Software Defined Networking for Heterogeneous Networks

Marc Mendonca, Bruno Nunes Astuto, Katia Obraczka, Thierry Turletti

Software Defined Networking for Heterogeneous Networks

Marc Mendonca*, Bruno Astuto A. Nunes†, Katia Obraczka* and Thierry Turletti†
*University of California, Santa Cruz, USA, Email: {msm, katia}@soe.ucsc.edu
†INRIA, France, Email: {bruno.astuto-arouche-nunes, thierry.turletti}@inria.fr

I. INTRODUCTION

Software–Defined Networking (SDN) has been proposed as a way to programmatically control networks, making it easier to deploy new applications and services, as well as tune network policy and performance. The key idea behind SDN is to decouple the data- from the control plane by: (1) removing control decisions from the forwarding hardware, (2) allowing the forwarding hardware to be "programmable" via an open interface, and (3) having a separate entity called "controller" define by software the behavior of the network formed by the forwarding infrastructure, thereby creating a "software-defined network". OpenFlow[3] has been proposed as the de-facto standard protocol used for communication between the controller and "programmable" switches. The latter forward data according to a "flow table" containing an entry for each flow along with an action (or "rule") to be invoked when forwarding packets belonging to that flow. A switch's flow table is built based on the rules sent to the switch by the controller specifying how to forward data for a given flow. SDN techniques to–date, largely target infrastructure–based networks, for example, those found in data centers.

Motivated by a vision of a fully connected world, we explore how SDN can be utilized to support both infrastructure-based and infrastructure–less networks. We also discuss the research challenges involved in augmenting the current SDN model to operate in heterogeneous networked environments. While previous work has examined the use of SDN in wireless environments, their scope has primarily focused on infrastructure-based wireless deployments (e.g., WiMAX, Wi-Fi access points). For example, the idea of a flexible wireless infrastructure supported by OpenFlow was introduced in [7], [6]. The use of OpenFlow in wireless mesh environments has been explored in [1], [2].

However, to our knowledge, no efforts have investigated the challenges and benefits offered by extending the SDN paradigm to heterogeneous networked environments. This paper aims at bridging this gap by exploring the use of software–defined networking in such heterogeneous environments. In Section II, we examine example scenarios that would benefit from enabling SDN in heterogeneous networks. Section III discusses how the current SDN paradigm could be extended to operate in heterogeneous networked environments and the research challenges that will result.

II. USER-ASSISTED CONNECTIVITY

We consider heterogeneous networked scenarios that include mobile end-user devices with limited or intermittent connectivity to the network infrastructure, i.e., wired-, cellular- or WiFi infrastructure, but are able to form ad-hoc networks with other nearby units. Additionally, some of the mobile units have multiple network interfaces (e.g., wired/802.11 or 802.11/cellular). In such environment, users connecting through their mobile devices may want to communicate and/or retrieve or store content in the "cloud". For this use case, we examine two scenarios, one in which SDN is not enabled (called the "traditional" scenario) and the other in which SDN is enabled. We identify and discuss the benefits of the SDN-enabled scenario to both the users and network providers. In our discussion, we assume that the mobile units have agreed to some form of external control insofar as routing decisions are concerned. This of course, raises several issues, which we discuss in Section III.

Let us consider that in the scenario depicted in Figure 1, a user "Alice" wishes to connect to the Internet to access the Web. Unfortunately, she is unable to connect to the infrastructure and joins an ad hoc network instead. Suppose that another user, "Bob", is connected to both the ad hoc network and an infrastructure-based wireless access network. In our SDN-based architecture, a device such as Bob's is considered a "Gateway" (GW) device.

