Self-* Features for Semantic Networking

Ludovic Noirie, Emmanuel Dotaro, Giovanna Carofiglio, Arnaud Dupas, Pascal Pecci, Daniel Popa, Georg Post

Self-* Features for Semantic Networking

Ludovic Noirie, Emmanuel Dotaro, Giovanna Carofiglio, Arnaud Dupas,
Pascal Pecci, Daniel Popa, Georg Post

***Abstract*— We propose the Semantic Networking concept as a candidate for the Internet of the Future. Re-thinking of the architectural and functional paradigms is needed to face scalability and complexity issues in the current Internet developments. A fundamental of our proposal is to reconsider all the networking and service operations based on the flow granularity, thus beyond packet or circuit paradigms. This is enabled by the awareness of the transported traffic, thanks to a combined Deep Packet Inspection and Behavioral Analysis approach. Together with the flow-based and traffic-aware features, Autonomic Networking is considered as a pillar of this concept which leads in turn to specific requirements. This paper is an introduction to autonomic features which should be instantiated as per the Semantic Networking goals, within the traffic-aware data plane ("Semantic Analysis", "Elastic Fluid Switching"), the flow-based control plane ("Flow Admission Control", "Flow Policing", "Traffic Aware Routing"), and the self-management plane ("Network Mining", "Knowledge Plane"). We describe each of these functional building blocks, their interactions, the requirements for their autonomic (or self-*) features, and their localization in transport network nodes to transform them into "semantic network nodes".**

***Index Terms*— Autonomic, Flow, Semantic, Traffic-Awareness**

I. Introduction

Semantic Networking is a promising concept we propose as a candidate for the Internet of the Future. Several world-wide initiatives [1]-[5] are driving the research for the Internet of the Future, to overcome the limitations of today's state of the art inherited from incremental evolution and the mismatch with current and future services requirements. While designed for other purpose, the Internet must evolve from a "best effort black box" towards a transparent box mostly self-operated and enabling premium value through ubiquitous services.

As a tentative answer to the required change in paradigm, Semantic Networking aims at solving some known or forecasted Internet limitations, such as scalability, flexibility, operational complexity, etc. Focusing on the natural granularity of traffic, which is the flow [6]-[7], it is first a flow-based approach. By "semantic" we mean that the network is aware of the transported traffic, self-discovering its nature by means of Deep Packet Inspection and/or Behavioral Analysis, in order to associate the right Quality of Service to each flow. One of the main pillar of the Semantic Networking concept is the embedded autonomic networking principles, spread within each of its functional building blocks. Autonomous (or self-*) features are the key elements of this concept, in order to face the increasing complexity of network evolution, while decreasing the complexity of the configuration by human operators.

The main objectives of this paper are to introduce this new concept of Semantic Networking, give a closer look at its self-* features, and explain how it could work in a node architecture. The full concept implementation and evaluation are for further work.

The paper is organized as follows. First, the rationales and the principles of the Semantic Networking proposal are given in Section II, in which we also introduce the main functional building blocks and their interactions. In Section III, each of the functional building blocks are detailed, focusing on their self-* features and the corresponding requirements. In Section IV, we illustrate what are these functional building blocks by showing how to implement them in a "semantic network node". Finally, we conclude in Section V by giving some perspectives for further works.

II. The Semantic Networking Concept

A. Rationales

Despite a successful evolution through incremental developments in both technologies and capacities, the current Internet limitations foster research efforts towards a radical change of paradigms as granting the failure of repeated updates that leave the core structure unchanged. Huge investments and investigations already started in world-wide initiatives ([1]-[5]) aiming at (re-)defining the relevant architectural and functional paradigms which will be candidate for the expected evolutions or revolutions.

If network performance and Quality of Service (QoS) prerogatives remain important issues to be tackled by the research community, a number of further Internet features are becoming more critical.

The scalability issue comes immediately in mind. Facing the explosion of network dimensions in terms of users, equipments, traffic volume and services, a fundamental and legitimate question rises with respect to the quasi-universal

Manuscript received October 12, 2008. This work was done in the framework of the INRIA and Alcatel-Lucent Bell Labs Joint Research Lab on Self Organized Networks.

L. Noirie, E. Dotaro, G. Carofiglio, A. Dupas, P. Pecci, D. Popa and G. Post are with Alcatel-Lucent Bell Labs, Nozay, 91620 France (E-mails: {Ludovic.Noirie; Emmanuel.Dotaro; Giovanna.Carofiglio; Arnaud.Dupas; Pascal.Pecci; Daniel.dp.Popa; Georg.Post}@alcatel-lucent.com).

packet and circuit paradigms. Scalability concerns affect all network dimensions from data to control, management and service planes, resulting in bottlenecks over data and control planes as well as in a decoupling between the intrinsic content operations and the networking ones.

The increasing complexity may also be considered as a worrying issue directly related to the incredible diversity in Internet traffic currently accommodated into a network infrastructure essentially agnostic in its resources and tools to users/services differentiation. With thousands of protocols for provisioning, monitoring, protection, etc, the probability of using the exact matching combination is more than uncertain.

