to build user-friendly Web interfaces according to W3C standards. By doing that, we could develop responsive interfaces to support modern mobile devices, such as smartphones and tablets.

Through the *Traces manager* an end-user can submit a traffic trace by filling a form, and uploading the trace file. This form demands meta data information about the traffic trace, *i.e.*, name of the network, owner, description of the measurement point, collecting period, and additional information about the trace. The submitted traces are stored in the SNMP traces repository. In this module the end-user can also manage traffic traces in order to grant or revoke access to other users.

In the *Scritps manager*, the end-user can interact in two main ways: access the analysis scripts repository; and submit a new analysis script. In the first one, the end-user can view a list of analysis scripts that are available. For each analysis script the user can view a description, the developer info, and the semantic of the output data produced by script. To submit a new analysis script, the user fills a form to explain the script goal and the output data, to indicate users who will evaluate it, and to suggest a visualization technique to aid in the SNMP observations. During the evaluation period, the involved users can exchange information. After the evaluation period, the script can be accepted or denied.

The *Visualizations* and *Analyses* module are integrated. Basically, an analysis (*e.g.*, *a1* in Figure 2) is a set of data generated by an analysis script. These data are generated from an analysis script that processes a traffic trace in readable format. Depending on the structure and semantic of the data, a given analysis may be visualized by one or more visualization techniques. This composition is possible because all of analysis scripts are associated to least one visualization. Additionally, the *Visualizations* module provides features in which user can take notes about his/her observations and control the sharing of such information.

An important aspect refers to the fact that information processed by the analysis scripts are summarized and stored in the *System database*. This approach intends optimize the amount of data for a better performance in the features that run on the client-side, in special, for the Visualizations. Specifically, to record the data produced from an analysis script, we have used a customized mechanism. The proposed mechanism is shown in Figure 4. Basically, when a new analysis script is added to *mtAnalyzerV2*, two relations are created, as follow:

- ***Control Relation (CR):*** relation (e.g., *s1_control* as shown in Figure 4) responsible to store the operator identifier (an user of *mtAnalyzerV2*), the traffic trace identifier, and an internal identifier that will be used to reference the data recorded in the Data Relation;
- ***Data Relation (DR):*** relation (*e.g.*, *s1_data* as shown in Figure 4) responsible to store the processed data from a specific analysis script performed from a SNMP traffic trace by a given user.

Basically, the CRs provide a lightweight way to retrieve information about traffic traces processed by users for a specific analysis script. The DRs strategy allows reducing the response time of database queries, once the vertically grow (number of rows) of relations is slower. This approach is feasible since we assume that the semantic of the data generated by an analysis script is preset, *i.e.*, the structure of a DR is designed based on the semantics of the data of its corresponding analysis script. By doing that, is simpler to execute operations such to compare two or more traffic traces from different operators in a cooperative fashion, for example.

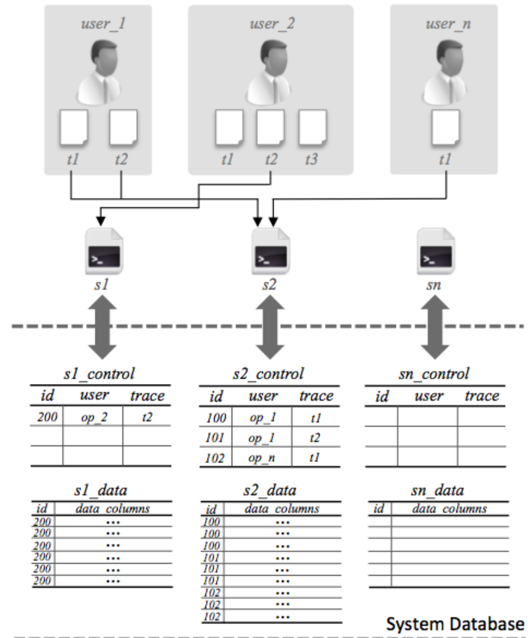

Figure 4. Custom approach to store data from analysis scripts

Through the *Visualizations* and *Traces manager* modules, end-users can fill forms to provide complementary information such as types of managed devices (*e.g.*, router, switch, host), device vendors (*e.g.*, Cisco, Juniper, Huawei), monitoring system (*e.g.*, IBM Tivolli, Cacti, Zabbix), and usage preferences (*e.g.*, poll intervals, SNMP versions, traps enabled).

