A Similarity Model for Virtual Networks Negotiation

Rafael L. Gomes, Luiz F. Bittencourt, Edmundo R. M. Madeira
Institute of Computing (IC), University of Campinas (UNICAMP), Brazil
{rafaellgom, bit, edmundo}@ic.unicamp.br

ABSTRACT

Many companies use the Internet as a basis for their services, defining Service Level Agreements (SLA) with their respective Internet Service Providers (ISP). However, the current Internet works in a best effort manner, that points toward the concept of network virtualization and Software Defined Networks (SDN) to support the Future Internet. Within this context, this work proposes a similarity model and a similarity metric that enable the client to negotiate protocols for SDN and Virtual Networks (VN). The proposed model enables the free competition among providers and allows the client to compare protocols offered by the providers to identify which ones best fulfill the requested requirements. Experiments showed the effectiveness of the proposed model.

Categories and Subject Descriptors

C.2.1 [**Computer Communication Networks**]: Network Architecture and Design;
C.2.2 [**Computer Communication Networks**]: Network Protocols

General Terms

Management, Standardization

Keywords

Similarity, Network Virtualization, Software Defined Networks, Negotiation, Future Internet.

1. INTRODUCTION

Internet has been growing and many companies use it as a basis for their services. Currently, there is no guarantee of service level on the Internet. Hence, there is a consensus that it needs to be updated, creating the "Future Internet". Along with this, the Network Virtualization (NV) arises as one of the important technologies for the Future Internet. NV is a technology that enables the deployment of multiple environments over the same physical infrastructure [3]. The flexibility of virtualization allows users and providers to negotiate several virtual services, with aspects related to both resources and features utilized, thus being the customization a characteristic of Virtual Networks.

Following the same way, the idea of Software Defined Networks (SDNs) arises as an important approach to be part of the Future Internet [6]. SDN is a network architecture which decouples the control plane and the forwarding task, enabling the programmability of the network [5].

The SDN and NV approaches can be merged using technologies as Flowvisor [16], which enables the slicing of the SDN in layers with configured resources and an independent network controller in each slice. With this, the Internet Service Provider (ISP) can isolate the slices in the SDN and deploy the functionalities that the client requests, as for example packet routing, resource reservation, and others. In this work, we consider VNs as networks that can be deployed as both SDN as well as with traditional virtualization approaches.

Based on the fact that different applications have distinct network requirements, when deploying a VN, the client negotiates a Service Level Agreement (SLA) with the ISPs to choose which one has the best proposal (i.e., the VN that best fits its requirements). Providers have different infrastructures and protocols to perform several tasks in the network, and some of these protocols could be private and others public. As an example, for a routing task one provider could utilize the Open Shortest Path First (OSPF), while other provider utilizes Routing Information Protocol (RIP).

The client is not necessarily concerned about which protocol is being used by the ISP. Actually, the client wants a protocol with some properties, which defines its behavior as a whole, according to the type of the application. For example, the client may want a protocol that has a low convergence time and is scalable. To the best of our knowledge, there is no protocol characterization model that enables the comparison between protocols of the same kind (which focus in the same task).

Within this context, this work proposes a protocol similarity model and a similarity for virtual networks negotiation. Our proposal focuses on two aspects of VN negotiation: (i) it describes a model to characterize the main kind of protocols that can be customized in a VN/SDN; and, (ii) it proposes a metric to evaluate the similarity between protocols of the same kind. The proposed model enables the free and fair competition between providers and allows the

client to identify which protocols offered by the providers best fulfill the requested requirements.

For example, if an ISP has an infrastructure based on an SDN technology, our similarity model allows it to send SLA proposals since it can describe a VN in the same way as a traditional ISP with a TCP/IP network. The ISPs with distinct infrastructure technologies can offer an equivalent service to the client, since they can deploy the features requested by the client independently of the infrastructure technology by following the similarity model.

This paper is organized as follows. Section 2 presents related work regarding similarity models and virtual networks negotiation, while Section 3 describes the proposed similarity model. Section 4 presents some basic concepts about similarity. In Section 5 the proposed approach to measure the similarity between virtual networks is introduced. A case study is shown in Section 6, and Section 7 summarizes the paper and presents future work.