The purpose here is not to elaborate an exhaustive list of those concerns, but rather to highlight the fundamental problems and then describe the solutions integrated in the proposal of the Semantic Networking architecture that we are proposing. It takes its root in the research of autonomic paradigms (also referred as self-* in the paper) which re-think networking operations as the result of the dynamic understanding of traffic communications (awareness of traffic, this is what we call "semantics" in the context of networks).

B. Principles

Neither segmented in packets nor nested in pre-established circuits, the natural communication entity of Semantic Networking is the flow. Even though this belief is shared by previous work (e.g., [6],[7]), Semantic Networking comes out as the first fully integrated flow-based networking approach. All basic networking operations are then modulated on a flow-basis as flow admission control, flow policing, flow switching and flow routing. The immediate expected effect is a dramatic reduction of the number of operations compared to classical packet or circuit approaches, alleviating both the above mentioned scalability and complexity issues.

Following the bottom-up principle from the semantic of the flow to the network control, the concept leans on traffic-awareness. The process of acquisition of traffic flow information and traffic characterization is accomplished in the Semantic Networking design by what is referred to as the Semantic Analysis, which provides implicit and explicit relevant discriminators for all networking decisions (admission, policing, routing, switching).

The definition of such networking operations according to the "autonomic paradigm" yields to a significant cut in control/management operational costs by simplifying the associated constructs (control/management/decision planes). For this purpose, like for many Internet of the Future proposals, the self-* features become critical enablers.

The rest of the paper introduces the Semantic Networking architecture, detailed in its functional building blocks and their inherent self-* features.

C. Functional Building Blocks

Fig. 1 shows that the main "semantic" functional building blocks interact in a loop, starting at the Semantic Analysis (SA) functional block, within the traffic-aware data plane, going through the self-management plane and the flow-based control plane, and ending in the Elastic Fluid Switching functional block within the traffic-aware data plane. Additional interactions between the SA functional block and other ones form shorter and faster loops as explained below. Let us describe in detail the main loop in Fig.1 starting from the SA.

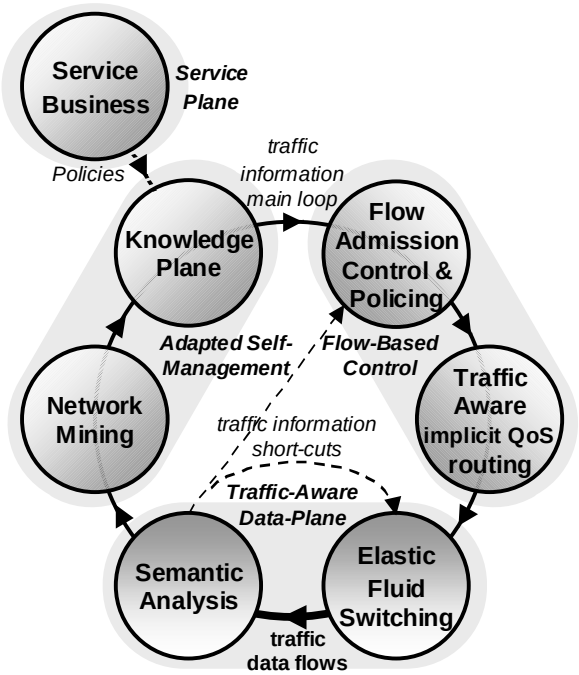

Fig. 1. Semantic Networking functional building blocks and interactions

Traffic-aware data plane, semantic analysis

At each network node, the incoming traffic flows are identified and measured by the "Semantic Analysis" (SA) building block. It groups all mechanisms that make the network "traffic-aware", based on Deep Packet Inspection (DPI) and Behavioral Analysis (BA) techniques as detailed in Section III.B. Current limitations in fully DPI-based classification techniques motivate the choice of a combined DPI/BA approach which assigns to the DPI the task of flow reconstruction (from individual packets in-flight) and to the BA the task of classifying flows according to the applications behind, by inferring statistical properties in traffic patterns.

The goal of the SA is to enable service differentiation for the processing of the different traffic flows in a self-adaptive fashion. It also helps to get real-time monitoring of the bandwidth usage per service.

Adapted self-management

The "Network Mining" (NM) functional block retrieves the relevant information about the traffic from the SA, mostly via aggregation (e.g., per application type) in order to avoid information overflow. The NM is expected to pre-analyze the raw information (filtering/aggregation) and feed it to the "Knowledge Plane" (KP).

The KP is responsible of the transformation of the information into knowledge (cognitive process) and the