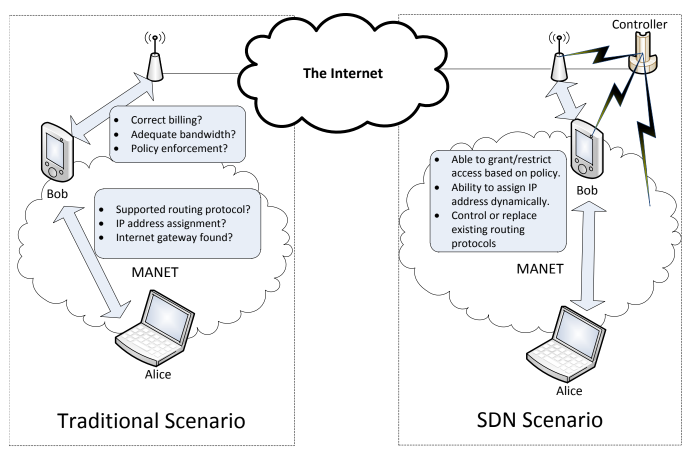

Fig. 1. Heterogeneous SDN use case scenario

A. Traditional vs. SDN Enabled Scenarios

Traditional Scenario: Even if we assume the ad hoc network learns how to route to Bob as a gateway, and Bob allows his device to be used as a NAT router by strangers, the mobile data service provider is not aware of the existence of Alice. Bob's connection is not assigned additional bandwidth, possibly harming performance; the Internet Service Provider is not able to differentiate Alice from Bob and cannot apply any QoS rules, access restriction or any sort of polices over Alice without also applying it over Bob. Furthermore, Bob will be held responsible for Alice's traffic by the service provider for any possible data overages or illegal activity.

SDN Enabled Scenario: The service provider is made aware when Alice joins the ad hoc network. Therefore, it may decide to offer service to Alice via Bob and provision Bob's connection accordingly. The service provider may decide to sell Alice a temporary connection plan on the spot, or Alice may have an existing contract on another device. Available resources, past user behavior, or any number of factors can be used on deciding whether to offer service to Alice. The service provider is thus able to maintain control of its network policy while being granted an opportunity for additional business. Alice is able to seamlessly connect to the Internet using a service plan. For his part, Bob may be offered incentives by the service provider, while avoiding performance loss or being held liable for Alice's traffic.

B. Multiple Gateways

An extension to the base case previously discussed is a scenario with multiple gateways. For example, shortly after Alice joins, a user "Charlie" with access to wired infrastructure also connects to the ad hoc network. In the traditional scenario, traffic is routed solely based on how the MANET protocol handles multiple gateways. In the SDN scenario, the network capacity can be managed based on the policies of the service providers and the characteristics of the available resources. For example, Alice's traffic may continue to flow through the slower mobile data network instead of the wired network, because she only has a service plan with the mobile data provider; alternatively, the mobile data provider may have an agreement with the wired network such that even Bob's traffic will flow through Charlie to either increase Bob's performance or reduce the load on the mobile data network.

C. Service Optimizations

In another possible situation, a group of users in the ad hoc network may be viewing the same content simultaneously (e.g., live streaming of a sport event). Using the base case from above, Bob is the link to the Internet from which the content originates. In the traditional scenario, any optimizations such as caches or CDN are performed either in the provider network or in the cloud; the result may be that Bob's link to the provider gets saturated with duplicate content. SDN enables routing policies to evolve and promotes the creation of new services; for example, it may be possible to reduce the strain on the limited infrastructure connectivity by caching and retrieving common content locally, or by creating multicast streams on-the-fly for live content.