2. RELATED WORK

In this section we describe some important works related to protocols similarity, protocols behavior analysis and virtual networks negotiation.

Kwon [12] analyzes the behavior of sensor network protocols, aiming to exhibit nontrivial variability that can result in a different performance of WSN testbeds.

Kalai et al. [10] describe a model to represent similarity among a set of items, aiming to reflect a human notion of similarity. It is constructed based on human-performed similarity evaluations of adaptively-chosen items, where multiple users were asked to judge similarity among items.

Zaheer et al. [17] show V-Mart, an open market model for automated service negotiation in Network Virtual Environments for Virtual Network Providers (VNP) and Infrastructure Providers (InP). For InPs, V-Mart fosters an open competition environment through auctioning, and the VNP can disseminate a request for quotation when it desires to set up a VN.

Gomes et al. [9] propose an SLA negotiation protocol for virtual networks, which negotiates the network resources and the protocol stack of VNs. However, it does not formalizes a model for a fair comparison between network protocols offered by different ISPs in the VN/SDN context.

None of the papers found in the literature focuses on the definition of a similarity model to allow a free and fair competition in the behavior of a virtual network negotiation, which is the proposal of this work.

3. SIMILARITY MODEL

Methods for calculating similarity among objects have been applied in many areas. The most popular approach is to define a features vector that represents the properties of the object according to its kind, where each position of the features vector represents a property of the object.

In this work, we apply a binary features vector approach, i.e., the positions of the features vector represent the presence or absence of a property, usually depicted by the values 1 and 0, respectively.

A *kind* represents the focus of the network protocol, i.e., which tasks this protocol performs. *Kinds* are used to allow the client/provider to identify in the negotiation process which protocols have the same applicability. For example, we cannot compare the OSPF with the MPLS in a negotiation process. So, identifying MPLS as label switching protocol and OSPF as a routing protocol, each protocol will be compared only with protocols of the same kind.

So, based on recently works [4, 14, 15], we modeled the properties of the main kinds of protocol that can be customized in a VN/SDN. Note that the modeling of properties needed in the diverse kinds of network protocols is not restricted to the set presented in this work. The set of features vectors definition that is part of the proposed similarity model is presented next in Subsections 3.1 to 3.4.

3.1 Routing Protocols

In this section the main properties that characterize the behavior of routing protocols are described. A routing protocol specifies how nodes communicate with each other, propagating information that allows them to select routes between any two nodes on a computer network [11].

In the network virtualization context, we focus on protocols which exchange routing information within a single routing domain. The most popular protocols are [1]: OSPF, RIP, Interior Gateway Routing Protocol (IGRP) and Intermediate System to Intermediate System (IS-IS).

Deciding what kind of protocol to use without considering other options can severely limit the client's choices, who must consider which protocol (or protocols) best suits his/her needs, and then use a preference for one type over another. The main properties that define a routing protocol behavior, and thus should be considered to characterize a routing protocol are:

1. Convergence Time: This property represents the amount of time taken by the protocol to adapt when changes in the network occur. If the protocol is considered of fast convergence time, the features vector has the value 1, and if it is considered slow it gets the value 0.

2. Resource consumption: Refers to the amount of router memory and processing that is used by the protocol. When a protocol has a low resource utilization, the protocol gets the value 1, and the value 0 otherwise.

3. Network Consumption: Represents how much network resources the routing protocol consumes. It considers the network bandwidth consumed by the protocol messages, focusing in the size of the messages and frequency of message exchange between the nodes. If a protocol has a low network consumption, the protocol assumes the value 1, assuming 0 otherwise.

4. Multiple Paths: In this property, it is evaluated how well the protocol deals with multiple paths to a destination. In this property, a protocol gets a value 1 if it supports a multipath approach, and the value 0 otherwise.

5. Scalability: an important property is how well the network protocol will scale with the size of the network. Therefore, a protocol assumes value 1 if it scales well, and 0 if it does not.