The *Knowledge database* and *Dashboard* complement the layer L1. *Knowledge database* provides features to submit or to search any information related to SNMP traffic analysis. The information stored in the *Knowledge database* are classified by grades assigned by users, which is used as a main criterion to show search results. The *Dashboard* is composed by an integrated interface that enables end-user to access the other modules, visualize notifications from other users, and manage scheduled tasks.

IV. Proof of Concept

In this section we introduce the first results obtained by implementing the proposed solution. It is important to highlight that *mtAnalyzerV2* is under construction, *i.e.*, we have considered that current development stage as a release prototype. In addition, our goal is focused on the *mtAnalyzerV2* features, *i.e.*, discussions about SNMP analysis are out of the scope of this proof of concept.

We start from the network management topology interface (Figure 5). Basically, network management topology inherits visual and interactive features of our previous visualizations [4]. For instance, network operators can submit a SNMP traffic trace and the devices that act as managers, agents, or both are identified and plotted in a node-link graph representation. Additionally, interaction features on management topology have been maintained, such as: zooming and panning of the view; tooltip exhibition when nodes or edges are spotted; the possibility of moving the nodes around the view in order to edit the graph layout; and restore the initial layout. However, several novel features have been added.

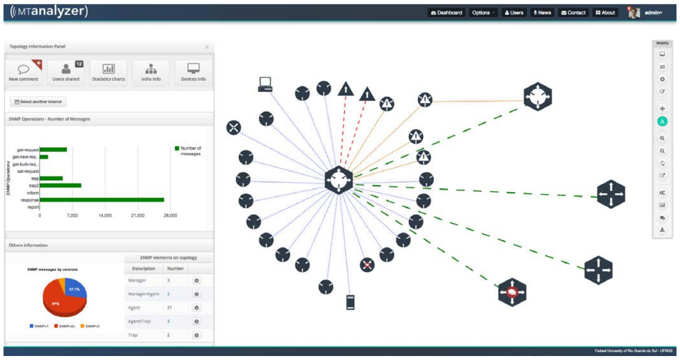

Figure 5. Network management topology, menu options, and topology dashboard

We have introduced a floating menu for faster and intuitive access by user. By doing that, users could access a set of options, beyond the abovementioned features. Add new nodes or connections, edit of nodes or the style of connections, remove nodes and connections are examples of operations that can be made. In this interface, nodes are represented by SVG glyphs. This approach allows an iconic pattern to recognize the meaning of each node on the topology (*e.g.*, SNMP agents, SNMP managers). In addition, SVG is a vector format that allows high-quality images in a lightweight way. As shown in Figure 5, the glyphs are not restricted to an abstract representation. In this sense, users could change a glyph that represents a SNMP agent to a glyph that represents the real device (*e.g.*, router, switch, server).

About collaborative capabilities, the management topology interface has a float dashboard on the left side. This dashboard combines a set of features. For instance, it displays traditional charts (*e.g.*, bar, pie, scatter plot) and tabular data from the statistics of the management topology. However, the main function of dashboard is to enable users to control, visualize, and share the information related to the network management topology. On top is placed a menu in which the user can add comments about his/her observations (*e.g.*, about a recognized pattern or an unexpected behaviour), share this information, control the users that have access to management topology information, provide information about the topology (*e.g.*, type of environment, monitoring tools, poll intervals), and information about devices that compose the topology (*e.g.*, types of device, device vendors). Additionally, we have implemented glyphs to visually notify users when any information is posted for the topology or some device. For instance, when a user is allowed to access a certain topology and adds a comment to collaborate on the analysis about a specific device behavior, this device is highlighted with balloons inside a red circle.

We have implemented parallel coordinates as a second visualization technique in our proof of concept (Figure 6). Parallel coordinates technique enables users to compare a set of traffic traces by analyzing multivariate data. This is an expected feature in a collaborative solution, since users can gain insights by observing multiple information from different SNMP traffic traces. Basically, each parallel axes represents a kind of information about a SNMP traffic trace. In our case, each axis represents, respectively, a quantifier of the number of managers, agents, get-request, get-next-request , get-bulk-request, set-request, trap , trap2, information, response, and report operations. In addition, we have used an interaction mechanism called *brushing*. *Brush* is a way to select a set of polylines in a choosen vertical axis to better understand the data relationships. Figure 6-A shows a selection window in the get-bulk-request axis.