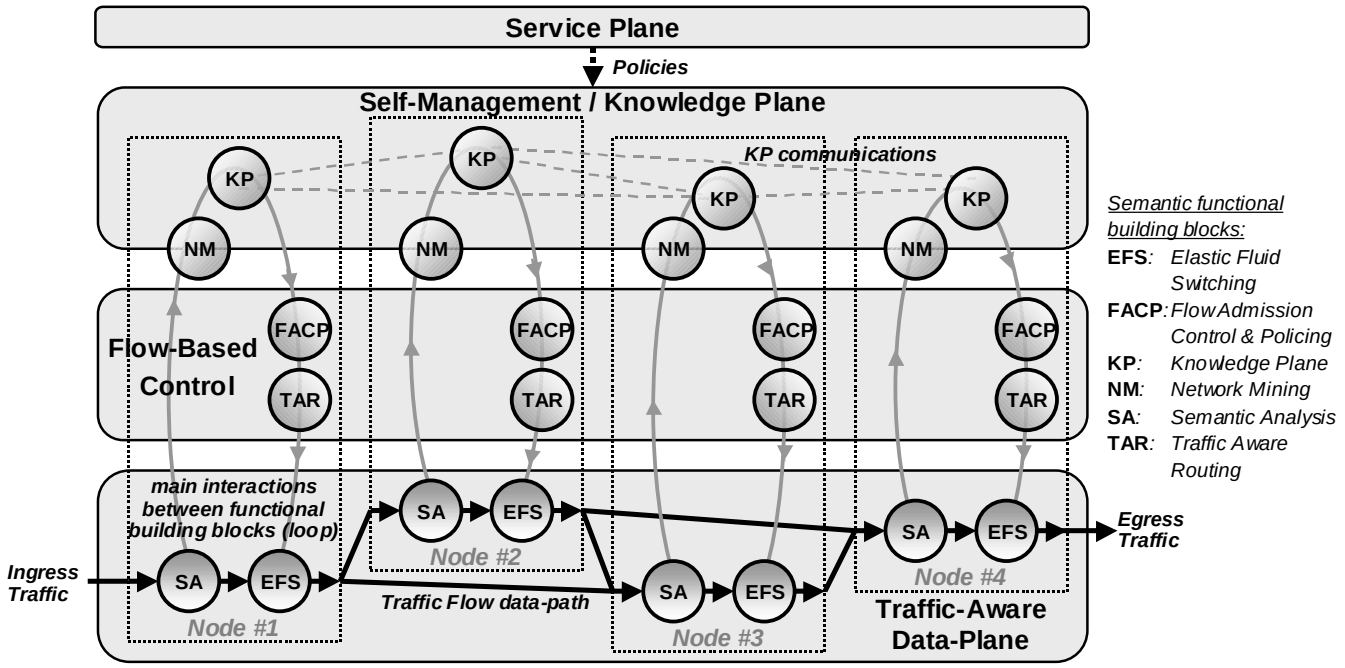

Fig. 2. Network view of the Semantic Networking functional building blocks and their interactions.

diffusion of the relevant information within the network (communicative process). It is expected not to flood the same information everywhere, but to deliver the right information to the right place, being either preventive, predictive or reactive. The KP is also enriched with external information such as business policies, objectives, etc, from the Service Plane.

Flow-based control plane

The consistency of control decisions is ensured overall by the KP which holds a global picture of network status and distributes it to the control functions of each network element.

The first function is the "Flow Admission Control" (FAC), which decides at the beginning of the life of each flow, accepting/rejecting it. FAC takes benefits from network-wide information coming from the KP and local traffic information provided by the SA to decide the acceptance of a given flow.

Once a flow has been accepted, the "Flow Policing" (FP) takes over the FAC to control the evolution of the flow during its whole life, mainly considering local traffic information from the SA about the statistics of the flow and the aggregated traffic (total and per application type).

The third function is the "Traffic Aware Routing" (TAR) which takes decisions about dynamic flow routing under the QoS constraints per application (equivalently per traffic class) and in an implicit way, which avoids explicit signaling as done today with OSPF-TE and RSVP-TE.

Traffic-aware data plane, elastic fluid switching

To close the loop, according to the FAC, FP and TAR decisions, the traffic flows are scheduled and switched towards the right destination ports of each network node by the "Elastic Fluid Switching" (EFS) functional building block, which includes queue management, scheduling and switching. Real-time measurements on traffic flows by the SA feed the scheduling of the traffic in the node. Considering the flow granularity and the aggregation per class of transported applications, the number of operations to be performed can be decreased a lot compared to packet-based operations, so reducing significantly hardware and software complexity.

Some short-cut in the loop

Different time-scales intervene in loop interactions among functional blocks, forming shorter loops with shortcuts. This allows fast reactions when it is required and possible.

The full loop is mainly required to get the global picture of the traffic state in the network. It is useless and unrealistic to get such a global picture at the sub-second time-scale, so the NM and KP have time to retrieve and diffuse this information over the whole network.

Shortcuts are required to get the local picture of the traffic state at sub-second time-scales (µs-ms) in a line-card of the given node, for local decisions on individual flows (scheduling, switching, admission control and policing). Combining information both from long term (seconds to days) global traffic status and short-term (sub-second) local traffic status allows the optimization of control and switching decisions in each network node.

D. Network view

As represented in Fig. 2, all functional building blocks are located within each node of the network. Like in the functional view of Fig. 1, they interact in a loop. The closing of the loop between the EFS and SA functional building blocks must be understood between adjacent nodes, through the traffic-aware

data-plane. The traffic flows that are switched by the EFS function of a given node are analyzed in the SA function of the next node, corresponding to hop-by-hop forwarding of the traffic flows within the network data plane.

Admission control (FAC), policing (FP) and routing (TAR) decisions for traffic flows are taken locally in each node, avoiding explicit signaling of bandwidth reservation for each flow as it is done in today's network with RSVP-TE. Such local decisions are enabled thanks to the network-wide information given by the KP in the main loop of interactions, but also with the local information from the SA (not represented in Fig. 2 to avoid surcharging it).

The global consistency of the local decisions taken by each node is ensured by the communications inside the network-wide distributed KP, which gets the information from the SA and through the NM, and distributes the right pieces of information to the right nodes (no flooding).