6. Loop avoidance: if a protocol prevents a loop route, it gets a value of 1, and 0 otherwise.

Using the properties cited in this section, a features vector for each routing protocol can be generated. For example,

we can define the following features vector to characterize the RIP, OSPF, IS-IS and IGRP protocols: $RIP_{featV} = [0, 1, 0, 0, 0, 0]$, $OSPF_{featV} = [1, 0, 1, 1, 1, 1]$, $IS-IS_{featV} = [1, 0, 1, 0, 1, 1]$ and $IGRP_{featV} = [0, 1, 0, 1, 0, 0]$. Each position of the features vector represents a property enumerated before, so the first position represents the convergence time, the second the resources consumption, and so on.

3.2 Management Protocols

A network management protocol acts on the operation of devices such as routers and switches as well as PCs and servers. The Network Management Protocol describes an application layer protocol and a set of data objects [11].

The most popular management protocol is the Simple Network Management Protocol (SNMP). SNMP is a standard protocol for managing devices, widely applied to the management and monitoring of network devices. In general, two versions of SNMP are used: version 1[1] and version 3[2].

The set of network management properties cited before is described to specify the model. So, for the following properties, a protocol gets the value 1 if it can support the specific kind of management, and gets the value 0 otherwise.

1. Fault Management: The goal of fault management is to recognize, isolate, correct and log faults that happen in the network, providing a way to the administrator to identify possible planning, configuration and hardware problems.

2. Configuration management: The goals of configuration management include gather, store, and update configuration from network devices in an easy way, and track changes in the network devices configurations.

3. Administration management: Its goals are to administer the set of authorized users by establishing users, passwords, and permissions.

4. Performance management: Enables the manager to determine the efficiency of the current network configuration. The network performance addresses the percentage utilization, error rates, and response time issues.

5. Security management: This property represents the control access to configure the network. Usually, it can be achieved with authentication and encryption approaches.

6. Secure Transmission: Messages among administration agents are encrypted, ensuring that it cannot be read by unauthorized entities.

Using SNMPv1 and SNMPv3 for example, the following features vector is produced according to the set of properties listed in this section: $SNMPv1_{featV} = [1, 1, 1, 1, 1, 0]$ and $SNMPv1_{featV} = [1, 1, 1, 1, 1, 1]$.

3.3 Label Switching

Label Switching is a technique to switch the network packets at a lower level. This label switching technique is much faster than the traditional routing method where each packet is examined before a forwarding decision is made [8].

[1]http://tools.ietf.org/html/rfc1157
[2]http://tools.ietf.org/html/rfc3411

The most widely used approach of label switching is the MultiProtocol Label Switching (MPLS)[3]. One of the main benefits of MPLS is the elimination of the dependence on a particular data link layer technology. Another important benefit is the removal of the need for multiple layer-2 networks to satisfy different types of traffic [8].

Next, the main properties that should be considered to characterize a label switching technique are shown. This set of properties defines the protocol behavior. In all the following properties, a protocol gets the value 1 if it can support that specific kind of management, and gets the value 0 otherwise.

1. Traffic Engineering (TE): This property allows the ISP to establish alternative paths for the traffic based on certain criteria. With that, the usage of the network resources can be optimized.

2. Tunneling: Is the process that encapsulates a payload protocol in another network protocol. Applying the tunneling approach the information of the packets can be transmitted, not necessarily inside the same network, through a secure path.

3. VPN Support: This property enables the deployment and administration of VPNs in the ISP backbone. Usually, VPN enhances some services, as for example: (i) real time applications; (ii) data hosting network commerce; and others.

4. Class of Service (CoS): This property allows the ISP to provide differentiated types of service across the network. This differentiation can satisfy the diverse requirements of the applications by applying distinct approaches according to its CoS.

5. Local Protection (or Fast Reroute): This property characterizes a local restoration network resiliency mechanism, which each path passing through the network has a backup path. It provides faster recovery in situation of device(s) failure(s).

6. Connection-Oriented Packet-Switched (CO-PS): It represents the support of a communication mode that establishes a session before any traffic flows through the network, delivering packets in order and with the desired throughput. It guarantees some QoS requirements usually necessary for multimedia applications.

Using the properties cited in this section, a features vector for Label Switching can be generated. For example, we can define the following features vector to characterize the MPLS-TE [4] and MPLS-FR[5]: $MPLS-TE_{featV} = [1, 1, 0, 1, 0, 0]$ and $MPLS-FR_{featV} = [1, 1, 0, 1, 1, 0]$.