III. Requirements and Challenges

Enabling SDN in heterogeneous networked environments raises several requirements and research challenges. We discuss some of them below.

a) End-user device limitations: Unlike infrastructure-based networks, in infrastructure-less networked environments, such as multi-hop wireless networks, or MANETs, there is no real distinction between network elements (i.e., switches, routers) and end-user devices. The latter perform core network functions like routing and forwarding, as well as source and sink application traffic. Therefore, end devices should be able to communicate with controllers and understand how to handle traffic forwarding rules. But, because in these types of networks, devices are often limited in terms of power, processing, communication, and storage capabilities, protocol overhead should be minimized.

b) Gateway device incentives: From the use case scenario discussed in Section II, it is clear that incentives are necessary to ensure collaboration between nodes in order for gateway devices to agree to forward traffic from other nodes. These new incentive schemes should be able to use the revenue collected through the new offered service and the bandwidth shared by the GW device to reward to contributing GW devices.

c) Resource discovery: Infrastructure-less networks tend to be heterogeneous in terms of the devices they interconnect and the links use to interconnect them. Therefore, a variety of factors should be considered when choosing an end device as gateway ranging from battery lifetime, network connectivity, and trust, to name a few. Clearly, a controller that learns this information would be better equipped to make decisions.

d) Control plane: Several of the independently-operated devices participating in an infrastructure-less network may not be SDN-capable and thus unable to communicate with a SDN controller. However, such devices could receive control information through some other protocol, for example, routing. This calls for a "hybrid" control plane that combines different ways to convey control information to non SDN-capable devices. In the use case example discussed in Section II, Alice should still be able to connect to the Internet even if Bob is the only SDN-enabled device in the infrastructure-less network. This could be done through a standard MANET routing protocol such as OLSR.

e) Security: Though SDN can be used to improve network control and traffic policy enforcement, keeping the network secure and guaranteeing confidentiality, integrity, and availability is quite challenging, especially in the types of heterogeneous networks we are considering. In particular, in an infrastructure-less network with independently-owned end devices also acting as forwarding nodes, it may be difficult to establish trust and ensure a secure channel end-to-end. Since a wide variety of threats ranging from jamming at the physical layer to worms at the application layer must be considered, solutions will likely need to take a multi-layered approach.

Although security in MANETs has been explored in the MANET community [5], security challenges are exacerbated by the heterogeneous SDN architecture which needs to employ a distributed control plane using independently run controllers.

While a switch in an infrastructure-based network may easily be configured to securely connect to a pre-determined controller, devices and controllers in infrastructure-less networks must discover each other without prior knowledge of the network topology. Furthermore, it is not enough that control messages successfully and securely reach their destination; both endpoints must be able to trust each other, i.e., before accepting control, forwarding nodes need to be able to trust that the discovered controller is not malicious. Likewise, the controller must be able to trust that forwarding nodes that have accepted control are following instructions. For this trust to exist, mechanisms must be in place to ensure the legitimacy of nodes and controllers, the authenticity of the control traffic, and to verify that devices act as expected in response to instructions.

f) Distributed Control Plane: Heterogeneous networks may span multiple domains of control. As illustrated by our use case, an ad hoc network may have gateways connecting to two different infrastructure networks. While previous work [4] considered using a transparent proxy to allow multiple controllers, devices in an infrastructure-less network must be able to discover and connect to multiple controllers on their own as they may not be able to rely on an outside proxy.

g) Flexible rules and actions: Current specifications that target infrastructure-based networks often limit the types of rules that can be performed on flows, often due to performance or hardware constraints. Although the latest OpenFlow 1.3 specification already supports user-specified flow match fields, compliant switches do not have to support this feature and are only required to handle a small, pre-defined set of rules. Because of the inherent heterogeneity and limitations of wireless infrastructure-less networks, supporting flexible rules (e.g. flow matching on custom headers) is critical to enable SDN in these kinds of networks.

IV. Conclusion and Future Work

In this paper, motivated by the vision that future internets will comprise infrastructure–based and infrastructure–less networks, we explore the use of the Software–Defined Networking (SDN) paradigm in these so–called “heterogeneous” networked environments. To make the case for SDN in heterogeneous networks, we examine an application scenario in which SDN is a key enabling technology. We also identify the additional requirements imposed by the SDN paradigm and discuss the research challenges they raised.

References

[1] A. Coyle and H. Nguyen. A frequency control algorithm for a mobile adhoc network. In *Military Communications and Information Systems Conference (MilCIS)*, Canberra, Australia, November 2010.