III. Autonomic Feature Requirements of the Semantic Networking Functional Building Blocks

A. Autonomic Networking General Requirements

The purpose of this paper is not to discuss generic Autonomic Networking model. Nevertheless, applicability of self-* features need to be investigated in the scope of Semantic Networking.

At the lower level we consider autonomic behaviors linked to the data plane and thus participating to the Network Mining. It applies for instance to adaptive level of Semantic Analysis according to traffic evolution and dynamics. The distribution of network wide information is supposed to be controlled by the knowledge plane which in turn enables the flow-based control. This simple organization is close to the 4D architecture described in [8].

The common objective of autonomic networking proposals is to overcome to the complexity of future of Internet management. It is thus derived in numerous operations such as self-configuration, self-healing, self-protection, self-optimization, self-diagnostic, etc. The focus of this paper being Semantic Networking, we do not detail each of them, but we rather describe the specific autonomic features for each functional building block.

B. Specific Requirements for the Semantic Analysis

At the core of Semantic Networking is the cognitive process of acquiring knowledge of what's going on as a necessary step for reacting and controlling the network in an adaptive way.

The centrality of traffic semantics distinguishes the Semantic Networking approach from previous/alternative Internet reorganization proposals and drives the design of the main network functionalities. The knowledge of in-transit traffic is, in addition, a fundamental functionality to be realized in autonomic systems which determines the behavior of all control/management blocks at various levels. When talking about traffic knowledge it is worth specifying the object of the cognitive process, which is the traffic flow in Semantic Networking architecture.

Hence, the semantic analysis has the primary objective of reconstructing the flows from packets, though is not limited to it. The actual Deep Packet Inspection (DPI) technology is a candidate for that purpose. In today's networks, the DPI is used to monitor the traffic in the access part and to better understand the user behavior. First techniques of DPI using fixed pattern matching were originally used in Intrusion Detection Systems [9]-[10]. They have evolved toward flexible pattern matching in order to increase memory efficiency [11] and the reprogrammable functionality.

Even if challenging, a full-DPI from layer 2/3 (Ethernet, IP) to layer 7 involves high power consumption. Moreover, because it is a supervised approach requiring external inputs (classification rules), it is unable to adapt to new types of traffic (new applications, encrypted flows, etc). This is in clear contrast with the paradigm of autonomic systems. Within the framework of Semantic Networking, the idea is to only exploit DPI techniques for flow identification while performing a behavioral analysis for traffic characterization. Indeed, a behavioral approach is more suited for a detailed analysis of traffic flows in that it provides a passive characterization through the evaluation of visible statistical properties in traffic patterns, without the need of static external rules and without inspecting packet payload.

In the following we will detail the operations involved by what we refer to as Behavioral Analysis (BA). It is worth remarking that there is no clear definition in literature of such a statistical-based approach aimed at traffic characterization.

The Behavioral Analysis (BA) acts in principle on all incoming flows in two phases: online on in-flight packets during flow lifetime and offline on full flows for a finer characterization of traffic classes based on the application (or group of applications). The application identification is important for a customized treatment of traffic with different requirements in terms of Quality of Service (QoS). The static parameters involved in the BA range from those computed on first packets (average packet size, inter-arrival time, etc) to attributes of full flows (average flow size, duration, etc).

For short flows it may happen that the few number of packets limits the online BA. In addition, the well known dichotomy in flow size distribution between large flows ("elephants") and small flows ("mice"), also confirmed by recent works ([12]), suggests to analyze individually elephants only while controlling mice as an aggregate. Indeed, as [12] outlines, the majority of traffic flows (>90%) is represented by "mice" carrying a limited portion of traffic (<1%) whereas "elephants" represent the majority of traffic in volume but are limited in number. Letting the BA operate on the aggregate volume of "mice" allows then to decrease significantly the complexity of the node implementation.

Finally, it is worth to remark that the added value of BA consists in permitting the network to self-construct and enrich as time passes a knowledge base of traffic characteristics (self-learning) which can lead to the prediction of future

trends, thus helping network control. The right implementation solution for the SA is a combination of BA and DPI principles, because distinction of the different individual flows is required to work properly. This can be done by coupling the BA with a "light" version of DPI that identifies for example IP addresses, IP port numbers, and TCP/UDP port numbers.

C. Specific Requirements for the Network Mining and Knowledge Plane

The two main components of the self-management plane are the Network Mining (NM) and the Knowledge Plane (KP).

The NM is the operation of data mining of information about the network state and, in the scope of Semantic Networking, the traffic transported in the network. The NM collects "raw" data coming from a single point of the network or from a larger area, spatially/temporally aggregating and correlating data. Many examples of metrics have been proposed by the IETF IPPM working group [13] such as the round trip time, the one way losses, etc. They could be analyzed offline and classified to feed the KP. If some data could not or do not need to be processed at the line rate, sampling or filtering can limit the data exchange both at the collecting or at the exporting steps. These two tasks fulfill IETF PSAMP working group recommendations in order to have relevant and not biased overview of the traffic [14].