3.4 Resource Reservation

A Resource Reservation (RR) protocol is applied to specify qualities of service of the network for particular applications or flows [8].

The Resource Reservation Protocol (RSVP)[6] is often used when a client wants an RR protocol. RSVP is a unicast

[3]http://www.ietf.org/rfc/rfc3031
[4]http://tools.ietf.org/html/rfc4124
[5]http://tools.ietf.org/html/rfc4090
[6]http://tools.ietf.org/html/rfc2205

and multicast signaling protocol, developed to establish and maintain reservation state in each network device through a path of a flow [7]. Recently, the Next Steps in Signaling (NSIS)[7] IETF working group was created to evolve the RR approaches, aiming mainly to support multiple signaling.

Next, the main properties that should be considered to characterize an RR protocol, and therefore define its behavior, are shown. For all the following properties, a protocol gets the value 1 if it supports the specific kind of management, and gets the value 0 otherwise.

1. Self-Routing: This property refers to the capacity of the protocol to define the route where resources will be reserved.

2. Custom Specification: This property relates to the capacity to customize the information used to identify a flow.

3. Traffic Engineering: This property deals with the ability of integrating the resource reservation protocol with traffic engineering technologies.

4. Channel Security: This property represents a security association to be created between the endpoints through some authentication approach. The channel security can provide many different types of protection in the signaling, as integrity, replay protection and encryption.

A features vector for RSVP-TE[8] can be constructed as follows: $RSVP-TE_{featV} = [0, 1, 1, 0]$.

3.5 General Aspects

The proposed set of features vectors definition allows a fair competition between the providers in an environment where VN negotiation occurs. Usually, the client wants a network with an infrastructure that best fits the requirements of the applications that flow through the virtual network. So, when the client specifies a set of protocols to be deployed in the virtual network, he/she wants the virtual network to have a set of properties that characterize its behavior.

Therefore, the proposed similarity model raises the possibility of a provider to offer a certain protocol (private or not) that is not necessarily exactly the same required by the client. The provider can offer the protocol considered most similar to comply with the properties requested for that kind of protocol.

Using the similarity model, the client specifies the set of properties that he/she desires through the features vector. At the same way, each provider receives the features vector, and measures the similarity between the requested features vector and the available protocols, then choosing which available protocol best fits the client's specification.

4. SIMILARITY MEASUREMENT

Similarity is defined as a quantitative degree of how similar two objects are. Binary similarity metrics are used specially for the measurement of similarity in binary data sets (attributes are either 1 or 0). Each binary similarity metric has its own properties and features, since each one focus on different aspects of similarity measurement.

[7]http://tools.ietf.org/html/rfc4080
[8]http://www.ietf.org/rfc/rfc3209

The Operational Taxonomic Unit (OTU) has often been used to present binary similarity and dissimilarity measurements [2]. Given a set of n attributes for each object to be analyzed, we associate each variable a, b, c, d presented in Table 1 with the number of times each pair (i, j) of attributes corresponds to the line/row combination of "presence" and "absence".

Thus, a is the number of attributes where both variables i and j have 1 (or presence) as their value, meaning *positive matches*, b is the number of attributes where the value of variables i and j is (0,1), meaning i *absence mismatches* (or positive mismatches), c is the number of attributes where the value of variables i and j is (1,0), meaning j *absence mismatches* (or negative mismatches), and d is the number of attributes where both variables i and j have 0 (or absence) as their value, meaning *negative matches*.

Table 1: OTU for binary data [2]

OTU	1 or Presence	0 or Absence
1 or Presence	a	b
0 or Absence	c	d

The sum of $a + d$ represents the total number of matches between variables i and j, while $b + c$ represents the total number of mismatches between variables i and j. The total sum of the table, $a+b+c+d$, is always equal to the number of attributes in the features vectors (n). In this work, the set of properties of the requested protocol is represented by the features vector i, and the protocol offered by the provider is represented by the variable j.

4.1 Popular Similarity Metrics

Different similarity metrics estimate different aspects of taxonomic relationships between two objects. Some metrics only account for positive matches, some include negative matches, while some apply weights on either matches or mismatches or both.