[2] P. Dely, A. Kassler, and N. Bayer. Openflow for wireless mesh networks. In *Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*, pages 1–6. IEEE, 2011.

[3] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. Openflow: enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, 38(2):69–74, 2008.

[4] R. Sherwood, M. Chan, A. Covington, G. Gibb, M. Flajslik, N. Handigol, T. Huang, P. Kazemian, M. Kobayashi, J. Naous, et al. Carving research slices out of your production networks with openflow. *ACM SIGCOMM Computer Communication Review*, 40(1):129–130, 2010.

[5] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang. Security in mobile ad hoc networks: challenges and solutions. *Wireless Communications, IEEE*, 11(1):38–47, 2004.

[6] K. Yap, M. Kobayashi, R. Sherwood, T. Huang, M. Chan, N. Handigol, and N. McKeown. Openroads: Empowering research in mobile networks. *ACM SIGCOMM Computer Communication Review*, 40(1):125–126, 2010.

[7] K. Yap, R. Sherwood, M. Kobayashi, T. Huang, M. Chan, N. Handigol, N. McKeown, and G. Parulkar. Blueprint for introducing innovation into wireless mobile networks. In *Proceedings of the second ACM SIGCOMM workshop on Virtualized infrastructure systems and architectures*, pages 25–32. ACM, 2010.

Marc Mendonca was a visiting student researcher at the INRIA Plante project in Sophia Antipolis. He recently received his M.S. in Computer Engineering from the University of California, Santa Cruz and previously completed his B.S. in Computer Engineering at the University of California, Santa Barbara.

Bruno Astuto A. Nunes is a Pos-doc at INRIA Sophia Antipolis, France. He received his B.Sc. in Electronic Engineering at the Federal University of Rio de Janeiro (UFRJ), Brazil, where he also completed his M.Sc. degree in Computer Science. He received his PhD degree in Computer Engineering from UC Santa Cruz, USA.

Katia Obraczka is Professor of Computer Engineering at UC Santa Cruz. Before joining UCSC, she held a research scientist position at USC’s Information Sciences Institute and a joint appointment at USC’s Computer Science Department. Her research interests span the areas of computer networks, distributed systems, and Internet information systems. She is the director of the Internetwork Research Group (i-NRG) at UCSC and has been a PI and a co-PI in a number of projects sponsored by government agencies (NSF, DARPA, NASA, ARO, DoE, AFOSR) as well as industry. Prof. Obraczka has edited one book, wrote a number of book chapters, and published over 200 technical papers in journals and conferences. She is co-recipient of the Best Paper Award at IFIP Networking 2007 for the paper ”On-Demand Routing in Disrupted Environments”. She is also co-recipient of one of three Best Paper Awards at IEEE MASS 2007 for the paper ”DYNAMMA: A DYNAmic Multi-channel Medium Access Framework for Wireless Ad Hoc Networks”. She has served on the Editorial Board of the Elsevier Ad Hoc Networks Journal. She has been involved with the organization of several technical conferences in her area including IEEE Global Internet, IEEE SECON, IEEE MASS, ACM Mobicom, and ACM Mobihoc, IEEE NetSciCom. She received the USC ISI’s Meritorious Service Award in 1999. She is a senior member of the IEEE.

Thierry Turletti received the M.S. (1990) and the Ph.D. (1995) degrees in computer science from the University of Nice - Sophia Antipolis, France. He has done his PhD studies in the RODEO group at INRIA where he designed the Inria Videoconferencing System (IVS). During the year 1995-96, he was a postdoctoral fellow in the Telemedia, Networks and Systems group at LCS, MIT and worked in the area of Software Defined Radio (SDR). He is currently a senior research scientist at the Diana team at INRIA Sophia Antipolis. His current research interests include information centric network architectures, trustable network evaluation platforms and wireless networking.