For traffic information exchange and collecting by the NM, a good candidate is the currently developed IETF protocol called IPFIX (IP Flow Information eXport). The export of the information could be done in push mode, regularly, but also on-demand through self-configuration, according to the feed-back received from the KP. This is fully compliant with a network having self-characteristics. The IETF IPFIX working group uses a protocol that is simple, flexible and have high chances to be widely spread across the network [15].

The information on traffic properties gathered by the SA and pre-processed by the NM (filtering, aggregation) is fed to the KP, whose primary task is to transform it into knowledge and spread it into the network to enable control/management process. The knowledge plane in the semantic networking vision behaves as an intelligent entity that bridges the data plane (where the SA is performed) to the control/management plane where decisions are autonomously taken in real time on flow-aware routing, admission control and policing in respect of external policies/objectives enforced by the service plane.

The cognitive process takes place in presence of possibly inconsistent/incomplete information and has to be robust to it by creating correlations and making inferences from sampled data. An advanced feature of the cognitive process is the prediction capability based both on the information collected in real time by the NM in every node of the network and on the behavioral analysis performed offline per traffic class (i.e. per application or group of them) by the SA and the NM.

If the main task of the knowledge plane is what we can call the information "digestion" (cognitive function), the other fundamental prerogative of KP is the knowledge diffusion (communicative function), which allows the optimal control of network traffic and thus the optimization of network resources utilization. The KP maintains a network wide view of the topology which is self-adapting to structural changes and the communication process conforms to it.

Indeed, the communication is performed in an intelligent way which avoids flooding and hence redundancy both in space and in time. In compliance with the autonomic paradigm, the communication process reacts to events that change the network status and is activated in order to prevent future events. The design of the KP, which is clearly tailored on semantic networking needs, inherits the self-* features (in cognitive and communicative prerogatives) already present in [8] or [16] where it springs from the clean slate rethinking of control/management planes oriented to a progressive simplification required by next generation networks.

D. Specific Requirements for the Flow Admission Control, Flow Policing and Traffic Aware Routing

Thanks to the local SA and the globally distributed KP, flow control mechanisms will have access to detailed and aggregated information about traffic flow characteristics and the network state. This feature permits admission control mechanisms to have local and global vision on the state of network resources; in addition, it avoids the end-to-end signaling used in today's admission control mechanisms and allows flow control mechanisms to move towards autonomy and self-configuration, which will greatly help at improving the efficiency of control decisions.

The autonomic/self-* features require algorithms governing the control functionalities to incorporate new parameters that take into account information about flow characteristics and the state of network resources and adapt the decisions for each individual or aggregated flow at the network state.

The Flow Admission Control (FAC) relies on the optimization of the matching between the traffic flow requirements (e.g., bandwidth and QoS) and the state of the network resources [17]. In today's networks, admission control requires declaration of the flow characteristics by the users and end-to-end signaling. This leads to complex tasks for the users and inaccurate configurations of the control parameters. In the Semantic Networking proposal, the self-discovery feature of the Semantic Analysis provides "on the fly" identification and classification of traffic flows, and gives a local picture of bandwidth usage. Combined with information about the state of network resources from the KP, it allows FAC self-configuration with a better control of undeclared flows, and avoids end-to-end signaling for each individual flows.

The Flow Policing (FP) enforces the network protection against unintentional or malicious misbehavior of accepted traffic flows and their configuration is tightly related to the admission control decision. Most popular policing mechanisms uses token buckets or leaky buckets with static parameter configuration, where the parameters are set-up using peak-rate allocations [18]-[19]. However, finding optimal parameters for such static bucket configuration is extremely challenging because the traffic flow characteristics and the state of network

resources vary as a function of time. Therefore, as the major part of the traffic in the Internet is variable, policing mechanisms have to take into account the variability of the traffic and the state of the network resources, rather than statically police, drop or mark packets as non-conforming. Thanks to local information from SA and global information from KP, self-learning and autonomic policing algorithms will adapt parameters to changes in the state of network resources and traffic characteristics. This feature will guarantee an efficient mapping of flow bandwidth and QoS requirements into the state of network resources.

Routing relies on single- and/or multi-path optimization between the source and destination of a flow [20]. Traditionally, routing algorithms determine a path or a set of paths between any pair of source and destination, using metrics such as the number of hops or the link/trunk capacities. Such metrics do not take into account the traffic variation on time-scales smaller than one hour and they are usually static and manually configured. This represents an extremely challenging task in the context of an increasing network heterogeneity and complexity. In Semantic Networking, the routing algorithms have to be more intelligent, traffic-aware and (self-)adaptive. They should incorporate new parameters which take into account information about the traffic flow characteristics and the state of network resources, and adapt routing decisions at the network state, for each individual or aggregated flow [21]. They should re-configure at time scales larger than the flow life-time to avoid routing oscillations, while keeping a low convergence time. They should also be robust to a certain degree of inaccuracy of the information distributed by the KP.

The aforementioned flow control functions are under the control of dependent loops, the decisions on one side impacting directly the other one. So local autonomic behavior have to take consistent decisions, avoiding traffic loops. Management of transient states due to failures or simple adaptations to network dynamics must be executed trough proven distributed algorithmic, including back-up solutions.