Some similarity metrics only account for positive matches, some include negative matches, while some others apply weights on either match or mismatch or both. Three of the most popular binary similarity metrics are *Jaccard* (S_J), *Sokal & Michener* (S_{SM}) and *Lance & Williams* (S_{LW}) [2, 13], which are presented in Equation 1.

The *Jaccard* coefficient excludes the negative matches (d). Therefore, it is defined as the ratio of the number of positive matches (a) to the total number of attributes minus the number of negative matches ($(a+b+c+d)-d$). The *Sokal & Michener* similarity metric is defined as the ratio of the total matches (including negative matches) to the total number of attributes. Both metrics try to evaluate which properties are present in the analyzed feature vectors, where *Jaccard* uses only the positive matches and *Sokal & Michener* uses both positive and negative matches.

In contrast, distance-based metrics calculate the dissimilarity/distance between two binary features vector, where the distance is estimated by the number of mismatches. Thus, the larger the distance, the lesser is the similarity. The *Lance & Williams* (LW) distance metric has a range from 0 to 1.

Each similarity metric has its own properties and features. Different binary similarity metrics estimate different aspects of taxonomic relationships between two feature vectors. Clearly, applying different binary metrics can lead to different results even for the same two objects.

$$S_J = \frac{a}{a+b+c} \quad ; \quad S_{SM} = \frac{a+d}{a+b+c+d} \quad ; \quad S_{LW} = 1 - \frac{b+c}{2a+b+c} \tag{1}$$

5. PROPOSED SIMILARITY METRIC

As shown in the previous section, different similarity metrics estimate different aspects of relationships between objects. In this work, the considered objects are the protocols for the virtual networks, characterized by the features vector according to the definitions presented in Section 3.

Usually, the client requests a set of protocols that he/she wants to have deployed in the VN, and the providers answer this request offering a protocol that is not always exactly the one desired by the client. A protocol is a set of properties that define its behavior.

To evaluate how appropriated the offered protocol for the VN is, we must consider the requested properties that are met by the offered protocol, denoted by a, as a good point. In contrast, we must assess as a bad point the properties that are not fulfilled by it, represented by b.

Moreover, if the offered protocol has some properties that were not requested by the client, it just adds functionalities to the requested one, representing a good point in the similarity calculation process.

Hence, we developed a similarity metric, called $S_{Corr-VN}$, that gives a higher importance for the presence of the requested properties, considering the absence of some desired properties and extra properties as equivalent, since the absence of a property can be suppressed by another one not specified by the client.

The $S_{Corr-VN}$ metric is shown in Equation 2. If the calculated similarity yields a negative value, it is rounded up to zero, making the metric be in the range $[0, 1]$. The metric is molded to consider the presence of a requested property equivalent to three extra properties, aiming to enhance the capacity of a provider to deploy the set of requested properties (represented by a).

$$S_{Corr-VN} = \frac{3a + c - b}{3a + c + b} \tag{2}$$

The behavior of the proposed metric is plotted in Figure 1. For easy visualization, Figure 1 limits the feature vector size to ten properties, omitting the unconsidered negative matches. Note that the total sum, $a + b + c + d$, is equal to the number of properties in the feature vectors (n), so the gaps in the graphs are cases where the properties have not appeared because they are part of the negative matches (d).

6. CASE STUDY

This section details a case study to evaluate the capacity of the similarity model to represent the client's requirements and its capacity to identify, among a set of available protocols, which one is more suitable for the client's desire. The client's request specifies the properties of the protocol, i.e., the features vector.

We assume that the providers do not have exactly what the client requests. With that, we can analyze the similarity measure process of the proposed similarity model.