Figure 6. Parallel coordinate visualization

In order to make easier the data understanding, information represented in the parallel coordinates are detailed in a grid below. Each column of the data grid represents a parallel axis in the visualization and each row represents a SNMP traffic trace. The grid is also integrated with the *brushing* interaction, *i.e.*, when user *brush* a set of data in a certain parallel axis, the grid is updated and proceeds to show just the data in the selection window of *brush*. In addition, the *mouseover* event for each row of the grid highlights the row values in the grid, as well as the polyline in the parallel coordinates visualization. Figure 6-B shows an example of this interactive function. About collaborative features, users can post or view comments for the selected trace traffic by clicking with right button upon the grid line.

We have also implemented a set of traditional features to improve collaboration and user experience. Firstly, we have implemented two asynchronous communication tools using e-mail messages and comments. The first one, can be used by an end-user to send invitations for a group of users to cooperate. The second is related to take notes or to comment about the insights obtained from the visualizations. In the user dashboard, users can also control the traffic traces, notifications from other users that collaborate with him/her, a list of online users, news about novel visualizations, and a task scheduler. In addition, we have implemented a first version of the knowledge database using a self-service portal.

V. Conclusions and Future Work

In this paper, we introduced a solution named *mtAnalyzerV2* to improve collaboration among network operators in SNMP traffic measurements and analysis. This solution uses the methodology described in RFC 5345 as base and provides an additional end-user layer on top of the methodology, in which visualizations techniques and a set of user-friendly capabilities are employed to achieve collaboration among network operators. We also presented a Web tool prototype to demonstrate the feasibility of our solution.

The main concepts related to the proposed solution are not properly novel. For instance, the 3C model for collaboration has been widely deployed in groupware applications. However, we observe that the lack of user-friendly capabilities and collaboration are a clearly gap to cope in order to encourage the involvement of network operators in SNMP traffic analysis. In this sense, the visual features provided by *mtAnalyzerV2* and its support to collaboration are promising. We believe that the user can obtain several insights from visualization. The parallel coordinate technique is an example. In this way, take notes about some recognized pattern is an important tool to register analysis information, as well as can contribute in cooperation among network operators. Finally, the use of novel Web trends can increase the user-experience of network operators by providing rich interfaces with no plugins or standalone installations, using the widely known Web features.

As future work, we plan to extend *mtAnalyzerV2* with novel visualizations that support collaboration. Additionally, we intend to investigate about human-centric evaluation techniques to quantify the benefits arising from collaboration. We further plan to explore other types of management traffics (*e.g.*, SSH/TELNET and ICMP traffics) in order to have support on other network management technologies.

References

[1] J. Schoenwaelder, "Simple network management protocol (snmp) traffic measurements and trace exchange formats," RFC 5345 (Informational), Oct. 2008. [Online]. Available: http://datatracker.ietf.org/doc/rfc5345/

[2] E. Salvador and L. Granville, "An investigation of visualization techniques for snmp traffic traces," in *Network Operations and Management Symposium, 2008. NOMS 2008. IEEE*, 2008, pp. 887–890.

[3] E. M. Salvador and L. Z. Granville, "Using visualization techniques for snmp traffic analyses." in *ISCC*. IEEE, 2008, pp. 806–811. [Online]. Available: http://dblp.uni-trier.de/db/conf/iscc/iscc2008.html#SalvadorG08

[4] P. T. Barbosa and L. Z. Granville, "Interactive snmp traffic analysis through information visualization." in *NOMS*. IEEE, 2010, pp. 73–79. [Online]. Available: http://dblp.uni-trier.de/db/conf/noms/noms2010.html#BarbosaG10

[5] M. Bostock, V. Ogievetsky, and J. Heer, "D3 data-driven documents," *Visualization and Computer Graphics, IEEE Transactions on*, vol. 17, no. 12, pp. 2301–2309, 2011.