E. Specific Requirements for the Elastic Fluid Switching

Most large-volume and/or high-bandwidth packet flows are considered to be elastic; the transmitter side is sensitive to network loss such as congestion events in a node. A "semantic node" that integrates information about the transported flows thanks to the SA and the flow-based control has the potential for more efficient scheduling and switching. Research on flow-aware scheduling and switching functions should concentrate on features for self-configuration and intrinsic quality of service, that save money in two ways at least:

- The future node has a far-reaching autonomy on quality-of-service policy per flow. If the network does not need to bother with cumbersome QoS protocols (like Diffserv, Intserv), operation cost goes down. This was also the motivation in [22].
- The traffic management systems should be able to take decisions on Active Queue Management (AQM) and on auto-adaptive local resource allocation for flows and subsets (aggregates) of flows. For example, current standard features like AQM based on W-RED have individual parameters for thousands of queues that are too difficult for human operators to optimize.

The statistics of Internet traffic show [12] that the flows can be split into "mice" and "elephants" (e.g., flow sizes < 10K and > 10K bytes). After flow recognition, scheduling should be automated to give priority (fast switch-fabric transit) to the mice that are numerous but represent a small part of the total traffic volume, and to efficiently regulate the competition for bandwidth among the elephants, which highly reduces the workload for forwarding schedulers.

Automated AQM policies should work out the set-points of buffer-size limits, for example, based on the knowledge of the node-wide traffic-demand matrix and its predictable variations with time-of-day, day-of-week, and so on.

The intelligent aggregation of flows into tunnels, for local use inside the node, is another path to self-optimization. The idea is that large network nodes have multi-stage switch fabrics and so are themselves miniature networks. A light-weight form of dynamic circuit switching could be operated. The scheduler could dynamically set up and tear down the tunneling circuits of self-configured bandwidths, priorities and lifetimes inside the node. The advantage would be fewer different queues and simpler packet-forwarding schedulers.

IV. SEMANTIC TRANSPORT NODE ARCHITECTURE

A. Generic transport node architecture

A generic transport node is made of switching matrix cards and line-cards (Fig. 3). A line-card can be functionally split into input and output parts. Here we first describe the main functional blocks of today's switching node architectures, which will be replaced by the Semantic Networking ones in a "semantic" network node.

The main functional blocks in the input line-cards are:

- *Network Processor (NP)*. It identifies, classifies and marks the incoming packets. It may also modifies the headers of the packets if required. It monitors some characteristics of the packet flows.
- *Traffic Manager (TM) with input buffers*. It received the packets from the NP and stores them into buffers that can be organized into Virtual Output Queues (VOQ, per output port destination and eventually per class of traffic). It participates to the global scheduling of the packet forwarding towards the outputs (input scheduling), for example by sending requests to the outputs and arbitrating the received grants between its VOQs. The grants may come from the output schedulers and/or the matrix scheduler.
- *Control and management (CTRL) of the line-card*. It controls and monitors the packet processing in the input line-card. It gives instructions to the network processor and the traffic manager (for admission control, policing and routing), and it receives reporting and alarms from

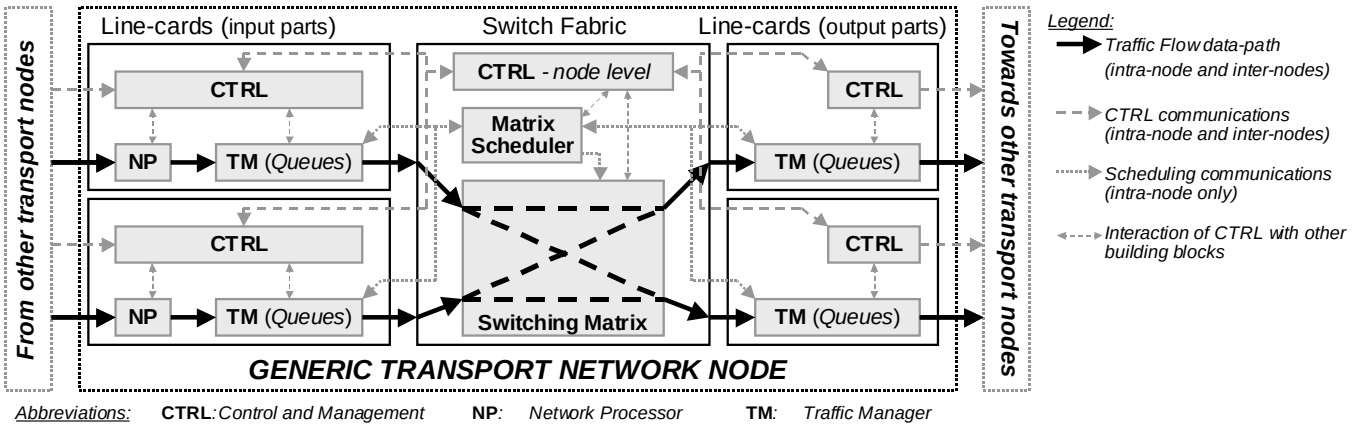

Fig. 3. Generic switching node architecture for packet transport networks, including traffic data path and various control flows.