The case study presents a negotiation of a routing protocol. The routing protocol negotiation was chosen due to its applicability in the current scenario of virtualization of traditional TCP/IP networks as well as SDNs, using for example approaches like the RouteFlow [14]. For example, if

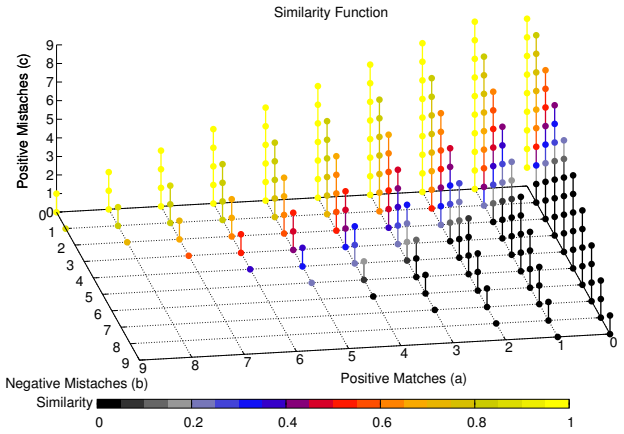

Figure 1: Behavior of $S_{Corr-VN}$ metric.

an ISP has a network infrastructure with RouteFlow, it can use the proposal of this work to offer to a client the Routing as a Service (RaaS) approach, since the client can measure the effectiveness of the RouteFlow. This shows the capacity of the proposal to allow a fair and free competition between the ISPs with different network technologies.

In the case study, a client requests the IGRP protocol and four providers offer different options. The IGRP protocol was chosen to exemplify a situation where a private protocol is requested and not all providers could deploy it. However, this does not mean that the providers can not deploy a network with the properties presented in this requested protocol. So, the proposed similarity model is applied to designate to the client which offered protocol best reflects the properties of the requested one.

The protocols offered to the client are: RIP, IS-IS, OSPF and a "Generic" routing protocol. In this case, the Generic protocol is a protocol with fast convergence time, low general consumption (network and resources), support multipath, has a good scalability, and avoids loops. It deploys all the desirable features, so it has the features vector $Generic_{featV} = [1, 1, 1, 1, 1, 1]$.

As we can see in the features vector shown in Section 3.1, the IGRP protocol deploys just two features: (i) low resource consumption and (ii) multipaths support. So, Table 2 presents the measurement information regarding to IGRP and the offered protocols, which are the base for similarity definition.

Table 2: OTU Measurements for IGRP

Protocol	a	b	c	d
RIP	1	1	0	4
OSPF	1	1	4	0
IS-IS	0	2	4	0
Generic	2	0	4	0

Table 3 shows the similarity values computed by each similarity metric (presented in Section 4) and the proposed $S_{Corr-VN}$ metric (described in Section 5), where the highest values provided by each metric are highlighted in bold.

Based on information presented in Table 3, it is observed that, despite the proposed $S_{Corr-VN}$ which determines the Generic protocol, all metrics choose the RIP protocol as best

Table 3: Similarity Measurements for IGRP

Routing	RIP	OSPF	IS-IS	Generic
S_{LW}	**0.66**	0.28	0.00	0.50
S_{SM}	**0.83**	0.16	0.0	0.33
S_J	**0.50**	0.16	0.00	0.33
$S_{Corr-VN}$	0.50	0.75	0.33	**1.00**

option for IGRP protocol. It happens because the RIP protocol has one of the two requested properties (represented by a) and it does not has all the four non required properties (represented by d), enhancing the OTU values used in the similarity metrics, as shown in Table 2.

Thus, it is noted that existing similarity metrics are not suitable for the virtual networks negotiation context, since it favors the protocol which has common properties, where it does not necessarily represents the aggregation of functionalities to the network.

On the other hand, the proposed $S_{Corr-VN}$ metric focuses on the deployed properties, identifying when a protocol is more beneficial to the client: the more properties deployed by the protocol the higher quality in the provided service.

In the same way, if the Generic protocol did not exist, the $S_{Corr-VN}$ metric would consider the OSPF protocols the more suitable option, not the RIP as existing metrics. This fact shows that the proposed metric can identify the protocol that best fits the desired properties, even when not all properties could be deployed by the offered protocols.

Therefore, the similarity model offers the client the opportunity to deploy, in a negotiated virtual network, the protocol that best fits the desired properties, and consequently is the most suitable option for the client's application.

The proposed similarity model enables the client to choose, from a set of protocols offered by ISPs, which one is most similar to the required protocol, providing to the client the capacity to deploy a virtual network that best fits his/her applications. With that, the client has the opportunity to shape the VN according to a certain traffic class, and the application that will be part of it.

