Network Neutrality and Its Impact on Innovation

Schahram Dustdar
TU Wien

Elias P. Duarte Jr.
Federal University of Paraná

The debate around network neutrality (NN) has become more intense and controversial. It is undeniable that NN fosters innovation in the Internet, ensuring fair competition and freedom of choice. The papers in this special issue explore multiple facets of the problem, including the economical factors behind NN, dealing with multiple NN jurisdictions across international Internet paths and designing in-network caching strategies that are neutral.

The debate around network neutrality (NN) has intensified in the past nearly two decades. The basic principle behind NN states that all traffic on the Internet must be treated equally.[1] Therefore, an Internet service provider (ISP) cannot slow down, prioritize, or block any type of specific traffic, regardless of its origin, destination, and/or content. This means that traffic differentiation (TD) practices are not allowed. Multiple countries around the world have adopted laws and rules to enforce NN. On the other hand, a large number of NN violation cases have been reported worldwide.[2] ISPs have employed TD to deal with congestion, or because of commercial agreements, or even to benefit their own services. The motivations for an ISP to slow down the traffic of specific applications/sources include postponing the need for upgrading the infrastructure, prioritizing the traffic from providers that are willing to pay for it (the so-called fast lanes), and prioritizing its own services or degrading competitors services to attract more users, thereby increasing revenue. On the other hand, those against NN argue that less restrictions to the ISPs might result in a more competitive market.[3] Regardless of the position, TD practices should at least be transparent, since they can significantly affect end-users and content/service providers.

One of the most relevant aspects of the global NN debate is how to ensure that the Internet continues to be an environment that fosters innovation for all interested parties.[4] Traffic discrimination threatens innovation, fair competition, and consumer's freedom of choice on the Internet. In a non-neutral Internet, an ISP and partners can control which services consumers are most likely to use, and thus which services are most likely to succeed. This type of control can certainly represent a tool for powerful corporations to influence online behavior. This environment is hostile to new service providers and independent innovators that lack the same amount of resources, thus they might not be able to compete fairly with more established services. Innovative services might struggle to succeed or they might not even see the light of day because of poor performance, e.g., higher response times

Published by the IEEE Computer Society
1089-7801/18/$33.00 ©2018 IEEE

caused by their traffic being discriminated. Thus, NN is essential for ensuring a level playing field for the development of new applications and services on the Internet. Cloud services, over-the-top services, and Internet of Things devices and software are examples of applications and services that need NN to adequately flourish in the future.

IN THIS ISSUE

The papers in this special issue examine three different facets of NN: the economical factors behind NN, dealing with multiple NN jurisdictions across international Internet paths, and designing in-network caching strategies that are neutral.

In the first paper "Network Neutrality is About Money, Not Packets" the author argues that the most common NN definition, the "principle by which all traffic on the Internet must be treated equally" is misleading and does not address key economic, engineering, and policy concerns. The fact that NN is often seen as a technical problem is challenged, as disputes about details of traffic management have never arisen on purely technical grounds: the conflict is about economic incentives. These economic incentives include for instance the reduction of competition for vertically integrated services offered by ISPs; charging backbone operators and CDNs for network access and privileges. However, there are only a few practical ways to charge for intra-network QoS guarantees, each with their own competitive and neutrality challenges. These include ISP-provided applications negotiated with third parties. Concerns about economic discrimination, particularly if the ISP offers competing services, certainly need to be monitored for anticompetitive behavior.

The second paper "To be Neutral or Not Neutral? The In-Network Caching Dilemma" describes the Internet as a complex service-delivery chain where ISPs own and manage the infrastructures that content providers (CPs) exploit to offer services to their end-users. Network caching is the process by which ISPs store in their networks the most popular contents to reduce traffic. By using this strategy, contents are retrieved from closer servers and users experience a superior QoS. However, by its very nature and issues such as the selection of what is cached, in-network caching intrinsically raises discriminatory concerns. The authors discuss this issue taking into account the wide use of encryption, which hinders caching. Cooperative alliances among ISPs and CPs should be carefully assessed so that they are compliant to NN principles. The authors advocate the specification of open protocols that enable NN-compliant caching schemes and nondiscriminatory cooperations.

Finally, the third paper "Considering Jurisdiction When Assessing Network Neutrality" examines the impact on NN regulations on international Internet paths that cross multiple countries. The problem is that different countries have different laws and rules that define the NN principles adopted, and specify which situations correspond to NN violations. A normative is defined by legislators and regulatory agencies whose acts are limited to their jurisdiction, i.e., the borders of a country. NN violations can happen anywhere in the path between two communication endpoints on the Internet. The authors argue that NN monitoring must explicitly consider where violations occur. They discuss the architecture of a system that is built on existing TD monitoring tools adding the capability of determining exactly where, along an Internet path, TD is happening.

We would like to thank all authors for their submissions, reviewers for their expert work, and AEiC George Pallis for his support during the whole process. We hope the Special Issue will contribute to the debate around NN, and that the Internet will remain an environment that fosters innovation, competition and freedom of choice.

REFERENCES

1. B. van Schewick and D. Farber, "Point/counterpoint: Network neutrality nuances," *Commun. ACM*, vol. 22, no. 60, pp. 31–37, Feb. 2009.
2. T. Garrett, L. Setenareski, L. Peres, L. Bona, and E. P. Duarte Jr., "Monitoring network neutrality: A survey on traffic differentiation detection," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2486–2517, Jul.–Sep. 2018.
3. A. Joch, "Debating net neutrality," *Commun. ACM*, vol. 52, no. 10, pp. 14–15, Oct. 2009.
4. D. J. Weitzner, "Net neutrality. . . seriously this time," *IEEE Internet Comput.*, vol. 12, no. 3, pp. 86–89, May 2008.

ABOUT THE AUTHORS

Schahram Dustdar (F'16) is a Full Professor of Computer Science (Informatics) with a focus on Internet technologies, heading the Distributed Systems Group, TU Wien, Austria. He is the Chairman of the Informatics Section of the Academia Europaea (since 2016). He is a member of the IEEE Conference Activities Committee (since 2015). He was the recipient of the ACM Distinguished Scientist award (2009), the IEEE TCSVC Outstanding Leadership Award (2018), and the IBM Faculty Award (2012). He is an Associate Editor of the IEEE Transactions on Services Computing, IEEE Transactions on the Cloud, *ACM Transactions on the Web*, and *ACM Transactions on Internet Technology*, and is on the editorial board of IEEE Computer and IEEE Internet Computing. He is the Co-Editor-in-Chief for *ACM Transactions on Internet of Things* and Editor-in-Chief of the Springer *Computing* journal. You may reach him at dustdar@dsg.tuwien.ac.at.

Elias P. Duarte Jr. (SM'15) is a Full Professor of Computer Science with Federal University of Parana (UFPR), Brazil, Department of Informatics, where he is the Leader of the Computer Networks and Distributed Systems Lab (LaRSiS). He is an Associate Editor of IEEE Transactions on Dependable and Secure Computing, and has served as a Chair of more 20 conferences and workshops. His research interests include computer networks and distributed systems, their dependability, management and algorithms. He is a member of the Brazilian Computer Society. You may reach him at elias@inf.ufpr.br.