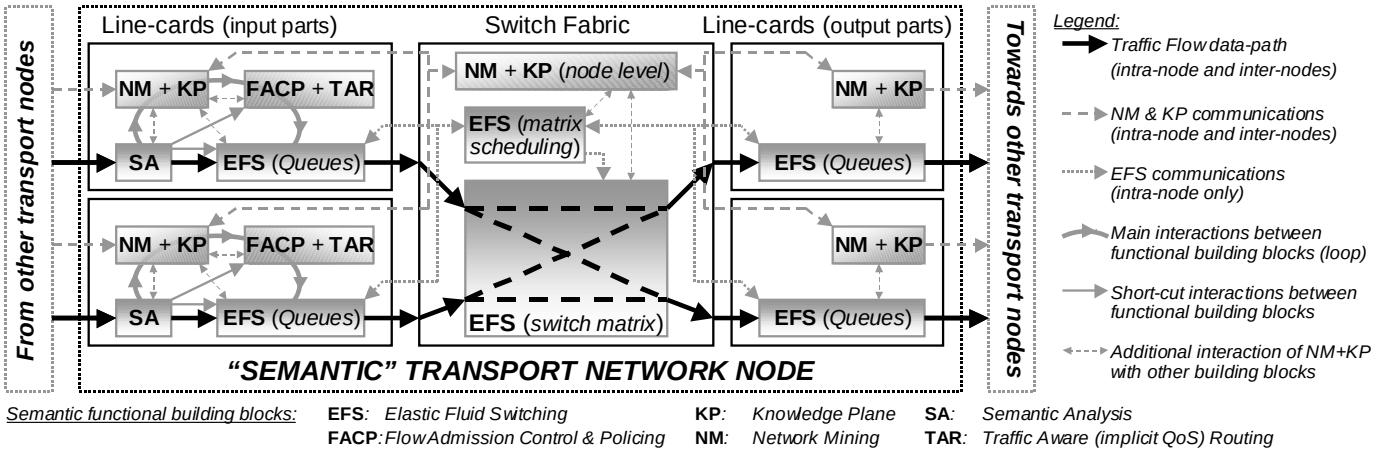

Fig. 4. Mapping of the Semantic Networking functional building blocks into the generic transport network node architecture.

them. It also processes all the control and management traffic received from the other nodes. It communicates with the node-level control. Within the node and between nodes, this control and management traffic can be transported by in-band or out-of-band signaling.

The main functional blocks of the switching fabric card are:

- *Switching Matrix*. It is made of high-speed electronics that forward the data from the inputs toward the outputs, according to the matrix scheduler decisions.
- *Matrix Scheduler*. It dynamically arbitrates the bandwidth between inputs and outputs of the switching matrix, solving the contention in coordination with input and output scheduling in the TMs (e.g., by receiving requests from the output TMs and giving grants to the input TMs).
- *Control and management (CTRL) of the node*. It performs the control and management operations for the whole node. It communicates with the line-card CTRL and may be implemented in a separate control and management card instead of the switching card.

The main functional blocks in the output line-cards are:

- *Traffic Manager (TM) with output buffers*. It receives the packets from the switching matrix and stores them into buffers (Output Queues, OQs). It participates to the global scheduling of the packet forwarding (output scheduling), by sending grants and backpressure to the inputs and requests to the matrix scheduler for example.
- *Control and management (CTRL) of the line-card*. It is the counter-part of the one of the input line-card. It communicates with the node-level control. It controls and monitors all the packet processing in the output line-card, by giving instructions to the traffic manager, and receiving reporting and alarms from it. It also processes all the control and management traffic to be sent towards the other nodes.
- Usually the packets go through the *Network Processor* also for the output data path but the operations are more limited than for the input data path: mainly reformatting of the packets – if required – before sending them to the next node. We do not represent it in Fig. 3.

B. Mapping of the Semantic Networking Functional Building Blocks on the Generic Transport Node Architecture

Fig. 4 gives a possible distribution of the Semantic Networking functional building blocks into the generic architecture of a transport network node. One can find a correspondence between the current functionalities and the semantic networking ones, as the functions that are realized in today's nodes must be replaced by other ones in "semantic" nodes. The difference is in the way these functions are

performed, giving more autonomy to the traffic processing in the node, and thus requiring less human intervention in the node configuration. In Section III we explained how they differ from the current building blocks with the incorporation of autonomic/self-* features.

The correspondence is as follows:

- The SA essentially replaces the current Network Processor operations for identification, classification and traffic monitoring in line-cards.
- The EFS is distributed in all parts of the node, replacing the TMs in the input and output line-cards, the matrix scheduler and the switching matrix in the switching matrix cards.
- The NM and KP replace the Control and Management operations inside the node (in the line-cards and the switching matrix cards), and between nodes.
- The FAC, FP and TAR complete the Control operations in the input line-cards, replacing the classical packet admission control, policing and routing functions.

The main loop of Fig. 1 between all building blocks and the short-cuts from the SA to the flow-based control and the EFS are implemented in the input line-cards. The EFS is distributed through all the line-cards and the switching matrix cards, giving a node-level consistence for the switching of traffic flows. The NM and KP are distributed between all the parts of the node and also between nodes, through inter-node communication, in order to give a network-wide consistence for the knowledge about the traffic and the network state.

As explained in Section §II.D, the closing of the main loop between the EFS and SA functional building blocks must be understood between adjacent nodes. The traffic flows that are switched by the EFS function of a given node are analyzed in the SA function of the next node, leading to hop-by-hop forwarding of traffic flows.