7. CONCLUSION

This paper presents a similarity model for virtual networks negotiation. The proposed model tackles two main aspects in the context of virtual networks negotiation: (i) the free competition between providers, since ISPs with different infrastructure technologies can deploy the same properties for the VN; and (ii) allows the client to compare and identify which protocol offered by the providers best fulfills requested requirements.

A case study was performed to analyze the effectiveness of the proposed model in fulfilling the requirements defined by the client, where the consistency of the proposal was assessed.

As future work, we intend to deeply analyze the protocols properties to apply a weighted approach in the similarity measure, enhancing the particularities of each type of protocol.

Acknowledgment

The authors would like to thank São Paulo Research Foundation (FAPESP - grant 2012/04945-7), RNP and CNPq for the financial support.

8. REFERENCES

[1] S. Ballew. *Managing IP Networks with Cisco Routers*. O'Reilly Media, 1997.

[2] S. S. Choi, S. H. Cha, and C. Tappert. A Survey of Binary Similarity and Distance Measures. *Journal on Systemics, Cybernetics and Informatics*, 8(1), 2010.

[3] N. M. K. Chowdhury and R. Boutaba. A survey of network virtualization. *Computer Networks*, 54(5):862–876, April 2010.

[4] S. Das, G. Parulkar, and N. McKeown. Why openflow/sdn can succeed where gmpls failed. In *European Conference and Exhibition on Optical Communication*. Optical Society of America, 2012.

[5] F. de Oliveira Silva, J. de Souza Pereira, P. Rosa, and S. Kofuji. Enabling future internet architecture research and experimentation by using software defined networking. In *European Workshop on Software Defined Networking (EWSDN)*, 2012.

[6] D. Drutskoy, E. Keller, and J. Rexford. Scalable network virtualization in software-defined networks. *IEEE Internet Computing*, 17(2):20–27, 2013.

[7] D. Durham and R. Yavatkar. *Inside the Internet's Resource Reservation Protocol: Foundations for Quality of Service*. John Wiley & Sons, Inc., New York, NY, USA, 1999.

[8] J. Evans and C. Filsfils. *Deploying IP and MPLS QoS for Multiservice Networks: Theory & Practice*. The Morgan Kaufmann Series in Networking. 2010.

[9] R. L. Gomes, L. F. Bittencourt, and E. R. M. Madeira. A generic sla negotiation protocol for virtualized environments. In *Proceedings of 18th IEEE International Conference On Networks (ICON)*, 2012.

[10] A. Kalai, O. Tamuz, C. Liu, O. Shamir, and S. Belongie. Adaptively learning a similarity model (patent), 2012.

[11] J. Kurose and K. Ross. *Computer Networking: A Top-down Approach*. Pearson Education, 2010.

[12] T. Kwon. *Reasoning about Wireless Protocol Behavior*. Ohio State University, 2012.

[13] M. Lesot, M. Rifqi, and H. Benhadda. Similarity measures for binary and numerical data a survey. *Int. J. Knowl. Eng. Soft Data Paradigm.*, 1(1):63–84, 2009.

[14] C. E. Rothenberg, M. R. Nascimento, M. R. Salvador, C. N. A. Corrêa, S. Cunha de Lucena, and R. Raszuk. Revisiting routing control platforms with the eyes and muscles of software-defined networking. In *Proceedings of the first workshop on Hot topics in software defined networks (HotSDN 2012)*, pages 13–18, 2012.

[15] A. R. Sharafat, S. Das, G. Parulkar, and N. McKeown. Mpls-te and mpls vpns with openflow. In *Proceedings of the ACM SIGCOMM 2011 conference*, SIGCOMM '11, pages 452–453, New York, NY, USA, 2011. ACM.

[16] R. Sherwood, G. Gibb, K.-K. Yap, G. Appenzeller, M. Casado, N. McKeown, and G. Parulkar. Flowvisor: A network virtualization layer. *OpenFlow Switch Consortium, Tech. Rep*, 2009.

[17] F. Zaheer, J. Xiao, and R. Boutaba. Multi-provider service negotiation and contracting in network virtualization. In *12th IEEE/IFIP Network Operations and Management Symposium*, 2010.