[6] S. K. Card, J. Mackinlay, and B. Shneiderman, *Readings in Information Visualization: Using Vision to Think*, 1st ed. San Diego, CA, USA: Academic Press, 1999.

[7] A. Pras, J. Schoenwaelder, M. Burgess, O. Festor, G. Martinez Perez, R. Stadler, and B. Stiller, "Key research challenges in network management," *IEEE communications magazine*, vol. 45, no. 10, pp. 104–110, October 2007. [Online]. Available: http://doc.utwente.nl/64389/

[8] R. S. Gilbert and W. B. Kleinöoder, "Cnmgraf – graphic presentation services for network management," *SIGCOMM Comput. Commun. Rev.*, vol. 15, no. 4, pp. 199–206, Sep. 1985. [Online]. Available: http://doi.acm.org/10.1145/318951.319049

[9] B. Anderson and R. Linebarger, "A graphical representation for network management," in *Local Computer Networks, 1989., Proceedings 14th Conference on*, 1989, pp. 106–124.

[10] R. A. Becker, S. G. Eick, and A. R. Wilks, "Visualizing network data," *IEEE Transactions on Visualization and Computer Graphics*, vol. 1, no. 1, pp. 16–28, Mar. 1995. [Online]. Available: http://dx.doi.org/10.1109/2945.468391

[11] K. C. Cox and S. G. Eick, "Case study: 3d displays of internet traffic," in *Proceedings of the 1995 IEEE Symposium on Information Visualization*, ser. INFOVIS '95. Washington, DC, USA: IEEE Computer Society, 1995, pp. 129–. [Online]. Available: http://dl.acm.org/citation.cfm?id=857186.857581

[12] S. Eick, "Aspects of network visualization," *Computer Graphics and Applications, IEEE*, vol. 16, no. 2, pp. 69–72, 1996.

[13] E. Koutsofios, S. North, R. Truscott, and D. Keim, "Visualizing large-scale telecommunication networks and services," in *Visualization '99. Proceedings*, 1999, pp. 457–461.

[14] R. Rohrer and E. Swing, "Web-based information visualization," *Computer Graphics and Applications, IEEE*, vol. 17, no. 4, pp. 52–59, 1997.

[15] T. Munzner, E. Hoffman, K. Claffy, and B. Fenner, "Visualizing the global topology of the mbone," in *Information Visualization '96, Proceedings IEEE Symposium on*, 1996, pp. 85–92, 129.

[16] H. Shiravi, A. Shiravi, and A. A. Ghorbani, "A survey of visualization systems for network security," *IEEE Transactions on Visualization and Computer Graphics*, vol. 18, no. 8, pp. 1313–1329, Aug. 2012. [Online]. Available: http://dx.doi.org/10.1109/TVCG.2011.144

[17] J. Oberheide, M. Goff, and M. Karir, "Flamingo: Visualizing internet traffic," in *Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP*, 2006, pp. 150–161.

[18] R. Hofstede and T. Fioreze, "Surfmap: A network monitoring tool based on the google maps api," in *Integrated Network Management, 2009. IM '09. IFIP/IEEE International Symposium on*, 2009, pp. 676–690.

[19] J. Schoenwaelder, A. Pras, M. Harvan, J. Schippers, and R. van de Meent, "Snmp traffic analysis: Approaches, tools, and first results," in *Proceedings of the Tenth International Symposium on Integrated Network Management, Munich, Germany*. Piscataway: IEEE Computer Society, May 2007, pp. 324–332.

[20] J. Schoenwaelder, "Overview of the 2002 iab network management workshop," RFC 3535 (Informational), May 2003. [Online]. Available: http://datatracker.ietf.org/doc/rfc3535/

[21] C. J. P. Lucena, A. B. Raposo, M. A. Gerosa, and H. Fuks, "Applying the 3c model to groupware development," *International Journal of Cooperative Information Systems*, vol. 14, no. 02n03, pp. 299–328, 2005. [Online]. Available: http://www.worldscientific.com/doi/abs/10.1142/S0218843005001171

[22] I. Jacobs, J. Jaffe, and P. Hegaret, "How the open web platform is transforming industry," *Internet Computing, IEEE*, vol. 16, no. 6, pp. 82–86, 2012.