V. Conclusion

In this paper, we introduced the Semantic Networking approach for the Internet of the Future. In order to face the scalability and complexity challenges, this global concept coherently mixes flow-based networking, traffic-awareness, and autonomic networking. We described the interactions between its functional building blocks, focusing on autonomic/self-* features. To illustrate this new concept, we also mapped these functions into a generic node architecture.

Fully based on Autonomic Networking, Semantic Networking requires specific self-* features. The constraints goes beyond previous applicability of self-management while being used in real time for regular networking operations. Semantic Networking is ambitious and disruptive, opening numerous research challenges of general interest. Further work will focus on the design and implementation of its functional building blocks, and on their integration, performance evaluation and applicability for future networks. Some partial application in current network elements will also enable a migration path towards Semantic Networks.

Acknowledgment

The authors would like to thank the INRIA people involved in the common research lab between INRIA and Alcatel-Lucent Bell Labs on "self-organizing networks", for their inputs and valuable discussions on the “semantic networking” research activity: Sara Alouf, Eitan Altman, Konstantin Avrachenkov, Damiano Carra, Dinil Mon Divakaran, Paulo Goncalves, Isabelle Guérin-Lassous, Pierre-Solen Guichard, Matthieu Imbert, Philippe Nain, Pascale Vicat-Blanc Primet.

References

[1] Future Internet Assembly (FIA), http://www.future-internet.eu.
[2] Future InterNet Design (FIA), http://www.nets-find.net.
[3] Global Environment for Network Innovation (GENI), http://www.geni.net.
[4] Future Internet Forum (FIF), http://mmlab.snu.ac.kr/fif.
[5] Photonic Internet Forum (PIF), http://www.scat.or.jp/photonic/english/index.html.
[6] S. Oueslati, and J. Roberts, “A New Direction for Quality of Service: Flow-Aware Networking,” in *Proc. Conf. Next Generation Internet Network* , Rome, Italy, 2005), pp. 226-232.
[7] Anagram, FR-1000 white paper, 2007, http://www.anagran.com/products_fr_1000_intelligent.php.
[8] Albert Greenberg, Gisli Hjalmtysson, David A. Maltz, Andy Myers, Jennifer Rexford, Geoffrey Xie, Hong Yan, Jibin Zhan, and Hui Zhang, “A Clean Slate 4D Approach to Network Control and Management,” *ACM SIGCOMM Computer Communication Review*, vol. 35, no. 5, Oct. 2005, pp. 41-54.
[9] SNORT®, “Network Intrusion Detection System,” http://www.snort.org.
[10] Bro Intrusion Detection system, http://www.bro-ids.org.
[11] F. Yu, Z. Chen, Y. Diao, T.V. Lakshman, and R.H. Katz, “Fast and Memory Efficient Regular Expression Matching for Deep Packet Inspection,” *ACM/IEEE Symposium on Architecture for Networking and Communications Systems*, San Jose, CA, 2006, pp. 93-102.
[12] D. Collange and J.-L. Costeux, “Passive Estimation of Quality of Experience,” *J. Universal Computer Science*, vol. 14, no. 5, 2008, pp. 625-641.
[13] IP Performance Metrics (IPPM) IETF Working Group, http://www.ietf.org/html.charters/ippm-charter.html.
[14] Packet Sampling (PSAMP) IETF Working Group, http://www.ietf.org/html.charters/psamp-charter.html.
[15] IP Flow Information Export (IPFIX) IETF Working Group, http://www.ietf.org/html.charters/ipfix-charter.html.
[16] D. Clark, C. Partridge, J.C. Ramming, and J. Wroclawski, “A Knowledge Plane for the Internet,” in *Proc. Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communications*, ACM SIGCOMM’03, Karlsruhe, Germany, 2003, pp. 3-10.
[17] H.G. Perros, and K.M. Elsayed, “Call Admission Control Schemes: A Review,” *IEEE Comm. Mag.*, vol. 34, no. 11, Nov. 1996, pp. 82-91.
[18] E.P. Rathgeb, “Modelling and Performance Comparison of Policing Mechanisms for ATM Networks,” *IEEE J. Selected Areas in Communications*, vol. 9, no. 3, 1991, pp. 325-334.
[19] B. Lague, B, C. Rosenberg, and F. Guillemin, “A generalization of some policing mechanisms,” in Proc. IEEE INFOCOM'92 , vol. 2, May 1992, pp.767-775.
[20] W.H. Wang, M. Palaniswami, and S.H. Low, “Optimal flow control and routing in multi-path networks,” *Performance Evaluation*, vol. 2, no. 2-3, 2003, pp. 119-132.
[21] X. Masip-Bruin, M. Yannuzzi, J. Domingo-Pascual, A. Fonte, M. Curado, E. Monteiro, F. Kuipers, P. Van Mieghem, S. Avallone, G. Ventre, P. Arranda-Gutierrez, M. Hollick, R. Steinmetz, L. Iannone, and K. Salamatian, “Research challenges in QoS routing,” *Computer Communications*, Elsevier, vol. 29, no. 5, 2006, pp. 563-581.
[22] A. Kortebi, S. Oueslati, and J. Roberts, “Cross-Protect: Implicit Service Differentiation and Admission Control,” in *Proc. Workshop on High Performance Switching and Routing*, Phoenix (HPSR'04), AZ, 2004, pp. 56-60.